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

INSTITUTO NACIONAL DE PESQUISAS DA AMAZÔNIA (INPA)

CARGO 61: TECNOLOGISTA PLENO 2 – ESPECIALIDADE: T11
ÁREA DE ATUAÇÃO: INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO E REDES DE COMPUTADORES (INFRA-REDES)

Prova Discursiva – Questão 1

Aplicação: 24/03/2024

PADRÃO DE RESPOSTA DEFINITIVO

O(A) candidato(a) deve abordar que pela LGPD, não havendo decisão judicial nem autorização pelo titular, a transferência internacional de dados pessoais pode ocorrer em caso de cooperação jurídica internacional e em caso de proteção da vida ou incolumidade física do titular dos dados ou de terceiro. Assim, o(a) candidato(a) deve mencionar que um exemplo prático em que isso poderia ocorrer sem ferir a LGPD seria um processo judicial em outro país relativo a algum crime digital. Caso as evidências do crime digital indiquem sua origem em um endereço IP (endereço de Internet) no Brasil, uma autoridade judiciária, sem decisão judicial, pode solicitar a um provedor de acesso brasileiro os dados de acesso de um usuário e fornecer esses dados a autoridade judiciária de outro país caso haja acordo de cooperação judicial entre o Brasil e o país solicitante.

QUESITOS AVALIADOS

QUESITO 2.1 Cooperação judicial internacional
Conceito 0 – Não citou a cooperação judicial internacional.
Conceito 1 – Citou a cooperação internacional, mas não disse que era judicial.
Conceito 2 – Citou corretamente sobre a cooperação judicial internacional.

QUESITO 2.2 Proteção à vida ou incolumidade física do titular ou de terceiro
Conceito 0 – Não citou a proteção à vida nem a incolumidade física.
Conceito 1 – Citou a proteção à vida, mas não a incolumidade física.
Conceito 2 – Citou a incolumidade física, mas não a proteção à vida.
Conceito 3 – Citou corretamente sobre a proteção à vida e a incolumidade física.

QUESITO 2.3 Exemplo prático de caso em que pode haver a transferência internacional de dados pessoais sem decisão judicial nem autorização do titular dos dados
Conceito 0 – Não deu exemplo.
Conceito 1 – Deu exemplo genérico, reescrevendo a resposta com outras palavras.
Conceito 2 – Deu exemplo completo, explicando uma situação hipotética ou real.

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

INSTITUTO NACIONAL DE PESQUISAS DA AMAZÔNIA (INPA)

CARGO 61: TECNOLOGISTA PLENO 2 – ESPECIALIDADE: T11
ÁREA DE ATUAÇÃO: INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO E REDES DE COMPUTADORES (INFRA-REDES)

Prova Discursiva – Questão 2

Aplicação: 24/03/2024

PADRÃO DE RESPOSTA DEFINITIVO

O(A) candidato(a) deve abordar sobre a governança de TI e a estratégia de segurança de TI, deve mencionar que elas estão intrinsecamente interligadas, com a eficácia de uma influenciando significativamente a outra. A governança de TI pode ser afetada pela estratégia de segurança de TI através de: alinhamento com os objetivos de negócios através de *frameworks* como ITIL e COBIT; alocação de recursos e priorização de investimentos; utilização de *frameworks* de gestão de risco; identificação e aplicação de requisitos de conformidade e regulatórios; utilização de ferramentas de monitoramento e relatórios de desempenho; supervisão, auditoria e responsabilização.

As organizações devem desenvolver e implementar uma estratégia abrangente de segurança de TI que integre políticas eficazes, mecanismos eficazes e melhores práticas do setor requer uma abordagem sistemática e uma consideração cuidadosa de diversos fatores. Entre os principais fatores que devem ser considerados pelas organizações estão: a avaliação e análise de risco; o desenvolvimento e a documentação de políticas; a classificação e a proteção de dados; a configuração de *firewall* e a segmentação de rede; o controle de acesso remoto; a adoção das melhores práticas da indústria e a melhoria contínua.

Avaliação e análise de risco: priorizar os riscos com base na sua probabilidade e impacto potencial para concentrar esforços e recursos nas áreas mais críticas.

