EMGEPRON

CONCURSO PÚBLICO
EMGEPRON
EMPRESA GERENCIAL DE PROJETOS NAVAIS

EDITAL Nº 01/2021

ANALISTA DE PROJETOS NAVAIS

ANALISTA TÉCNICO (SEGURANÇA DA INFORMAÇÃO)

Duração: 03h00min (três horas)

Leia atentamente as instruções abaixo:

01 Você recebeu do fiscal o seguinte material:

a) Este Caderno, com 50 (cinquenta) questões da Prova Objetiva, sem repetição ou falha, conforme distribuição abaixo:

LÍNGUA PORTUGUESA	RACIOCÍNIO LÓGICO	CONHECIMENTOS ESPECÍFICOS
01 a 10	11 a 20	21 a 50

b) Um Cartão de Respostas destinado às respostas das questões objetivas.

02 Verifique se este material está em ordem e se o seu nome e número de inscrição conferem com os que aparecem no Cartão de Respostas. Caso contrário, notifique imediatamente o fiscal.

03 Após a conferência, o candidato deverá assinar no espaço próprio do Cartão de Respostas, com caneta esferográfica de tinta na cor azul ou preta.

04 No Cartão de Respostas, a marcação da alternativa correta deve ser feita cobrindo a letra correspondente ao número da questão e preenchendo todo o espaço interno, com caneta esferográfica de tinta na cor azul ou preta, de forma contínua e densa.

Exemplo: Ⓐ ● Ⓒ Ⓓ

05 Para cada uma das questões objetivas, são apresentadas 4 (quatro) alternativas classificadas com as letras (A, B, C e D), mas só uma responde adequadamente à questão proposta. Você só deve assinalar uma alternativa. A marcação em mais de uma alternativa anula a questão, mesmo que uma das respostas esteja correta.

06 Somente depois de decorrida 01 (uma) hora do início da prova, o candidato poderá entregar seu Cartão de Respostas, seu Caderno de Questões e retirar-se da sala de prova. O candidato que insistir em sair da sala de prova, descumprindo o aqui disposto, deverá assinar o Termo de Ocorrência declarando sua desistência do Concurso, que será lavrado pelo Coordenador do Local.

07 Ao candidato, será permitido levar seu CADERNO DE QUESTÕES, a partir de 01 (uma) hora para o término da prova e desde que permaneça em sala até esse momento.

08 Não será permitida a cópia de gabarito no local de prova. Ao terminar a prova de Conhecimentos, o candidato entregará, obrigatoriamente, ao fiscal de sala, o seu CARTÃO DE RESPOSTAS e o seu CADERNO DE QUESTÕES, ressalvado o estabelecido no item 7.

09 Reserve os 30 (trinta) minutos finais para marcar seu Cartão de Respostas. Os rascunhos e as marcações assinaladas no Caderno de Questões não serão levados em consideração.

10 Os 3 (três) últimos candidatos permanecerão sentados até que todos concluam a prova ou que termine o seu tempo de duração, devendo assinar a ata de sala e retirar-se juntos.

LÍNGUA PORTUGUESA

Texto I (para as questões de 1 a 10)

Pandemia reverte progressos na igualdade de gênero

A pandemia do coronavírus reverteu o progresso global no alcance da igualdade entre homens e mulheres, concluiu o Fórum Econômico Mundial (FEM) em seu relatório Global Gender Gap de 2021, divulgado nesta quarta-feira (31/03). As consequências, segundo o órgão, podem ser duradouras.

O índice anual, que rastreia a evolução de lacunas na paridade de gênero desde 2006, avalia o progresso na obtenção da igualdade de gênero em quatro esferas principais: participação e oportunidade econômica, realização educacional, saúde e sobrevivência e representação política.

A lacuna global de paridade de gênero está atualmente 68% fechada, de acordo com o relatório deste ano, que abrangeu 156 países. Isso representa uma redução de meio ponto percentual em relação ao ano anterior. Continuando nesse ritmo, levará 133,4 anos para alcançar a paridade global entre homens e mulheres.

Segundo o documento, o declínio mundial na paridade de gênero foi impulsionado principalmente pelo fraco desempenho em grandes economias avançadas e emergentes.

Neste contexto, o coronavírus foi apontado como parcialmente responsável por reabrir essas lacunas. Dados preliminares sugerem que as consequências econômicas e sociais da pandemia afetaram mais a ala feminina, com 5% de todas as mulheres que tinham alguma ocupação tendo perdido seus empregos até o momento, em comparação com 3,9% dos homens. Outros dados também mostraram um declínio significativo no número de mulheres contratadas para cargos de liderança, revertendo o progresso recente em um a dois anos.

A crise sanitária provocada pela covid-19 também acelerou a digitalização e a automação, levando a rápidas inovações no mercado de trabalho. Mas os dados indicam que as disparidades de gênero são mais prováveis justamente no setor de inovação tecnológica. As mulheres, segundo o relatório, representam um terço ou menos da força de trabalho nos setores de computação em nuvem, engenharia e dados e inteligência artificial. A baixa chegada de novos talentos em tais setores é um sinal de que a proporção de mulheres que ingressam aumentou apenas marginalmente, ou mesmo caiu, nos últimos anos.

Dos oito setores de empregos analisados, apenas dois ("Pessoas e Cultura" e "Produção de Conteúdo") alcançaram a paridade de gênero. Enquanto isso, as mulheres continuam severamente sub-representadas em muitos setores. Um novo indicador introduzido este ano aponta inclusive que é ainda mais difícil para as mulheres fazerem a transição para campos onde elas já estão sub-representadas.

No contexto da pandemia, as mulheres também estão mais propensas ao estresse devido a uma longa "dupla jornada" de trabalho remunerado e não remunerado, devido ao fechamento de escolas e à oferta limitada de serviços de assistência. Este seria outro obstáculo para as mulheres conquistarem posições de liderança ou ingressarem em novos setores.

As condições agravadas pela pandemia, adverte o relatório, podem deixar "cicatrizes" nas oportunidades econômicas para as mulheres no futuro.

Com apenas 22,3% de sua lacuna fechada, a representação política é a menos desenvolvida das quatro lacunas de gênero analisadas pelo FEM. A diferença aumentou 2,4 pontos percentuais desde o relatório do ano passado. Em todos os países avaliados, as mulheres representaram apenas 25,7% dos cerca de 35,5 mil assentos no parlamento e 22,8% dos mais de 3,4 mil ministros em todo o mundo. No ritmo atual, levará 145,5 anos para alcançar a paridade de gênero na esfera política.

