SECRETARIA DO PLANEJAMENTO E GESTÃO DO ESTADO DO CEARÁ (SEPLAG/CE)

CARGO 3: ANALISTA DE GESTÃO PÚBLICA
ÁREA DE ESPECIALIDADE: CIÊNCIA DA COMPUTAÇÃO OU AFINS NA ÁREA DA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Prova Discursiva P_4 – Situação-Problema

Aplicação: 21/07/2024

PADRÃO DE RESPOSTA DEFINITIVO

1 Integrar a gestão de identidades ao sistema de gestão de segurança da informação (SGSI) de uma organização é um fator crítico de sucesso para garantir que as pessoas autorizadas tenham acesso a informações confidenciais e críticas. Inicialmente, será necessário estabelecer políticas claras de controle de acesso, que definam quem pode acessar quais dados e em que circunstâncias. A implementação de um sistema de gestão de identidade deve começar com a definição de responsabilidades específicas para a administração de identidades e credenciais e garantir que todos os usuários sejam verificados antes de receber acessos. Os processos de autenticação devem ser robustos e, se possível, utilizar mecanismo de autenticação multifator para aumentar a segurança. A gestão de identidades deve ser diretamente integrada ao SGSI, com procedimentos regulares de revisão de acessos para assegurar que os direitos de acesso ainda são apropriados às funções e necessidades atuais do usuário. Além disso, é fundamental que todos os sistemas de controle de acesso registrem *logs* detalhados de atividades, que devem ser monitorados para detectar qualquer tentativa de acesso não autorizado ou eventos anormais. Essa integração reforça a segurança dos dados e alinha a gestão de identidades com as metas de segurança da informação da organização, conforme definido pela ISO/IEC 27001.

2 Durante o recrutamento e a contratação de novos colaboradores em uma organização pública do governo federal, é importante adotar medidas de segurança específicas para proteger a integridade e a confidencialidade das informações. O processo deve começar com a verificação de antecedentes dos(as) candidatos(as) para garantir que eles(as) não tenham histórico de atividades ilícitas ou que comprometam a segurança. Além disso, é importante que os termos e condições de emprego incluam compromissos explícitos relacionados à segurança da informação, que devem ser acordados antes de o trabalho efetivamente começar. A organização também deve implementar programas de conscientização e treinamento em segurança da informação, destinados a novos colaboradores, para garantir que eles entendam suas responsabilidades e os procedimentos de segurança desde o primeiro dia. Esses programas devem incluir informações sobre como manusear dados sensíveis e a importância de seguir as políticas de segurança da organização. Essas práticas protegem a organização contra riscos internos e garantem que novos colaboradores estejam imediatamente alinhados à cultura de segurança da informação da organização.

3 Fortalecer a segurança física dos espaços onde os dados são armazenados e processados em uma organização pública é fundamental para a proteção contra acessos não autorizados, desastres naturais e outros riscos físicos. É importante estabelecer áreas de segurança controladas, onde o acesso seja restrito apenas a pessoal autorizado. Isso inclui a utilização de medidas de segurança como sistemas de controle de acesso, monitoramento por câmeras de segurança e alarmes. Além disso, a organização deve implementar proteções contra ameaças ambientais e desastres naturais, como inundações, incêndios e terremotos, através da instalação de detectores e sistemas de supressão adequados. A segurança dos equipamentos, também, deve ser garantida, assegurando-se que eles estejam adequadamente protegidos contra interferências e danos. Essas medidas fortalecem a proteção dos dados e asseguram a continuidade dos serviços críticos da organização, minimizando o risco de interrupções e perda de dados em situações adversas.

As informações a seguir constam na norma ABNT NBR ISO/IEC 27002 e, se utilizadas pelo(a) candidato(a), também devem ser consideradas corretas.