Desenvolvimento e documentação de políticas: desenvolver e documentar, de maneira clara e concisa, políticas e procedimentos abrangentes de segurança de TI que descrevam os objetivos, funções e responsabilidades de segurança da organização, uso aceitável de recursos, critérios de classificação de dados e protocolos de resposta a incidentes.

Classificação e proteção de dados: implementar um esquema de classificação de dados para categorizar informações confidenciais com base em sua sensibilidade, confidencialidade e requisitos regulatórios e aplicar controles de segurança e mecanismos de criptografia apropriados para proteger os dados.

Configuração de *firewall* e segmentação de rede: implantar e configurar *firewalls* para monitorar e controlar o tráfego de entrada e saída da rede, aplicar políticas de segurança e impedir o acesso não autorizado aos recursos da rede. Implementar a segmentação de rede para dividir a rede em zonas de segurança separadas com base em níveis de confiança.

Controle de acesso remoto: implementação de VPN e soluções similares. Garantir que apenas usuários legítimos e autorizados tenham acesso remoto aos recursos da organização.

Adoção das melhores práticas da indústria: utilização de *frameworks* como a ISO/IEC 27001 para garantir que a estratégia de segurança de TI esteja alinhada com as melhores práticas e os requisitos atuais de segurança cibernética da indústria.

Melhoria contínua: realizar auditorias regulares, avaliações de vulnerabilidade e exercícios de testes de penetração para identificar pontos fracos e áreas de melhoria.

QUESITOS AVALIADOS

QUESITO 2.1 Relação entre governança de TI e estratégia de segurança de TI

Conceito 0 – Não abordou o quesito.

Conceito 1 – Mencionou de forma precária ou equivocada a forte interligação entre governança e segurança de TI.

Conceito 2 – Mencionou de forma explicita a forte interligação entre governança e segurança de TI, mas não mencionou como a governança de TI pode ser afetada pela estratégia de segurança de TI.

Conceito 3 – Mencionou de forma explicita a forte interligação entre governança e segurança de TI, mas mencionou apenas de forma superficial como a governança de TI pode ser afetada pela estratégia de segurança de TI.

Conceito 4 – Mencionou de forma explicita a forte interligação entre governança e segurança de TI e mencionou pelo menos dois exemplos de como a governança de TI pode ser afetada pela estratégia de segurança de TI.

QUESITO 2.2 Principais fatores a considerar para implementar uma estratégia de segurança de TI

Conceito 0 – Não abordou o quesito.

Conceito 1 – Mencionou de forma precária ou equivocada os principais fatores que devem ser considerados na implementação de uma estratégia de segurança de TI.

Conceito 2 – Mencionou corretamente apenas dois fatores que devem ser considerados na implementação de uma estratégia de segurança de TI.

Conceito 3 – Mencionou corretamente apenas três fatores que devem ser considerados na implementação de uma estratégia de segurança de TI.
Conceito 4 – Mencionou corretamente quatro ou mais fatores que devem ser considerados na implementação de uma estratégia de segurança de TI.

QUESITO 2.3 Ações para cada um dos principais fatores dos principais fatores a considerar para implementar uma estratégia de segurança de TI
Conceito 0 – Não abordou o quesito.
Conceito 1 – Mencionou de forma precária ou equivocada as ações para implementação dos fatores do quesito 2.2.
Conceito 2 – Mencionou corretamente ações para apenas dois fatores que devem ser considerados na implementação de uma estratégia de segurança de TI.
Conceito 3 – Mencionou corretamente ações para apenas três fatores que devem ser considerados na implementação de uma estratégia de segurança de TI.
Conceito 4 – Mencionou corretamente ações para quatro ou mais fatores que devem ser considerados na implementação de uma estratégia de segurança de TI.