Participação e oportunidade econômica, por sua vez, compõem a segunda lacuna de menor evolução. Após um ano de ligeira melhora, o índice mais recente mediu a lacuna como 58% fechada. Por enquanto, serão necessários 257,2 anos para que a participação e as oportunidades econômicas sejam iguais para homens e mulheres.

Quando se trata de realização educacional, saúde e sobrevivência, entretanto, as lacunas estão quase fechadas. A lacuna global de realização educacional entre homens e mulheres, por exemplo, encontra-se 96,3% fechada. No ritmo atual, a paridade total deve ser alcançada em 13 anos, sendo que 30 países já a conquistaram.

Já a lacuna de saúde e sobrevivência está 95,6% fechada atualmente, após um pequeno declínio no ano passado (não relacionado à covid-19). O tempo que levará para o fechamento dessa lacuna não foi definido.

Pelo décimo segundo ano consecutivo, a Islândia foi classificada como o país com maior igualdade de gênero no mundo.

A Europa Ocidental continuou sendo a região que mais progrediu em direção à paridade de gênero, com 77,5% da lacuna fechada, seguida pela América do Norte, com 76,4%. Por outro lado, com apenas 61,5% de lacunas fechadas, o Oriente Médio e o Norte da África foram novamente as regiões que têm um caminho mais longo pela frente.

Os maiores avanços deste ano foram observados

na Lituânia, Sérvia, Timor-Leste, Togo e Emirados Árabes Unidos. Timor-Leste e Togo ficaram entre os únicos quatro países (incluindo a Costa do Marfim e a Jordânia) que conseguiram melhorar suas lacunas de participação e oportunidade econômica em pelo menos um ponto percentual desde o último relatório.

Para alcançar um futuro com maior igualdade entre homens e mulheres, o FEM recomenda um maior investimento no setor de cuidados, bem como políticas de licenças iguais para homens e mulheres. Políticas e práticas direcionadas também são necessárias para superar a segregação ocupacional por gênero. Por último, o relatório apela para políticas de requalificação e práticas gerenciais em meio de carreira que incorporem práticas sólidas e imparciais para contratação e promoções.

(Adaptado de: dw.com/pt-br)

1. No quinto parágrafo, um dos critérios utilizados para comparação do aumento da desigualdade de gênero, no contexto da pandemia, é:

A) índice de reajuste de salários
B) percentual de perda de empregos
C) acesso a planos de saúde privados
D) forma de ingresso em curso superior

2. No segundo parágrafo, o emprego dos dois-pontos tem o objetivo de:

A) apresentar uma sequência em gradação
B) introduzir uma enumeração de elementos
C) sintetizar um conjunto de aspectos indicados
D) estabelecer comparação entre grupos de fatores

3. No sétimo parágrafo, a segunda frase é introduzida e ligada à primeira por expressão que tem o valor de:

A) simultaneidade
B) conformidade
C) probabilidade
D) finalidade

4. No oitavo parágrafo, o conectivo que pode ser usado para unir a segunda frase à primeira, explicitando a relação de sentido estabelecida, é:

A) entretanto
B) embora
C) logo
D) se

5. "Continuando nesse ritmo, levará 133,4 anos para alcançar a paridade global entre homens e mulheres" (3º parágrafo).
Reescrevendo o trecho inicial, a formulação que mantém o sentido original é:

A) ainda que continue nesse ritmo
B) a fim de continuar nesse ritmo
C) antes de continuar nesse ritmo
D) caso continue nesse ritmo

Trecho para a questão 6.

> "Este seria outro obstáculo para as mulheres conquistarem posições de liderança ou ingressarem em novos setores" (8º parágrafo)
> "O tempo que levará para o fechamento dessa lacuna não foi definido" (13º parágrafo)

6. Nas frases acima, os verbos "seria" e "levará" encontram-se, respectivamente, nos seguintes tempo e modo:

A) pretérito imperfeito do subjuntivo/futuro do subjuntivo
B) futuro do pretérito do indicativo/futuro do presente do indicativo
C) futuro do presente do indicativo/pretérito imperfeito do subjuntivo
D) pretérito mais-que-perfeito do indicativo/futuro do pretérito do indicativo

7. Uma expressão verbal na voz passiva encontra-se em:

A) "as consequências econômicas e sociais da pandemia afetaram mais a ala feminina, com 5% de todas as mulheres"
B) "As mulheres, segundo o relatório, representam um terço ou menos da força de trabalho nos setores de computação em nuvem"
C) "Por enquanto, serão necessários 257,2 anos para que a participação e as oportunidades econômicas sejam iguais para homens e mulheres"
D) "o declínio mundial na paridade de gênero foi impulsionado principalmente pelo fraco desempenho em grandes economias avançadas e emergentes"

8. Um verbo transitivo indireto é apresentado em:

A) "A pandemia do coronavírus reverteu o progresso global no alcance da igualdade entre homens e mulheres, concluiu o Fórum Econômico Mundial (FEM)" (1º parágrafo)
B) "Dados preliminares sugerem que as consequências econômicas e sociais da pandemia afetaram mais a ala feminina, com 5% de todas as mulheres" (5º parágrafo)
C) "Em todos os países avaliados, as mulheres representaram apenas 25,7% dos cerca de 35,5 mil assentos no parlamento" (10º parágrafo)
D) "Por último, o relatório apela para políticas de requalificação e práticas gerenciais em meio de carreira que incorporem práticas sólidas e imparciais para contratação e promoções" (17º parágrafo)

9. A palavra formada a partir de um verbo é:

A) região
B) inovação
C) transição
D) condição

10. Uma paroxítona se encontra acentuada em:

A) gênero
B) índices
C) prováveis
D) econômicas

RACIOCÍNIO LÓGICO

11. Um funcionário resolveu criar senhas com uma sequência de 3 das 8 letras da sigla EMGEPRON. Por exemplo, MEE, GMN e EME são três diferentes senhas. O número máximo de senhas distintas que esse funcionário poderá criar é igual a:

A) 318
B) 336
C) 384
D) 392

12. Admite-se que a probabilidade de um candidato passar em um concurso seja 2%. Se dois irmãos fazem esse concurso, a probabilidade de apenas um passar é igual a:

A) 2%
B) 1%
C) 1,96%
D) 3,92%

13. Cerca de 38 funcionários de uma empresa responderam um questionário com três perguntas de múltipla escolha. O resultado obtido foi:

18 funcionários acertaram a questão número1;
25 acertaram a questão número 2;
30 acertaram a questão número 3;
10 acertaram as três questões;
13 acertaram somente uma das questões;
nenhum errou as três questões.