QUESITO 2.1
Controle A.9.1.1 - Política de controle de acesso
Convém que a política leve em consideração os seguintes itens:
a) requisitos de segurança de aplicações de negócios individuais;
b) política para disseminação e autorização da informação, por exemplo, o princípio “necessidade de conhecer” e níveis de segurança e a classificação das informações;
c) consistência entre os direitos de acesso e as políticas de classificação da informação de sistemas e redes;
d) legislação pertinente e qualquer obrigação contratual relativa à proteção de acesso para dados ou serviços;

e) gerenciamento de direitos de acesso em um ambiente distribuído e conectado à rede que reconhece todos os tipos de conexões disponíveis;
f) segregação de funções de controle de acesso, por exemplo, pedido de acesso, autorização de acesso, administração de acesso;
g) requisitos para autorização formal de pedidos de acesso;
h) requisitos para análise crítica periódica de direitos de acesso;
i) remoção de direitos de acesso;
j) arquivo dos registros de todos os eventos significantes, relativos ao uso e gerenciamento das identidades do usuário e da informação de autenticação secreta; e
k) regras para o acesso privilegiado.

Controle A.9.4.2 - Gerenciamento de acesso privilegiado
Convém que o procedimento para entrada no sistema operacional seja configurado para minimizar a oportunidade de acessos não autorizados. Convém que o procedimento de entrada *(log-on*) revele o mínimo de informações sobre o sistema ou aplicação, de forma a evitar o fornecimento de informações desnecessárias a um usuário não autorizado. Convém que um bom procedimento de entrada no sistema (*log-on*):
a) não mostre identificadores de sistema ou de aplicação até que o processo tenha sido concluído com sucesso;
b) mostre um aviso geral informando que o computador seja acessado somente por usuários autorizados;
c) não forneça mensagens de ajuda durante o procedimento de entrada (*log-on*) que poderiam auxiliar um usuário não autorizado;
d) valide informações de entrada no sistema somente quando todos os dados de entrada estiverem completos. Caso ocorra uma condição de erro, o sistema não indique qual parte do dado de entrada está correta ou incorreta;
e) proteja contra tentativas forçadas de entrada no sistema (*log-on*);
f) registre tentativas de acesso ao sistema, sem sucesso e bem-sucedida;
g) comunique um evento de segurança caso uma tentativa potencial ou uma violação bem-sucedida de entrada no sistema (*log-on*) seja detectada;
h) mostre as seguintes informações quando o procedimento de entrada no sistema (*log-on*) finalizar com sucesso:
   1) data e hora da última entrada no sistema (*log-on*) com sucesso; e
   2) detalhes de qualquer tentativa sem sucesso de entrada no sistema (*log-on*) desde o último acesso com sucesso;
i) não mostre a senha que está sendo informada;
j) não transmita senhas em texto claro pela rede;
k) encerre sessões inativas após um período definido de inatividade, especialmente em locais de alto risco, como locais públicos, ou áreas externas ao gerenciamento de segurança da organização ou quando do uso de dispositivos móveis; e
l) restrinja os tempos de conexão para fornecer segurança adicional nas aplicações de alto risco e para reduzir a janela de oportunidade para acesso não autorizado.

Controle A.9.2.5 - Revisão de direitos de acesso do usuário
Convém que a análise crítica dos direitos de acesso considere as seguintes orientações:
a) os direitos de acesso de usuários sejam revisados em intervalos regulares e depois de quaisquer mudanças, como promoção, remanejamento ou encerramento do contrato;
b) os direitos de acesso de usuários sejam analisados criticamente e realocados quando movidos de um tipo de atividade para outra na mesma organização;
c) autorizações para direitos de acesso privilegiado especial sejam revisadas em intervalos mais frequentes;
d) as alocações de privilégios sejam verificadas em intervalo de tempo regular para garantir que privilégios não autorizados não foram obtidos; e
e) as modificações para contas privilegiadas sejam registradas para análise crítica periódica.