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

INSTITUTO NACIONAL DE PESQUISAS DA AMAZÔNIA (INPA)

CARGO 61: TECNOLOGISTA PLENO 2 – ESPECIALIDADE: T11
ÁREA DE ATUAÇÃO: INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO E REDES DE COMPUTADORES (INFRA-REDES)

Prova Discursiva – Questão 3

Aplicação: 24/03/2024

PADRÃO DE RESPOSTA DEFINITIVO

A integração de infraestrutura ágil, DevOps e escalabilidade representa um desafio significativo para empresas que buscam se manter competitivas no mercado digital. A falta de comunicação eficaz e colaboração entre as equipes de desenvolvimento, operação e segurança pode resultar em atrasos e falhas nos projetos. Solucionar esse desafio requer a implementação de processos claros e ferramentas de comunicação integradas. Por exemplo, a adoção de plataformas de colaboração como Slack ou Microsoft Teams pode facilitar a interação entre equipes. A automação de processos é fundamental para alcançar eficiência e consistência na implantação e no gerenciamento de infraestrutura. No entanto, o nível de maturidade da empresa em relação à automação pode variar. Soluções como ferramentas de automação de infraestrutura (por exemplo, Terraform, Ansible) e *pipelines* de CI/CD (*continuous integration*/*continuous deployment*) podem ajudar a superar esse desafio. Garantir a segurança da infraestrutura e dos dados é crítico em um ambiente ágil e escalável. Isso inclui a integração da segurança em todos os estágios do ciclo de vida do desenvolvimento de *software*, bem como o uso de ferramentas de análise de vulnerabilidades e conformidade. São exemplos a integração de *scanners* de segurança automatizados nos *pipelines* de CI/CD e a implementação de políticas de segurança como código (*security as code*). Implementar um sistema eficaz de monitoramento e observabilidade é essencial para detectar e solucionar problemas rapidamente. Isso envolve a coleta e análise de métricas e *logs* em tempo real. Soluções como Prometheus para monitoramento de métricas e ELK Stack (Elasticsearch, Logstash, Kibana) para análise de *logs* podem ser úteis.

Como principais soluções, a adoção de práticas DevOps, como integração contínua (CI) e entrega contínua (CD), é fundamental para promover a colaboração e a automação. Exemplos incluem o uso de ferramentas como Jenkins para automação de *builds* e *deploys*. Além disso, a implementação de ferramentas de automação, como Docker para contêineres e Kubernetes para orquestração de contêineres, pode simplificar o gerenciamento de infraestrutura e aplicativos. Por fim, a adoção de uma arquitetura de microsserviços pode facilitar a escalabilidade e a manutenção de aplicativos. Por exemplo, a decomposição de um monólito em microsserviços independentes pode permitir atualizações mais frequentes e escalonáveis.

A integração eficaz de infraestrutura ágil, DevOps e escalabilidade pode reduzir o tempo de lançamento de novos produtos e serviços, permitindo uma resposta mais rápida às demandas do mercado. Ademais, aumentar a capacidade de dimensionar infraestrutura e aplicativos de forma eficiente pode garantir uma experiência consistente para os usuários, independentemente do aumento da demanda. Além disso, a integração de práticas de segurança e monitoramento pode aumentar a confiabilidade da infraestrutura e dos dados, reduzindo o risco de falhas e violações de segurança. Por fim, a automação de processos e a adoção de arquiteturas modernas podem otimizar o uso de recursos e reduzir custos operacionais, aumentando a eficiência e a competitividade da empresa.

Em resumo, a integração eficaz de infraestrutura ágil, DevOps e escalabilidade requer um esforço conjunto em termos de comunicação, colaboração, automação e segurança. No entanto, os benefícios resultantes, incluindo agilidade, escalabilidade, confiabilidade e eficiência, podem ser significativos para empresas que buscam se destacar em um mercado digital altamente competitivo.

QUESITOS AVALIADOS

QUESITO 2.1 Aspectos essenciais dos desafios
Conceito 0 – Não apresentou nenhum dos seguintes aspectos essenciais dos desafios: comunicação e colaboração; automação; segurança; monitoramento e observabilidade.
Conceito 1 – Apresentou aspectos de apenas um tópico dos listados anteriormente.
Conceito 2 – Apresentou aspectos de dois tópicos dos listados anteriormente.
Conceito 3 – Apresentou aspectos de três ou mais dos tópicos listados anteriormente.

QUESITO 2.2 Aspectos essenciais das soluções
Conceito 0 – Não apresentou nenhum dos aspectos essenciais das soluções: implementação de práticas DevOps; utilização de ferramentas de automação; implementação de contêineres; microsserviços.
Conceito 1 – Apresentou aspectos de apenas um tópico dos listados anteriormente.
Conceito 2 – Apresentou aspectos de dois tópicos dos listados anteriormente.
Conceito 3 – Apresentou aspectos de três ou mais dos tópicos listados anteriormente.