Se **n** é o número de funcionários que acertaram somente duas questões desse teste, a soma dos algarismos de **n** é igual a:

A) 6
B) 7
C) 8
D) 9

14. Na proposição "André é analista de sistema e Raul é engenheiro", o conectivo lógico utilizado denomina-se:

A) condicional
B) bicondicional
C) disjunção
D) conjunção

15. A negação de "Camila é advogada ou Bruno é analista técnico" está corretamente indicada na seguinte opção:

A) Camila não é advogada ou Bruno não é analista técnico.
B) Camila não é advogada e Bruno não é analista técnico.
C) Camila não é advogada ou Bruno é analista técnico.
D) Camila não é advogada e Bruno é analista técnico.

16. Um gerente de produção fez a seguinte declaração:

"Se o funcionário é bem remunerado, então a produção é alta."

Uma proposição logicamente equivalente à do gerente está indicada na seguinte opção:

A) Se a produção não é alta, então o funcionário não é bem remunerado.
B) Se a produção não é alta, então o funcionário é bem remunerado.
C) Se o funcionário não é bem remunerado, então a produção não é alta.
D) Se o funcionário não é bem remunerado, então a produção é alta.

17. Sejam A, B e C três conjuntos distintos e não vazios tal que $B \cap C = A$. Pode-se afirmar corretamente que $C \cup (B - A)$ é igual ao seguinte conjunto:

A) ϕ
B) $B \cup C$
C) $A \cup C$
D) C

18. Considere as proposições:

p : O número de permutações simples de 5 elementos distintos é igual a 120.
q : O conjunto A={1;2;3;4;5} possui 20 subconjuntos distintos com 3 elementos.

Os valores lógicos verdade (V) e falsidade (F) das proposições p e q são, respectivamente:

A) V e V
B) F e F
C) V e F
D) F e V

19. Retira-se de uma caixa 2/3 do total de **n** bolas e em seguida 1/5 do restante. Se nessa caixa restaram exatamente 12 bolas, na primeira retirada saiu a seguinte quantidade de bolas:

A) 5
B) 15
C) 30
D) 45

20. Em um grupo de 20 analistas de projetos, todos falam inglês ou francês. Se 18 falam inglês e 16 falam francês, escolhendo-se ao acaso um desses analistas, a probabilidade de ele falar apenas um dos idiomas é igual a:

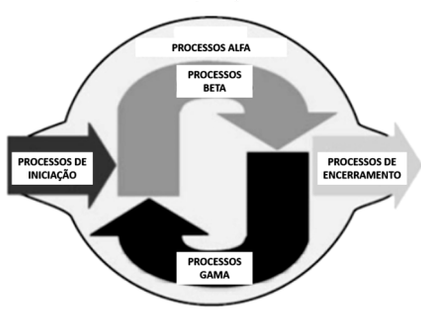
A) 20%
B) 30%
C) 50%
D) 70%

CONHECIMENTOS ESPECÍFICOS

21. Um gerente de projetos da EMGEPRON está desenvolvendo um determinado projeto que produz um tipo específico de *software.* No momento, está prestes a definir funções, responsabilidades e relações de subordinação de projetos, o que significa concluir que esse gerente está trabalhando no seguinte processo do planejamento:

A) mobilizar a equipe do projeto
B) estimar os recursos das atividades
C) implementar o Plano de Contingência
D) desenvolver o Plano de Recursos Humanos

22. Os processos de gerenciamento de projetos organizam e descrevem a realização do projeto. A figura abaixo apresenta um conjunto de cinco grupos de processos, em conformidade com o PMBoK, todos inter-relacionados e dependentes uns dos outros, executados por pessoas, de maneira muito parecida com as fases de projeto.



Os processos ALFA, BETA e GAMA são denominados, respectivamente:

A) PLANEJAMENTO, MONITORAMENTO e CONTROLE e EXECUÇÃO
B) PLANEJAMENTO, EXECUÇÃO e MONITORAMENTO e CONTROLE
C) MONITORAMENTO e CONTROLE, PLANEJAMENTO e EXECUÇÃO
D) MONITORAMENTO E CONTROLE, EXECUÇÃO e PLANEJAMENTO

23. No que diz respeito ao desenvolvimento de um projeto e em conformidade com o PMI/PMBoK, a seguir são listados três processos.

I. Orientar e gerenciar a execução do projeto
II. Monitorar e controlar o trabalho do projeto
III. Desenvolver o plano de gerenciamento de projeto

Esses processos fazem parte da área de conhecimento denominada Gerenciamento de:

A) Tempo do Projeto
B) Integração do Projeto
C) Aquisições do Projeto
D) Riscos do Projeto

24. A sigla COBIT tem por significado *"Control Objectives for Information and related Technology"* e constitui uma estrutura criada pela ISACA (Associação de Auditoria e Controle de Sistemas de Informação) para governança e gerenciamento de TI. O COBIT é um conjunto de práticas fundamental para garantir a governança de TI e, como consequência, melhorar a gestão. Numa abordagem ampla, o *framework* do COBIT 5 identifica um conjunto de habilitadores da governança e do gerenciamento que inclui cerca de 37 processos. A camada de gerenciamento é definida por quatro domínios, dos quais dois são descritos a seguir.

I. Diz respeito à identificação de como a TI pode contribuir melhor com os objetivos de negócio. Processos específicos desse estão relacionados com a estratégia e táticas de TI, arquitetura empresarial, inovação e gerenciamento de portfólio.
II. Diz respeito à entrega dos serviços de TI necessários para atender aos planos táticos e estratégicos. Este domínio inclui processos para gerenciar operações, requisições de serviços e incidentes, assim como o gerenciamento de problemas, continuidade, segurança e controle de processos de negócio.

