Concurso Público Celesc S.A.

Edital 001/2024

14 de julho de 2024

Cargo Analista de Sistemas – Infraestrutura Operação e Segurança

_____

Preencha seu nome por extenso, neste espaço.
Item 11.2 do edital

Instruções

1. Confira se o nome impresso no Cartão Resposta corresponde ao seu, e se as demais informações estão corretas. Caso haja qualquer irregularidade, comunique imediatamente ao fiscal. Assine-o no local indicado.

2. A prova é composta por 60 questões objetivas, de múltipla escolha, com cinco alternativas de resposta – A, B, C, D e E – das quais, somente uma deverá ser assinalada como correta. Confira o **CARGO**, a impressão e o número das páginas do Caderno de Prova. Caso necessário, solicite um novo Caderno.

3. As questões deverão ser resolvidas no Caderno de Prova e transcritas para o Cartão Resposta, utilizando caneta esferográfica, tubo transparente, com tinta indelével, de cor preta (preferencialmente) ou azul.

4. Não serão prestados quaisquer esclarecimentos sobre as questões das provas durante a sua realização. O candidato poderá, se for o caso, interpor recurso no prazo definido pelo Edital.

5. O Cartão Resposta não será substituído em caso de marcação errada, rasura ou destaque inadequado.

6. Não será permitido ao candidato manter em seu poder qualquer tipo de equipamento eletrônico ou de comunicação, mesmo que desligado, devendo o mesmo ser colocado **OBRIGATORIAMENTE** no saco plástico. Caso essa exigência seja descumprida, implicará a eliminação do candidato.

7. Todo o material, portado pelo candidato, deve ser acomodado em local a ser indicado pelos fiscais de sala de prova.

8. Também não será permitido qualquer tipo de consulta (livros, revistas, apostilas, resumos, dicionários, cadernos, anotações, réguas de cálculo etc.), ou uso de óculos escuros, protetor auricular ou quaisquer acessórios de chapelaria (chapéu, boné, gorro, lenço ou similares), ou o porte de qualquer arma. O não cumprimento dessas exigências implicará a eliminação do candidato.

9. Somente será permitida a sua retirada da sala após uma hora e trinta minutos do início da prova que terá, no máximo, quatro horas de duração. Os três últimos candidatos deverão permanecer em sala até que todos concluam a prova e possam sair juntos.

10. O tempo de resolução das questões objetivas, incluindo o tempo de transcrição para o Cartão Resposta personalizado, é de **QUATRO HORAS**.

11. Ao concluir a prova, permaneça em seu lugar e comunique ao fiscal de sala.

12. Aguarde autorização para entregar o Caderno de Prova e o Cartão Resposta.

13. Diante de qualquer dúvida, comunique-se com o fiscal de sala.

CONHECIMENTOS GERAIS

Texto 1

Preconceito linguístico nos meio digital: ele existe?

Por acaso, ao ler o título, o que lhe saltou aos olhos foi o “erro” de concordância em “nos meio digital”? E, a partir dessa constatação, você concluiu que esta reportagem não tem credibilidade e cogitou a possibilidade de não fazer a leitura? Desculpe-nos ser insistentes, car@ leitor@, mas se você se identificou, aí é que precisa lê-la.
Não é novidade que a internet e, consequentemente, as redes sociais, estão presentes e influenciam nosso cotidiano. Embora, por um lado, elas tenham ressignificado as formas de nos relacionarmos, por outro, ainda reproduzem algumas condutas comuns nos meios não digitais.
Você já deve ter presenciado alguém ser constrangido pela forma que fala, certo? Da mesma maneira, já deve ter visto algum comentário em postagem de rede social desqualificando a opinião/posição de uma pessoa simplesmente pelo jeito que ela escreve, por não seguir estritamente o que se concebe como “língua padrão”. Em outras palavras, por apresentar variação em relação a ela.
Sejam vídeos que circulam no YouTube sejam as famosas pérolas divulgadas nas redes em época de vestibular, o preconceito linguístico ocorre em diversas situações.
Respondendo à pergunta-título: sim, existe preconceito linguístico nos meios digitais. Muitas pessoas podem “torcer o nariz” para essa questão ou achar que é mais uma invenção de uma geração problematizadora, que não vê humor em situações aparentemente inocentes. Ou, ainda, entender que é uma liberação para todo mundo falar “errado”.
O que essas pessoas não entendem é que o direito linguístico é (ou deveria ser) um direito humano fundamental. Todos deveriam poder se expressar, demonstrar suas emoções, compartilhar suas visões de mundo e transmitir seus conhecimentos sem coerção, da forma que se sentem fluentes e capazes. As pessoas devem se sentir livres para poder falar a sua língua – ou variante dela.

Adaptado de: RODRIGUES, Oscar; ALVES; Rafael. Preconceito linguístico nos meio digital: ele existe? **O Consoante**. 22 julho 2017. Disponível em: http://oconsoante.com.br/2017/07/22/preconceito-linguistico-nos-meio-digital-ele-existe/. Acesso em: 03 jun. 2024.

01) Em relação ao Texto 1, analise as afirmativas que seguem.

1. Os autores empregam o solecismo como estratégia discursiva para chamar a atenção dos leitores para o tema do texto.
2. O discurso indireto é adotado no texto para que as ideias fluam de forma mais suave e coesa, em vez de se destacarem como citações diretas.
3. A linguagem coloquial adotada pelos autores é inadequada no contexto de comunicações acadêmico-científicas, ainda que coerente com textos de opinião.
4. A perspectiva dos autores em relação ao papel da linguagem na expressão e perpetuação de preconceitos se revela não apenas pelo conteúdo, mas também na forma.

É **CORRETO** o que se afirma em:

A) 2, 3.
B) 1, 2, 3, 4.
C) 2, 3, 4.
D) 1, 3, 4.
E) 1, 4.

Justificativa
Afirmativa 1: Correta. O erro gramatical do título, além de expressões como “o jeito que ela escreve” são exemplos de solecismo usado de forma intencional no texto.
Afirmativa 2: Incorreta. O texto não emprega o discurso indireto, pois não se constrói como uma paráfrase das palavras de outrem.
Afirmativa 3: Correta: O texto é um artigo de opinião que usa a linguagem dialogada e coloquial, a qual não é recomendada em publicações acadêmico-científicas.
Afirmativa 4: Correta: A presença da expressão “car@ leitor@”, além da linguagem simples, demonstra a preocupação em retratar na forma da expressão a ideia de inclusão.

Referência
AZEREDO, José Carlos De. **Gramática Houaiss da língua portuguesa**. São Paulo: Parábola, 2021.
BECHARA, Evanildo. **Compreender e interpretar os textos**: Para todo tipo de prova de Língua Portuguesa. Rio de Janeiro: Nova Fronteira, 2020.

Nível	Superior
Disciplina	Português
Eixo Temático	Texto e Discurso
Tema	Leitura e interpretação de textos.
Tópico do Conteúdo	Variedade de textos e adequação de linguagem. Discurso direto e indireto. Figuras de linguagem. Uso de linguagem não violenta.

---

02) A partir da leitura do Texto 1, é **CORRETO** concluir que:

A) As línguas não são homogêneas e as variações linguísticas representam possibilidades válidas de expressão.
B) Os autores não dominam o registro formal da língua, por este motivo o texto apresenta desvios da norma culta.
C) O preconceito linguístico é uma forma de exclusão social, que escapa ao âmbito das comunicações virtuais.
D) Hoje o preconceito linguístico é absolutamente reconhecido e rechaçado nos meios digitais e não digitais.
E) Os autores defendem a perspectiva de que as pessoas devem ter o direito de poder falar errado.

Justificativa
Correta: No texto, se afirma que há uma variedade considerada “padrão” juntamente com outras, e que as “pessoas devem se sentir livres para poder falar a sua língua – ou variante dela.”
Incorreta: Ao longo do texto. os autores empregam majoritariamente o registro culto, por exemplo, quanto à concordância e colocação pronominal, sendo empregadas poucas formas distintas do uso culto de maneira proposital pelos autores.
Incorreta: No texto, fica claro que o preconceito linguístico também se manifesta no meio digital.
Incorreta: Conforme o texto, ainda há aqueles que não reconhecem o preconceito linguístico: “Muitas pessoas podem ‘torcer o nariz’ para essa questão ou achar que é mais uma invenção de uma geração problematizadora”.
Incorreta: Os autores demonstram questionar o conceito de “falar errado”, pelo próprio uso do termo entre aspas, pois compreendem a língua como um conjunto de variações, ao mesmo tempo, defendem o direito a todos poderem se expressar em sua variedade linguística.

Referência
BECHARA, Evanildo. **Compreender e interpretar os textos**: Para todo tipo de prova de Língua Portuguesa. Rio de Janeiro: Nova Fronteira, 2020.

Nível	Superior
Disciplina	Português
Eixo Temático	Texto e discurso
Tema	Leitura e interpretação de textos.
Tópico do Conteúdo	Informações literais e inferências.

Texto 2

Ecossistema de aprendizagem on-line: Construções teórico-metodológicas

A cultura digital impacta a relação dicotômica entre ambientes físicos e on-line. O cenário sociotécnico da educação ainda está descompassado em relação às competências digitais e é socialmente segregário. Nesse sentido, desde a revisão sistemática da literatura, identificamos estudos que apontam os ecossistemas de aprendizagem on-line como possíveis estruturas metodológicas congruentes às demandas dessa convergência. A revisão incluiu 206 produções, das quais 14 foram elegíveis a partir do método *Preferred Reporting Items for Systematic Reviews and Meta-Analyses*. Os resultados revelaram que tais ecossistemas impactam e alteram as relações convencionais entre professor e estudante, organização de sala de aula e compreensão dos processos mediados por tecnologias.

FONTE: SANTOS, W. A. C.; MERCADO, L. P. L.; OLIVEIRA, C. A. de. Ecossistema de aprendizagem on-line: Construções teórico-metodológicas. **Cadernos de Pesquisa**, v. 53, p. e10172, 2023. Disponível em: https://doi.org/10.1590/1980531410172. Acesso em: 03 jun. 2024.

---

03) Em relação às informações apresentadas no Texto 2, assinale a alternativa que apresenta uma afirmativa **CORRETA**

A) De acordo com os pesquisadores, as tecnologias digitais aplicadas à educação, além de impactarem a organização da sala de aula, também tem a capacidade de equalizar as relações sociais.
B) Os pesquisadores identificaram que as competências digitais utilizadas na educação se alinham ao contexto social de uso das tecnologias de comunicação e informação.
C) O estudo sobre os ecossistemas de aprendizagem on-line foi realizado através de uma revisão sistemática da literatura, cujo resultado incluiu a análise de 206 obras.
D) Conforme o estudo, a cultura digital ampara a relação de oposição exclusiva na qual se encontram os ambientes digital e físico.
E) Já na fase da pesquisa bibliográfica, foi possível verificar que a educação digital apresenta métodos e estratégias que apoiam o estreitamento da relação entre físico e digital.

Justificativa
Correta: "Já na fase da pesquisa bibliográfica foi possível verificar que a educação digital apresenta métodos e estratégias que apoiam o estreitamento da relação entre físico e digital". Conforme o texto, a partir da revisão da literatura, foram identificados estudos que apontam que os ecossistemas de aprendizagem on-line são possíveis estruturas metodológicas compatíveis com a necessidade de convergência do físico com o virtual.

Incorreta: "Os pesquisadores identificaram que as competências digitais utilizadas na educação se alinham ao contexto social de uso das tecnologias de comunicação e informação." O texto menciona que o cenário sociotécnico da educação ainda está descompassado em relação às competências digitais.

Incorreta: "O estudo sobre os ecossistemas de aprendizagem on-line foi realizado através de uma revisão sistemática da literatura, cujo resultado incluiu a análise de 206 obras." O texto menciona especificamente que a revisão sistemática da literatura incluiu 206 produções, mas, destas, apenas 14 foram elegíveis para compor os resultados da análise.

Incorreta: "De acordo com os pesquisadores, as tecnologias digitais aplicadas à educação, além de impactarem a organização da sala de aula, também tem a capacidade de equalizar as relações sociais." O texto indica que os processos mediados por tecnologias alteram a organização da sala de aula, mas que o cenário sociotécnico é segregário.

Referência
BECHARA, Evanildo. **Compreender e interpretar os textos**: Para todo tipo de prova de Língua Portuguesa. Rio de Janeiro: Nova Fronteira, 2020.

Nível	Superior
Disciplina	Português
Eixo Temático	Texto e Discurso
Tema	Compreensão e interpretação de textos.
Tópico do Conteúdo	Informações literais e inferências

---

04) No Texto 2, a expressão "nesse sentido" pode ser substituída sem prejuízo de sentido por:

A) Em virtude disso.
B) Portanto.
C) Além disso.
D) Analogamente.
E) Desse modo.

Justificativa
Correta: "além disso". No texto 2, a relação que se apresenta entre as ideias ligadas por "nesse sentido" é de adição e continuidade. Verificou-se uma dicotomia entre o físico digital e identificou-se que ela pode ser superada através de ferramentas digitais de educação.
Incorreta: "portanto". A relação entre as ideias não é de conclusão, uma ideia não decorre logicamente da outra.
Incorreta: "em virtude disso". A relação entre as ideias não é de consequência.
Incorreta: "analogamente". A relação entre as ideias não é analogia.
Incorreta: "desse modo". A relação entre as ideias não é de conclusão.

Referência

AZEREDO, José Carlos De. **Gramática Houaiss da língua portuguesa**. São Paulo: Parábola, 2021.

Nível	Superior
Disciplina	Português
Eixo Temático	Texto e discurso
Tema	Estruturação do texto
Tópico do Conteúdo	Recursos de coesão

---

05) "O cenário sociotécnico da educação [...] é socialmente segregário." Sobre a palavra destacada, considere as possibilidades de análise abaixo:

1. Pertence à classe dos substantivos, pois funciona como núcleo do sintagma nominal.
2. Pode ser analisada em: SE- (prefixo que significa "à parte") + GREG- (radical que significa "pertencente a um grupo") + -ÁRIO (sufixo que expressa noção de função).
3. Consiste em um neologismo, construído por analogia à palavra "gregário" e com sentido oposto ao desta.

É **CORRETO** apenas o que se afirma em:

A) 3.
B) 1, 2.
C) 2, 3.
D) 2.
E) 1, 3.

Justificativa
Afirmativa 1: Incorreta. A palavra no contexto é um adjetivo.
Afirmativa 2: Incorreta. A palavra é formada pelo radical "segreg-" e do sufixo "-ário".
Afirmativa 3: Correta: O uso adjetivo do termo "segregar" é inovador e segue a mesma lógica de construção do adjetivo. "gregário", com o qual apresenta relação de antonímia.

Referência
AZEREDO, José Carlos De. **Gramática Houaiss da língua portuguesa**. São Paulo: Parábola, 2021.

Nível	Superior
Disciplina	Português
Eixo Temático	Léxico
Tema	Morfologia
Tópico do Conteúdo	Classes de palavras. Estrutura do vocábulo. Formação de palavras.

---

06) Assinale a afirmativa **CORRETA** sobre o uso da palavra "ecossistemas" no Texto 2.

A) Trata-se de uma palavra na qual ocorreu uma catacrese, devido à mudança do significado original por esmaecimento do sentido original.
B) Trata-se de uso denotativo do termo, pois refere-se ao conjunto das relações de interdependência que seres estabelecem entre si e com o ambiente que os cerca.
C) É um exemplo braquilogia, pois, no texto, emprega-se uma expressão mais curta, equivalente a outra mais ampla ou de estruturação mais complexa.
D) É um caso de hiperonímia, pois o termo expressa, de uma forma mais abrangente, o sentido de "ambientes digitais de aprendizagem".
E) Representa um uso figurado da palavra, consistindo em uma metáfora que relaciona a complexidade das relações na ecologia às da educação digital.

Justificativa
Correta: O termo "ecossistemas" é usado em sentido metafórico, pois é a apropriação de um termo da ecologia, que descreve relações complexas entre seres e ambientes, aplicado para descrever as relações entre atores e sistemas na educação digital.
Incorreta: O uso do termo é conotativo e não denotativo ou literal.
Incorreta: Braquilogia é uma forma abreviada de uma expressão, não se aplica ao caso.
Incorreta: Não há relação de hiponímia ou hiperonímia, mas de uma comparação.

Incorreta: Não se trata de emprego por mudança de sentido, mas sim a aplicação de sentido metafórico.

Referência
BECHARA, Evanildo. **Compreender e interpretar os textos**: Para todo tipo de prova de Língua Portuguesa. Rio de Janeiro: Nova Fronteira, 2020.
AZEREDO, José Carlos De. **Gramática Houaiss da língua portuguesa**. São Paulo: Parábola, 2021.

Nível	Superior
Disciplina	Português
Eixo Temático	Texto e Discurso
Tema	Semântica
Tópico do Conteúdo	Figuras de linguagem

---

07) Qual item abaixo **NÃO** se refere à qualidade do produto energia elétrica, segundo os procedimentos de distribuição de energia elétrica da Aneel (PRODIST, 2021):

A) Variação de tensão em regime permanente.
B) Potência instalada.
C) Harmônicas.
D) Variação de frequência.
E) Fator de potência.

Justificativa
Os aspectos considerados pela Aneel para avaliar a qualidade do produto energia elétrica são apresentados no Anexo VIII da Resolução Normativa Aneel n.º 956, de 7 de dezembro de 2021 – Procedimentos de Distribuição de Energia Elétrica – PRODIST (Módulo 8 – Qualidade de Fornecimento de Energia Elétrica). A potência instalada da edificação não é considerada. Todos os demais itens são considerados.

Referência
LEGISLAÇÃO DO SETOR ELÉTRICO BRASILEIRO. PRODIST – Procedimentos de Distribuição de Energia Elétrica (Módulo 8 - Qualidade de Fornecimento de Energia Elétrica). Resolução Normativa Aneel n.º 956, de 7 de dezembro de 2021.

Nível	Superior
Disciplina	Distribuição e transmissão de energia elétrica
Eixo Temático	Planejamento de redes de distribuição
Tema	Qualidade na distribuição de energia elétrica. Indicadores de continuidade
Tópico do Conteúdo	Qualidade do serviço energia elétrica

---

08) Atualmente, no Brasil, existem diversos agentes atuando no mercado de energia elétrica e, dentre estes, destaca-se o que a Aneel define como: "[...] pessoa jurídica ou consórcio de empresas que recebe concessão ou autorização para explorar aproveitamento hidrelétrico ou central geradora termelétrica e respectivo sistema de transmissão associado e para comercializar, no todo ou em parte, a energia produzida por sua conta e risco". Esta definição corresponde ao:

A) Comercializador de energia.
B) Cogerador.
C) Produtor independente de energia.
D) Autoprodutor.
E) Agente importador de energia.

Justificativa
Esta definição está no Anexo I da Resolução Normativa Aneel n.º 956, de 7 de dezembro de 2021 – Procedimentos de Distribuição de Energia Elétrica – PRODIST (Módulo 1 – Glossário de Termos Técnicos do PRODIST).

Referência
LEGISLAÇÃO DO SETOR ELÉTRICO BRASILEIRO. PRODIST – Procedimentos de Distribuição de Energia Elétrica (Módulo 1 - Glossário de Termos Técnicos). Resolução Normativa Aneel n.º 956, de 7 de dezembro de 2021.