QUESITO 2.2
Controle A.7.1.1 - Triagem antes do emprego
Convém que as verificações levem em consideração toda a legislação pertinente relativa à privacidade, proteção da informação de identificação pessoal e do emprego e, onde permitido, incluam os seguintes itens:
a) disponibilidade de referências de caráter satisfatórias, por exemplo uma profissional e uma pessoal;
b) uma verificação (da exatidão e completeza) das informações do curriculum vitae do candidato;
c) confirmação das qualificações acadêmicas e profissionais;
d) verificação independente da identidade (passaporte ou documento similar); e
e) verificações mais detalhadas, como verificações de crédito ou verificações de registros criminais.

Convém que, quando um indivíduo for contratado para desempenhar o papel de segurança da informação, a organização certifique-se de que o candidato:
a) tem a competência necessária para executar o papel de segurança da informação; e
b) possa ser confiável para desempenhar o papel, especialmente se o papel for crítico para a organização.

Controle A.7.1.2 - Termos e condições de emprego
Convém que as obrigações contratuais para funcionários e partes externas reflitam as políticas para segurança da informação da organização, esclarecendo e declarando:
a) que todos os funcionários, fornecedores e partes externas que tenham acesso a informações sensíveis assinem um termo de confidencialidade ou de não divulgação, antes de lhes ser dado o acesso aos recursos de processamento da informação;
b) as responsabilidades legais e direitos dos funcionários e partes externas, e quaisquer outros usuários, por exemplo, com relação às leis de direitos autorais e legislação de proteção de dados;

c) as responsabilidades pela classificação da informação e pelo gerenciamento dos ativos da organização, associados com a informação, com os recursos de processamento da informação e com os serviços de informação conduzidos pelos funcionários, fornecedores ou partes externas;
d) as responsabilidades dos funcionários ou partes externas pelo tratamento da informação recebida de outras companhias ou partes interessadas; e
e) ações a serem tomadas no caso de o funcionário ou partes externas, desrespeitar os requisitos de segurança da informação da organização.

Controle A.7.2.2 - Durante o emprego
Convém que o treinamento em conscientização seja realizado conforme requerido pelo programa de conscientização em segurança da informação da organização. Convém que o treinamento em conscientização use diferentes formas de apresentação, incluindo treinamento presencial, treinamento à distância, treinamento baseado em *web*, autodidata e outros.
Convém que o treinamento e a educação em segurança da informação também contemplem aspectos gerais, como:
a) declaração do comprometimento da direção com a segurança da informação em toda a organização;
b) a necessidade de tornar conhecido e estar em conformidade com as obrigações e regras de segurança da informação aplicáveis, conforme definido nas políticas, normas, leis, regulamentações, contratos e acordos;
c) responsabilidade pessoal por seus próprios atos e omissões, e compromissos gerais para manter segura ou para proteger a informação que pertença à organização e partes externas;
d) procedimentos de segurança da informação básicos (como notificação de incidente de segurança da informação) e controles básicos (como, segurança da senha, controles contra *malware* e política de mesa limpa e tela limpa); e
e) pontos de contato e recursos para informações adicionais e orientações sobre questões de segurança da informação, incluindo materiais de treinamento e educação em segurança da informação.

