-- CONHECIMENTOS ESPECÍFICOS --

Questão 41

Um invasor pode ser uma pessoa que, mesmo sem conhecimento técnico, busca roubar informações, geralmente seguindo um processo. Nos ataques de engenharia social, o invasor segue, sucessivamente, as etapas de

A pesquisa, seleção do alvo, relacionamento e exploração.
B representação, conversação, relacionamento e exploração.
C pesquisa, seleção do alvo, construção do aplicativo e relacionamento.
D representação, seleção do alvo, construção do aplicativo e exploração.

Questão 42

No contexto *framework* da governança da segurança da informação, o estado desejado é aquele que pode ser obtido por meio de um conjunto de ferramentas que permitem o alcance de condições relevantes dentro desse cenário, como, por exemplo, processos, *frameworks*, serviços etc. Entre as várias abordagens em segurança da informação que proveem o alcance do estado desejado, encontra-se o

A PMBOK.
B Balanced Scorecard.
C Scrum.
D Ideal Model.

Questão 43

A avaliação do risco em uma organização deve contemplar a identificação, quantificação e priorização do risco em relação ao critério de aceitação do risco. Os riscos que não puderem ser aceitos pela organização deverão ser tratados. Nesse sentido, uma opção adequada de resposta ao risco é

A compartilhar o risco, implementando ações e aplicando o correto controle para reduzir o nível de aceitação do risco.
B evitar o risco, aplicando-se os controles apropriados para reduzir os impactos do risco.
C mitigar o risco, transferindo-o para outros parceiros — por exemplo, fornecedores ou seguradoras.
D aceitar o risco, conhecendo-o, e não implementar ações, pois o risco atende os critérios de aceitação.

Questão 44

Na auditoria de processo, o auditor deve proceder ao registro das evidências, à avaliação dos controles das forças e fraquezas e à elaboração de relatórios que informem o gerenciamento desses insumos. Para isso, o gerenciamento da auditoria deve garantir recursos e ferramentas adequadas para a execução da auditoria. Um processo típico para gerenciar e administrar projetos a serem auditados inclui a fase de

A comunicação, em que se coletam os requisitos e se elaboram os relatórios.
B planejamento, em que se adquire o dado e se definem os insumos de descoberta e validação.
C monitoração, em que se registram evidências para desenhar e suportar as opiniões e conclusões da auditoria.
D trabalho de campo e documentação, em que se determinam o contexto da auditoria e os procedimentos.

Questão 45

Em uma pequena organização XPTO que não implementa a segregação de funções, um funcionário desempenha a função de operador de computador e programador de aplicativos.

Nessa situação hipotética, o auditor de sistemas da informação deve recomendar

A procedimentos que verifiquem se apenas as mudanças aprovadas no programa foram implementadas.
B a criação de uma equipe adicional para proporcionar a segregação de funções.
C o registro automatizado das alterações nas bibliotecas de desenvolvimento.
D controles de acesso para evitar que o operador faça modificações no programa.

Questão 46

DoS é um tipo de ataque em que o serviço oferecido por um sistema ou uma rede é negado, reduzindo-se a funcionalidade ou impedindo-se o acesso aos recursos, mesmo para os legítimos usuários. Considerando as várias técnicas para a realização de ataques DoS, assinale a opção correta.

A Nos ataques de largura de banda, o invasor envia muitas solicitações com endereço de IP de origem falso, de modo que a vítima fica com a conexão amarrada.
B No ataque permanente de negação de serviço, o invasor usa solicitações por meio do protocolo ICMP e, assim, sobrecarrega o alvo, sem esperar pela resposta, e os recursos do dispositivo, negando o serviço.
C O ataque de inundação requer várias fontes, conhecidas como *zombies*, para gerar solicitações com o intuito de sobrecarregar o destino por meio do ataque distribuído.
D O ataque *peer-to-peer* explora *bugs* em servidores com tecnologia *peering*, utilizando o protocolo Direct Connect para explorar os *hosts* distribuídos e permitir que o invasor lance o ataque ao alvo.

Questão 47

Existem três categorias distintas de computação em nuvem: públicas, privadas e híbridas. A primeira categoria é caracterizada por

A oferecer tanto SaaS como PaaS e IaaS para seus clientes, em que os recursos computacionais, como processadores, memória e armazenamento, são localizados em *datacenters* pertencentes a uma organização que fornece os serviços tarifados de computação em nuvem para outras empresas.
B iniciativas governamentais em que os recursos computacionais são pertencentes a órgãos de governo com vistas a prover serviços para a população, sem custos para os cidadãos, de modo que os recursos sejam compartilhados entre os membros da comunidade.
C ser construída pela própria organização com vistas a atender a necessidades específicas da empresa, sendo necessário gerenciar a infraestrutura física para suprir suas necessidades.
D oferecer recursos disponibilizados por meio da Internet, com granularidade grossa e livre, ou seja, o cliente externo aloca o necessário para sua empresa de forma gratuita.

Questão 48

Assinale a opção que apresenta o modelo de serviços na nuvem em que o cliente, para usufruto do serviço, deve instalar e configurar, por conta própria, os recursos necessários, como compiladores, banco de dados e o próprio sistema operacional.

A IaaS (*Infrastructure as a Service*)
B CaaS (*Containers as a Service*)
C SaaS (*Software as a Service*)
D PaaS (*Platform as a Service*)

Questão 49

Em relação ao COBIT 2019, julgue os itens a seguir.