Nível	Superior
Disciplina	Distribuição e transmissão de energia elétrica
Eixo Temático	Planejamento de redes de distribuição
Tema	Agentes do sistema elétrico
Tópico do Conteúdo	Legislação do setor elétrico brasileiro

---

09) Por meio do controle das interrupções e da apuração dos indicadores de continuidade de serviço, as distribuidoras, os consumidores, as centrais geradoras e a Aneel, podem avaliar a qualidade do serviço prestado e o desempenho do sistema elétrico. Um destes indicadores utilizados pela Aneel é baseado em um indicador internacional, denominado SAIDI – System Average Interruption Duration Index. O indicador de continuidade Aneel equivalente ao SAIDI é:

A) DMIC.
B) FEC.
C) DICRI.
D) DEC.
E) FIC.

Justificativa
O indicador de continuidade DEC significa Duração Equivalente de Interrupção por Unidade Consumidora, sendo equivalente ao SAIDI.

Referência
LEGISLAÇÃO DO SETOR ELÉTRICO BRASILEIRO. PRODIST – Procedimentos de Distribuição de Energia Elétrica (Módulo 8 - Qualidade de Fornecimento de Energia Elétrica). Resolução Normativa Aneel n.º 956, de 7 de dezembro de 2021.

Nível	Superior
Disciplina	Distribuição e transmissão de energia elétrica
Eixo Temático	Planejamento de redes de distribuição
Tema	Qualidade na distribuição de energia elétrica. Indicadores de continuidade
Tópico do Conteúdo	Qualidade do serviço energia elétrica

---

10) Com relação ao processo de reestruturação do setor elétrico brasileiro, ocorrido na década de 1990, analise as afirmações abaixo:

I. Houve uma desverticalização da indústria de energia elétrica, separando-se os segmentos de geração, transmissão, distribuição e comercialização de energia elétrica.
II. Introduziu-se competição nas atividades de geração e comercialização de energia elétrica.
III. As atividades de transmissão e distribuição de energia continuaram estatais.
IV. Um dos objetivos da reestruturação foi garantir a expansão da capacidade instalada do sistema elétrico.

As opções acima que estão **CORRETAS** são:

A) I, II e IV.
B) II, III e IV.
C) I, III e IV.
D) III e IV.
E) Todas estão corretas.

Justificativa
A maior parte das distribuidoras e transmissoras de energia elétrica no Brasil foram privatizadas. Assim, a única afirmação incorreta é a afirmação III.

Referência
SILVA, Edson Luiz da. **Formação de preços em mercados de energia elétrica**. RS: editora Sagra-Luzzatto. 2001.

Nível	Superior
Disciplina	Estruturação do setor elétrico e mercado de energia elétrica
Eixo Temático	Histórico da reestruturação
Tema	Histórico
Tópico do Conteúdo	Legislação do setor elétrico brasileiro

11) A Aneel – Agência Nacional de Energia Elétrica exerce diversas atribuições importantes dentro do atual modelo do setor elétrico brasileiro. Dentre as afirmações abaixo, assinale qual NÃO é uma atribuição da Aneel:

A) Promover as atividades de outorgas de concessão, permissão e autorização de empreendimentos e serviços de energia elétrica.
B) Regular as atividades do setor elétrico brasileiro.
C) Fiscalizar as concessões, permissões e os serviços de energia elétrica.
D) Estabelecer tarifas.
E) Controlar a operação das instalações de geração e transmissão de energia elétrica no Sistema Interligado Nacional.

Justificativa
Controlar a operação do Sistema Interligado Nacional é atribuição do Operador Nacional do Sistema Elétrico (ONS). As demais são atribuições da Aneel, constantes em seu estatuto e definidas pela Lei n.º 9.427, de 26 de dezembro de 1996 e pelo Decreto n.º 2.335, de 06 de outubro de 1997.

Referência
LEGISLAÇÃO DO SETOR ELÉTRICO BRASILEIRO. Lei n.º 9.427, de 26 de dezembro de 1996.

Nível	Superior
Disciplina	Estruturação do setor elétrico e mercado de energia elétrica
Eixo Temático	Histórico da reestruturação
Tema	Agentes do sistema elétrico
Tópico do Conteúdo	Legislação do setor elétrico brasileiro

---

12) Sobre a geração distribuída no Brasil, assinale a afirmação abaixo que **NÃO** está **CORRETA**.

A) O sistema de compensação de energia elétrica, o qual permite que os consumidores com sistemas de geração distribuída fotovoltaica possam injetar a energia excedente na rede elétrica e obter créditos da concessionária, foi estabelecido inicialmente pela Resolução Normativa Aneel n.º 482, de 2012.
B) A energia elétrica gerada de forma distribuída pelos sistemas fotovoltaicos pode ser comercializada livremente na Câmara de Comercialização de Energia Elétrica, de acordo com a legislação atual brasileira.
C) A Resolução Normativa Aneel n.º 687, de 2015, ampliou as regras estabelecidas pela Resolução Normativa Aneel n.º 482, de 2012, introduzindo novas modalidades de geração distribuída, tais como a geração compartilhada.
D) A Lei n.º 14.300, de 2022, instituiu o marco legal da microgeração e da minigeração, o sistema de compensação de energia elétrica e o programa de energia renovável social.
E) Conforme a Lei n.º 14.300, de 2022, a minigeração distribuída é definida como a central geradora que possua potência instalada, em corrente alternada, maior que 75 kW e menor ou igual a 3 MW para as fontes não despacháveis.

Justificativa
De acordo com a legislação atual, a energia gerada de forma distribuída pelos sistemas fotovoltaicos não pode ser comercializada, mas sim o seu excedente pode ser injetado na rede de distribuição, sendo que o consumidor pode receber créditos. Este sistema é chamado de sistema de compensação de energia e foi criado inicialmente pela Resolução Aneel n.º 482/2012, e depois aperfeiçoado pela Lei n.º 14.300/2022. A minigeração distribuída foi definida pela Lei 14.300/2022, sendo classificada de 75 kW até 3 MW para as fontes não despacháveis, como é a geração distribuída fotovoltaica.

Referência
LEGISLAÇÃO DO SETOR ELÉTRICO BRASILEIRO. Resoluções Normativas Aneel n.º 482/2012 e n.º 687/2015, e Lei n.º 14.300/2022.

Nível	Superior

Disciplina	Distribuição e transmissão de energia elétrica
Eixo Temático	Planejamento de redes de distribuição
Tema	Qualidade na distribuição de energia elétrica. Indicadores de continuidade
Tópico do Conteúdo	Qualidade do serviço energia elétrica

---

13) Amanda, Bruna e Camila ganharam um prêmio em dinheiro por formarem a equipe com o melhor rendimento trimestral na empresa em que trabalham. Elas resolveram dividir o prêmio de R$12.580,00 em partes inversamente proporcionais aos seus salários. O salário de Amanda equivale a 8 salários-mínimos, o de Bruna, a 10 salários-mínimos e o de Camila a 12 salários-mínimos. Quanto coube a Camila receber do prêmio?

A) R$ 3.352,00.
B) R$ 3.400,00.
C) R$ 4.080,00.
D) R$ 5.028,00.
E) R$ 5.100,00.

Justificativa
Se o valor do prêmio é dividido em partes inversamente proporcionais aos salários, temos:
Amanda + Bruna + Camila = 12.580.
Amanda, Bruna e Camila são inversamente proporcionais aos números 8, 10 e 12, respectivamente.
Assim,
Amanda = $\frac{k}{8}$, Bruna = $\frac{k}{10}$, Camila = $\frac{k}{12}$.

Substituindo esses valores na equação Amanda + Bruna + Camila = 12.580, obtemos:

$\frac{k}{8}+\frac{k}{10}+\frac{k}{12}=12.580$

$\left(\frac{1}{8}+\frac{1}{10}+\frac{1}{12}\right)k=12.580$

$\left(\frac{15+12+10}{120}\right)k=12.580$

$\left(\frac{37}{120}\right)k=12.580$

$k=40.800$

Então,

Camila = $\frac{k}{12}=\frac{40.800}{12}=3.400$

Referência
SILVEIRA, Ênio. **Matemática**: compreensão e prática. 3. ed. Moderna, 2015.

Nível	Superior
Disciplina	Matemática
Eixo Temático	Álgebra
Tema	Proporção
Tópico do Conteúdo	Sequências de números inversamente proporcionais

---

14) Entre 10 moradores de um condomínio, quatro afirmam ter animais domésticos. Três moradores são escolhidos ao acaso. Qual a probabilidade de pelo menos dois terem animais domésticos?

A) 1/2.
B) 1/3.

C) 1/4.
D) 2/3.
E) 3/4.

Justificativa
Se três moradores são escolhidos ao acaso entre os 10, então temos um total de possibilidades formado por uma combinação.

$\binom{10}{3} = 120.$

O evento A que nos interessa é formado por todas as combinações tais que, em cada uma, há 2 ou 3 moradores que afirmam ter animais domésticos.

$A = \binom{4}{2}\binom{6}{1} + \binom{4}{3} = 40$. Assim,

$P(A) = \frac{40}{120} = \frac{1}{3}$

Referência
HAZZAN, Samuel. **Fundamentos de matemática elementar, 5**: combinatória, probabilidade. 8. ed. São Paulo: Atual, 2013.

Nível	Superior
Disciplina	Matemática
Eixo Temático	Estatística e probabilidade
Tema	Probabilidade
Tópico do Conteúdo	Probabilidade de um evento num espaço equiprovável

---

15) Ao comprar um produto à vista, obtive um desconto de R$ 125,00, que corresponde a 12% do preço original. O valor pago pelo produto foi de:

A) R$ 937,50.
B) R$ 967,50.
C) R$ 1.041,66.
D) R$ 1.040,00.
E) R$ 1.166,66.

Justificativa
O valor pago pelo produto corresponde a 90% do valor original, logo:

12% ⟶ R$125,00

90% ⟶ (valor pago)

(valor pago) = (125 x 90) / 12

(valor pago) = R$937,50

Referência
SILVEIRA, Ênio. **Matemática**: compreensão e prática. 3. ed. Moderna, 2015.

Nível	Superior
Disciplina	Matemática
Eixo Temático	Álgebra
Tema	Porcentagens
Tópico do Conteúdo	Descontos e acréscimos

---

16) Uma pesquisa de opinião coletou dados de x indivíduos. Entre os participantes, 32**%** eram mulheres. Entre os homens, 75% possuíam nível universitário. Qual alternativa representa, em função de x, a quantidade de homens entrevistados que não possuem formação universitária?

A) 0,83x
B) 0,08x
C) 0,2176x
D) 0,24x
E) 0,17x

Justificativa
De acordo com o enunciado, há 0,32x mulheres, logo a porcentagem de homens é 0,68x. Entre os homens, 75% têm nível universitário, logo 25% não. Assim, o número de homens sem formação universitária é:
(0,25)0,68x = 0,17x.

Referência
IEZZI, Gelson. **Fundamentos de matemática elementar, 11**: matemática comercial, matemática financeira, estatística descritiva. 9. ed. São Paulo: Atual, 2013.

Nível	Superior
Disciplina	Matemática
Eixo Temático	Álgebra
Tema	Porcentagens
Tópico do Conteúdo	Porcentagens

---

17) Um fotógrafo profissional precisa organizar suas fotos de acordo com a data em que foram tiradas. Assinale a alternativa **CORRETA**, que apresenta a ferramenta do Windows a qual ele pode utilizar para realizar essa tarefa de forma eficiente.

A) Prompt de Comando.
B) Gerenciador de Arquivos.
C) Explorador de Arquivos (com visualização em detalhes).
D) Painel de Comando.
E) Software de Edição de Fotos.

Justificativa
A alternativa A é a correta, pois o Explorador de Arquivos no Windows oferece uma visualização em detalhes que permite visualizar e organizar arquivos por diferentes colunas, incluindo a data de criação. Essa funcionalidade é ideal para organizar fotos por data, pois permite visualizar rapidamente a data em que cada foto foi tirada e agrupá-las de acordo com essa informação.
A alternativa B está incorreta, pois o Gerenciador de Arquivos é um termo genérico que pode se referir a diferentes ferramentas de gerenciamento de arquivos, incluindo o Explorador de Arquivos. A resposta não especifica qual ferramenta específica do Gerenciador de Arquivos seria a mais adequada para a tarefa.
A alternativa C está incorreta, pois o Prompt de Comando é uma ferramenta baseada em texto, que pode ser utilizada para executar comandos e automatizar tarefas. Embora seja possível organizar arquivos por data usando o Prompt de Comando, o processo seria mais complexo e menos intuitivo do que usar o Explorador de Arquivos.
A alternativa D está incorreta, pois o Painel de Controle fornece acesso a diversas configurações do sistema Windows, mas não possui funcionalidades específicas para organizar arquivos.
A alternativa E está incorreta, pois Softwares de edição de fotos geralmente focam na edição e manipulação de imagens, e não em sua organização. Embora alguns softwares possam oferecer recursos de organização por data, o Explorador de Arquivos do Windows já fornece essa funcionalidade de forma integrada.

Referência
CUNHA, R. O. **Windows 10 do Zero**. Editora Ricardo Oliveira, 2022.
RATHBONE, A. **Windows 10 para Leigos**. Alta Books, 2016.

Nível	Superior
Disciplina	Informática
Eixo Temático	Microsoft Word
Tema	Barra de Ferramentas do Word

Tópico do Conteúdo	Comandos do Word

18) Uma empresa de marketing digital está explorando o uso de inteligência artificial (IA) generativa para melhorar suas campanhas publicitárias. A equipe está discutindo como essa tecnologia pode ser utilizada para criar conteúdo personalizado e interativo para seus clientes, além de otimizar o processo criativo, economizando tempo e recursos. Assinale a alternativa **CORRETA**, que traz a aplicação da IA generativa mais adequada para uma empresa de marketing digital que deseja melhorar suas campanhas publicitárias.

A) Usar IA generativa para produzir e-mails de marketing altamente personalizados e segmentados.
B) Utilizar IA generativa para criar estratégias de SEO (Search Engine Optimization) personalizadas.
C) Implementar IA generativa para gerenciar o atendimento ao cliente via chatbots.
D) Aplicar IA generativa para automatizar processos de recrutamento e seleção de novos funcionários.
E) Empregar IA generativa para desenvolver softwares de contabilidade interna.

Justificativa
A alternativa A é a correta, pois a IA generativa pode analisar grandes volumes de dados sobre os comportamentos e preferências dos clientes, criando e-mails de marketing altamente personalizados e segmentados, o que pode aumentar significativamente as taxas de abertura e engajamento. Esta aplicação alinha-se diretamente com o objetivo da empresa de melhorar suas campanhas publicitárias, tornando-as mais eficazes e atraentes para o público-alvo.
A alternativa B está incorreta, pois, embora a IA possa ajudar na análise de dados e na geração de insights para SEO, essa tarefa geralmente requer uma compreensão mais profunda dos algoritmos de busca e tendências, algo que vai além das capacidades típicas da IA generativa focada na criação de conteúdo.
A alternativa C está incorreta, pois, embora os Chatbots baseados em IA sejam úteis para atendimento ao cliente, isso não está diretamente relacionado com a melhoria de campanhas publicitárias. O foco aqui é na interação e suporte ao cliente, não na criação de conteúdo publicitário.
A alternativa D está incorreta, pois, embora a automação de recrutamento e seleção possa ser beneficiada pela IA, isso não contribui diretamente para o objetivo de melhorar campanhas publicitárias, que é a necessidade específica da empresa de marketing digital.
A alternativa E está incorreta, pois a aplicação da IA na contabilidade interna está fora do escopo das campanhas publicitárias e do marketing digital. Esse uso é mais voltado para a eficiência operacional interna da empresa, não para a criação de conteúdo de marketing.

Referência
CARRARO, F. **Inteligência Artificial e Chat GPT**. Casa do Código – Alura, 2023.
LEÂO, L. **Inteligência Artificial Generativa**: modo de usar. Clube dos Autores, 2023. e-book.
MOURA, F. **Futuro da IA Generativa**. Clube dos Autores, 2023.

Nível	Superior
Disciplina	Informática
Eixo Temático	Business Intelligence
Tema	Inteligência Artificial
Tópico do Conteúdo	Inteligência Artificial Generativa

19) Durante um treinamento interno, os funcionários de uma empresa estão aprendendo a usar o Excel para melhorar suas habilidades em análise de dados. O instrutor explica a diferença entre fórmulas e funções e demonstra como usá-las para realizar cálculos e análises de forma eficiente. Assinale a alternativa que descreve **CORRETAMENTE** o uso da função PROCV no Excel.

A) A função PROCV é usada para concatenar (juntar) texto de várias células em uma única célula.
B) A função PROCV é usada para calcular a média de um intervalo de células.
C) A função PROCV é empregada para contar o número de células que contêm números em um intervalo.
D) A função PROCV é utilizada para procurar um valor em uma coluna e retornar um valor em uma linha correspondente.
E) A função PROCV é utilizada para aplicar formatação condicional com base em critérios específicos.

Justificativa
A alternativa A é a correta, pois a função VLOOKUP (Vertical Lookup) no Excel é usada para procurar um valor específico em uma coluna (primeira coluna de um intervalo) e retornar um valor na mesma linha de uma coluna especificada. É amplamente utilizada para buscar dados em tabelas organizadas verticalmente.

A alternativa B está incorreta, pois a função utilizada para calcular a média de um intervalo de células é a função AVERAGE, não a VLOOKUP. A VLOOKUP é especificamente para buscas de valores.
A alternativa C está incorreta, pois a função COUNT é usada para contar o número de células que contêm números em um intervalo. A VLOOKUP não realiza contagens.
A alternativa D está incorreta, pois a função usada para concatenar texto de várias células é a função CONCATENATE (ou CONCAT no Excel mais recente), e não a VLOOKUP.
A alternativa E está incorreta, pois a formatação condicional é uma funcionalidade do Excel que permite aplicar formatação a células que atendem a certos critérios, mas não é realizada pela função VLOOKUP. A formatação condicional é configurada através da ferramenta específica no menu "Formatação Condicional".

Referência
GONÇALVES, R. **O Grande Livro do Excel** – intermediário e avançado. Camelot Editora, 2021.
JELEN, B., SYRSTAD, T., AMORIM, R. **Microsoft Excel 2019**: VBA e Macros. Alta Books, 2021.
SABINO, R. **Excel Básico para o mundo do trabalho**. SENAC São Paulo, 2019.

Nível	Superior
Disciplina	Informática
Eixo Temático	Excel
Tema	Ferramentas do Excel
Tópico do Conteúdo	Fórmulas

---

20) Uma empresa de tecnologia está realizando um workshop para seus funcionários sobre segurança cibernética, e um dos temas refere-se aos diferentes tipos de ameaças digitais, destacando suas características e impactos no ambiente corporativo. Assinale a alternativa que descreve **CORRETAMENTE** a ameaça que se caracteriza por sequestrar dados, exigindo um resgate financeiro para liberar o acesso a esses dados.

A) Spyware.
B) Ransomware.
C) Vírus.
D) Malware.
E) Phishing.

Justificativa
A alternativa A é a correta, pois Ransomware é um tipo de malware que criptografa os dados da vítima e exige um pagamento (resgate) para liberar o acesso a esses dados. Ele é projetado especificamente para extorquir dinheiro das vítimas, tornando seus arquivos inacessíveis até que o resgate seja pago.
A alternativa B está incorreta, pois Spyware é um tipo de software malicioso que se infiltra em um sistema para coletar informações sobre o usuário sem o seu conhecimento. Ele monitora e transmite dados como hábitos de navegação, credenciais de login e outras informações sensíveis, mas não sequestra dados para exigir resgate.
A alternativa C está incorreta, pois Vírus é um tipo de malware que se replica e se espalha para outros arquivos ou programas dentro de um sistema. Ele pode danificar arquivos e sistemas, mas sua principal característica não é exigir um resgate financeiro.
A alternativa D está incorreta, pois o Malware é um termo genérico que engloba qualquer software malicioso, incluindo vírus, spyware, ransomware e outros. Embora ransomware seja uma categoria de malware, o termo "malware", por si só, não especifica o sequestro de dados e a exigência de resgate.
A alternativa E está incorreta, pois Phishing é uma técnica de engenharia social usada para enganar as pessoas para fornecerem informações sensíveis, como senhas e números de cartão de crédito, geralmente através de e-mails falsos ou sites fraudulentos. Não envolve o sequestro de dados e a exigência de resgate.