QUESITO 2.3
Controle A.11.1.1 - Áreas seguras
Convém que as seguintes diretrizes sejam consideradas e implementadas, onde apropriado, para os perímetros de segurança física:
a) convém que os perímetros de segurança sejam claramente definidos e que a localização e a capacidade de resistência de cada perímetro dependam dos requisitos de segurança dos ativos existentes no interior do perímetro e dos resultados da avaliação de riscos;
b) convém que os perímetros de um edifício ou de um local que contenha as instalações de processamento da informação sejam fisicamente sólidos (ou seja, não é recomendável que o perímetro tenha brechas nem pontos onde poderia ocorrer facilmente uma invasão); convém que as paredes externas do local sejam de construção robusta e todas as portas externas sejam adequadamente protegidas contra acesso não autorizado por meio de mecanismos de controle (por exemplo, barras, alarmes, fechaduras); as portas e janelas sejam trancadas quando estiverem sem monitoração e uma proteção externa para as janelas seja considerada, principalmente para as que estiverem situadas no andar térreo;
c) convém que seja implantada uma área de recepção, ou um outro meio para controlar o acesso físico ao local ou ao edifício; convém que o acesso aos locais ou edifícios fique restrito somente ao pessoal autorizado;
d) convém que sejam construídas barreiras físicas, onde aplicável, para impedir o acesso físico não autorizado e a contaminação do meio ambiente;
e) convém que todas as portas corta-fogo do perímetro de segurança sejam providas de alarme, monitoradas e testadas juntamente com as paredes, para estabelecer o nível de resistência exigido, de acordo com normas regionais, nacionais e internacionais aceitáveis; convém que elas funcionem de acordo com os códigos locais de prevenção de incêndios e prevenção de falhas;
f) convém que sistemas adequados de detecção de intrusos, de acordo com normas regionais, nacionais e internacionais, sejam instalados e testados em intervalos regulares, e cubram todas as portas externas e janelas acessíveis; convém que as áreas não ocupadas sejam protegidas por alarmes o tempo todo; também é recomendável que seja dada proteção a outras áreas, por exemplo, salas de computadores ou salas de comunicações; e
g) convém que as instalações de processamento da informação gerenciadas pela organização fiquem fisicamente separadas daquelas que são gerenciadas por partes externas.

Controle A.11.1.2 - Controles de entrada física
Convém que sejam levadas em consideração as seguintes diretrizes:
a) convém que a data e a hora da entrada e saída de visitantes sejam registradas, e todos os visitantes sejam supervisionados, a não ser que o seu acesso tenha sido previamente aprovado; convém que as permissões de acesso só sejam concedidas para finalidades específicas e autorizadas, e sejam emitidas com instruções sobre os requisitos de segurança da área e os procedimentos de emergência. Convém que a identidade dos visitantes seja autenticada por meios apropriados;
b) convém que o acesso às áreas em que são processadas ou armazenadas informações sensíveis seja restrito apenas ao pessoal autorizado pela implementação de controles de acesso apropriados, por exemplo, mecanismos de autenticação de dois fatores, como, cartões de controle de acesso e PIN (*personal identification number*);
c) convém que uma trilha de auditoria eletrônica ou um livro de registro físico de todos os acessos seja mantida e monitorada de forma segura;
d) convém que seja exigido que todos os funcionários, fornecedores e partes externas, e todos os visitantes, tenham alguma forma visível de identificação e que eles avisem imediatamente ao pessoal de segurança, caso encontrem visitantes não acompanhados ou qualquer pessoa que não esteja usando uma identificação visível;
e) às partes externas que realizam serviços de suporte, convém que seja concedido acesso restrito às áreas seguras ou às instalações de processamento da informação sensíveis, somente quando necessário; convém que este acesso seja autorizado e monitorado; e

f) convém que os direitos de acesso a áreas seguras sejam revistos e atualizados em intervalos regulares, e revogados quando necessário.

Controle A.11.1.4 - Proteção contra ameaças externas e ambientais
Convém que sejam levadas em consideração as seguintes diretrizes:
a) o pessoal só tenha conhecimento da existência de áreas seguras ou das atividades nelas realizadas, se for necessário;
b) seja evitado o trabalho não supervisionado em áreas seguras, tanto por motivos de segurança como para prevenir as atividades mal-intencionadas;
c) as áreas seguras, não ocupadas, sejam fisicamente trancadas e periodicamente verificadas; e
d) não seja permitido o uso de máquinas fotográficas, gravadores de vídeo ou áudio ou de outros equipamentos de gravação, como câmeras em dispositivos móveis, salvo se for autorizado.