Os domínios descritos em I e II são denominados:

A) APO (Align - Plan – Organize) e DSS (Entregar, Servir e Suportar)
B) APO (Align - Plan – Organize) e MEA (Monitor - Evaluate - Assess)
C) BAI (Build – Acquire - Implement) e DSS (Entregar, Servir e Suportar)
D) BAI (Build – Acquire - Implement) e MEA (Monitor - Evaluate - Assess)

25. A sigla ITIL tem por significado "Information Technology Infrastructure Library", um conjunto de melhores práticas, sendo atualmente a principal referência para gerenciamento de serviços de TI. Recentemente, foi lançada a ITIL 4, trazendo o sistema de valor de serviço (SVS), um componente chave que descreve como todos os componentes e atividades de uma organização trabalham juntos para permitir a criação de valor. No centro da SVS está a cadeia de valor de serviços, um modelo operacional flexível para a criação, entrega e melhoria contínua dos serviços. O ITIL 4 inclui 34 práticas de gerenciamento, agrupadas em três categorias:

I. Práticas gerais de gerenciamento
II. Práticas de gerenciamento de serviço
III. Práticas de gerenciamento técnico

Três exemplos de práticas de gerenciamento de cada uma das categorias I / II / III são, respectivamente, gerenciamento:

A) de disponibilidade / de infraestrutura / da segurança da informação
B) de capacidade e desempenho / de riscos / de ativos de TI
C) de projetos / da estratégia / do catálogo de serviços
D) do portfólio / de liberação / de implantação

26. O termo *Balanced Scorecard* pode ser definido como uma metodologia de gestão, considerando que auxilia na mensuração do progresso dos colaboradores e da empresa, em relação às metas organizacionais de longo prazo. É vista como uma poderosa ferramenta para Gestão Empresarial, alinhando quatro perspectivas, das quais duas são caracterizadas a seguir.

I. Os gestores conseguem demonstrar se a execução das estratégias está contribuindo para a melhoria dos principais resultados da empresa como lucro líquido, retorno sobre o investimento, criação de valor econômico e geração de caixa.
II. Os gestores conseguem identificar os pontos críticos de operação, devendo a empresa atuar com mais vigor para alcançar o nível de excelência nos métodos de produção, ações e decisões no âmbito da organização, tendo como objetivos estratégicos obter vantagem competitiva direcionada a redução e gestão de custos ou à diferenciação de produtos.

As abordagens em I e II são conhecidas como perspectivas:

A) Financeira e de Processos Internos
B) Estratégica e de Processos Internos
C) Financeira e de Aprendizado e Crescimento
D) Estratégica e de Aprendizado e Crescimento

27. O mapa estratégico auxilia o *Balanced Scorecard* na rotina de execução dos processos de curto prazo, mas mantendo o foco na visão de longo prazo. Assim, para garantir que toda a estratégia do Planejamento Estratégico seja seguida, é necessário conhecer quatro conceitos.

I. Define o que a empresa deseja alcançar em cada perspectiva estratégica.
II. Indica o desempenho de qualidade da empresa, referente a cada item a ser alcançado.
III. Indica o nível de performance esperado que se deve atingir, em função dos padrões de desempenho e qualidade.
IV. Estabelece as ações e intervenções que devem ser tomadas para se chegar aos níveis de desempenho previstos e esperados.

Os conceitos em I, II, III e IV são denominados, respectivamente:

A) Indicadores, Metas, Iniciativas e Objetivos
B) Metas, Iniciativas, Objetivos e Indicadores
C) Iniciativas, Objetivos, Indicadores e Metas
D) Objetivos, Indicadores, Metas e Iniciativas

28. Entre as Normas da ISO/IEC 27000, a ISO 27001 é uma norma relacionada ao Sistema de Gerenciamento da Segurança da Informação (ISMS) no que diz respeito ao seguinte aspecto:

A) guia para auditoria do ISMS
B) processo de certificação e registro do ISMS
C) especificação formal associada aos requisitos do ISMS
D) diretriz de ISMS para empresas de telecomunicações

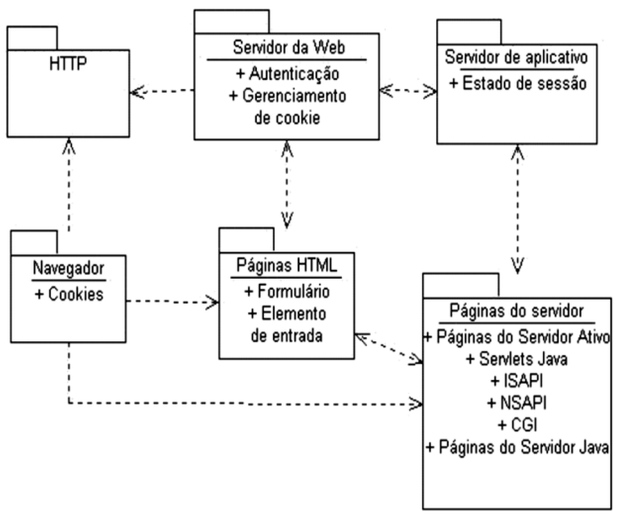
29. Entre as Normas da ISO/IEC 27000, a ISO 27002 trata da adoção das práticas, imprescindíveis para blindar a empresa contra ataques cibernéticos e demais ameaças. Duas dessas práticas são descritas a seguir.

I. É indispensável realizar a definição dos procedimentos e das responsabilidades da gestão e a operação de todos os recursos ligados ao processamento das informações. Para isso, é preciso gerenciar os serviços terceirizados, o planejamento dos recursos dos sistemas para reduzir riscos de falhas, a criação de processos para gerar cópias de segurança, a recuperação e a administração segura das redes de comunicação.
II. Antes de contratar funcionários ou fornecedores, é preciso fazer uma análise cuidadosa, principalmente se forem ter acesso a informações sigilosas. O objetivo dessa atitude é eliminar o risco de roubo, mau uso ou fraude dos recursos. Uma vez atuando na organização, o funcionário deve ser conscientizado sobre as ameaças que expõem a segurança da informação, bem como sobre as suas obrigações e responsabilidades.

As práticas descritas em I / II são denominadas, respectivamente:

A) Gerenciamento de operações e comunicações/ Segurança física e do ambiente
B) Gerenciamento de operações e comunicações/ Segurança em Recursos Humanos
C) Gestão de incidentes de segurança da informação/ Segurança física e do ambiente
D) Gestão de incidentes de segurança da informação/ Segurança em Recursos Humanos

30. Uma aplicação *web* é composta por dois atores principais, o cliente e o servidor. Nesse contexto, a figura abaixo ilustra uma arquitetura para aplicativos baseados na Internet, para os quais pode-se garantir apenas a configuração mínima no cliente.



Os principais componentes do padrão dessa arquitetura estão no servidor. Entre os principais componentes, dois são detalhados a seguir.