Referência
MITNICK, K.; SIMON, W.L. **A arte de enganar ataques de hackers**: controlando o fator humano na segurança da informação. Pearson Universidades, 2003.
WEIDMAN, G. **Testes de invasão**: uma introdução prática ao hacking. Novatec Editora, 2014.
WINDT, E., JORGE, H. **Crimes Cibernéticos**: ameaças, procedimentos e investigação. 3. ed. Brasport, 2021.

Nível	Superior
Disciplina	Informática
Eixo Temático	Segurança da Informação
Tema	Conceitos e Definições
Tópico do Conteúdo	Ameaças mais comuns

CONHECIMENTOS ESPECÍFICOS

21) Durante um seminário sobre Arquitetura de Computadores, um professor está explicando os conceitos de concorrência, paralelismo e computação distribuída. Ele destaca como esses conceitos são aplicados em diferentes contextos e a importância de cada um na melhoria do desempenho dos sistemas computacionais. Qual das seguintes opções descreve **CORRETAMENTE** a diferença entre concorrência, paralelismo e computação distribuída?

A) Concorrência é a execução simultânea de múltiplas tarefas em diferentes sistemas, paralelismo envolve a execução sequencial de tarefas em múltiplos processadores, e computação distribuída se refere à execução de tarefas por um único sistema com múltiplos núcleos.
B) Concorrência e paralelismo são sinônimos e ambos se referem à execução de múltiplas tarefas ao mesmo tempo em diferentes processadores, enquanto computação distribuída se refere a múltiplos sistemas compartilhando a mesma memória.
C) Concorrência é a execução de tarefas de forma sequencial em um único processador, paralelismo se refere à execução de múltiplas tarefas em um único processador, e computação distribuída envolve múltiplos sistemas independentes sem comunicação entre eles.
D) Concorrência é a capacidade de um sistema realizar múltiplas tarefas ao mesmo tempo em múltiplos processadores, paralelismo é a execução de uma única tarefa por vários processadores ao mesmo tempo, e computação distribuída é a utilização de um único processador para executar todas as tarefas.
E) Concorrência se refere à execução simultânea de múltiplas tarefas em um único processador, paralelismo envolve múltiplos processadores executando diferentes partes de uma tarefa, e computação distribuída é a divisão de tarefas entre múltiplos sistemas independentes.

Justificativa
A alternativa E é correta pois Concorrência se refere à capacidade de um sistema de lidar com múltiplas tarefas ao mesmo tempo, frequentemente em um único processador, através do agendamento inteligente das tarefas. Paralelismo, por outro lado, envolve a utilização de múltiplos processadores para executar diferentes partes de uma tarefa simultaneamente, o que pode aumentar significativamente a eficiência e o desempenho. A computação distribuída envolve a divisão de tarefas entre múltiplos sistemas independentes que se comunicam através de uma rede, permitindo que grandes problemas sejam resolvidos através da colaboração de múltiplas máquinas.
A alternativa A é incorreta, pois Concorrência ocorre em um único processador ou sistema, não em diferentes sistemas. Paralelismo envolve a execução simultânea, não sequencial, de tarefas. A definição de computação distribuída está incorreta; ela envolve múltiplos sistemas independentes.
A alternativa B é incorreta, pois Concorrência e paralelismo não são sinônimos; eles referem-se a diferentes técnicas de execução de tarefas. Além disso, na computação distribuída, os sistemas independentes não compartilham a mesma memória.
A alternativa C é incorreta, pois Concorrência não envolve execução sequencial, e paralelismo não ocorre em um único processador. Na computação distribuída, os sistemas independentes se comunicam entre si.
A alternativa D é incorreta, pois Concorrência normalmente ocorre em um único processador, e a definição de computação distribuída está incorreta. A computação distribuída envolve múltiplos sistemas independentes, não um único processador.

Referência
SILVA, L.R.M. **Organização e Arquitetura de Computadores**: uma jornada do fundamental ao inovador. Freitas Bastos, 1ª. Ed., 2024. ISBN:6556753580.
STALLINGS, W. **Arquitetura e Organização de Computadores**. Pearson Universidades, 10ª. Ed., 2017. ISBN: 8543020530.
TANENBAUM, A. S. **Organização de Computadores**. Pearson Universidades, 6ª. Ed., 2013. ISBN: 8581435394.

Nível	Superior
Disciplina	Arquitetura de Computadores
Eixo Temático	Conceitos Básicos
Tema	Técnicas de Execução de Tarefas
Tópico do Conteúdo	Concorrência, Paralelismo e Computação Distribuída

22) Uma empresa de tecnologia está migrando sua arquitetura monolítica para microserviços, utilizando Kubernetes para orquestração e gerenciamento de contêineres. Durante uma sessão de treinamento, o engenheiro de DevOps explica como Kubernetes facilita o gerenciamento, a escalabilidade e a resiliência dos microserviços através de

suas funcionalidades de gerenciamento de contêineres. Qual das seguintes opções descreve **CORRETAMENTE** um benefício do uso de Kubernetes para o gerenciamento de microserviços?

A) Kubernetes permite a execução de múltiplas instâncias de um microserviço em diferentes nós, facilitando a escalabilidade horizontal.
B) Kubernetes compila automaticamente o código-fonte dos microserviços e cria imagens de contêiner no cluster.
C) Kubernetes elimina a necessidade de registros de contêiner, armazenando todas as imagens localmente em cada nó.
D) Kubernetes gerencia microserviços executando scripts diretamente nos nós, sem a necessidade de contêineres.
E) Kubernetes utiliza servidores físicos dedicados para cada microserviço, garantindo isolamento completo e desempenho otimizado.

Justificativa
A alternativa A é correta pois Kubernetes facilita a escalabilidade horizontal ao permitir que múltiplas instâncias (pods) de um microserviço sejam executadas em diferentes nós dentro do cluster. Isso melhora a capacidade de resposta e a disponibilidade dos serviços, pois a carga de trabalho pode ser distribuída eficientemente entre os nós do cluster.
A alternativa B é incorreta pois Kubernetes não compila código-fonte nem cria imagens de contêiner automaticamente. A criação de imagens é um processo separado que deve ser realizado antes do deployment no Kubernetes.
A alternativa C é incorreta pois Kubernetes utiliza registros de contêiner para armazenar e puxar imagens conforme necessário. Armazenar todas as imagens localmente em cada nó não é prático e não é uma funcionalidade do Kubernetes.
A alternativa D é incorreta pois Kubernetes gerencia a execução de contêineres, não de scripts diretamente nos nós. A utilização de contêineres é fundamental para a portabilidade e isolamento dos microserviços.
A alternativa E é incorreta pois Kubernetes utiliza um cluster de nós (que podem ser servidores físicos ou virtuais) para executar contêineres. Não é necessário dedicar servidores físicos inteiros a cada microserviço, pois o isolamento é garantido através da virtualização de contêineres.

Referência
BURNS, B., BEDA, J., HIGHTOWER, K. **Kubernetes Básico**. Novatec, 2020. ISBN: 9788575228241.
IBRAYAM, B., HUB, R. **Padrões Kubernetes**. Novatec, 2019. ISBN: 9788575228142.
SANTANA, F.Z. **Back-end Java**: microsserviços, Spring Boot e Kubernetes. Casa do Código, 2021. Ebook.

Nível	Superior
Disciplina	Engenharia de Software
Eixo Temático	Qualidade de Software
Tema	Métricas de Software
Tópico do Conteúdo	Pontos por Função

---

23) Considerando os fundamentos do ITIL (Information Technology Infrastructure Library), correlacione os processos do ITIL na coluna da esquerda com suas respectivas descrições na coluna da direita.

1) Gerenciamento de Incidentes.
2) Gerenciamento de Problemas.
3) Gerenciamento de Mudanças.
4) Gerenciamento de Liberação e Implantação.
5) Gerenciamento de Configuração e Ativos de Serviço.

( ) A) Processo responsável por identificar e resolver a causa raiz de incidentes recorrentes.
( ) B) Processo que controla o ciclo de vida das mudanças, minimizando interrupções nos serviços.
( ) C) Processo que restaura a operação normal do serviço o mais rápido possível após uma interrupção.
( ) D) Processo responsável pela entrega e implantação de novos serviços ou alterações nos serviços existentes.
( ) E) Processo que mantém informações precisas sobre os ativos de TI e suas relações.

A sequência **CORRETA**, de cima para baixo, dessa associação é:

A) 1 – D; 2 – E; 3 – C; 4 – A; 5 – B.
B) 1 – E; 2 – B; 3 – D; 4 – A; 5 – C.
C) 1 – C; 2 – A; 3 – B; 4 – D; 5 – E.
D) 1 – B; 2 – D; 3 – E; 4 – C; 5 – A.
E) 1 – E; 2 – A; 3 – C; 4 – B; 5 – D.

Justificativa
A alternativa correta é a C, pois:
- O gerenciamento de incidentes é focado em restaurar a operação normal do serviço o mais rápido possível após uma interrupção, minimizando o impacto negativo nos negócios.
- O gerenciamento de problemas busca identificar e resolver a causa raiz de incidentes recorrentes, prevenindo que ocorram novamente.
- O gerenciamento de mudanças controla o ciclo de vida das mudanças, assegurando que as alterações nos serviços de TI sejam feitas de maneira controlada e minimizando interrupções nos serviços.
- O gerenciamento de liberação e implantação é responsável pela entrega e implantação de novos serviços ou alterações nos serviços existentes, garantindo que tudo seja feito de acordo com os requisitos definidos.
- O gerenciamento de configuração de ativos de serviço mantém informações precisas sobre os ativos de TI e suas relações, assegurando que os dados de configuração estejam atualizados e disponíveis.

As demais alternativas não fazem as associações corretas.
Referência
FREITAS, M.A.S. **Fundamentos do Gerenciamento de Serviços de TI.** Brasport, 2ª. Ed., 2013. ISBN: 857452871.
LYRA, M.R. **Gerenciamento de serviços de TI com ITIL**: conhecendo o framework. Ed. do autor, 1ª Ed., 2020. Ebook.
MELO, J.L., OLIVEIRA, A.V., MAUSER, D. **Guia preparatório para a certificação ITIL 4 Foundation**. SF Editorial, 2022. ISBN: 6586399475.

Nível	Superior
Disciplina	Gerenciamento de Serviços de TI
Eixo Temático	Conceitos Básicos
Tema	ITIL - Information Technology Infrastructure Library
Tópico do Conteúdo	Processos de Gerenciamento do ITIL

---

24) A Resolução Normativa ANEEL Nº 964/2021, publicada em 14 de dezembro de 2021, dispõe sobre a implementação de políticas de segurança cibernética no setor de energia elétrica brasileiro. Considerando o contexto da Resolução, qual das alternativas a seguir **NÃO** está relacionada aos seus objetivos?

A) Promover a adoção de medidas de proteção contra-ataques cibernéticos, como criptografia de dados e controle de acesso.
B) Estabelecer diretrizes para a gestão de riscos cibernéticos pelos agentes do setor elétrico.
C) Estimular o investimento em pesquisa, desenvolvimento e inovação em segurança cibernética no setor elétrico.
D) Assegurar a continuidade dos serviços essenciais de energia elétrica em caso de incidentes cibernéticos.
E) Definir obrigações de notificação de incidentes cibernéticos às autoridades competentes.

Justiticativa
A alternativa C é a correta. Embora a Resolução Normativa ANEEL Nº 964/2021 reconheça a importância da pesquisa, desenvolvimento e inovação (PD&I) em segurança cibernética, seu foco principal está em estabelecer **obrigações e diretrizes** para que os agentes do setor elétrico implementem medidas de proteção contra-ataques cibernéticos. A Resolução **não define mecanismos específicos** para estimular o investimento em PD&I, cabendo às empresas do setor buscarem soluções inovadoras para aprimorar sua segurança cibernética.
A alternativa A é incorreta. A Resolução determina a adoção de medidas de proteção contra-ataques cibernéticos, como criptografia de dados, controle de acesso, segmentação de redes e testes de vulnerabilidade.
A alternativa B é incorreta. A Resolução estabelece diretrizes para a gestão de riscos cibernéticos, definindo metodologias para identificar, avaliar e tratar os riscos cibernéticos a que os agentes do setor estão expostos.
A alternativa D é incorreta. A Resolução visa assegurar a continuidade dos serviços essenciais de energia elétrica em caso de incidentes cibernéticos, exigindo dos agentes a implementação de planos de resposta a incidentes e medidas de recuperação de sistemas.
A alternativa E é incorreta. A Resolução define obrigações de notificação de incidentes cibernéticos às autoridades competentes, estabelecendo prazos e procedimentos para a comunicação de eventos de segurança.

Referência
Resolução Normativa ANEEL Nº 964/2021, encontra-se disponível em: https://www2.aneel.gov.br/cedoc/ren2021964.html

Nível	Superior
Disciplina	Compliance
Eixo Temático	Segurança Cibernética
Tema	Resoluções
Tópico do Conteúdo	Resolução Normativa ANEEL Nº 964/2021

---

25) Um usuário precisa enviar um e-mail confidencial contendo informações sigilosas para um destinatário. Qual tipo de criptografia ele deve utilizar para garantir a confidencialidade da mensagem?

A) Nenhum tipo de criptografia, pois o e-mail não é um meio seguro para enviar informações confidenciais.
B) Criptografia simétrica, utilizando a mesma chave para criptografar e descriptografar a mensagem.
C) Criptografia simétrica, utilizando uma chave diferente para criptografar e descriptografar a mensagem.
D) Assinatura digital, utilizando uma chave privada para assinar a mensagem e uma chave pública para verificar a assinatura.
E) Criptografia assimétrica, utilizando uma chave pública para criptografar a mensagem e uma chave privada para descriptografá-la.

Justificativa
A alternativa E é correta. A criptografia assimétrica é ideal para enviar mensagens confidenciais por e-mail, pois garante que apenas o destinatário pretendido possa ler a mensagem. Isso porque a chave pública, utilizada para criptografar a mensagem, é de conhecimento público e pode ser distribuída livremente. Já a chave privada, utilizada para descriptografar a mensagem, é mantida em segredo pelo destinatário e só ele tem acesso a ela.
A alternativa A é incorreta. O e-mail pode ser um meio seguro para enviar informações confidenciais, desde que sejam tomadas as medidas adequadas de segurança, como a utilização de criptografia assimétrica e assinatura digital.A alternativa B é incorreta. A criptografia simétrica exige que o remetente e o destinatário compartilhem a mesma chave secreta, o que pode ser um problema em termos de segurança, pois a chave pode ser interceptada durante a troca.
A alternativa C é incorreta. A utilização de chaves diferentes para criptografar e descriptografar a mensagem não garante a segurança da comunicação, pois o remetente precisa enviar a chave de descriptografia para o destinatário, o que a torna vulnerável a interceptação.
A alternativa D é incorreta. A assinatura digital garante a autenticidade da mensagem e impede que ela seja repudiada pelo remetente, mas não criptografa o conteúdo da mensagem, o que significa que qualquer pessoa que tiver acesso ao e-mail poderá ler o conteúdo.

Referência
STALLINGS, W. **Criptografia e Segurança de Redes**: princípios e práticas. Pearson Universidades, 6ª. Ed., 2014. ISBN: 8543005898.
WYKES, S. **Criptografia Essencial**: a jornada do criptógrafo. GEN LTC, 1ª Ed., 2016. ISBN: 8535286055.
ZOCHIO, M.F. **Introdução a Criptografia**. Novatec Editora, 1ª. Ed., 2016. ISBN: 8575225154.

Nível	Superior
Disciplina	Segurança da Informação
Eixo Temático	Criptografia
Tema	Conceitos Básicos
Tópico do Conteúdo	Criptografia Simétrica e Assimétrica

---

26) Uma empresa está considerando migrar seus sistemas e dados para a nuvem pública. Qual dos seguintes modelos de arquitetura de serviços de nuvem pública é mais adequado para atender às suas necessidades de escalabilidade, flexibilidade e segurança?

A) Modelo de Infraestrutura como Serviço (IaaS).
B) Modelo de Software como Serviço (SaaS).
C) Modelo de Plataforma como Serviço (PaaS).
D) Modelo Híbrido de Nuvem.
E) Modelo de Computação em Borda.

Justificativa
A alternativa D está correta, pois o modelo Híbrido de Nuvem combina os benefícios de diferentes modelos de arquitetura de serviços de nuvem pública, como SaaS, PaaS e IaaS, permitindo que a empresa escolha o ambiente ideal para cada tipo de aplicativo ou dado. Isso oferece maior flexibilidade, escalabilidade e segurança para atender às necessidades específicas da empresa.
A alternativa A está incorreta, pois o modelo IaaS oferece à empresa controle total sobre a infraestrutura de nuvem, mas exige expertise técnica e recursos para gerenciar e manter os sistemas.
A alternativa B está incorreta, pois o modelo SaaS oferece apenas a utilização de softwares pré-configurados e gerenciados pelo provedor de nuvem, o que pode limitar a flexibilidade e o controle da empresa sobre seus sistemas.
A alternativa C está incorreta, pois o modelo PaaS fornece uma plataforma para desenvolvimento e execução de aplicativos, mas a empresa ainda precisa gerenciar a infraestrutura subjacente, o que pode ser complexo e custoso.
A alternativa E está incorreta, pois o modelo de Computação em Borda processa dados e executa aplicativos mais próximos dos dispositivos finais, o que pode ser ideal para aplicações com baixa latência, mas não se aplica à migração completa de sistemas e dados para a nuvem pública.

Referência
SANTOS, T. **Fundamentos da Computação em Nuvem**. Editora Senac São Paulo, 1ª. Ed., 2018.
VERAS, M. **Arquitetura de Nuvem**. Brasport, 1ª. Ed., 2013. ISBN: 8574525685.
VERAS, M., DIOGENES, Y. **Computação em nuvem**. Brasport, 1ª. Ed., 2015. ISBN: 8574527475.

Nível	Superior
Disciplina	Computação em Nuvem
Eixo Temático	Arquitetura em Nuvem
Tema	Arquitetura de Serviços
Tópico do Conteúdo	Arquitetura de serviços em nuvem pública

---

27) Uma empresa está buscando implementar um sistema de controle de acesso robusto para sua rede corporativa. Qual protocolo entre AAA (Autenticação, Autorização e Contabilidade), IEEE 802.1X, RADIUS e TACACS é mais adequado para atender às suas necessidades de segurança e gerenciamento centralizado?

A) AAA (Autenticação, Autorização e Contabilidade) - Um modelo conceitual que define os componentes básicos do controle de acesso, mas não um protocolo específico.
B) Combinação de IEEE 802.1X para autenticação inicial e RADIUS para autenticação e autorização adicionais - Uma solução abrangente que combina os pontos fortes de ambos os protocolos.
C) IEEE 802.1X - Um protocolo padrão para autenticação de dispositivos em redes LAN baseadas em Ethernet, mas focado apenas na autenticação e não em autorização ou contabilidade.
D) RADIUS (Remote Authentication Dial-In User Service) - Um protocolo centralizado para autenticação e autorização de usuários em redes, mas com recursos de contabilidade limitados.
E) TACACS+ (Terminal Access Controllers Access Control System Plus) - Um protocolo proprietário da Cisco para autenticação, autorização e contabilidade de usuários em redes, mas com menor interoperabilidade em comparação ao RADIUS.