Controle A.11.2.1 - Colocação e proteção de equipamentos
Convém que sejam levadas em consideração as seguintes diretrizes para proteger os equipamentos:
a) convém que os equipamentos sejam colocados no local, a fim de minimizar o acesso desnecessário às áreas de trabalho;
b) convém que as instalações de processamento da informação que manuseiam dados sensíveis sejam posicionadas cuidadosamente para reduzir o risco de que as informações sejam vistas por pessoal não autorizado durante a sua utilização;
c) convém que as instalações de armazenamento sejam protegidas de forma segura para evitar acesso não autorizado;
d) convém que os itens que exigem proteção especial sejam protegidos para reduzir o nível geral de proteção necessário;
e) convém que sejam adotados controles para minimizar o risco de ameaças físicas potenciais e ambientais, como furto, incêndio, explosivos, fumaça, água (ou falha do suprimento de água), poeira, vibração, efeitos químicos, interferência com o suprimento de energia elétrica, interferência com as comunicações, radiação eletromagnética e vandalismo;
f) convém que sejam estabelecidas diretrizes quanto a comer, beber e fumar nas proximidades das instalações de processamento da informação;
g) convém que as condições ambientais, como temperatura e umidade, sejam monitoradas para a detecção de condições que possam afetar negativamente as instalações de processamento da informação;
h) convém que todos os edifícios sejam dotados de proteção contra raios e todas as linhas de entrada de força e de comunicações tenham filtros de proteção contra raios;
i) para equipamentos em ambientes industriais, é recomendado considerar o uso de métodos especiais de proteção, como membranas para teclados; e
j) convém que os equipamentos que processam informações sensíveis sejam protegidos, a fim de minimizar o risco de vazamento de informações em decorrência de emanações eletromagnéticas.

QUESITOS AVALIADOS

QUESITO 2.1 Integração da gestão de identidades ao sistema de gestão de segurança da informação (SGSI) da organização
Conceito 0 – Não abordou o aspecto ou o fez de forma totalmente equivocada.
Conceito 1 – Abordou o aspecto apenas de forma superficial, sem desenvolvê-lo.
Conceito 2 – Abordou o aspecto de forma parcialmente correta, citando informações apenas sobre um controle a ser adotado.
Conceito 3 – Abordou corretamente o aspecto, citando informações sobre mais de um controle a ser adotado.

QUESITO 2.2 Medidas de segurança a serem adotadas durante o recrutamento e a contratação de novos colaboradores da organização
Conceito 0 – Não abordou o aspecto ou o fez de forma totalmente equivocada.
Conceito 1 – Abordou o aspecto apenas de forma superficial, sem desenvolvê-lo.
Conceito 2 – Abordou o aspecto de forma parcialmente correta, citando informações adequadas apenas sobre um controle a ser adotado.
Conceito 3 – Abordou corretamente o aspecto, citando informações sobre mais de um controle a ser adotado.

QUESITO 2.3 Medidas de segurança física dos espaços onde os dados são armazenados e processados na organização
Conceito 0 – Não abordou o aspecto ou o fez de forma totalmente equivocada.
Conceito 1 – Abordou o aspecto apenas de forma superficial, sem desenvolvê-lo.
Conceito 2 – Abordou o aspecto de forma parcialmente correta, citando informações adequadas apenas sobre um controle a ser adotado.
Conceito 3 – Abordou corretamente o aspecto, citando informações adequadas sobre mais de um controle a ser adotado.

Cebraspe
Centro Brasileiro de Pesquisa em Avaliação e Seleção e de Promoção de Eventos

SECRETARIA DO PLANEJAMENTO E GESTÃO DO ESTADO DO CEARÁ (SEPLAG/CE)

CARGO 3: ANALISTA DE GESTÃO PÚBLICA
ÁREA DE ESPECIALIDADE: CIÊNCIA DA COMPUTAÇÃO OU AFINS NA ÁREA DA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Prova Discursiva P_4 – Questão 1

Aplicação: 21/07/2024

PADRÃO DE RESPOSTA DEFINITIVO

1. Definição de mineração de dados e seu objetivo
A mineração de dados é um processo de descoberta e análise de padrões significativos e tendências em grandes conjuntos de informações, por meio de análise matemática. Seu objetivo é encontrar padrões, correlações e mesmo anomalias, de modo a prever resultados futuros para resolver problemas, minimizar riscos, analisar o impacto de decisões e aumentar a produtividade, possibilitando a construção de modelos e algoritmos que possam prever resultados específicos com precisão crescente.