I. Representa o principal ponto de acesso para todos os navegadores de cliente, que acessam o sistema por meio de pedidos de páginas em HTML estático ou páginas do servidor. Dependendo da solicitação, esse componente pode iniciar algum processamento no próprio servidor. Se o pedido de página for para um módulo da página com *scripts* do servidor, esse componente delegará o processamento para o interpretador de *script* ou módulo executável apropriado. De qualquer forma, o resultado será uma página em formato HTML, apropriada para ser processada por um *browser.*

II. Representam páginas da *web* que passam por implementações no servidor por meio de *scripts,* processadas por meio de um filtro no servidor do aplicativo ou de módulos executáveis. Essas páginas têm possibilidade de acesso a todos os recursos do servidor, incluindo componentes da lógica do negócio, bancos de dados, sistemas legados e sistemas de contabilidade comercial.

Os componentes da arquitetura detalhados em I e II são denominados, respectivamente:

A) Servidor de Aplicativos e Páginas de Servidor
B) Servidor de Aplicativos e Páginas HTML
C) Servidor *Web* e Páginas de Servidor
D) Servidor *Web* e Páginas HTML

31. De acordo com o Modelo OSI/ISO, a camada de rede é responsável pelo endereçamento dos pacotes de rede, também conhecidos por datagramas, associando endereços lógicos (IP ou Internet Protocol) aos físicos (MAC), de forma que os pacotes cheguem corretamente ao destino. Entre os principais protocolos desta camada, são funções do ARP /ICMP, respectivamente:

A) descobrir o endereço físico MAC de um computador que tem um dado endereço lógico IP/informar erros ao nível IP de origem sem qualquer responsabilidade sobre a correção destes
B) descobrir o endereço físico MAC de um computador que tem um dado endereço lógico IP/permitir que um *host* anuncie sua associação de grupo de *multicast* a *switches* e roteadores vizinhos
C) descobrir o endereço físico IP de um computador que tem um dado endereço lógico MAC/informar erros ao nível IP de origem sem qualquer responsabilidade sobre a correção destes
D) descobrir o endereço físico IP de um computador que tem um dado endereço lógico MAC/permitir que um *host* anuncie sua associação de grupo de *multicast* a *switches* e roteadores vizinhos

32. A arquitetura OLAP representa um método que garante que os dados corporativos sejam analisados de forma mais ágil, consistente e interativa pelos gerentes, analistas, executivos e outros interessados nas informações. Constitui uma interface com o usuário e não uma forma de armazenamento de dados, porém se utiliza do armazenamento para poder apresentar as informações. Entre os métodos de armazenamento, quatro são descritos a seguir.

I. Os dados são armazenados de forma relacional.
II. Os dados são armazenados de forma multidimensional.
III. Uma combinação dos métodos caracterizados em I e em II.
IV. O conjunto de dados multidimensionais deve ser criado no servidor e transferido para o *desktop,* além de permitir portabilidade aos usuários OLAP que não possuem acesso direto ao servidor.

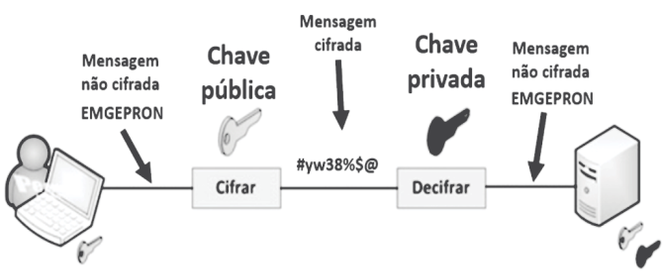
O métodos descritos em I, II, III e IV são conhecidos, respectivamente, pelas siglas:

A) DOLAP, ROLAP, MOLAP e HOLAP
B) ROLAP, MOLAP, HOLAP e DOLAP
C) MOLAP, HOLAP, DOLAP e ROLAP
D) HOLAP, DOLAP, ROLAP e MOLAP

33. A Lei Geral de Proteção de Dados Pessoais é regida pela Lei nº 13.709, de 14 de agosto de 2018. No seu Art. 5º, ficou estabelecida a existência de duas pessoas naturais ou jurídicas, de direito público ou privado, com competências bem definidas. À primeira cabem as decisões referentes ao tratamento de dados pessoais e, à segunda, a realização em si do tratamento de dados pessoais.
Essas pessoas naturais ou jurídicas são denominadas, respectivamente:

A) gerente e agente
B) titular e suplente
C) supervisor e executor
D) controlador e operador

34. A criptografia é a ciência e arte de escrever mensagens em forma cifrada ou em código, constituindo um dos principais mecanismos de segurança que se pode usar para se proteger dos riscos associados ao uso da Internet. Entre os métodos utilizados, um é ilustrado por meio da figura e das características a seguir.



- Utiliza duas chaves distintas, uma pública, que pode ser livremente divulgada, e uma privada, que deve ser mantida em segredo por seu dono.
- Quando uma informação é codificada com uma das chaves, somente a outra chave do par pode decodificá-la.
- A chave privada pode ser armazenada de diferentes maneiras, como um arquivo no computador, um *smartcard* ou um *token.*
- Exemplos desse método criptográfico são RSA, DSA, ECC e Diffie-Hellman.

Esse método é conhecido como criptografia de chaves:

A) assimétricas
B) assíncronas
C) simétricas
D) síncronas

35. O *IDS (Intrusion Detection System)* é um sistema de detecção de intrusão, um componente essencial em um ambiente corporativo, que possibilita a coleta e o uso de informações dos diversos tipos de ataques em prol da defesa de toda uma infraestrutura de rede. Dessa forma, é possível identificar pontos ou tentativas de invasão, dando permissão para registro e possibilitando a melhoria contínua do ambiente de segurança. Entre os tipos existentes, dois são caracterizados a seguir.

I. Este IDS monitora o tráfego do segmento de rede, geralmente com a interface de rede atuando em modo promíscuo. A detecção é realizada com a captura e análise dos cabeçalhos e conteúdos dos pacotes, que são comparados com padrões ou assinaturas conhecidas. É um tipo eficiente contra ataques como *port scanning, IP spoofing* ou *SYN flooding.*
II. Este IDS se baseia em algum tipo de conhecimento, na qual as detecções são realizadas a partir de uma base de dados com informações sobre ataques conhecidos. Seu funcionamento é semelhante a um antivírus, no qual o IDS procura por um padrão ou uma assinatura de ataque que esteja na base de dados. Um conjunto de assinaturas representa tipos de conexões e tráfegos, que podem indicar um ataque em progresso. A taxa de erros desse método é considerada aceitável e boa, porém depende da atualização constante da base de conhecimentos que, por sua vez, depende do sistema operacional, da versão, da plataforma e da aplicação.