Justificativa
Alternativa B, correta. A combinação de IEEE 802.1X e RADIUS oferece uma solução de controle de acesso abrangente e robusta para redes corporativas, aproveitando os pontos fortes de cada protocolo:

- **IEEE 802.1X:**
  - Autenticação forte e segura de dispositivos na camada de acesso à rede, utilizando mecanismos como EAP (Extensible Authentication Protocol) e cartões inteligentes.
  - Proteção contra-ataques "man-in-the-middle" e falsificação de endereços MAC.
- **RADIUS:**
  - Autenticação e autorização centralizadas de usuários em diversos sistemas e serviços de rede.
  - Suporte a políticas de acesso granulares com base em atributos e funções dos usuários.
  - Registro de auditoria detalhado para investigação de incidentes de segurança.

Alternativa B, incorreta. AAA (Autenticação, Autorização e Contabilidade) é um modelo conceitual que define os componentes básicos do controle de acesso, mas não um protocolo específico.
Alternativa C, incorreta. O IEEE 802.1X é focado apenas na autenticação de dispositivos na camada de acesso à rede, não fornecendo recursos de autorização ou contabilidade.

Alternativa D, incorreta. O RADIUS oferece autenticação e autorização centralizadas, mas seus recursos de contabilidade são limitados em comparação ao TACACS+.
Alternativa E, incorreta. O TACACS+ fornece autenticação, autorização e contabilidade abrangentes, mas é um protocolo proprietário da Cisco com menor interoperabilidade em comparação ao RADIUS.

Referência
ROHLING, L.J. **Segurança de Redes de Computadores**. Ed. Contentus, 2018. ISBN: 9786559350629.
SOUSA, L.B. **Gerenciamento e Segurança de Redes**. SENAI – SP Editora, 2017. ISBN: 9788583938668.
TANENBAUM, A., FEAMSTER, N., WETHERRALL, D. **Redes de Computadores**. Bookmann, 2021. ISBN: 9788582605608.

Nível	Superior
Disciplina	Rede de Computadores
Eixo Temático	Segurança em Redes
Tema	Protocolos
Tópico do Conteúdo	Protocolos de Autenticação

---

28) Uma empresa está modernizando sua infraestrutura de TI e implementando um sistema de AAA para consolidar seus dados corporativos. A equipe de infraestrutura está aprendendo sobre os conceitos de Data Warehouse, OLAP (Online Analytical Processing) e Data Mining para melhor entender como essas tecnologias podem ajudar na análise de dados e na tomada de decisões estratégicas.

Qual das seguintes alternativas descreve **CORRETAMENTE** a principal função de um Data Warehouse, OLAP e Data Mining no contexto de análise de dados corporativos?

A) Um Data Warehouse armazena dados históricos, OLAP realiza análise multidimensional dos dados e Data Mining descobre padrões ocultos nos dados.
B) Um Data Warehouse realiza análise multidimensional dos dados, OLAP armazena dados históricos e Data Mining gerencia transações diárias.
C) Um Data Warehouse gerencia transações diárias, OLAP descobre padrões ocultos nos dados e Data Mining armazena dados históricos.
D) Um Data Warehouse descobre padrões ocultos nos dados, OLAP gerencia transações diárias e Data Mining realiza análise multidimensional dos dados.
E) Um Data Warehouse realiza a análise de dados em tempo real, OLAP armazena dados em formato bruto e Data Mining organiza dados para relatórios operacionais.

Justificativa
Alternativa A, correta. Ela apresenta as funções corretas para Data Warehouse, OLAP e Data Mining.
Alternativa B, incorreta, pois apresenta uma inversão das funções. Data Warehouse armazena dados históricos, OLAP realiza análises multidimensionais e Data Mining descobre padrões, não gerencia transações diárias.
Alternativa C, incorreta, pois Data Warehouse não gerencia transações diárias, que é uma função dos sistemas de processamento transacional (OLTP). OLAP realiza análise multidimensional e Data Mining descobre padrões ocultos, não armazena dados históricos.
Alternativa D, incorreta, pois as funções estão incorretamente atribuídas. Data Warehouse armazena dados históricos, OLAP realiza análise multidimensional e Data Mining descobre padrões ocultos.
Alternativa E, incorreta, pois Data Warehouse armazena dados históricos e não realiza análise em tempo real. OLAP realiza análise multidimensional, não armazena dados em formato bruto, e Data Mining descobre padrões ocultos, não organiza dados para relatórios operacionais.

Referência
GOLDSCHMIDT, R. **Data Mining**: conceitos, técnicas, algoritmos, orientações e aplicações. GEN LTC, 2ª. Ed, 2015. ISBN: 8535278222.
MACHADO, F.N.R. **Tecnologia e projeto de Data Warehouse**. Editora Érica, 6ª. Ed, 2013. ISBN: 8536500123.
SOUZA, A.; SOTTO, E.C.S., ARAUJO, L.S., FERNANDES, P.L.B., CARDOSO, T.A.,
THOMSEN, E. **OLAP**. Elsevier, 2ª Ed, 2002. ISBN: 8535211284.

Nível	Superior
Disciplina	Business Intelligence
Eixo Temático	Infraestrutura de Business Intelligence
Tema	Conceitos Básicos

Tópico do Conteúdo	Data Warehouse, Data Mining, OLAP

29) A equipe de infraestrutura de uma empresa está avaliando a implementação de sistemas de detecção e prevenção de intrusão (IDPS - Intrusion Detection and Prevention Systems) para melhorar a segurança da rede. Durante uma sessão de treinamento, o gerente de segurança explica as diferenças entre IDS (Intrusion Detection System) e IPS (Intrusion Prevention System) e a importância de cada um no ambiente corporativo.

Qual das seguintes alternativas descreve **CORRETAMENTE** a principal diferença entre um Sistema de Detecção de Intrusão (IDS) e um Sistema de Prevenção de Intrusão (IPS)?

A) Um IDS é usado exclusivamente para detectar malware, enquanto um IPS é usado para prevenir ataques de negação de serviço.
B) Um IDS bloqueia ataques em tempo real, enquanto um IPS apenas monitora e gera alertas.
C) Um IDS é integrado diretamente aos firewalls, enquanto um IPS funciona de forma independente.
D) Um IDS monitora a rede e gera alertas sobre atividades suspeitas, enquanto um IPS pode bloquear ativamente essas atividades.
E) Um IDS precisa ser configurado manualmente para cada tipo de ataque, enquanto um IPS detecta e previne ataques automaticamente sem configuração prévia.

Justificativa
Alternativa D, correta, pois: IDS (Intrusion Detection System) monitora o tráfego de rede e sistemas em busca de atividades suspeitas ou maliciosas e gera alertas quando detecta tais atividades e não interfere diretamente no tráfego de rede. Já o IPS (Intrusion Prevention System), além de monitorar e detectar atividades suspeitas, possui a capacidade de bloquear ou prevenir ativamente essas atividades, tomando ações como bloquear pacotes de dados maliciosos.
Alternativa A, incorreta pois IDS e IPS não são usados exclusivamente para essas funções específicas. Ambos podem detectar e prevenir uma variedade de ameaças, incluindo malware e ataques de negação de serviço.
Alternativa B, incorreta. A descrição está incorreta. É o IPS que bloqueia ataques em tempo real, enquanto o IDS apenas monitora e gera alertas.
Alternativa C, incorreta pois tanto IDS quanto IPS podem ser integrados com firewalls ou funcionar de forma independente. A principal diferença não está na integração com firewalls, mas na capacidade de bloqueio.
Alternativa E, incorreta, pois tanto IDS quanto IPS requerem configuração para detectar ataques específicos. Nenhum deles funciona sem configuração prévia, e ambos podem usar assinaturas e heurísticas para detectar ameaças.

Referência
AVILA, D., KONAGALA, P. **Abordagens de Detecção de Intrusão Baseadas em Modelos para Segurança em MANETS**. Edições Nosso Conhecimento, 2024. ISBN: 6207183606.
FERREIRA, E. **Sistema de Detecção de Intrusão**: uma proposta baseada em transformadas wavelets e redes neurais artificiais. Novas Edições Acadêmicas, 2015. ISBN: 97838417001570.
MORAES, A.F. **Segurança em redes**: fundamentos. Ed. Érica, 2010. ISBN: 8536503254

Nível	Superior
Disciplina	Rede de Computadores
Eixo Temático	Segurança em Redes
Tema	Detecção e Prevenção de intrusão
Tópico do Conteúdo	Sistemas de detecção e prevenção de intrusão

30) A equipe de infraestrutura de uma empresa de pesquisa científica precisa processar grandes volumes de dados para realizar simulações complexas. Qual tipo de arquitetura de computação é mais adequado para atender às suas necessidades: computação em cluster ou computação em grid?

A) Computação em grid: arquitetura que distribui tarefas de processamento em uma rede descentralizada de computadores, geralmente geograficamente dispersos, ideal para tarefas que exigem alto desempenho e baixo custo.
B) Computação em cluster: arquitetura que reúne vários computadores próximos para compartilhar recursos e processar tarefas em paralelo, ideal para tarefas que exigem alta disponibilidade e baixa latência.
C) As duas arquiteturas são igualmente adequadas para qualquer tipo de tarefa de processamento.
D) A escolha entre computação em cluster e computação em grid depende apenas do orçamento da empresa.
E) A escolha entre computação em cluster e computação em grid depende apenas da quantidade de dados a serem processados.

Justificativa
Alternativa A, correta. A computação em grid é a arquitetura mais adequada para atender às necessidades da equipe de pesquisa científica por diversos motivos: (i) **Processamento de grandes volumes de dados:** pois permite distribuir o processamento de grandes volumes de dados em diversos computadores, o que aumenta significativamente a capacidade de processamento e a velocidade de execução das tarefas; (ii) **Baixo custo:** pois pode utilizar recursos computacionais ociosos de computadores existentes na empresa ou em outras instituições, o que reduz os custos de infraestrutura; (iii) **Flexibilidade:** pois permite adicionar ou remover computadores da rede dinamicamente, de acordo com as necessidades de processamento; (iv) e. **Tolerância a falhas:** pois se um dos computadores da rede falhar, a tarefa pode ser redirecionada para outro computador, garantindo a continuidade do processamento.
Alternativa B, incorreta, pois a computação em cluster é mais adequada para tarefas que exigem alta disponibilidade e baixa latência, como aplicações web ou bancos de dados.
Alternativa C, incorreta pois a escolha entre computação em cluster e computação em grid depende das características da tarefa e dos recursos disponíveis.
Alternativa D, incorreta pois o orçamento da empresa é apenas um dos fatores a serem considerados na escolha da arquitetura de computação.
Alternativa E, incorreta, pois a quantidade de dados a serem processados é apenas um dos fatores a serem considerados na escolha da arquitetura de computação.

Referência
CHEDE, C.T. **Grid Computing**: um novo paradigma computacional. Brasport, 2004. ISBN: 9788574521930.
DANTAS, M. **Computação Distribuída de Alto Desempenho**: redes, clusters e grids computacionais. Axcel Editora, 2015.
PITANGA, M. **Computação em Cluster**: o estado da arte da computação. Brasport, 2003. ISBN: 9788574521565.

Nível	Superior
Disciplina	Computação de alto desempenho
Eixo Temático	Computação em nuvem
Tema	Conceitos Básicos
Tópico do Conteúdo	Computação em Cluster e Computação em grids.

---

31) Uma empresa de tecnologia está implementando uma nova política de segurança da informação para proteger seus ativos digitais e garantir a conformidade com regulamentos de privacidade de dados. Uma das medidas adotadas é a realização de avaliações periódicas de risco. Qual das alternativas abaixo descreve a principal finalidade dessas avaliações de risco?

A) Criação de uma política de segurança da informação que defina os princípios, responsabilidades e procedimentos para a proteção da informação.
B) Aquisição de ferramentas de segurança de última geração, como firewalls, antivírus e sistemas de detecção de intrusão.
C) Contratação de especialistas em segurança da informação para realizar avaliações de risco e implementar medidas de controle.
D) Treinamento dos funcionários para conscientizá-los sobre os riscos de segurança da informação e as boas práticas de segurança.
E) Implementação de um sistema de gestão da segurança da informação (SGSI) baseado em um padrão internacional, como ISO 27001.

Justificativa
Alternativa A, correta. A criação de uma política de segurança da informação é a base fundamental para um programa de sucesso, pois define os princípios, responsabilidades e procedimentos para a proteção da informação da empresa. A política deve ser: (i) abrangente e abordar todos os aspectos da segurança da informação, desde a confidencialidade e integridade dos dados até o controle de acesso e a recuperação de desastres; (ii) clara e concisa, escrita em linguagem simples e fácil de entender por todos os funcionários; (iii) comunicada e implementada, sendo divulgada para todos os funcionários e integrada em todos os processos da empresa; e (iv) revisada e atualizada periodicamente, para garantir que esteja sempre alinhada com as necessidades da empresa e os riscos de segurança da informação.
Alternativa B, incorreta, pois as ferramentas de segurança são importantes, mas não podem substituir uma política de segurança da informação bem definida.
Alternativa C, incorreta pois os especialistas em segurança da informação podem auxiliar na implementação do programa, mas a política deve ser definida pela empresa.
Alternativa D, incorreta pois o treinamento é essencial, mas precisa ser baseado em uma política de segurança da informação bem definida.

Alternativa E, incorreta, pois a implementação de um SGSI (Sistema de Gerenciamento da Segurança da Informação) é um passo importante, mas a política de segurança da informação é a base fundamental.

Referência

CABRAL, C., OKUHARA, C. **Trilha em Segurança da Informação**: caminhos e ideias para proteção de dados. Brasport, 2015. Ebook.
FONTES, E.L.G. **Segurança da Informação**. Editora Saraiva, 2017. ISBN: 9788502122192.
MANOEL, S. S. **Governança de Segurança da Informação**: como criar oportunidades para o seu negócio. Brasport, 2014. Ebook.

Nível	Superior
Disciplina	Segurança da Informação
Eixo Temático	Gestão de Governança da Segurança da Informação
Tema	Conceitos Básicos
Tópico do Conteúdo	Políticas de Segurança da Informação

---

32) Um desenvolvedor está trabalhando em um banco de dados Oracle e precisa criar um procedimento armazenado em PL/SQL que insira um novo registro na tabela **EMPREGADOS**. O procedimento deve aceitar os parâmetros **emp_id, emp_nome** e **emp_salario** e realizar a inserção. Qual das alternativas abaixo mostra **CORRETAMENTE** como esse procedimento pode ser escrito?

A)
```
CREATE PROCEDURE add_empregados(emp_id NUMBER, emp_nome VARCHAR2, emp_salario NUMBER)
AS
BEGIN
   INSERT INTO EMPREGADOS (emp_id, emp_nome, emp_salario);
END;
```

B)
```
CREATE PROCEDURE add_empregados(emp_id NUMBER, emp_nome VARCHAR2, emp_salario NUMBER)
IS
BEGIN
   INSERT INTO EMPREGADOS (ID, NOME, SALARIO) VALUES (emp_id, emp_nome, emp_salario);
END;
```

C)
```
CREATE PROCEDURE add_empregados(emp_id NUMBER, emp_nome VARCHAR2, emp_salario NUMBER)
BEGIN
   INSERT INTO EMPREGADOS (ID, NOME, SALARIO) VALUES (emp_id, emp_nome, emp_salario);
END add_empregados;
```

D)
```
CREATE PROCEDURE add_empregados(emp_id IN NUMBER, emp_nome IN VARCHAR2, emp_salario IN NUMBER)
IN
BEGIN
   INSERT INTO EMPREGADOS (ID, NOME, SALARIO) VALUES (emp_id, emp_nome, emp_salario);
END;
```

E)
```
CREATE PROCEDURE add_empregados(emp_id IN NUMBER, emp_nome IN VARCHAR2, emp_salario IN NUMBER)
AS
BEGIN
   INSERT INTO EMPREGADOS (ID, NOME, SALARIO) VALUES (emp_id, emp_nome, emp_salario);
END;
```

Justificativa

Alternativa E, correta, pois define o procedimento corretamente usando **AS** (ou **IS**, ambos são válidos) e especifica os modos dos parâmetros (**IN**), que é a sintaxe correta para procedimentos armazenados em PL/SQL. A instrução **INSERT INTO** também está corretamente formulada com a lista de colunas e os valores.

Alternativa A, incorreta, já que contém um erro na instrução **INSERT INTO**, pois a lista de colunas está ausente. O correto é especificar as colunas (**ID, NOME, SALARIO**) antes dos valores.
Alternativa B, incorreta, pois não especifica os modos dos parâmetros (**IN**), o que é uma prática recomendada para clareza e para evitar ambiguidades.
Alternativa C, incorreta, pois além de não especificar os modos dos parâmetros, essa alternativa usa uma sintaxe incorreta ao adicionar **add_empregados** após o **END**, o que não é permitido em PL/SQL.
Alternativa D, incorreta, pois não usa a palavra-chave **AS**, que é usada para definir procedimentos e pacotes em PL/SQL, e utiliza **IN** que não é uma palavra-chave em PL/SQL.

Referência
GONÇALVES, E. **PL/SQL – Domine a linguagem de banco de dados Oracle**. Casa do Còdigo, 2015. ISBN: 8555190738.
MC LAUGHKUN, M. **Oracle Database 12c PL/SQL Programming**. Mc Graw Hill, 2014. ISBN: 0071812431.
PRICE, J. **Oracle Database 11G SQL. Domine SQL e PL/SQL no banco de dados Oracle**. Bookman, 2008. ISBN: 857780335X.

Nível	Superior
Disciplina	Sistemas de Gerenciamento de Banco de Dados
Eixo Temático	Linguagens
Tema	PL/SQL
Tópico do Conteúdo	Comandos Básicos

---

33) Um programador está escrevendo um script Perl para ler um arquivo de texto chamado "dados.txt" e contar quantas vezes a palavra "Perl" aparece no arquivo. Qual das alternativas abaixo mostra **CORRETAMENTE** como esse script pode ser escrito?

A)
```
open(FILE, "<dados.txt") or die "Não foi possível abrir o arquivo.";
my $count = 0;
while (<FILE>) {
    $count += tr/Perl/Perl/;
}
close(FILE);
print "A palavra 'Perl' aparece $count vezes.\n";
```

B)
```
open(FILE, "dados.txt") or die "Não foi possível abrir o arquivo.";
my $count = 0;
while (<FILE>) {
    #count++ while /Perl/g;
}
close(FILE);
print "A palavra 'Perl' aparece $count vezes.\n";
```

C)
```
open(FILE, "<dados.txt") or die "Não foi possível abrir o arquivo.";
my $count = 0;
while (my $line = <FILE>) {
    $count++ if $line =~ /Perl/;
}
close(FILE);
print "A palavra 'Perl' aparece $count vezes.\n";
```

D)
```
open(FILE, "dados.txt") or die "Não foi possível abrir o arquivo.";
my $count = 0;
while (<FILE>) {
    $count += () = /Perl/g;
}
close(FILE);
print "A palavra 'Perl' aparece $count vezes.\n";
```

E)
```
open(FILE, "<dados.txt") or die "Não foi possível abrir o arquivo.";
my $count = 0;
```

```
while (<FILE>) {
   else ($_ =~ /Perl/g) {
      $count++;
   }
}
close(FILE);
print "A palavra 'Perl' aparece $count vezes.\n";
```

Justificativa

Alternativa D, correta, pois utiliza a expressão regular **/Perl/g** juntamente com a atribuição a um **array vazio () =**, que permite contar todas as ocorrências da palavra "Perl" em cada linha do arquivo. Esse método é eficiente e conciso para obter a contagem total das ocorrências.