2. Descrição de classificação e associação, considerando as técnicas e tarefas de mineração de dados
A classificação é uma técnica complexa de mineração de dados que treina o algoritmo de *machine learning* para classificar dados em categorias distintas; ela usa métodos estatísticos, como "árvore de decisão", One-Class SVM e "vizinho mais próximo" ou (KNN) para identificar a categoria. Já a associação é uma tarefa que visa encontrar relacionamentos entre dois conjuntos de dados diferentes e aparentemente não relacionados; ela se aplica aos casos em que um grupo de valores determina outro grupo, ou está associado a outro grupo ou faixa de valores, como o algoritmo Apriori.

3. Definição de aprendizado de máquina e descrição de seus três principais tipos/categorias.
Aprendizado de máquina é um ramo da inteligência artificial que se concentra no desenvolvimento de algoritmos e modelos capazes de aprender padrões a partir de dados de treinamento sem programação explícita. Seus três principais tipos/categorias são:

1 aprendizagem supervisionada: o algoritmo é treinado com um conjunto de dados rotulados, ou seja, dados que já possuem uma resposta certa associada a eles;
2 aprendizagem não supervisionada: envolve o uso de dados não rotulados. O algoritmo busca identificar padrões e estruturas nos dados por conta própria, sem ter exemplos prévios de saídas desejadas, agrupando dados por similaridade e descobrindo grupos automaticamente; e
3 aprendizagem por reforço: o algoritmo interage repetidamente com um ambiente dinâmico a fim de se atingir um objetivo específico. Ele treina o *software* para tomar decisões em busca dos melhores resultados. Assim, as ações de *software* que atingem sua meta são reforçadas, enquanto as ações que prejudicam a meta são ignoradas.

QUESITOS AVALIADOS

QUESITO 2.1 – Definição de mineração de dados e seu objetivo
Conceito 0 – Não respondeu ou respondeu de maneira totalmente equivocada.
Conceito 1 – Definiu mineração de dados de maneira incompleta, e não apresentou seu objetivo.
Conceito 2 – Definiu corretamente mineração de dados, mas não apresentou seu objetivo.
Conceito 3 – Definiu mineração de dados e apresentou seu objetivo, mas o fez de maneira parcialmente correta.
Conceito 4 – Definiu corretamente mineração de dados e apresentou corretamente seu objetivo.

QUESITO 2.2 – Descrição de classificação e associação
Conceito 0 – Não respondeu ou respondeu de maneira totalmente equivocada.
Conceito 1 – Descreveu, de maneira incompleta, apenas uma das técnicas/tarefas solicitadas.
Conceito 2 – Descreveu ambas as técnicas/tarefas solicitadas, mas o fez de maneira incompleta.
Conceito 3 – Descreveu corretamente uma das técnicas/tarefas solicitadas, mas descreveu a outra de maneira incompleta.
Conceito 4 – Descreveu corretamente ambas as técnicas/tarefas solicitadas.

QUESITO 2.3 – Definição de aprendizado de máquina e três principais tipos/categorias
Conceito 0 – Não respondeu ou respondeu de maneira totalmente equivocada.
Conceito 1 – Apresentou corretamente a definição de aprendizado de máquina, mas sequer mencionou seus tipos/categorias.

Conceito 2 – Apresentou corretamente a definição de aprendizado de máquina, mas apenas mencionou seus tipos/categorias, sem descrevê-los.
Conceito 3 – Apresentou corretamente a definição de aprendizado de máquina, mas descreveu corretamente apenas um de seus tipos/categorias.
Conceito 4 – Apresentou corretamente a definição de aprendizado de máquina, mas descreveu corretamente apenas dois de seus tipos/categorias.
Conceito 5 – Apresentou corretamente a definição de aprendizado de máquina e descreveu corretamente seus três tipos/categorias.