QUESITO 2.3 Benefício da integração
Conceito 0 – Não apresentou nenhum benefício da integração.
Conceito 1 – Apresentou apenas um dos seguintes benefícios: agilidade; escalabilidade; confiabilidade; eficiência.
Conceito 2 – Apresentou dois benefícios entre os listados anteriormente.
Conceito 3 – Apresentou três ou mais dos benefícios listados anteriormente.

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

INSTITUTO NACIONAL DE PESQUISAS DA AMAZÔNIA (INPA)

CARGO 61: TECNOLOGISTA PLENO 2 – ESPECIALIDADE: T11
ÁREA DE ATUAÇÃO: INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO E REDES DE COMPUTADORES (INFRA-REDES)

Prova Discursiva – Questão 4

Aplicação: 24/03/2024

PADRÃO DE RESPOSTA DEFINITIVO

O protocolo AODV é reativo (só cria uma rota para um destino quando precisa enviar um pacote a este destino), é mais escalável (cada rota guarda apenas o próximo nó da rota, portanto uma rota não precisa guardar muita informação e uma atualização de rota não precisa afetar todos os nós da rota, sendo mais rápida) e se adapta bem a uma RSSF com nós de alta mobilidade (é mais fácil e mais rápido atualizar uma rota, já que esta guarda pouca informação).

O protocolo DSR também é reativo, é menos escalável (cada rota contém todo o caminho até o destino, portanto guarda mais informação) e é mais difícil de se adaptar a redes com uma quantidade grande de nós e a uma mudança de caminho.

Exemplo: uma RSSF para monitoramento ambiental de precipitação (chuva) em regiões de uma floresta. Nesse tipo de rede, os nós tipicamente ficam parados, não havendo muita necessidade de atualização de rotas, exceto quando um nó deixa de funcionar ou é adicionado à rede. Dessa forma, o protocolo DSR é o mais indicado, pois trabalha bem com redes de baixa ou nenhuma mobilidade.

QUESITOS AVALIADOS

QUESITO 2.1
Conceito 0 – Não mencionou da escalabilidade dos algoritmos.
Conceito 1 – Mencionou que o AODV é escalável, mas não explicou.
Conceito 2 – Mencionou que o DSR é menos escalável, mas não explicou.
Conceito 3 – Mencionou que o AODV é mais escalável que o DSR em virtude de guardar menos informação por rota.

QUESITO 2.2
Conceito 0 – Não mencionou a reatividade dos algoritmos, ou errou a resposta.
Conceito 1 – Respondeu que um dos algoritmos é reativo, mas não mencionou o outro ou não acertou.
Conceito 2 – Respondeu que ambos os algoritmos são reativos, mas não explicou.
Conceito 3 – Respondeu que ambos os algoritmos são reativos e explicou que eles só criam uma rota para um destino quando precisam enviar algo para lá.

QUESITO 2.3
Conceito 0 – Não mencionou a adequação à mobilidade ou errou a resposta.
Conceito 1 – Respondeu que o AODV se adapta melhor a redes de maior mobilidade, mas não mencionou o DSR.
Conceito 2 – Respondeu que o DSR não se adapta bem a redes de alta mobilidade, mas não mencionou o AODV.
Conceito 3 – Respondeu que o AODV se adapta a redes de alta mobilidade e o DSR não se adapta, mas não explicou o motivo.
Conceito 4 – Respondeu que o AODV se adapta a redes de alta mobilidade e que o DSR não se adapta bem, explicando que isso se deve à quantidade de informação por rota (muita informação por rota no DSR e pouca no AODV).

QUESITO 2.4
Conceito 0 – Não deu exemplo de RSSF.
Conceito 1 – Deu exemplo de RSSF, mas não indicou que algoritmo é o melhor.
Conceito 2 – Deu exemplo de RSSF e indicou que algoritmo é melhor, mas não justificou.
Conceito 3 – Deu exemplo de RSSF e indicou que algoritmo é melhor, justificando corretamente a resposta.