Alternativa A, incorreta, pois usa **tr///**, que é para contar caracteres específicos, não palavras. Por isso, não funcionaria corretamente para contar a palavra "Perl".

Alternativa B, incorreta, pois a forma de incrementar é **$count** e não **#count**.

Alternativa C, incorreta, pois conta apenas uma ocorrência da palavra "Perl" por linha, o que está incorreto. Ela não conta múltiplas ocorrências dentro da mesma linha.

Alternativa E, incorreta, pois a estrutura de **while – else** não existe. O correto seria **while – while**. Ou seja, uma estrutura de while aninhado:

```
while (<FILE>) {
   else ($_ =~ /Perl/g) {
      $count++;
   }
}
```

Referência

ASTHAMA, A. **Perl & Shell Scripting Interview Questions**: another interview masterpiece. Independently Published, 2023.

SANCHEZ, T.G. **Programando com Perl**. Brassport, 1ª. Ed., 2012. ISBN: 8574524859.

SCHWARTZ, R., FOY, B., PHOENIX, T. **Learning Perl**: Making Easy Things Possible. O´Reilly Media, 8th ed., 2021. ISBN: 1492094951.

Nível	Superior
Disciplina	Desenvolvimento de Sistemas
Eixo Temático	Linguagem de Programação
Tema	Linguagem de Script
Tópico do Conteúdo	Perl

---

34) Em um cenário onde empresas estão migrando suas operações para a nuvem, a segurança se torna uma preocupação crítica. Duas abordagens emergentes para garantir a segurança em ambientes de nuvem são a Secure Access Service Edge (SASE) e o Zero Trust Network Access (ZTNA). A empresa X está avaliando a melhor maneira de proteger seus dados e acessos à nuvem, considerando as características de cada uma dessas arquiteturas.

A empresa X está preocupada com a segurança do acesso a seus serviços em nuvem e está avaliando a adoção de SASE e ZTNA. Qual das afirmações a seguir melhor descreve a principal diferença entre essas duas abordagens?

A) O SASE combina funcionalidades de rede e segurança em um único serviço entregue na nuvem, enquanto o ZTNA foca em garantir que cada acesso seja verificado individualmente, sem confiar em localização ou rede.
B) O ZTNA combina funcionalidades de rede e segurança em um único serviço entregue na nuvem, enquanto o SASE foca em garantir que cada acesso seja verificado individualmente, sem confiar em localização ou rede.
C) O SASE é um modelo de segurança focado apenas em acessos internos, enquanto o ZTNA é focado em acessos externos à rede corporativa.
D) O ZTNA é uma tecnologia desatualizada e não é mais usada nas arquiteturas de segurança modernas, ao contrário do SASE, que é amplamente adotado.
E) O SASE e o ZTNA são exatamente a mesma coisa, com apenas uma diferença terminológica.

Justificativa

Alternativa A, correta pois reflete precisamente a essência de cada abordagem. O SASE (Secure Access Service Edge) integra serviços de rede e segurança, fornecendo funcionalidades como firewall, segurança de acesso à internet e SD-WAN em uma solução baseada na nuvem. Já o ZTNA (Zero Trust Network Access) adota uma filosofia de "nunca confiar, sempre verificar", garantindo que cada tentativa de acesso seja autenticada e autorizada independentemente da localização do usuário ou do dispositivo.
Alternativa B, incorreta, pois inverte as definições. O ZTNA não combina funcionalidades de rede e segurança em um único serviço; essa é uma característica do SASE.
Alternativa C, incorreta pois o SASE não é focado apenas em acessos internos. Ele é uma solução abrangente que inclui tanto acesso interno quanto externo. O ZTNA, por sua vez, aplica o princípio de verificação contínua a qualquer tipo de acesso, seja interno ou externo.
Alternativa D, incorreta pois o ZTNA não é uma tecnologia desatualizada. Pelo contrário, é uma abordagem moderna e crescente na segurança de rede, assim como o SASE.
Alternativa E, incorreta, pois o SASE e o ZTNA não são a mesma coisa. Eles são complementares, mas distintos. O SASE é uma arquitetura que combina rede e segurança, enquanto o ZTNA é uma abordagem de segurança focada na verificação contínua de acessos.

Referência
VARELLA, W.A. **Arquitetura de Solução de Computação em Nuvem**. Editora SENAC São Paulo, 1ª. Ed., 2019. Ebook.
VERAS, M. **Arquitetura de Nuvem**. Brasport, 2013. ISBN: 9788574526041.
WATANABE, H. **Segurança de Serviços em Nuvem na Prática ISO 27017**. Clube dos Autores, 2024. ISBN: 9786500932409.

Nível	Superior
Disciplina	Computação em Nuvem
Eixo Temático	Arquitetura em Nuvem
Tema	Segurança de serviços em Nuvem
Tópico do Conteúdo	Arquitetura de Solução de Computação em Nuvem

---

35) Leia atentamente o trecho a seguir:

> Art. 26. O valor da vantagem auferida ou pretendida corresponde ao equivalente monetário do produto do ilícito, assim entendido como os ganhos ou os proveitos obtidos ou pretendidos pela pessoa jurídica em decorrência direta ou indireta da prática do ato lesivo.
> § 1º O valor da vantagem auferida ou pretendida poderá ser estimado mediante a aplicação, conforme o caso, das seguintes metodologias:
> I - pelo valor total da receita auferida em contrato administrativo e seus aditivos, deduzidos os custos lícitos que a pessoa jurídica comprove serem efetivamente atribuíveis ao objeto contratado, na hipótese de atos lesivos praticados para fins de obtenção e execução dos respectivos contratos;
> II - pelo valor total de despesas ou custos evitados, inclusive os de natureza tributária ou regulatória, e que seriam imputáveis à pessoa jurídica caso não houvesse sido praticado o ato lesivo pela pessoa jurídica infratora; ou
> III - pelo valor do lucro adicional auferido pela pessoa jurídica decorrente de ação ou omissão na prática de ato do Poder Público que não ocorreria sem a prática do ato lesivo pela pessoa jurídica infratora.
> § 2º Os valores correspondentes às vantagens indevidas prometidas ou pagas a agente público ou a terceiros a ele relacionados não poderão ser deduzidos do cálculo estimativo de que trata o § 1º.

Este trecho se refere a:

A) Código de Conduta Ética da CELESC.
B) Lei de Improbidade Administrativa 8249/1992.
C) Lei Geral de Proteção de Dados.
D) Lei Antitruste 12.529/2011.
E) Lei Federal Anticorrupção 12.846/2013.

Justificativa
O Artigo 26 disposto na Lei Federal Anticorrupção pode ser acessado em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/decreto/d11129.htm

Nível	Superior

Disciplina	Compliance
Eixo Temático	Legislação
Tema	Lei Federal Anticorrupção
Tópico do Conteúdo	Acordo de Leniência

---

36) Uma empresa de TI está planejando virtualizar sua infraestrutura de servidores para melhorar a eficiência e reduzir custos. O gestor de TI da empresa está delineando um plano que inclui todas as etapas necessárias para a implementação bem-sucedida da virtualização. Ele precisa garantir que cada etapa seja realizada corretamente para minimizar os riscos e maximizar os benefícios da virtualização. Qual das seguintes opções descreve **CORRETAMENTE** a sequência adequada das etapas principais no processo de virtualização de servidores?

A) Avaliação da infraestrutura atual, migração das aplicações, configuração dos hypervisors, monitoramento e manutenção.
B) Avaliação da infraestrutura atual, configuração dos hypervisors, migração das aplicações, monitoramento e manutenção.
C) Configuração dos hypervisors, avaliação da infraestrutura atual, migração das aplicações, monitoramento e manutenção.
D) Migração das aplicações, avaliação da infraestrutura atual, configuração dos hypervisors, monitoramento e manutenção.
E) Monitoramento e manutenção, configuração dos hypervisors, avaliação da infraestrutura atual, migração das aplicações.

Justificativa
Alternativa B, correta. Esta opção descreve a sequência correta das etapas no processo de virtualização de servidores: (i) Avaliação da infraestrutura atual: Identificar e avaliar os recursos disponíveis, as necessidades de desempenho e as aplicações que serão virtualizadas; (ii) Configuração dos hypervisors: Instalar e configurar os hypervisors, que são as plataformas de virtualização que permitem a criação e gestão de máquinas virtuais; (iii) Migração das aplicações: Transferir as aplicações e serviços dos servidores físicos para as máquinas virtuais; e (iv) Monitoramento e manutenção: Após a migração, é crucial monitorar o desempenho e realizar a manutenção contínua para garantir a estabilidade e eficiência do ambiente virtualizado.
Alternativa A, incorreta, pois migrar as aplicações antes de configurar os hypervisors não é viável, já que os hypervisors são necessários para criar o ambiente virtual onde as aplicações serão hospedadas.
Alternativa C, incorreta, visto que, configurar os hypervisors antes de avaliar a infraestrutura atual é um erro, pois a avaliação é necessária para entender os requisitos e capacidades antes de qualquer configuração.
Alternativa D, incorreta, pois migrar as aplicações antes da avaliação e configuração dos hypervisors não é possível, pois a migração depende das etapas de avaliação e configuração.
Alternativa E, incorreta, pois monitoramento e manutenção são atividades contínuas que ocorrem após a migração, não no início do processo. Avaliação e configuração devem preceder a migração das aplicações.

Referência
VERAS, M. **Virtualização**: componente central do datacenter. Brasport, 2011. ISBN: 9788574524672.
VIANA, E.R.C. **Virtualização de servidores Linux**: sistemas de armazenamento virtual – guia prático. Vol 2. Ciência Moderna, 1ª. Ed. ISBN: 8539902206.

Nível	Superior
Disciplina	Gestão da Tecnologia da Informação
Eixo Temático	Infraestrutura
Tema	Gerenciamento de Recursos
Tópico do Conteúdo	Virtualização de servidores

---

37) Uma empresa de tecnologia está planejando implantar um gateway de aplicação para melhorar o gerenciamento de tráfego e aumentar a segurança das suas aplicações web. O gestor de TI está elaborando um plano detalhado para a implantação do gateway de aplicação e quer garantir que todas as etapas sejam seguidas corretamente para maximizar os benefícios dessa tecnologia. Qual das seguintes etapas é a primeira a ser realizada no processo de implantação de um gateway de aplicação?

A) Configuração das regras de balanceamento de carga.
B) Definição dos requisitos de rede e segurança.
C) Implementação do SSL offloading.

D) Teste de desempenho e monitoramento.
E) Migração de todas as aplicações para o gateway.

Justificativa
Alternativa B, correta, pois a primeira etapa no processo de implantação de um gateway de aplicação é definir os requisitos de rede e segurança. Isso envolve entender as necessidades específicas da empresa, como a quantidade de tráfego esperado, requisitos de segurança, políticas de acesso e compliance. Esta fase é crucial para planejar a configuração e implementação do gateway de forma que ele atenda adequadamente às necessidades da infraestrutura de TI da empresa.
Alternativa A, incorreta, pois, embora a configuração das regras de balanceamento de carga seja uma etapa importante, ela deve ser feita após a definição dos requisitos de rede e segurança. Sem uma compreensão clara dos requisitos, as regras de balanceamento podem não ser otimizadas para o ambiente da empresa.
Alternativa C, incorreta, pois o SSL offloading é uma função importante que pode ser configurada em gateways de aplicação, mas esta não é a primeira etapa. Antes de implementar o SSL offloading, é necessário definir os requisitos de segurança e a arquitetura da rede.
Alternativa D, incorreta, pois estes de desempenho e monitoramento são etapas posteriores que ocorrem após a configuração inicial do gateway e a implementação das políticas de segurança e balanceamento de carga. Eles garantem que o gateway funcione corretamente e de forma eficiente, mas não são a primeira etapa.
Alternativa E, incorreta, pois migrar as aplicações para o gateway é uma das etapas finais no processo de implantação. Antes de migrar, é necessário configurar e testar o gateway para garantir que ele atenda a todos os requisitos definidos anteriormente.

Referência
SOUSA, D.C., SOARES, J.A., SILVA, F.R., MACEDO, R.T.; MASCHIETTO, L.G., SILVA, M.S. **Gerenciamento de Redes de Computadores**. Editora Grupo A, 2021. ISBN: 9786556901411.
SOUSA, L.B. **Gerenciamento e Segurança de Redes**. SENAI-SP Editora, 2017.

Nível	Superior
Disciplina	Redes de Computadores
Eixo Temático	Gerenciamento de Infraestrutura
Tema	Gerenciamento de Tráfego e Segurança
Tópico do Conteúdo	Gateways de aplicação

---

38) Uma empresa de médio porte está expandindo sua infraestrutura de TI e contratou um novo administrador de sistemas. O gestor de TI quer garantir que o novo administrador esteja familiarizado com as principais ferramentas administrativas da Microsoft que serão utilizadas para gerenciar a rede e os serviços da empresa. Qual das seguintes ferramentas administrativas da Microsoft é responsável por gerenciar o diretório de usuários, computadores e outros recursos dentro de uma rede corporativa?

A) WSUS (Windows Server Update Services).
B) DNS (Domain Name System).
C) DHCP (Dynamic Host Configuration Protocol).
D) Active Directory.
E) IIS (Internet Information Services).

Justificativa
Alternativa D, correta, pois o Active Directory (AD) é a ferramenta administrativa da Microsoft responsável por gerenciar o diretório de usuários, computadores e outros recursos dentro de uma rede corporativa. O AD permite que os administradores de rede criem e gerenciem domínios, usuários, grupos e políticas, além de fornecer autenticação e autorização centralizadas para os recursos da rede.
Alternativa A, incorreta, o WSUS é uma ferramenta usada para gerenciar e distribuir atualizações e patches para sistemas operacionais Windows. Ele não está envolvido na gestão de diretórios de usuários e recursos.
Alternativa B, incorreta, pois, o DNS é uma ferramenta usada para resolver nomes de domínio em endereços IP. Embora seja uma parte essencial da infraestrutura de rede, não é responsável por gerenciar diretórios de usuários e recursos.
Alternativa C, incorreta, pois o DHCP é responsável pela atribuição dinâmica de endereços IP aos dispositivos na rede. Ele facilita a configuração automática de IPs, mas não gerencia diretórios de usuários e recursos.
Alternativa E, incorreta, pois o IIS é um servidor web da Microsoft usado para hospedar sites e serviços web. Ele não é usado para gerenciar diretórios de usuários e recursos dentro de uma rede corporativa.

Referência

CARDOSO, W**. Dominando o Centro de Administração do Microsoft 365**: um guia passo a passo. Clube dos Autores, 2024.
THOMPSON, M.A. **Windows Server, 2016**: Fundamentos. Editora Érica, 1ª. Ed., 2016. ISBN: 853652457X.

Nível	Superior
Disciplina	Banco de Dados
Eixo Temático	Bancos de Dados Relacional
Tema	Trigonometria
Tópico do Conteúdo	Funções trigonométricas

---

39) Uma empresa de serviços financeiros está revisando suas políticas de segurança da informação para garantir a conformidade com regulamentos e proteger dados sensíveis. O novo Diretor de Segurança da Informação (CISO) está criando um plano abrangente para atualizar e implementar essas políticas em toda a organização. Qual das seguintes opções descreve **CORRETAMENTE o principal objetivo de uma política de segurança da informação**?

A) Melhorar a eficiência dos processos de negócios.
B) Reduzir os custos operacionais da empresa.
C) Proteger a confidencialidade, integridade e disponibilidade das informações.
D) Aumentar a velocidade de processamento dos sistemas de TI.
E) Facilitar a atualização de software e hardware.

Justificativa
Alternativa B, correta. O principal objetivo de uma política de segurança da informação é proteger a confidencialidade, integridade e disponibilidade das informações (conhecido como o modelo CIA). Isso garante que os dados sejam acessíveis apenas por pessoas autorizadas (confidencialidade), não sejam alterados ou destruídos de maneira não autorizada (integridade) e estejam disponíveis quando necessários (disponibilidade).
Alternativa A, incorreta, pois, embora políticas de segurança da informação possam, indiretamente, contribuir para a redução de custos ao prevenir incidentes de segurança e perdas de dados, a redução de custos não é o principal objetivo dessas políticas.
Alternativa C, incorreta, pois a eficiência dos processos de negócios pode ser beneficiada por boas práticas de segurança, mas a principal meta das políticas de segurança da informação é proteger os dados e os sistemas, não diretamente melhorar a eficiência dos processos.
Alternativa D, incorreta, a velocidade de processamento dos sistemas de TI não é o foco das políticas de segurança da informação. Essas políticas são mais voltadas para a proteção contra ameaças e vulnerabilidades.
Alternativa E, incorreta, pois embora uma boa política de segurança da informação inclua procedimentos para a atualização de software e hardware (como patches de segurança), essa facilitação é um aspecto operacional e não o principal objetivo da política.

Referência
FONTES, E. **Políticas e Normas para a segurança da informação**. Brasport, 1ª ed., 2012. ISBN: 8574525154.
FREITAS, A. **Política de Segurança da Informação**. Ciência Moderna, 2020. ISBN: 8573937718.

Nível	Superior
Disciplina	Segurança da Informação
Eixo Temático	Gestão e Governança da Informação
Tema	Políticas de Segurança da Informação
Tópico do Conteúdo	Políticas de Segurança da Informação

---

40) Uma empresa de tecnologia está preocupada com a segurança de sua infraestrutura de TI e decidiu contratar uma equipe de segurança para realizar testes de penetração (pentests) e avaliações de vulnerabilidade. O objetivo é identificar e corrigir possíveis fraquezas antes que sejam exploradas por atacantes maliciosos. Qual das seguintes opções descreve corretamente a diferença principal entre um teste de penetração (pentest) e uma avaliação de vulnerabilidade?

A) Um pentest é focado na conformidade com regulamentos, enquanto uma avaliação de vulnerabilidade é focada na performance dos sistemas.
B) Um pentest é realizado apenas internamente, enquanto uma avaliação de vulnerabilidade é sempre feita por terceiros.

C) Um pentest tenta explorar vulnerabilidades, enquanto uma avaliação de vulnerabilidade apenas identifica e classifica vulnerabilidades.
D) Um pentest é realizado apenas em redes externas, enquanto uma avaliação de vulnerabilidade é feita apenas em redes internas.
E) Um pentest é um processo automatizado, enquanto uma avaliação de vulnerabilidade é realizada manualmente.

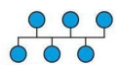
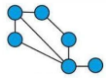
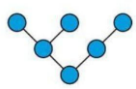
Justificativa
A alternativa A é correta. A principal diferença entre um teste de penetração e uma avaliação de vulnerabilidade é a abordagem e o objetivo. Um pentest é um teste ativo onde os profissionais de segurança tentam explorar vulnerabilidades para entender as reais implicações de segurança e demonstrar como um atacante pode comprometer os sistemas. Por outro lado, uma avaliação de vulnerabilidade é um processo mais passivo que envolve a identificação, análise e classificação de vulnerabilidades sem tentar explorá-las.
Alternativa B, incorreta, pois, tanto os pentests quanto as avaliações de vulnerabilidade podem ser realizados internamente ou por terceiros. A origem dos executores não é a principal diferença entre os dois processos.
Alternativa C, incorreta, pois, embora tanto pentests quanto avaliações de vulnerabilidade possam ajudar na conformidade com regulamentos, essa não é a principal diferença entre eles. Nenhum dos dois processos é focado na performance dos sistemas, mas sim na segurança.
Alternativa D, incorreta, pois pentests e avaliações de vulnerabilidade podem ser realizados em qualquer parte da infraestrutura de TI, seja interna ou externa, dependendo do escopo definido.
Alternativa E, incorreta, pois ambos os processos podem envolver tanto métodos automatizados quanto manuais. Pentests frequentemente combinam ferramentas automatizadas com exploração manual para aprofundar a análise, enquanto avaliações de vulnerabilidade geralmente utilizam ferramentas automatizadas para identificação e podem incluir uma análise manual para contextualização.