Cebraspe
Centro Brasileiro de Pesquisa em Avaliação e Seleção e de Promoção de Eventos

SECRETARIA DO PLANEJAMENTO E GESTÃO DO ESTADO DO CEARÁ (SEPLAG/CE)

CARGO 3: ANALISTA DE GESTÃO PÚBLICA
ÁREA DE ESPECIALIDADE: CIÊNCIA DA COMPUTAÇÃO OU AFINS NA ÁREA DA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Prova Discursiva P_4 – Questão 2

Aplicação: 21/07/2024

PADRÃO DE RESPOSTA DEFINITIVO

1 Nome e objetivo de quatro camadas do modelo de referência OSI

O(A) candidato(a) deverá citar quatro entre as sete camadas do modelo OSI a seguir.

- Camada física. A camada física coordena as funções necessárias para transportar um fluxo de *bits* através de um meio físico. A camada física trata da transmissão de *bits* normais por um canal de comunicação.
- Camada de enlace de dados. A camada de enlace de dados transforma a camada física, de um meio de transmissão bruto, em um *link* confiável. A principal tarefa da camada de enlace de dados é transformar um canal de transmissão normal em uma linha que pareça livre de erros de transmissão.
- Camada de rede. A camada de rede é responsável pela entrega de um pacote desde sua origem até o seu destino, provavelmente através de várias redes (*links*). A camada de rede da Internet é responsável pela movimentação, de um hospedeiro para outro, de pacotes da camada de rede, conhecidos como datagramas. Uma questão fundamental é determinar a maneira como os pacotes são roteados da origem até o destino.
- Camada de transporte. A camada de transporte é responsável pela entrega processo a processo de toda a mensagem. A camada de transporte da Internet carrega mensagens da camada de aplicação entre os lados do cliente e servidor de uma aplicação. A função básica da camada de transporte é aceitar dados da camada acima dela, dividi-los em unidades menores, se for preciso, repassar essas unidades à camada de rede e garantir que todos os fragmentos chegarão corretamente a outra extremidade.
- Camada de sessão. A camada de sessão é o controlador de diálogo da rede. Ela estabelece, mantém e sincroniza a interação entre sistemas que se comunicam entre si. A camada de sessão permite que os usuários em diferentes máquinas estabeleçam sessões de comunicação entre eles.
- Camada de apresentação. A camada de apresentação é responsável pela sintaxe e semântica das informações trocadas entre dois sistemas. É responsável pela tradução, compressão e criptografia. Está relacionada à sintaxe e à semântica das informações transmitidas.
- Camada de aplicação. A camada de aplicação habilita o usuário, seja ele humano ou *software*, a acessar a rede. A camada de aplicação contém uma série de protocolos comumente necessários para os usuários

2 Diferença entre WEP e WPA2

No WEP, a autenticação com uma chave previamente compartilhada acontece antes da associação; o uso é desencorajado em decorrência de falhas no projeto que tornam o WEP fácil de burlar. O esquema recomendado é o WPA2, que implementa a segurança conforme a definição no padrão IEEE 802.11i, no qual o PA pode falar com um servidor de autenticação, que tem um banco de dados de nomes de usuários e senhas, para determinar se a estação tem permissão para acessar a rede. Essa troca acontece após a associação.

Obs.: considerar quem inserir texto sobre o algoritmo de criptografia no WPA2: o algoritmo de criptografia para WPA2 é baseado no padrão de criptografia avançado ou AES (Advanced Encryption Standard)**.**

3 Objetivo do SIP

O SIP é utilizado para aplicações interativas em tempo real. Ele provê mecanismos para estabelecer/encerrar chamadas entre dois interlocutores por uma rede IP; permite que os participantes concordem com a codificação da mídia; e provê mecanismos para gerenciamento de chamadas, tais como adicionar novos fluxos de mídia, mudar a codificação, convidar outros participantes, tudo durante a chamada, e ainda transferir e segurar chamadas. SIP é cada camada de aplicação, sendo utilizada para aplicações interativas em tempo real.