Os tipos de IDS caracterizados em I e II são denominados, respectivamente:

A) Host-Based Intrusion Detection System (HIDS) e Knowledge-Based Intrusion Detection System (KIDS)
B) Host-Based Intrusion Detection System (HIDS) e Behavior-Based Intrusion Detection System (BIDS)
C) Network-Based Intrusion Detection System (NIDS) e Knowledge-Based Intrusion Detection System (KIDS)
D) Network-Based Intrusion Detection System (NIDS) e Behavior-Based Intrusion Detection System (BIDS)

36. No que se refere *softwares* maliciosos na internet, um é definido como um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido, para uso com os seguintes objetivos:

- remover evidências em arquivos de *log,*
- instalar outros códigos maliciosos, como *backdoors,* para assegurar o acesso futuro ao computador infectado,
- esconder atividades e informações, como arquivos, diretórios, processos, chaves de registro e conexões de rede,
- mapear potenciais vulnerabilidades em outros computadores, por meio de varreduras na rede e
- capturar informações da rede onde o computador comprometido está localizado, pela interceptação de tráfego.

Esse *software* malicioso é conhecido por:

A) *hoax*
B) *sniffer*
C) *rootkit*
D) *phishing*

37. No que diz respeito à segurança física de equipamentos de informática, três dispositivos devem ser instalados na entrada da alimentação elétrica de equipamentos de informática, particularmente os servidores de rede. As características de dois desses dispositivos são:

I. É o equipamento mais simples, que exerce sua função impedindo que flutuações na corrente elétrica passem diretamente ao sistema causando danos. Nesse dispositivo, o fusível é a única proteção existente. Em caso de uma brusca oscilação de energia ou mesmo queda, o fusível queima e esse dispositivo se sacrifica no lugar do equipamento sob proteção.
II. É o equipamento que busca manter a voltagem fornecida pela concessionária de energia elétrica em níveis próximos ao valor nominal. A função é manter a alimentação da carga o mais próximo possível da nominal (110/127V ou 220V).

Os dispositivos de proteção descritos em I e II são denominados, respectivamente:

A) *nobreak* e autotransformador
B) *nobreak* e estabilizador de tensão
C) filtro de linha e autotransformador
D) filtro de linha e estabilizador de tensão

38. Quando se pensa em segurança, inclui-se a da informação, que tem como objetivo proteger as dados de uma determinada pessoa ou empresa, não somente no aspecto corporativo, pois na medida em que as informações são geradas, as empresas armazenam e as distribuem para gerir seus negócios, com isso aumentando os riscos a que os dados ficam expostos. Atualmente, entre os princípios básicos da segurança da informação que atualmente norteiam a análise, o planejamento e a implementação da segurança dos dados, quatro são detalhados a seguir.

I. Consiste em garantir que apenas as pessoas que estão autorizadas a ter acesso à informação são capazes de fazê-lo.
II. Consiste na garantia de que as informações serão protegidas contra alterações não autorizadas e mantidas sua exatidão, tal qual como foi armazenada e disponibilizada.
III. Consiste em assegurar que os sistemas de informação e a informação estarão disponíveis e operacionais quando necessários, apoiando, assim, os processos de negócios.
IV. Consiste em garantir que a informação seja verdadeira, de fonte segura e que não sofreu alterações em seu percurso.

Os princípios detalhados em I, II, III e IV são denominados, respectivamente:

A) Autenticidade, Confidencialidade, Integridade e Disponibilidade
B) Confidencialidade, Integridade, Disponibilidade e Autenticidade
C) Integridade, Disponibilidade, Autenticidade e Confidencialidade
D) Disponibilidade, Autenticidade, Confidencialidade e Integridade

39. Uma Política de Segurança da Informação bem definida é a base para garantir o correto uso da informação, o que inclui a instalação de um *firewall* como um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança. Na configuração de *firewalls*, são implementados três tipos.

I. É o mais antigo e comum, inserido entre uma rede confiável e outra não confiável, operando nas camadas de rede e de transporte, tomando suas decisões baseadas no endereço IP e nos campos dos pacotes. Nessa configuração, permite ou proíbe o *forward* usando informações contidas nos cabeçalhos dos pacotes.
II. É implantado entre a aplicação de um cliente e a internet, segundo a arquitetura cliente/servidor, como um navegador *web,* servindo como ponte de acesso para a internet ou da internet. Nessa configuração, é feita uma conexão entre o cliente e o *proxy,* e outra entre o *proxy* e o servidor desejado. É empregado para registrar o uso da internet e para bloquear o acesso a um *site* da *web.*
III. É o tipo que provê o nível mais alto de segurança; atua na camada de aplicação da arquitetura TCP/IP, resultando em maior segurança em aplicações específicas, como por exemplo, serviços de FTP, Telnet, SNMP e garante que não existam conexões entre *hosts* externos e internos. Nessa configuração, é um tipo de *firewall* que fornece um maior grau de proteção, mas que apesar de eficiente, pode degradar a performance da rede.

Os três tipos descritos em I, II e III são denominados, respectivamente, *firewalls:*

A) Proxy Server, Gateway de Aplicação e Filtro de Pacotes
B) Proxy Server, Filtro de Pacotes e Gateway de Aplicação
C) Filtro de Pacotes, Proxy Server e Gateway de Aplicação
D) Filtro de Pacotes, Gateway de Aplicação e Proxy Server

40. Nos tempos atuais de *home office,* as VPN cresceram de importância, mas nem todas as VPN são iguais nem arquitetadas da mesma forma e, dependendo do protocolo VPN, aspectos como velocidade, capacidade ou até mesmo segurança e vulnerabilidades de privacidade podem diferir. Uma VPN transmite seu tráfego *online* por meio de túneis criptografados conduzindo-os até servidores VPN que designam um novo endereço IP ao seu dispositivo. Nesse contexto, dois protocolos são os mais utilizados nos dias atuais, tendo por características:

I. É um protocolo bastante popular e muito seguro, usado por muitos provedores VPN, funcionando tanto com protocolos de internet TCP quanto com UDP. Como vantagens é um protocolo de código aberto, é versátil no que diz respeito a uso, maior segurança, além de ignorar a maioria dos *firewalls,* fazendo com que não haja problemas em sua utilização. Como desvantagem, é um protocolo bastante complexo, o que pode ser um problema para usuários menos experientes. Constitui a melhor escolha em termos de segurança, principalmente para conexão às redes públicas de *wifi.*
II. É o protocolo responsável por lançar as bases para uma conexão VPN segura, tendo estabelecido conexões criptografadas e autenticadas. Foi desenvolvido pela Microsoft e pela Cisco especialmente para agir de modo estável e seguro. Como vantagens: é estável; opera com os melhores algoritmos de criptografia, fazendo com que ele seja um dos protocolos VPN's mais seguros; é rápido e veloz com baixo consumo de banda de conexão, além de ignorar *firewalls.* Como desvantagens, não é compatível com muitos sistemas e usa o método Diffie Hellman para processar chaves públicas na criptografia do fluxo de dados, que pode comprometer a segurança e a privacidade dos usuários.