Referência
BASTA, A., BASTA, N., BROWN, M. Segurança de Computadores e Teste de Inovação. Editora Cengage, 1ª. Ed., 2014. ISBN: 8522117993.
DAVIS, R. **Pentest em Redes de Computadores**: como assumir o controle de qualquer empesa no mundo. Novatec Editora, 1ª. Ed., 2021. ISBN: 6586057825.
WEIDMAN, G. **Testes de Invasão**. Novatec, 2014. ISBN: 9788575224076.

Nível	Superior
Disciplina	Redes de Computadores
Eixo Temático	Segurança em redes de computadores
Tema	Testes
Tópico do Conteúdo	Testes de Penetração e Vulnerabilidade de Ambientes

---

41) Uma empresa de desenvolvimento de software está redesenhando sua infraestrutura de rede para melhorar a eficiência, escalabilidade e redundância. O gerente de TI está avaliando diferentes topologias de rede para determinar qual estrutura melhor atende às necessidades da empresa. Qual das seguintes opções de topologia de rede é conhecida por sua alta redundância e resiliência, mas também pode ser mais complexa e cara de implementar?

A) Topologia em anel 
B) Topologia em barramento 
C) Topologia em malha 
D) Topologia em estrela 
E) Topologia em árvore 

Justificativa
A alternativa C é correta, pois a topologia em malha é conhecida por sua alta redundância e resiliência. Nesta topologia, cada dispositivo é conectado a vários outros dispositivos, criando vários caminhos para a transmissão de dados. Isso garante que, se um caminho falhar, os dados ainda podem ser roteados por outro caminho, aumentando a confiabilidade da rede. No entanto, essa topologia pode ser mais complexa e cara de implementar devido ao grande número de conexões necessárias.
A alternativa A é incorreta pois na topologia em anel, cada dispositivo está conectado a dois outros dispositivos, formando um círculo. Embora ofereça algum nível de redundância, já que os dados podem viajar em ambas as direções, ela não é tão resiliente quanto a topologia em malha. Se um único dispositivo ou conexão falhar, isso pode afetar a comunicação de toda a rede.
A alternativa B é incorreta, pois na topologia em barramento, todos os dispositivos estão conectados a um único cabo principal ou "barramento". Essa topologia é simples e barata de implementar, mas tem baixa redundância e é menos resiliente. Se o cabo principal falhar, toda a rede fica inoperante.
A alternativa D é incorreta pois na topologia em estrela, todos os dispositivos estão conectados a um dispositivo central (como um switch ou hub). Esta topologia é fácil de gerenciar e oferece boa performance. No entanto, se o dispositivo central falhar, toda a rede será interrompida, o que a torna menos redundante do que uma topologia em malha.
A alternativa E é incorreta pois a topologia em árvore é uma combinação de topologias em estrela e em barramento, com hierarquias de dispositivos conectados. Embora ofereça melhor organização e gerenciamento de grandes redes, ela não oferece a mesma redundância e resiliência que a topologia em malha.

Referência
KUROSE, J., ROSS, K. **Rede de Computadores e a Internet**: uma abordagem top-down. Pearson Universidades, 6ª. Ed., 2013. ISBN: 8581436773.
MENDES, D.R. **Redes de Computadores**. Novatec, 2015. ISBN: 9788575223660.
TANENBAUM, A. FEAMSTER, N., WETHERALL, D. VIEIRA, D. **Redes de Computadores**. Bookman, 6ª. Ed., 2021. ISBN: 8582605609.

Nível	Superior
Disciplina	Redes de Computadores
Eixo Temático	Infraestrutura de redes
Tema	Topologias de Rede
Tópico do Conteúdo	Tipos de Topologia

---

42) Uma empresa de tecnologia está contratando um novo administrador de rede. Durante a entrevista, o gerente de TI deseja avaliar o conhecimento do candidato sobre protocolos de rede e serviços comuns, como TCP/IP, DHCP, DNS, CIFS, BFS e SFTP, que são essenciais para a configuração e suporte de redes empresariais. Qual dos seguintes protocolos é usado para transferência segura de arquivos entre um cliente e um servidor na rede?

A) SFTP.
B) DHCP.
C) DNS.
D) CIFS.
E) BSF.

Justificativa
A alternativa A é a correta pois o Protocolo de Transferência de Arquivo Seguro (SFTP) é usado para a transferência segura de arquivos entre um cliente e um servidor na rede. Ele utiliza o SSH (Secure Shell) para fornecer uma camada de segurança, criptografando os dados durante a transferência para proteger contra interceptação e ataques.
A alternativa B é incorreta, pois o Protocolo de Configuração Dinâmica de Host (DHCP) é utilizado para a atribuição automática de endereços IP aos dispositivos em uma rede. Ele não é usado para transferência de arquivos.
A alternativa C é incorreta pois o sistema de Nomes de Domínio (DNS) é usado para resolver nomes de domínio em endereços IP. Ele facilita a localização de recursos na rede, mas não envolve transferência de arquivos.
A alternativa D é incorreta pois o Sistema de Arquivos de Internet Comum (CIFS) é um protocolo usado para compartilhamento de arquivos em redes, especialmente em ambientes Windows. Embora suporte transferência de arquivos, não oferece a mesma segurança que o SFTP, que é especificamente projetado para transferências seguras.
A alternativa E é incorreta pois BFS não é um protocolo padrão amplamente reconhecido no contexto de redes e transferência de arquivos. É provável que haja uma confusão com um outro protocolo ou serviço específico.

Referência

KUROSE, J., ROSS, K. **Rede de Computadores e a Internet**: uma abordagem top-down. Pearson Universidades, 6ª. Ed., 2013. ISBN: 8581436773.
MENDES, D.R. **Redes de Computadores**. Novatec, 2015. ISBN: 9788575223660.
TANENBAUM, A. FEAMSTER, N., WETHERALL, D. VIEIRA, D. **Redes de Computadores**. Bookman, 6ª. Ed., 2021. ISBN: 8582605609.

Nível	Superior
Disciplina	Servidores
Eixo Temático	Administração de Servidores
Tema	Servidores UNIX e Microsoft
Tópico do Conteúdo	Protocolos

---

43) Uma empresa de serviços financeiros está revisando suas práticas de segurança cibernética após um incidente de invasão. O novo Diretor de Segurança da Informação (CISO) está conduzindo uma avaliação de risco e quer garantir que todos os funcionários estejam cientes das melhores práticas e medidas de segurança. Qual das seguintes práticas é considerada essencial para proteger a integridade e a confidencialidade dos dados em um ambiente corporativo?

A) Desativar firewalls para melhorar a velocidade da rede.
B) Utilizar apenas senhas simples para facilitar o acesso.
C) Compartilhar senhas com colegas de trabalho para melhorar a colaboração.
D) Implementar autenticação multifator (MFA).
E) Manter o software desatualizado para evitar incompatibilidades.

Justificativa
A alternativa D é a correta, pois a autenticação multifator (MFA) é uma prática de segurança essencial que adiciona uma camada extra de proteção além da simples combinação de nome de usuário e senha. MFA requer que os usuários forneçam duas ou mais formas de identificação, o que torna muito mais difícil para os invasores comprometerem contas e acessarem dados confidenciais. Isso pode incluir algo que o usuário sabe (senha), algo que ele possui (token ou dispositivo móvel) e algo que ele é (impressão digital ou reconhecimento facial).
A alternativa A é incorreta, pois firewalls são uma linha de defesa crucial contra ameaças cibernéticas. Desativá-los expõe a rede a uma variedade de ataques, comprometendo a segurança dos dados.
A alternativa B é incorreta, pois senhas simples são fáceis de adivinhar ou quebrar usando técnicas de força bruta ou engenharia social. Essa prática compromete a segurança e aumenta o risco de invasões.
A alternativa C é incorreta, pois compartilhar senhas é uma prática insegura que compromete a segurança individual e da empresa. Isso pode levar ao acesso não autorizado e à falta de responsabilidade.
A alternativa E é incorreta, pois manter o software desatualizado é perigoso porque as atualizações frequentemente incluem correções para vulnerabilidades de segurança conhecidas. Usar software desatualizado deixa a rede e os dados vulneráveis a ataques.

Referência
FONTES, E.L. **Segurança da Informação**. Saraiva, 1a. Ed., 2017. Ebook.
MACHADO, F.R.N. **Segurança da Informação**: princípios e controles de ameaças. Editora Érica, 2014. ISBN: 8536507845.
PINHEIRO, P.H., SLEIMAN, C., ROCHA, H., LOTUFO, L. **Segurança digital** – proteção de dados nas empresas. Atlas, 1a. Ed., 2020. ISBN: 8597026057.

Nível	Superior
Disciplina	Redes de Computadores
Eixo Temático	Segurança da Informação
Tema	Gestão da Segurança da Informação
Tópico do Conteúdo	Práticas para Segurança da Informação

---

44) Uma empresa de e-commerce está planejando expandir suas operações online para suportar um maior número de usuários simultâneos e garantir que o sistema permaneça disponível mesmo em caso de falhas. O gerente de TI está avaliando diferentes topologias de bancos de dados relacionais para alcançar alta disponibilidade e escalabilidade. Qual das seguintes topologias de banco de dados relacionais é mais adequada para um ambiente que exige alta disponibilidade e escalabilidade?

A) Arquitetura monolítica com um único servidor de banco de dados.
B) Replicação master-slave com failover automático.
C) Banco de dados centralizado com backup diário.
D) Replica única com failover manual.
E) Arquitetura shard sem replicação.

Justificativa
A alternativa B é a correta. Esta topologia é altamente adequada para ambientes que exigem alta disponibilidade e escalabilidade. Na replicação master-slave, o banco de dados master trata todas as operações de escrita e replica os dados para um ou mais bancos de dados slave, que podem lidar com as operações de leitura. Se o master falhar, o sistema pode realizar um failover automático para um dos slaves, minimizando o tempo de inatividade. Além disso, essa topologia pode ser escalada horizontalmente adicionando mais slaves para distribuir a carga de leitura.
A alternativa A é incorreta, pois esta configuração não oferece alta disponibilidade nem escalabilidade. Se o único servidor falhar, todo o sistema ficará indisponível. Além disso, a capacidade de escalabilidade é limitada ao hardware do servidor único.
A alternativa C é incorreta, pois embora os backups diários sejam importantes para recuperação de desastres, eles não fornecem alta disponibilidade. Em caso de falha, a restauração a partir de um backup diário pode resultar em perda de dados e tempo de inatividade significativo.
A alternativa D é incorreta, pois ter apenas uma réplica e depender de um failover manual pode resultar em tempos de inatividade prolongados em caso de falha, já que a intervenção humana é necessária para ativar o failover. Isso compromete a alta disponibilidade.
A alternativa E é incorreta, pois o Sharding divide o banco de dados em vários pedaços menores (shards) para melhorar a escalabilidade. No entanto, sem replicação, cada shard é um ponto único de falha, o que compromete a alta disponibilidade. Se um shard falhar, os dados nele armazenados não estarão acessíveis.

Referência
DATE, C.J. **Projeto de Banco de Dados e Teoria Relacional**: formas normais e tudo o mais. Novatec Editora, 1a. Ed., 2015. ISBN: 8575224557.
TETILA, E.C. **Banco de Dados Relacional**: arquitetura, modelo entidade-relacionamento (ER), linguagem SQL e normalização de dados. Appris Editora, 1a Ed., 2021. ISBN: 6525005981.

Nível	Superior
Disciplina	Banco de Dados
Eixo Temático	Bancos de Dados Relacionais
Tema	Topologias de Banco de Dados
Tópico do Conteúdo	Topologias para ambientes com alta disponibilidade e escalabilidade

---

45) Uma empresa de serviços financeiros está implementando novas medidas de segurança para proteger as transações online de seus clientes. O gerente de TI está treinando a equipe sobre os conceitos de criptografia simétrica e assimétrica, certificados digitais e assinaturas digitais, para garantir que todos compreendam como essas tecnologias funcionam e como elas se complementam para garantir a segurança dos dados. Qual das seguintes afirmações sobre criptografia simétrica e assimétrica, certificados digitais e assinaturas digitais é **CORRETA**?

A) Assinaturas digitais utilizam criptografia simétrica para garantir que uma mensagem não seja alterada.
B) Criptografia simétrica utiliza um par de chaves pública e privada, enquanto a criptografia assimétrica utiliza a mesma chave para criptografar e descriptografar.
C) Certificados digitais são usados para garantir a integridade dos dados, enquanto assinaturas digitais são usadas para criptografar dados.
D) Criptografia assimétrica é geralmente mais rápida que a criptografia simétrica e é usada para criptografar grandes volumes de dados.
E) Certificados digitais fornecem uma forma de verificar a autenticidade da chave pública de uma entidade.

Justificativa
A alternativa E é a correta. Certificados digitais são emitidos por Autoridades Certificadoras (CAs) confiáveis e contêm a chave pública da entidade, além de informações sobre a identidade dessa entidade. Eles garantem que a chave pública realmente pertence à entidade, permitindo que outros confiem nas comunicações criptografadas com essa chave pública.
A alternativa A é incorreta, pois assinaturas digitais utilizam criptografia assimétrica para garantir a integridade e a autenticidade de uma mensagem. A assinatura digital é gerada com a chave privada do remetente e pode ser verificada com a chave pública correspondente.

A alternativa B é incorreta. A criptografia simétrica utiliza a mesma chave para criptografar e descriptografar os dados, enquanto a criptografia assimétrica utiliza um par de chaves (uma pública e uma privada).
A alternativa C é incorreta, pois certificados digitais são usados para autenticar a identidade e a chave pública de uma entidade. Assinaturas digitais são usadas para garantir a integridade e a autenticidade dos dados, não para criptografá-los.
A alternativa D é incorreta. A criptografia simétrica é geralmente mais rápida que a criptografia assimétrica e é mais adequada para criptografar grandes volumes de dados. A criptografia assimétrica, devido à sua complexidade, é mais lenta e normalmente usada para criptografar pequenas quantidades de dados ou para criptografar chaves simétricas.

Referência
FREIRE A., SANTOS, A., MUNIZ, A. **Jornada de Segurança da Informação**. Editora Brasport, 2024. ISBN: 6560960099.
SILVA, M.B.F. **Cibersegurança**: a visão panorâmica sobre a segurança da informação na internet. Freitas Bastos, 1a. Edição, 2023. ISBN: 6556752444.
THOMPSON, M.A. **A Bíblia Hacker**. 3a. Ed., 2022. Ebook.

Nível	Superior
Disciplina	Segurança da Informação
Eixo Temático	Segurança Cibernética
Tema	Criptografia
Tópico do Conteúdo	Criptografia Simétrica e Assimétrica, Certificados e Assinatura Digital

---

46) Uma empresa de desenvolvimento de software está trabalhando para fortalecer suas práticas de segurança cibernética, adotando o NIST Cybersecurity Framework. Durante uma reunião, o Diretor de Segurança da Informação (CISO) apresenta uma questão para a equipe sobre os componentes e a estrutura do framework, para assegurar que todos compreendem sua aplicação e importância. Qual das seguintes afirmações sobre o NIST Cybersecurity Framework está **CORRETA**?

A) O componente "Core" do framework detalha cinco funções principais: Identificar, Proteger, Detectar, Responder e Recuperar.
B) O framework é composto por quatro componentes principais: Identificar, Proteger, Detectar e Responder.
C) Os "Tiers" no framework indicam o nível de conformidade de uma organização com as regulamentações governamentais.
D) O "Profile" é um conjunto fixo de práticas de segurança que todas as organizações devem seguir.
E) O framework foi projetado exclusivamente para empresas do setor de saúde.

Justificativa
A alternativa A é a correta. O "Core" do NIST Cybersecurity Framework é um conjunto de atividades desejadas e resultados de segurança cibernética, organizados em cinco funções principais. Essas funções fornecem uma estrutura de alto nível para identificar e gerenciar riscos cibernéticos.
A alternativa B é incorreta. O framework tem cinco funções principais no "Core": Identificar, Proteger, Detectar, Responder e Recuperar.
A alternativa C é incorreta. Os "Tiers" descrevem o grau de rigor e sofisticação das práticas de gerenciamento de risco cibernético de uma organização, mas não são especificamente sobre conformidade com regulamentações governamentais. Eles ajudam a entender o contexto e a maturidade da postura de segurança cibernética da organização.
A alternativa D é incorreta. O "Profile" no NIST Cybersecurity Framework é uma representação personalizada das funções, categorias e subcategorias do "Core" que uma organização escolhe para alinhar com suas necessidades, objetivos e tolerância ao risco, não é um conjunto fixo de práticas.
A alternativa E é incorreta. O NIST Cybersecurity Framework foi projetado para ser utilizado por qualquer organização, independentemente do setor, incluindo, mas não se limitando ao setor de saúde. É aplicável a qualquer organização que queira melhorar sua segurança cibernética.

Referência
CALDER, A. **NIST Cybersecurity Framework**: a pocket guide. ITGP Illustrated, 2018. ISBN: 1787780406.
FREIRE A., SANTOS, A., MUNIZ, A. **Jornada de Segurança da Informação**. Editora Brasport, 2024. ISBN: 6560960099.
SILVA, M.B.F. **Cibersegurança**: a visão panorâmica sobre a segurança da informação na internet. Freitas Bastos, 1a. Edição, 2023. ISBN: 6556752444.
THOMPSON, M.A. **A Bíblia Hacker**. 3a. Ed., 2022. Ebook.

Nível	Superior
Disciplina	Segurança da Informação
Eixo Temático	Cyber Segurança
Tema	NIST
Tópico do Conteúdo	Conceitos Básicos

---

47) Uma empresa de consultoria em segurança da informação está conduzindo uma sessão de treinamento para uma equipe de desenvolvimento de software sobre os métodos de segurança em banco de dados. O instrutor destaca a importância de implementar medidas de segurança robustas para proteger os dados confidenciais armazenados em bancos de dados. Qual dos seguintes métodos é um componente essencial para garantir a segurança em um banco de dados?

A) Manter senhas padrão para facilitar o acesso ao banco de dados.
B) Criptografar os dados sensíveis armazenados no banco de dados.
C) Permitir acesso total a todos os usuários do banco de dados.
D) Não realizar backups regulares dos dados do banco de dados.
E) Armazenar todos os dados do banco de dados em um servidor público.

Justificativa
A alternativa B é a correta, pois criptografar dados sensíveis é um método fundamental para proteger informações confidenciais em um banco de dados. A criptografia garante que mesmo se os dados forem acessados por pessoas não autorizadas, eles não serão legíveis sem a chave de descriptografia adequada, fornecendo uma camada adicional de segurança.
A alternativa A é incorreta. Manter senhas padrão aumenta o risco de acesso não autorizado ao banco de dados, pois são mais fáceis de adivinhar ou explorar por atacantes.
A alternativa C é incorreta. Permitir acesso total a todos os usuários do banco de dados pode levar a violações de segurança e comprometer a integridade e a confidencialidade dos dados.
A alternativa D é incorreta. Essa é uma prática de segurança inadequada. A realização de backups regulares é essencial para garantir a disponibilidade e a integridade dos dados, permitindo a recuperação em caso de perda de dados devido a falhas técnicas, ataques cibernéticos ou outros incidentes.
A alternativa E é incorreta. Armazenar todos os dados do banco de dados em um servidor público é uma má prática de segurança. Armazenar dados do banco de dados em um servidor público expõe os dados a potenciais ataques cibernéticos e violações de segurança, especialmente se medidas adequadas de segurança não forem implementadas no servidor público.