4 Objetivo do protocolo IPsec

O protocolo IP de segurança, mais conhecido como IPsec, provê segurança na camada de rede. O IPsec protege os datagramas IP entre quaisquer entidades **da camada de rede**, incluindo-se hospedeiros e roteadores. O IPsec é usado para

criar redes virtuais privadas (VPNs) que trabalham em cima da Internet pública. Quando dois hospedeiros estabelecem uma sessão IPsec, todos os segmentos TCP e UDP enviados entre eles serão codificados e autenticados. O IPsec, portanto, oferece uma cobertura geral, protegendo toda a comunicação entre os dois hospedeiros para todas as aplicações de rede. IPsec é da camada de rede.

5 Objetivo do BGP

O BGP oferece, a cada sistema autônomo (AS) na Internet, meios de: obter de AS vizinhos informações de alcançabilidade de sub-redes; propagar a informação de alcançabilidade a todos os roteadores internos ao AS; determinar rotas "boas" para sub-redes com base na informação de alcançabilidade e na política do AS. BGP é da camada de rede.

QUESITOS AVALIADOS

QUESITO 2.1
Conceito 0 – Não atendeu ao solicitado ou o fez de forma totalmente equivocada.
Conceito 1 – Citou corretamente o nome de apenas uma das camadas do modelo de referência OSI.
Conceito 2 – Citou corretamente o nome de apenas duas das camadas do modelo de referência OSI.
Conceito 3 – Citou corretamente o nome de apenas três das camadas do modelo de referência OSI.
Conceito 4 – Citou corretamente o nome de quatro camadas do modelo de referência OSI.

QUESITO 2.2
Conceito 0 – Não atendeu ao solicitado ou o fez de forma totalmente equivocada.
Conceito 1 – Descreveu corretamente o objetivo de apenas uma das camadas citadas.
Conceito 2 – Descreveu corretamente o objetivo de apenas duas das camadas citadas.
Conceito 3 – Descreveu corretamente o objetivo de apenas três das camadas citadas.
Conceito 4 – Descreveu o objetivo das quatro camadas citadas, mas cometeu algum erro conceitual.
Conceito 5 – Descreveu corretamente o objetivo das quatro camadas citadas.

QUESITO 2.3
Conceito 0 – Não atendeu ao solicitado ou o fez de forma totalmente equivocada.
Conceito 1 – Descreveu de forma muito precária as diferenças em relação à segurança e não descreveu corretamente ou não citou a função de associação.
Conceito 2 – Descreveu de forma parcialmente correta as diferenças em relação à segurança e descreveu de forma parcialmente correta a função de associação.
Conceito 3 – Descreveu corretamente sobre as diferenças em relação à segurança e à função de associação.

QUESITO 2.4
Conceito 0 – Não atendeu ao solicitado ou o fez de forma totalmente equivocada.
Conceito 1 – Descreveu de forma muito precária o objetivo do protocolo ou apenas citou corretamente a camada a que ele está mais associado.
Conceito 2 – Descreveu de forma parcialmente correta o objetivo do protocolo e citou corretamente a camada a que ele está mais associado.
Conceito 3 – Descreveu corretamente o objetivo do protocolo citou corretamente a camada a que ele está mais associado.

QUESITO 2.5
Conceito 0 – Não atendeu ao solicitado ou o fez de forma totalmente equivocada.
Conceito 1 – Descreveu de forma muito precária o objetivo do protocolo ou apenas citou corretamente a camada a que ele está mais associado.
Conceito 2 – Descreveu de forma parcialmente correta o objetivo do protocolo e citou corretamente a camada a que ele está mais associado.
Conceito 3 – Descreveu corretamente o objetivo do protocolo citou corretamente a camada a que ele está mais associado.

QUESITO 2.6
Conceito 0 – Não atendeu ao solicitado ou o fez de forma totalmente equivocada.
Conceito 1 – Descreveu de forma muito precária o objetivo do protocolo ou apenas citou corretamente a camada a que ele está mais associado.
Conceito 2 – Descreveu de forma parcialmente correta o objetivo do protocolo e citou corretamente a camada a que ele está mais associado.
Conceito 3 – Descreveu corretamente o objetivo do protocolo citou corretamente a camada a que ele está mais associado.