Os protocolos caracterizados em I e II são conhecidos, respectivamente, por:

A) OpenVPN e L2TP/IPSec
B) OpenVPN e IPSec/IKEv2
C) Point to Point Tunneling Protocol e L2TP/IPSec
D) Point to Point Tunneling Protocol e IPSec/IKEv2

41. Os sistemas de autenticação geralmente são categorizados pelo número de fatores que eles incorporam. Os três fatores frequentemente considerados como a base da autenticação são:

- Algo que a pessoa conhece, por exemplo, uma senha.
- Algo que a pessoa tem, por exemplo, um crachá de identificação ou uma chave criptográfica.
- Algo que que a pessoa é, por exemplo, impressão de voz, impressão de polegar ou outro biométrico.

A seguir são listados dois métodos entre os mais utilizados nos sistemas de autenticação.

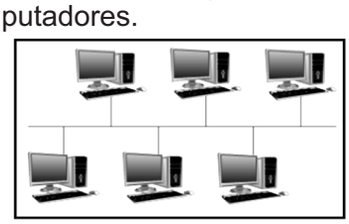
I. Usa senhas categorizadas como fatores de conhecimento, representadas por uma combinação de números, símbolos. É uma ótima maneira de proteção na Autenticação Digital.
II. Usa características fisiológicas ou comportamentais dos indivíduos que incluem, mas que não se limitam à impressão digital, geometria da mão, varredura de retina, varredura de íris, dinâmica de assinatura, dinâmica de teclado, impressão de voz e varredura facial.

Os métodos descritos em I e II são denominados, respectivamente, autenticação:

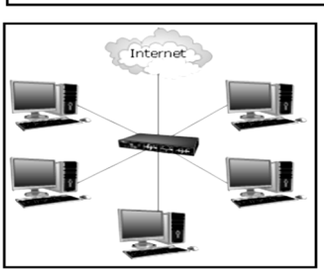
A) baseada em SMS e biométrica
B) baseada em PIN e biométrica
C) baseada em SMS e cognitiva
D) baseada em PIN e cognitiva

42. As figuras I e II representam duas topologias utilizadas na implementação de redes de computadores.

I.



II.



Do ponto de vista físico, as topologias em I e II são conhecidas, respectivamente, por:

A) bus ou barramento e estrela ou radial
B) bus ou barramento e malha ou hierárquica
C) descentralizada ou distribuída e estrela ou radial
D) descentralizada ou distribuída e malha ou hierárquica

43. No que diz respeito à instalação, suporte e configuração do DHCP, existe uma funcionalidade com as seguintes características:

- Permite a *switch* L3 e *roteadores* encaminharem mensagens DHCP via *broadcast* para servidores fora do domínio do *host,* o que vai viabilizar a utilização de um único DHCP em toda a rede LAN.
- O fato de as solicitações ao servidor DHCP de endereços IP ocorrerem via *broadcast* permite aos roteadores com essa funcionalidade configurada encaminharem mensagens em Unicast.
- Trata-se de uma otimização do tráfego de dados de configuração na rede, na qual o servidor DHCP envia ao computador do cliente o escopo com base na interface IP de origem da mensagem DHCP.
- Para o administrador da rede, basta apenas configurar os escopos no servidor.

Essa funcionalidade é conhecida por:

A) DHCP Agent
B) DHCP Relay
C) DHCP Binding
D) DHCP Repeater

44. No que diz respeito ao Modelo de Referência OSI/ISO, prover os processos e métodos que permitem a organização dos *bits* em *frames,* a detecção de erros, o controle do fluxo de dados e a identificação dos computadores num segmento de rede, é função da camada denominada:

A) apresentação
B) transporte
C) enlace
D) rede

45. Os servidores DNS são os responsáveis por localizar e traduzir para números IP os endereços dos *sites* digitados nos *browsers.* Se um internauta quiser ter um *site* próprio, ele precisa registrar o domínio e, se este tiver que terminar com **.br**, o procedimento pode ser feito no *site Registro.br.*
Quando se registra um domínio e se contrata um serviço de hospedagem, este pode oferecer subdomínios baseados em seu endereço para que o contratante possa acessar serviços de *e-mail,* servidor de FTP, entre outros. Em relação aos registros de DNS, três tipos são caracterizados como:

I. São os parâmetros que devem ser configurados para contas de *e-mail* no domínio *(@seusite.com.br),* por exemplo.
II. Indicam o início de uma zona, isto é, de um conjunto de registros localizado dentro de um espaço de nomes de DNS.
III. Servem para criar redirecionamentos para domínios ou subdomínios. É este parâmetro que dever ser utilizado, por exemplo, para criar um endereço do tipo *blog.seusite.com.br.*

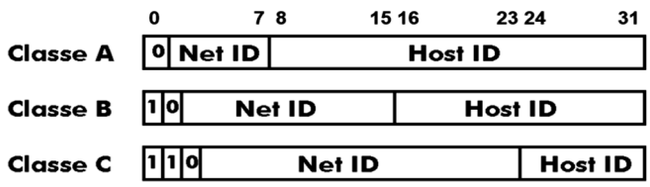
Os tipos de domínios caracterizados em I, II e III são, respectivamente:

A) MX, SOA e CNAME
B) NS, SRV e TXT
C) NS, SRV e CNAME
D) MX, SOA e TXT

46. A sigla SNMP é um acrônimo para “Simple Network Management Protocol” e representa o protocolo padrão para monitoramento e gerenciamento de redes, sendo na prática, o mais usado para saber o que acontece dentro de ativos de redes e serviços. Usa uma base de informações de gerenciamento para monitorar, gerenciar e analisar redes de computadores; opera em uma das camadas do modelo OSI e utiliza usualmente uma porta padrão conhecida na interação com o UDP da camada de transporte.
A sigla para referenciar a base de informações de gerenciamento, a camada e a porta são, respectivamente:

A) SIG, aplicação e 467
B) MIB, aplicação e 161
C) SIG, apresentação e 161
D) MIB, apresentação e 467

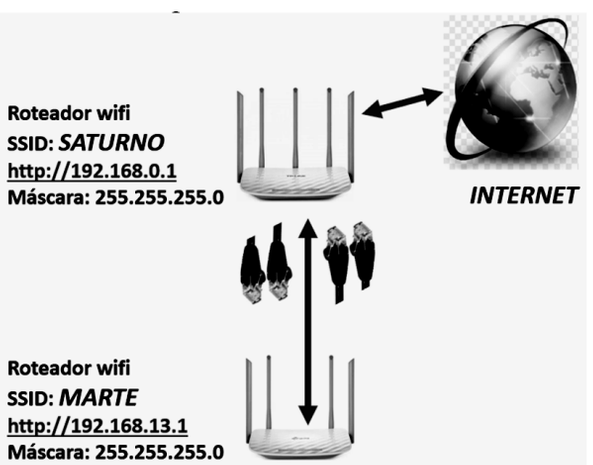
47. No IPv4, os endereços são organizados em pacotes de 32 *bits* divididos em blocos de 8 separados por pontos, onde grupos de *bits* identificam redes e *hosts.* A figura ilustra a estrutura do IPv4.



Nesse contexto, são exemplos válidos de endereços IPv4 de classes A, B e C, respectivamente:

A) 128.0.0.0, 192.0.0.255 e 248.139.128.0
B) 67.239.255.0, 143,255.169.1 e 240.0.0.255
C) 10.0.191.256, 172.16.0.255 e 300.128.150.200
D) 127.0.0.1,191.187.250.254 e 223.240.199.255

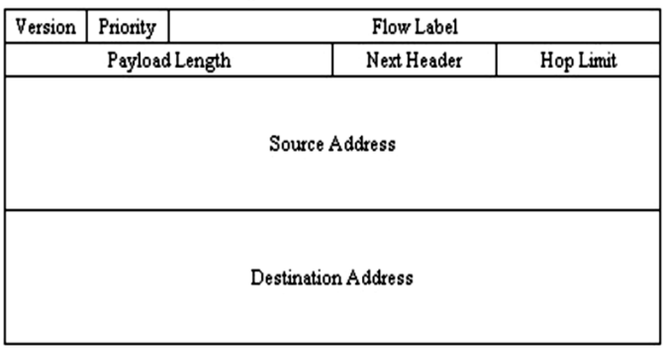
48. Uma rede de computadores com acesso à internet está configurada usando dois roteadores IEEE-802.11/ac, com acesso à internet, sendo o primeiro,SATURNO, de modo direto e o segundo, MARTE, por meio de SATURNO, conforme ilustrado. O endereço IP fornecido pelo provedor de internet para a conexão é 187.195.10.49



Para permitir o roteador MARTE acessar a internet por intermédio de SATURNO, é necessário configurar o roteador MARTE, atribuindo-se três parâmetros: um endereço IP, uma máscara e endereço para *gateway.* Conforme visualizado na figura acima, a máscara 255.255.255.0 é a mesma atribuída aos dois roteadores. Para que a configuração e o *link* funcionem de forma favorável, endereços válidos para o IP e para o *gateway* são, respectivamente:

A) 187.195.10.49 e 192.168.13.1
B) 192.168.0.255 e 192.168.13.1
C) 187.195.10.49 e 192.168.0.1
D) 192.168.0.13 e 192.168.0.1

49. O IPv6 é a versão mais recente do chamado Internet Protocol - IP, o padrão usado para a comunicação entre todos os computadores ligados à Internet. Uma característica fundamental do protocolo IP é que define para cada computador, servidor, celular, *tablet* ou outro dispositivo conectado à rede um endereço único, que serve como identificador perante toda a rede. O IPv6 introduziu um novo formato de cabeçalho, mostrado na figura e caracterizados a seguir.

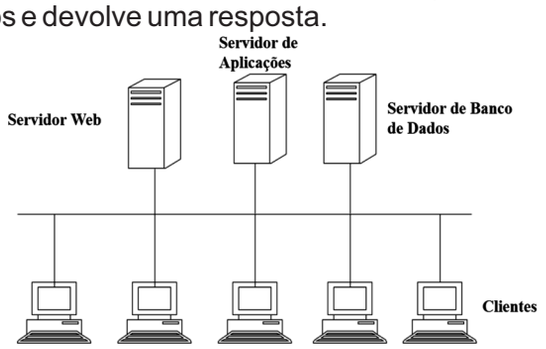


I. Todos os campos desse novo cabeçalho tem um tamanho fixo, o que acelera o processamento nos roteadores, visto que não há necessidade de calcular a extensão dos campos.
II. É um campo do cabeçalho que fornece o número máximo de roteamento entre roteadores que o pacote pode sofrer, sendo esse valor decrementado a cada roteamento. Quando o valor chega a zero, o pacote é descartado.
III. É um campo do cabeçalho que fornece o tamanho, em octetos, do restante do pacote, após o cabeçalho.

O tamanho fixo indicado em I e os identificadores dos campos em II e em III são, respectivamente:

A) 64 bytes, Hop Limit e Flow Label
B) 128 bytes, Hop Limit e Flow Label
C) 64 bytes, Hop Limit e Payload Length
D) 128 bytes, Hop Limit e Payload Length

50. A arquitetura cliente/servidor é aquela na qual o processamento da informação é dividido em módulos ou processos distintos. Um processo é responsável pela manutenção da informação (servidor), enquanto outro é responsável pela obtenção dos dados (cliente). Neste contexto, a figura abaixo ilustra a arquitetura em 4 camadas, por meio da qual o cliente informa a URL por meio do *browser* e o servidor de aplicações analisa a requisição do usuário, determina de que forma os dados serão utilizados, acessa os serviços e devolve uma resposta.



As aplicações são:

I. Acesso – navegação por meio de *browsers.*
II. Dados – com todas as informações necessárias.
III. Apresentação – onde serão feitas as alterações de interface.
IV. Lógica – onde serão feitas as alterações nas regras do negócio, quando necessárias.

Se a aplicação em I corresponde a Clientes, as demais em II, III e IV correspondem respectivamente, aos servidores:

A) de Banco de Dados, Web e de Aplicações
B) de Banco de Dados, de Aplicações e Web
C) de Aplicações, de Banco de Dados e Web
D) de Aplicações, Web e de Banco de Dados