Referência
BASTA, A., ZGOLA, M. **Database Security**. Cengage Learning, 2nd Ed., 2011. ISBN: 9781435453906.
DIAZ, C. **Database Security**: problems and solutions. Mercury Learning & Information, 2022. ISBN: 1683926633.
FONTES, E.L.G. **Segurança da Informação**. Editora Saraiva, 2017. ISBN: 9788502122192.

Nível	Superior
Disciplina	Banco de Dados
Eixo Temático	Segurança em Banco de Dados
Tema	Métodos de Segurança
Tópico do Conteúdo	Conceitos Básicos

---

48) Em uma política de segurança da informação, qual é uma medida adequada a ser incluída no plano de contingência para lidar com incidentes de segurança?

A) Desligar imediatamente todos os sistemas de TI da organização.
B) Ignorar o incidente e não tomar nenhuma ação imediata.
C) Isolar imediatamente o sistema afetado da rede para evitar a propagação do incidente.
D) Solicitar aos funcionários que apaguem imediatamente todos os registros relacionados ao incidente.
E) Continuar normalmente as operações sem fazer qualquer alteração.

Justificativa

A alternativa C é a correta, pois ao isolar imediatamente o sistema afetado da rede, a organização pode evitar a propagação do incidente para outros sistemas e dispositivos na rede, minimizando assim o impacto do incidente e permitindo que as investigações e medidas corretivas sejam realizadas de forma mais eficaz.
A alternativa A é incorreta, pois desligar todos os sistemas pode interromper as operações críticas da organização, causando impactos financeiros e operacionais significativos, sem necessariamente resolver o incidente de segurança.
A alternativa B é incorreta. Esta é uma resposta inadequada, pois ignorar um incidente de segurança pode levar a consequências graves, como perda de dados sensíveis ou comprometimento da integridade dos sistemas.
A alternativa D é incorreta. Apagar registros relacionados ao incidente pode prejudicar as investigações posteriores e violar regulamentos de conformidade, além de não resolver efetivamente o problema subjacente.
A alternativa E é incorreta. Continuar as operações normalmente sem tomar medidas para conter o incidente pode permitir que o problema se agrave, colocando em risco ainda mais os ativos de informação da organização.

Referência
BARBIERI, C. **Governança de dados: práticas, conceitos e novos caminhos**. Alta Books, 1ª. Ed., 2019. ISBN: 855081069X.
REGO, B.L. **Gestão e Governança de Dados**: promovendo dados como ativo de valor nas empresas. Brasport, 1ª. Ed., 2013. ISBN: 8574525898.

Nível	Superior
Disciplina	Engenharia de Software
Eixo Temático	Gerenciamento de Projetos
Tema	Metodologias Àgeis
Tópico do Conteúdo	SCRUM

---

49) Qual das alternativas a seguir **NÃO** representa uma característica fundamental da computação distribuída?

A) **Transparência:** Os usuários e aplicativos não precisam ter conhecimento da distribuição dos recursos ou da heterogeneidade da rede.
B) **Distribuição de recursos:** Os recursos computacionais, como memória, processamento e armazenamento, estão espalhados por diversos nós da rede.
C) **Heterogeneidade:** Os nós da rede podem ter diferentes hardwares, softwares e sistemas operacionais.
D) **Centralização:** Existe um único nó na rede que controla todos os recursos e a execução das tarefas.
E) **Concorrência:** Múltiplas tarefas podem ser executadas simultaneamente em diferentes nós da rede.

Justificativa
A alternativa D é a correta, pois **NÂO** representa uma característica da computação distribuída. A computação distribuída se caracteriza pela ausência de um ponto central de controle. Ao contrário do que ocorre em sistemas centralizados, onde um único servidor gerencia todos os recursos e a execução das tarefas, na computação distribuída, as responsabilidades são distribuídas entre diversos nós da rede. Isso permite maior escalabilidade, flexibilidade e tolerância a falhas.
A alternativa A é incorreta, pois a transparência é um dos objetivos da computação distribuída. Os usuários e aplicativos não precisam ter conhecimento da distribuição dos recursos ou da heterogeneidade da rede para utilizá-la. Isso facilita o desenvolvimento e a utilização de aplicações distribuídas.
A alternativa B é incorreta, pois a distribuição de recursos é uma característica fundamental da computação distribuída. Os recursos computacionais são distribuídos por diversos nós da rede para aumentar a capacidade de processamento e armazenamento e melhorar a disponibilidade dos serviços.
A alternativa C é incorreta, pois a heterogeneidade é outra característica comum em sistemas distribuídos. Os nós da rede podem ter diferentes hardwares, softwares e sistemas operacionais, o que exige mecanismos de comunicação e interoperabilidade adequados.
A alternativa E é incorreta, pois a concorrência é uma característica importante da computação distribuída. Múltiplas tarefas podem ser executadas simultaneamente em diferentes nós da rede, o que aumenta o desempenho e a eficiência do sistema.

Referência
DANTAS, M. **Computação Distribuída de Alto Desempenho**: redes, clusters e grids computacionais. Axcel, 2005. ISBN: 85733224104.
MACEDO, R. **Projetos de Sistemas Distribuídos e de Tempo Real para Automação**. Edufba, 2018. ISBN: 9788523216757.
SILVA, G.P., BIANCHENI, C., COSTA, E.B. **Programação paralela e distribuída com MPI, Open ACC, para computação de alto desempenho**. Casa do Código, 2022. Ebook.

Nível	Superior
Disciplina	Arquitetura de computadores
Eixo Temático	Computação de Alto Desempenho
Tema	Computação Distribuída
Tópico do Conteúdo	Conceitos Básicos

---

50) A empresa XYZ está expandindo sua rede para incluir várias filiais em diferentes cidades. Para garantir que o tráfego de dados seja encaminhado de forma eficiente entre todas as filiais, a equipe de TI está avaliando diferentes protocolos de roteamento dinâmico. Eles querem um protocolo que se adapte rapidamente às mudanças na topologia da rede e que seja adequado tanto para redes pequenas quanto grandes. Qual dos seguintes protocolos de roteamento dinâmico seria a escolha mais apropriada para a empresa XYZ, considerando a necessidade de adaptação rápida às mudanças na topologia da rede e a escalabilidade?

A) BGP (Border Gateway Protocol)
B) RIP (Routing Information Protocol)
C) OSPF (Open Shortest Path First)
D) EIGRP (Enhanced Interior Gateway Routing Protocol)
E) IS-IS (Intermediate System to Intermediate System)

Justificativa
A alternativa C é a correta, pois OSPF (Open Shortest Path First) é um protocolo de roteamento dinâmico de estado de link, que é altamente adequado para redes de diferentes tamanhos. Ele se adapta rapidamente às mudanças na topologia da rede devido à sua rápida convergência e ao uso de algoritmos avançados (como o algoritmo Dijkstra) para calcular as rotas mais curtas. OSPF é escalável e pode ser utilizado em grandes redes corporativas, oferecendo suporte para hierarquia de áreas para otimizar o roteamento.
A alternativa A é incorreta, pois BGP é usado principalmente para roteamento entre sistemas autônomos na internet (roteamento interdomínios) e não é ideal para roteamento interno em redes corporativas. Ele é mais complexo e destinado a ambientes onde a estabilidade é mais importante do que a rápida adaptação às mudanças na topologia.
A alternativa B é incorreta, pois RIP é um protocolo de roteamento de vetor de distância que é mais simples, mas não é adequado para redes grandes devido ao seu limite de 15 saltos e à lenta convergência. Ele também usa métricas simples, baseadas apenas na contagem de saltos, o que pode não ser eficiente para rotas complexas.
A alternativa D é incorreta, pois EIGRP é um protocolo de roteamento avançado da Cisco, que combina características de protocolos de vetor de distância e de estado de link. Embora seja eficiente e tenha rápida convergência, é um protocolo proprietário da Cisco, o que pode limitar a sua utilização em ambientes que não utilizam exclusivamente equipamentos da Cisco.
A alternativa E é incorreta, pois IS-IS é um protocolo de estado de link semelhante ao OSPF e também é escalável e eficiente. No entanto, é menos comum em ambientes corporativos em comparação com o OSPF, especialmente fora de redes de operadoras e grandes ISPs. A implementação e suporte para IS-IS pode ser mais desafiador em algumas redes corporativas.

Referência
BUNGART, J.W. **Redes de Computadores**: fundamentos e protocolos. SENAI – SP Editora, 1ª ed., 2017. ISBN: 8583937656.
SOUSA, L.B. **Protocolos e Serviços de Rede**. Editora Érica, 1ª ed., 2014. ISBN: 8536507675.

Nível	Superior
Disciplina	Redes de Computadores
Eixo Temático	Conceitos Básicos
Tema	Protocolos
Tópico do Conteúdo	Protocolos de Roteamento Dinâmico

---

51) Em um cenário que exige alta disponibilidade, escalabilidade horizontal e flexibilidade no armazenamento de dados, qual tipo de banco de dados NoSQL seria mais adequado?

A) Banco de dados de séries temporais: Armazena e otimiza dados de séries temporais, como sensores e IoT.
B) Banco de dados chave-valor: Armazena dados em pares chave-valor, ideal para consultas simples e eficientes.
C) Banco de dados relacional: Armazena dados em tabelas com linhas e colunas, seguindo um modelo relacional rígido.

D) Banco de dados em grafo: Armazena dados como entidades interligadas por relacionamentos, ideal para análise de redes e grafos.

E) Banco de dados orientado a documentos: Armazena documentos completos em formato JSON ou BSON, permitindo consultas estruturadas e semiestruturadas.

Justificativa

A alternativa correta é a E, visto que, considerando os requisitos de alta disponibilidade, escalabilidade horizontal e flexibilidade no armazenamento de dados, um banco de dados orientado a documentos como **MongoDB**, **CouchDB** ou **RavenDB** se destaca como a opção mais adequada, devido a características como:

Alta disponibilidade: Bancos de dados orientados a documentos geralmente oferecem replicação de dados entre vários nós, garantindo que os dados permaneçam disponíveis mesmo em caso de falha de um nó.

Escalabilidade horizontal: A estrutura flexível de documentos permite adicionar facilmente novos nós ao cluster, distribuindo a carga de trabalho e aumentando a capacidade de armazenamento e processamento conforme a demanda.

Flexibilidade no armazenamento: Documentos JSON ou BSON podem armazenar dados estruturados, semiestruturados e não estruturados, atendendo à necessidade de flexibilidade no armazenamento de diferentes tipos de dados.

A alternativa A é incorreta pois banco de dados de séries temporais é otimizado para armazenamento e consultas em séries temporais, mas não oferece a mesma flexibilidade no armazenamento de dados de diferentes formatos como os bancos de dados orientados a documentos.

A alternativa B é incorreta, pois **banco de dados chave-valor é i**deal para consultas simples e eficientes, mas menos adequado para cenários que exigem consultas complexas em documentos completos ou análise de relacionamentos entre entidades.

A alternativa C é incorreta pois o modelo relacional rígido pode limitar a flexibilidade no armazenamento de dados e dificultar a escalabilidade horizontal, além de não ser otimizado para consultas em grandes volumes de dados não estruturados.

A alternativa D é incorreta pois o banco de dados em grafo é ideal para análise de redes e grafos, mas menos adequado para cenários que exigem armazenamento e consultas em documentos completos ou séries temporais.

Referência

FOWLER, M, SADALAGE, P.J. **NoSQL Essencial um Guia Conciso Para o Mundo Emergente da Persistência Poliglota**. Novatec Editora, 2013. ISBN: 9788575223383.

PANIZ, O. **NoSQL: como armazenar os dados de uma aplicação moderna**. Casa do Código, 2016. ISBN: 9788555191923.

Nível	Superior
Disciplina	Banco de Dados
Eixo Temático	Conceitos Básicos
Tema	Tipos de Bancos de Dados
Tópico do Conteúdo	Banco de Dados NoSQL

---

52) Uma empresa de varejo online enfrenta um rápido crescimento no volume de dados de vendas e transações, ultrapassando a capacidade do seu banco de dados relacional tradicional. Qual seria a melhor solução para gerenciar esses dados de forma eficiente e escalável?

A) **Adotar um data warehouse:** Um data warehouse centralizado pode armazenar e analisar dados históricos de vendas, mas não é ideal para processamento em tempo real e grandes volumes de dados não estruturados.

B) **Otimizar o banco de dados relacional existente:** Implementar técnicas de otimização como normalização, indexação e particionamento pode melhorar o desempenho, mas pode ser insuficiente para lidar com o crescimento exponencial de dados.

C) **Adotar um banco de dados NoSQL orientado a documentos:** Bancos de dados NoSQL orientados a documentos como MongoDB ou CouchDB podem armazenar, consultar e analisar grandes volumes de dados de vendas e transações de forma eficiente e escalável.

D) **Implementar um lago de dados:** Um lago de dados pode armazenar todos os dados brutos de vendas e transações em formato nativo, mas requer ferramentas e expertise para análise e visualização dos dados.

E) **Utilizar um banco de dados NoSQL chave-valor:** Bancos de dados chave-valor como Redis ou Memcached oferecem alto desempenho para consultas simples, mas não são adequados para armazenar e analisar dados estruturados complexos.

Justificativa

A alternativa C é a correta. Considerando o rápido crescimento no volume de dados de vendas e transações, a melhor solução para a empresa de varejo online seria adotar um banco de dados NoSQL orientado a documentos como MongoDB ou CouchDB. As razões para isto seriam: (i) a **escalabilidade horizontal, pois b**ancos de dados NoSQL orientados a documentos permitem adicionar facilmente novos nós ao cluster, distribuindo a carga de trabalho e aumentando a capacidade de armazenamento e processamento conforme a demanda de dados; a **flexibilidade no armazenamento, pois d**ocumentos JSON ou BSON podem armazenar dados estruturados, semiestruturados e não estruturados, atendendo à necessidade de armazenar diferentes tipos de dados de vendas e transações, como logs, imagens e comentários de clientes; (iii) os bancos de dados NoSQL orientados a documentos oferecem consultas eficientes para analisar grandes volumes de dados, permitindo à empresa extrair insights valiosos sobre vendas, tendências de clientes e padrões de compra; e (iv) processamento em tempo real, pois alguns bancos de dados NoSQL orientados a documentos, como o MongoDB, suportam replicação e sharding, permitindo processamento e análise de dados em tempo real, o que é crucial para acompanhar as vendas e transações online.
A alternativa A é incorreta, pois um data warehouse é ideal para análise de dados históricos e relatórios, mas não é projetado para lidar com grandes volumes de dados em tempo real e não estruturados, como os dados de vendas e transações da empresa.
A alternativa B é incorreta, pois otimizar um banco de dados relacional pode melhorar o desempenho em curto prazo, mas não é uma solução escalável para lidar com o crescimento exponencial de dados. Além disso, bancos de dados relacionais não são adequados para armazenar e analisar dados não estruturados.
A alternativa D é incorreta, pois, um lago de dados pode armazenar todos os dados brutos, mas a empresa precisaria de ferramentas e expertise para analisar e visualizar esses dados, o que pode ser um desafio e exigir tempo adicional.
A alternativa E é incorreta, pois bancos de dados chave-valor como Redis ou Memcached oferecem alto desempenho para consultas simples, mas não são adequados para armazenar e analisar dados estruturados complexos de vendas e transações, que exigem consultas mais complexas e relacionamentos entre os dados.

Referências

FOWLER, M.; SADALAGE, P.J. **NoSQL Essencial**: um guia conciso para o mundo emergente da persistência poliglota. Novatec Editora, 2013. ISBN: 8575223380.
MELO, A.B. **Big Data e NoSQL: ontologias e estado da arte**. Independtly Published, 2020. ISBN: 979836705307.
PAUZ, D. **NoSQL**: como armazenar os dados de uma aplicação moderna. Alura, 2016. ISBN: 9788555195923.
SING, A. **Data Modeling with NoSQL Database**. 3rd Ed., 2022. Ebook.

Nível	Superior
Disciplina	Banco de Dados
Eixo Temático	Conceitos Básicos
Tema	Banco de Dados NoSQL
Tópico do Conteúdo	Big Data

---

53) Uma empresa de médio porte está considerando a implementação de uma Infraestrutura de Desktop Virtual (VDI – Virtual Desktop Infrastructure) para melhorar a segurança, a mobilidade e a gestão dos desktops dos funcionários. A equipe de TI está avaliando os benefícios e desafios associados a essa tecnologia. Qual das seguintes opções é um benefício significativo da implementação de uma Infraestrutura de Desktop Virtual (VDI)?

A) Eliminação total da necessidade de manutenção de hardware.
B) Redução do consumo de energia nos servidores.
C) Facilidade de escalabilidade e gestão centralizada.
D) Aumento do tempo de resposta das aplicações devido à latência de rede.
E) Redução dos custos iniciais de implementação.

Justificativa

A alternativa C é a correta, visto que a implementação de uma Infraestrutura de Desktop Virtual (VDI) proporciona uma gestão centralizada dos desktops, o que facilita a administração e a escalabilidade. Com VDI, os desktops virtuais são gerenciados a partir de um servidor central, permitindo que os administradores de TI apliquem atualizações, patches e políticas de segurança de maneira uniforme e eficiente. Isso resulta em uma operação mais simplificada e na capacidade de escalar rapidamente conforme necessário, respondendo de forma flexível às mudanças nas demandas empresariais.
A alternativa A é incorreta, pois a VDI pode reduzir a frequência de manutenção de hardware nos desktops dos usuários finais, mas não elimina a necessidade de manutenção de hardware nos servidores e na infraestrutura de rede que suporta a VDI. Esses componentes ainda requerem monitoramento, atualização e manutenção regular.
A alternativa B é incorreta, pois, embora a VDI possa ajudar a reduzir o consumo de energia em desktops individuais, os servidores que hospedam a infraestrutura virtual geralmente demandam mais energia para suportar a carga de múltiplas VMs (Máquinas Virtuais), o que pode até aumentar o consumo de energia total da infraestrutura.

A alternativa D é incorreta, pois este é um aspecto negativo, não um benefício. A latência de rede pode ser um desafio para a VDI, especialmente se os usuários estiverem acessando os desktops virtuais de locais remotos. A latência pode aumentar o tempo de resposta das aplicações, impactando negativamente a experiência do usuário.
A alternativa E é incorreta, pois a implementação inicial de uma infraestrutura VDI pode ser bastante dispendiosa devido aos custos de servidores, software de virtualização e infraestrutura de rede necessária. Embora haja potencial para redução de custos a longo prazo, os custos iniciais tendem a ser altos.

Referência
BLKDYK, G. **Virtual Desktop Infrastructure VDI**: a complete guide. 5Starscooks, 2018. ISBN: 8574527610.
VERAS, M., ANTONIO, M.A. **Virtualização**: tecnologia central do datacenter. Brasport, 2ª ed., 2015.

Nível	Superior
Disciplina	Redes de Computadores
Eixo Temático	Infraestrutura
Tema	Máquinas virtuais
Tópico do Conteúdo	Virtual Desktop Infrastructure

---

54) Uma empresa de tecnologia tem observado um aumento significativo em incidentes de segurança cibernética, incluindo infecções por vírus, ataques de ransomware e tentativas de phishing. O departamento de TI está realizando uma sessão de treinamento para educar os funcionários sobre esses tipos de ameaças e como se protegerem adequadamente. Qual das seguintes opções descreve **CORRETAMENTE** a principal diferença entre vírus, ransomware e phishing?

A) Vírus infectam dispositivos por e-mail, ransomware se propaga via redes sociais, e phishing ocorre apenas em sites falsos.
B) Ransomware encripta arquivos, enquanto vírus e phishing não causam nenhum dano.
C) Phishing é uma forma de ransomware, enquanto vírus são usados apenas para espionagem.
D) Vírus e ransomware são tipos de malware, enquanto phishing é uma técnica de engenharia social.
E) Vírus e phishing são evitáveis com backups regulares, enquanto ransomware não pode ser prevenido.

Justificativa
A alternativa correta é D, pois vírus e ransomware são ambas formas de malware, que é um software malicioso projetado para danificar ou comprometer sistemas. O ransomware, especificamente, encripta os arquivos da vítima e exige um pagamento para a recuperação dos dados. Por outro lado, o phishing é uma técnica de engenharia social que tenta enganar as pessoas para que revelem informações pessoais ou financeiras, geralmente por meio de e-mails ou sites fraudulentos.
A alternativa A é incorreta pois todos esses métodos de propagação podem variar. Vírus podem se propagar por e-mail, downloads, dispositivos USB etc. Ransomware pode se espalhar através de e-mails, downloads maliciosos e redes sociais. Phishing pode ocorrer por e-mails, mensagens de texto, chamadas telefônicas e sites falsos.
A alternativa B é incorreta, pois vírus também podem causar danos significativos, como corromper dados, roubar informações ou danificar sistemas. Phishing pode levar ao roubo de dados pessoais ou financeiros.
A alternativa C é incorreta, pois phishing e ransomware são tipos distintos de ameaças. Phishing é uma técnica de obtenção de informações sensíveis, enquanto ransomware é um tipo de malware. Vírus podem ter diversas finalidades, incluindo espionagem, mas não são limitados a isso.
A alternativa E é incorreta pois backups regulares são uma medida preventiva útil contra ransomware, mas eles não "evitam" a infecção inicial. Eles ajudam na recuperação dos dados. Boas práticas de segurança, como o uso de software antivírus, treinamento sobre phishing e manutenção de backups, são importantes para prevenir e mitigar todas essas ameaças.

Referências
BERNARDINI, D. **Virus**: aka Malware. Ethical Hacking, 2023. Ebook.
LISKA, A., GALLO, T. **Ransomware**: defendendo-se da extorsão digital. O´Reilly – Novatec Editora, 1ª. Ed., 2017. ISBN: 8575225510.
PROKISCH, C.A. **Cibersegurança**: como proteger seus dados no mundo digital. SENAC-SP Editora, 2023. Ebook.

Nível	Superior
Disciplina	Redes de Computadores
Eixo Temático	Segurança em Redes de Computadores
Tema	Conceitos Básicos
Tópico do Conteúdo	Vírus, Ransomware, Phishing

55) De acordo com o Código de Conduta Ética da Celesc, em sua 4ª edição, qual das alternativas a seguir **NÃO** é um dever dos colaboradores da empresa?

A) **Atuar com profissionalismo e ética em todas as relações:** Os colaboradores devem agir com honestidade, integridade, imparcialidade e responsabilidade em suas atividades.
B) **Participar de atividades político-partidárias durante o expediente:** os colaboradores não devem se envolver em atividades político-partidárias enquanto estiverem no local de trabalho ou representando a empresa.
C) **Manter o sigilo das informações confidenciais da empresa:** Os colaboradores não devem divulgar ou utilizar informações confidenciais da empresa para fins pessoais ou de terceiros.
D) **Prestar contas de seus atos e decisões à empresa:** Os colaboradores devem ser transparentes em suas ações e decisões e estar preparados para responder por elas.
E) **Evitar conflitos de interesse:** Os colaboradores devem evitar situações que possam gerar conflito de interesse entre seus interesses pessoais e os da empresa.

Justificativa
A alternativa correta é B, pois o Código de Conduta Ética da CELESC proíbe o **envolvimento em atividades político-partidárias durante o expediente** ou enquanto estiver representando a empresa. Isso significa que os colaboradores não devem usar o tempo de trabalho, recursos da empresa ou sua posição na empresa para promover ou se envolver em qualquer atividade político-partidária.
A alternativa A é incorreta, pois esta é uma obrigação fundamental de todos os colaboradores da CELESC, conforme previsto no Código de Conduta Ética.
A alternativa C é incorreta, pois a proteção das informações confidenciais da empresa é crucial para garantir a segurança da informação e evitar danos à empresa.
A alternativa D é incorreta pois a transparência e a responsabilidade são princípios importantes na gestão da CELESC. Os colaboradores devem estar preparados para responder por suas ações e decisões.
A alternativa E é incorreta pois os colaboradores devem evitar situações que possam gerar conflito de interesse entre seus interesses pessoais e os da empresa. O Código de Conduta Ética da CELESC fornece diretrizes para identificar e lidar com conflitos de interesse.

Referência
O Código de Conduta Ética da CELESC, em sua 4ª edição, pode ser encontrado no link: https://www.celesc.com.br/arquivos/politicas/Codigo-conduta-etica-Celesc-4a-revisao.pdf

Nível	Superior
Disciplina	Compliance
Eixo Temático	Legislação
Tema	Código de Conduta
Tópico do Conteúdo	Código de Conduta Ética da CELESC

56) Uma equipe de engenheiros de uma empresa de tecnologia está analisando a arquitetura de um novo processador para otimizar o desempenho dos seus sistemas. Durante a reunião, eles discutem diversos aspectos de arquitetura de computadores e métricas de avaliação de desempenho, como CPI (Ciclos por Instrução), frequência de clock e latência de memória. Qual dos seguintes fatores é mais crítico para melhorar o desempenho geral de um processador?

A) Diminuir o tamanho do pipeline.
B) Reduzir a largura do barramento de dados.
C) Aumentar o número de transistores por chip.
D) Reduzir a quantidade de cache L1.
E) Aumentar o número de instruções por ciclo (IPC).

Justificativa
A alternativa correta é E, pois aumentar o número de instruções que um processador pode executar por ciclo de clock (IPC) é um dos métodos mais eficazes para melhorar o desempenho geral de um processador. Um IPC mais alto significa que o processador é capaz de realizar mais trabalho por ciclo de clock, o que resulta em maior eficiência e desempenho, especialmente em aplicações que exigem processamento intensivo.

A alternativa A é incorreta, pois diminuir o tamanho do pipeline pode reduzir a eficiência do processador em lidar com instruções. Um pipeline mais longo pode processar múltiplas instruções simultaneamente (pipeline), aumentando o throughput. Reduzir o tamanho do pipeline pode simplificar o design, mas geralmente reduz o desempenho.
A alternativa B é incorreta, pois reduzir a largura do barramento de dados geralmente diminui a capacidade de transferência de dados entre componentes do sistema, o que pode levar a gargalos e piorar o desempenho geral, especialmente em operações que envolvem grandes volumes de dados.
A alternativa C é incorreta, pois embora aumentar o número de transistores possa permitir a implementação de mais núcleos ou caches maiores, por si só não garante um aumento de desempenho. A eficiência e a arquitetura dos transistores são igualmente importantes.
A alternativa D é incorreta, pois reduzir a quantidade de cache L1 diminui a quantidade de dados e instruções que podem ser armazenados perto do núcleo do processador, aumentando a latência de acesso à memória e piorando o desempenho.

Referência
HENNESSY, J.L, PATTERSON, D.A. **Arquitetura de Computadores**: uma abordagem quantitativa. Elsevier, 5ª. Ed, 2013. ISBN: 8535261222.
SILVA, L.R.M. **Organização e arquitetura de computadores**: uma jornada do fundamental ao inovador. Freitas Bastos, 1ª, ed., 2024. ISBN: 6556753580.
STALLINGS, W. **Arquitetura e Organização de Computadores**. Pearson Universidades, 10ª ed., 2017. ISBN: 8543020530.

Nível	Superior
Disciplina	Arquitetura de Computadores
Eixo Temático	Conceitos Básicos
Tema	Organização de computadores
Tópico do Conteúdo	Avaliação de Desempenho

---

57) Uma empresa está modernizando sua infraestrutura de rede e decidiu atualizar seus cabeamentos estruturados, passando do Cat5e para o Cat6, conforme a NBR 14565. A decisão foi tomada visando melhorar a performance e a capacidade de transmissão de dados. Considerando as especificações técnicas e os benefícios dos cabos Cat6 em comparação com os cabos Cat5e, qual das afirmações abaixo está **CORRETA**?

A) Cabos Cat6 suportam frequências de até 250 MHz, enquanto os cabos Cat5e suportam até 100 MHz.
B) A principal vantagem do cabo Cat6 sobre o Cat5e é a redução do custo de instalação.
C) Tanto o cabo Cat5e quanto o Cat6 possuem a mesma capacidade de redução de interferências externas.
D) A distância máxima recomendada para um canal de cabeamento com cabo Cat6 é menor que a do cabo Cat5e.
E) Cabos Cat5e e Cat6 são igualmente adequados para suportar redes Gigabit Ethernet, sem nenhuma vantagem significativa do Cat6.

Justificativa
A alternativa correta é A, pois A norma NBR 14565 especifica que os cabos Cat6 são projetados para suportar frequências de até 250 MHz, proporcionando uma melhor performance em termos de largura de banda e capacidade de transmissão de dados, em comparação com os cabos Cat5e, que suportam frequências de até 100 MHz. Isso permite ao Cat6 transmitir dados de maneira mais eficiente e com menos interferências, sendo uma escolha superior para redes que demandam maior desempenho.
A alternativa B é incorreta, pois os cabos Cat6 geralmente têm um custo de instalação mais elevado devido ao preço maior do material e à necessidade de técnicas de instalação mais cuidadosas para evitar perda de desempenho.
A alternativa C é incorreta, pois os cabos Cat6 possuem uma construção interna que inclui uma melhor blindagem e separadores internos que reduzem a interferência, tornando-os superiores aos cabos Cat5e nesse aspecto.
A alternativa D é incorreta, pois ambos os cabos têm a mesma distância máxima recomendada de 100 metros para aplicações típicas de rede Ethernet, mas o Cat6 oferece melhor desempenho dentro dessa distância.
A alternativa E é incorreta, pois embora ambos os cabos possam suportar redes Gigabit Ethernet, o Cat6 proporciona uma melhor margem de desempenho e menor risco de interferências e erros de transmissão, especialmente em ambientes com altos níveis de ruído eletromagnético.

Referência
CRUZ, E.C.A. **Cabeamento estruturado – desvendando cada passo**: do projeto à instalação. Érica, 2008. ISBN: 853650207X.
OLIVEIRA, A. **Projeto de uma rede de computadores utilizando cabeamento estruturado**: projeto de redes de computadores segundo a norma NBR 14565: 2000. Novas Edições Acadêmicas, 2016. ISBN: 9783330734579.

Nível	Superior
Disciplina	Redes de Computadores
Eixo Temático	Infraestrutura de redes
Tema	Cabeamento
Tópico do Conteúdo	Normal 14565

---

58) Uma empresa de médio porte está desenvolvendo uma política de segurança lógica para proteger seus dados e sistemas de TI. Como parte dessa política, o gestor de TI precisa escolher as medidas mais eficazes para garantir a segurança da informação, conforme as melhores práticas do mercado. Qual das seguintes medidas é a mais adequada para prevenir acessos não autorizados aos sistemas da empresa?

A) Implementar um sistema de backup diário para todos os dados críticos da empresa.
B) Adotar autenticação multifator (MFA) para todos os acessos aos sistemas da empresa.
C) Utilizar criptografia de dados em todos os dispositivos de armazenamento da empresa.
D) Realizar auditorias de segurança anuais nos sistemas da empresa.
E) Instalar e atualizar regularmente um software antivírus em todos os dispositivos da empresa.

Justificativa
A alternativa correta é B, pois a autenticação multifator (MFA) é uma medida de segurança eficaz que exige a verificação da identidade do usuário através de duas ou mais formas de autenticação independentes (algo que o usuário sabe, algo que o usuário possui, e/ou algo que o usuário é). Isso dificulta significativamente o acesso não autorizado, mesmo que as credenciais do usuário sejam comprometidas. A adoção de MFA é amplamente reconhecida como uma das melhores práticas em segurança da informação para proteger contra acessos não autorizados.
A alternativa A é incorreta, pois embora essencial para a recuperação de dados em caso de falha ou ataque, o backup diário não previne acessos não autorizados aos sistemas. Ele é uma medida de recuperação e não de prevenção de acessos indevidos.
A alternativa C é incorreta, pois a criptografia é crucial para proteger dados em repouso, mas não impede acessos não autorizados aos sistemas se as credenciais forem comprometidas. A criptografia protege os dados, mas não controla quem pode acessá-los.
A alternativa D é incorreta, pois as auditorias de segurança são importantes para identificar e corrigir vulnerabilidades, mas sua frequência anual pode não ser suficiente para prevenir acessos não autorizados em tempo real. Auditorias ajudam na detecção e correção, mas não são uma medida de prevenção direta.
A alternativa E é incorreta, pois embora crucial para a proteção contra malware, o software antivírus não é suficiente para prevenir acessos não autorizados. Ele é uma parte importante de uma estratégia de segurança, mas não aborda especificamente o controle de acessos como a MFA faz.

Referência
SEMOLA, M.M. **Gestão da Segurança da Informação**. GEN LTC, 2ª. Ed., 2013. ISBN: 8535271783.
SILVA, M.B.F. **Cibersegurança**: a visão panorâmica sobre a segurança da informação na internet. Freitas Bastos, 1a. Edição, 2023. ISBN: 6556752444.
WEILL, P., ROSS, J.W. **Governança de TI** – Tecnologia da Informação. MBooks, 1ª ed., 2005. ISBN: 8589387480.

Nível	Superior
Disciplina	Gestão da Tecnologia da Informação
Eixo Temático	Infraestrutura de Tecnologia da Informação
Tema	Segurança
Tópico do Conteúdo	Segurança Lógica

---

59) Em um cenário de crescente volume e sofisticação de ataques cibernéticos, qual das alternativas a seguir **NÃO** é uma função essencial de um Centro de Operações de Cibersegurança (SOC)?

A) **Gerenciamento de identidades e acessos (IAM):** O SOC implementa e gerencia controles de IAM para garantir que apenas usuários autorizados tenham acesso aos recursos da organização.
B) **Monitoramento contínuo da rede e dos sistemas:** O SOC monitora a rede e os sistemas da organização em busca de atividades suspeitas e maliciosas, 24 horas por dia, 7 dias por semana.
C) **Detecção e análise de incidentes de segurança:** O SOC identifica, analisa e investiga incidentes de segurança cibernética, tomando as medidas cabíveis para conter o dano e mitigar os riscos.

D) **Resposta a incidentes de segurança:** O SOC implementa planos de resposta a incidentes, isolando sistemas comprometidos, contendo a propagação de malware e restaurando os sistemas afetados.
E) **Gerenciamento de vulnerabilidades:** O SOC identifica, prioriza e remedia vulnerabilidades de segurança em softwares, sistemas e dispositivos da organização.

Justificativa
Alternativa A, correta, pois embora o IAM seja uma importante medida de segurança cibernética, a **gerenciamento de identidades e acessos** não é uma função **primária** do SOC. O foco principal do SOC está no monitoramento, detecção, análise e resposta a incidentes de segurança, utilizando ferramentas e tecnologias específicas para essa finalidade.
Alternativa B, incorreta, pois o monitoramento é essencial para detectar atividades maliciosas e responder a incidentes de forma proativa. O SOC utiliza ferramentas e técnicas avançadas para monitorar a rede e os sistemas em tempo real.
Alternativa C, incorreta, pois a capacidade de identificar, analisar e investigar incidentes de segurança é crucial para conter o dano e mitigar os riscos. O SOC possui especialistas em análise de segurança que investigam incidentes em profundidade e implementam as medidas cabíveis para remediá-los.
Alternativa D, incorreta, pois SOC possui planos de resposta a incidentes bem definidos, que são acionados em caso de ataques cibernéticos. Esses planos incluem medidas como isolamento de sistemas, contenção de malware e restauração de sistemas afetados.
Alternativa E, incorreta, pois a identificação e remediação de vulnerabilidades são essenciais para prevenir ataques cibernéticos. O SOC trabalha em conjunto com equipes de segurança da informação para gerenciar vulnerabilidades de forma proativa.

Referência
PROKISCH, C.A. **Cibersegurança**: como proteger seus dados no mundo digital. SENAC-SP Editora, 2023. Ebook.
SEMOLA, M.M. **Gestão da Segurança da Informação**. GEN LTC, 2ª. Ed., 2013. ISBN: 8535271783.
SILVA, M.B.F. **Cibersegurança**: a visão panorâmica sobre a segurança da informação na internet. Freitas Bastos, 1a. Edição, 2023. ISBN: 6556752444.
WEILL, P., ROSS, J.W. **Governança de TI** – Tecnologia da Informação. MBooks, 1ª ed., 2005. ISBN: 8589387480.

Nível	Superior
Disciplina	Rede de Computadores
Eixo Temático	Segurança da Informação
Tema	Gestão da Segurança da Informação
Tópico do Conteúdo	Centro de Operações de Cibersegurança

---

60) Uma empresa de tecnologia está em processo de implementação de um Sistema de Gestão de Segurança da Informação (SGSI). Durante esse processo, a empresa deve garantir a conformidade com normas internacionais que fornecem requisitos e diretrizes para a gestão da segurança da informação. Considerando as normas ISO 27001 e ISO 27002, qual das afirmações a seguir é CORRETA sobre a implementação e manutenção do SGSI?

A) A ISO 27002 é usada para auditar e certificar um SGSI, garantindo sua conformidade com os padrões internacionais.
B) A ISO 27001 fornece diretrizes práticas para o gerenciamento de riscos e controles específicos de segurança da informação.
C) A ISO 27002 é a norma que estabelece os requisitos obrigatórios para a certificação de um SGSI.
D) A ISO 27001 define um conjunto de controles específicos que devem ser implementados pela organização.
E) A ISO 27001 especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um SGSI.

Justificativa
Alternativa E, correta. A ISO 27001 é uma norma internacional que especifica os requisitos para um Sistema de Gestão de Segurança da Informação (SGSI). Ela fornece um modelo para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar continuamente o SGSI. A certificação ISO 27001 é baseada na conformidade com esses requisitos.
Alternativa A, incorreta, pois a ISO 27002 não é usada para auditar e certificar um SGSI. A certificação é feita com base na ISO 27001. A ISO 27002 serve como um guia de boas práticas para a implementação dos controles de segurança da informação descritos na ISO 27001.
Alternativa B, incorreta, pois a ISO 27001 não fornece diretrizes práticas para o gerenciamento de riscos e controles específicos de segurança da informação. Essa é a função da ISO 27002, que complementa a ISO 27001 oferecendo diretrizes detalhadas para a implementação dos controles de segurança.
Alternativa C, incorreta, pois a ISO 27002 não estabelece requisitos obrigatórios para a certificação de um SGSI. A norma que estabelece esses requisitos é a ISO 27001. A ISO 27002 fornece diretrizes para os controles listados na ISO 27001.

Alternativa D, incorreta, pois a ISO 27001 não define um conjunto de controles específicos que devem ser implementados. Ela estabelece requisitos para o SGSI e inclui um anexo (Anexo A) com uma lista de controles que podem ser selecionados com base na avaliação de riscos da organização, mas a implementação de controles específicos é determinada pela análise de risco individual de cada organização.

Referência
A descrição destas normas pode ser encontrada no site oficial da ISO/IEC: https://www.iso.org/standard/27001

Nível	Superior
Disciplina	Normas
Eixo Temático	Normas ISO
Tema	Segurança da Informação
Tópico do Conteúdo	Normas 27001 e 27002