I A versão do COBIT lançada em 2019 possui um conjunto de objetivos de controle para auxiliar a auditoria financeira a lidar mais bem com ambientes relacionados à tecnologia da informação.

II Na publicação **COBIT 2019 Framework — Introdução e Metodologia**, são detalhados os princípios-chave da governança e é explicada a estrutura geral do *framework* do COBIT, incluído seu modelo essencial.

III A versão de 2019 do COBIT teve como inovação as áreas de foco, que possibilitam definir áreas e temas na empresa para os quais os esforços da governança devem ser direcionados, como a segurança cibernética e a privacidade de dados.

Assinale a opção correta.

A Apenas o item I está certo.
B Apenas o item II está certo.
C Apenas os itens I e III estão certos.
D Apenas os itens II e III estão certos.

Questão 50

Para uma efetiva gestão de riscos, é preciso, inicialmente, fazer o levantamento das ameaças e seus impactos, da probabilidade de concretização das ameaças e dos riscos potenciais. Para a implementação da gestão de riscos, devem ser considerados três níveis, cujas respectivas finalidades são

I garantir a adequação técnica necessária ao tratamento adequado dos riscos;

II assegurar que as atividades que compreendem a gestão de riscos sejam consideradas de forma sistemática; e

III permitir que os funcionários e dirigentes identifiquem suas responsabilidades, conheçam os riscos e possam ajudar a reduzi-los e controlá-los.

No texto precedente, os itens I, II e III apresentam as funções, respectivamente, dos níveis

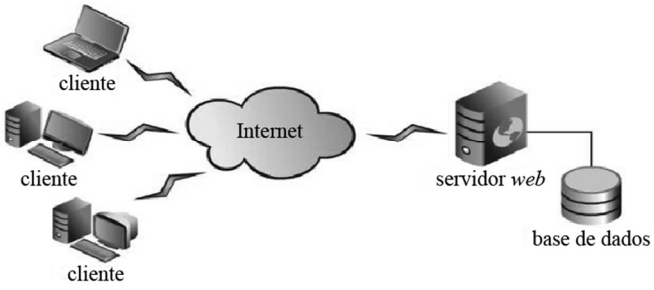
A ativos, ameaças e impactos.
B *hardwares*, *softwares* e dados.
C tecnologias, processos e pessoas.
D de importância, grau de severidade das perdas e custos envolvidos.

Questão 51

Na avaliação de riscos, procura-se uma base que sirva para efeitos de comparação, como a análise e a avaliação de riscos efetuadas em épocas anteriores. O conhecimento prévio de impactos e probabilidades de riscos é sempre relevante para uma avaliação adequada e completa. Por outro lado, há basicamente dois modos de realizar a avaliação de riscos, os quais se baseiam

A no controle e na classificação de recursos computacionais.
B nas estimativas quantitativa e qualitativa.
C no custo e benefício.
D nos níveis de tecnologia e processos.

Questão 52



Com base no modelo apresentado nessa figura, julgue os itens a seguir.

I Um servidor é um *host* que executa um ou mais serviços que compartilham recursos com os clientes. Um cliente não compartilha nenhum de seus recursos, mas solicita um conteúdo ou uma função do servidor.

II O modelo apresentado é chamado cliente-servidor, uma estrutura de aplicação que distribui tarefas e cargas de trabalho entre os fornecedores de um recurso ou serviço, designados como servidores, e os requerentes dos serviços, designados como clientes.

III No modelo apresentado, há dois processos envolvidos: um na máquina cliente e um na máquina servidora. A comunicação toma a forma do processo cliente, enviando-se uma mensagem pela rede ao processo servidor. Então, o processo cliente espera por uma mensagem em resposta. Quando o processo servidor recebe a solicitação, ele executa o trabalho solicitado ou procura pelos dados solicitados e envia de volta uma resposta.

Assinale a opção correta.

A Apenas os itens I e II estão certos.
B Apenas os itens I e III estão certos.
C Apenas os itens II e III estão certos.
D Todos os itens estão certos.

Questão 53

Assinale a opção que corresponde ao processo de identificação, classificação e tratamento das vulnerabilidades, em que o tratamento consiste ou na correção da vulnerabilidade e aplicação de controles para minimizar a probabilidade de exploração ou o impacto, ou na aceitação do risco.

A gestão de vulnerabilidades
B gestão de incidentes de segurança da informação
C *scanner* de vulnerabilidades
D auditoria de sistemas de informação

Questão 54

Na gestão de continuidade de negócios, o plano de continuidade de negócios

A deve ser testado ao menos uma vez, devendo os testes garantir que só uma fração dos integrantes da equipe de recuperação e outros funcionários relevantes possuam conhecimento dos planos.
B deve contemplar, em sua estrutura, ao menos responsabilidades coletivas requeridas e procedimentos de aplicação rotineira.
C deve ser integralmente implementado pela equipe de gerência de segurança e, posteriormente, avaliado pelos dirigentes da organização.
D deve passar por manutenção em intervalos regulares de tempo e ser atualizado em virtude de mudanças nos negócios, alteração na legislação e aquisição de novos equipamentos e sistemas.

Questão 55

De acordo com a ABNT NBR ISO/IEC 27005, assinale a opção que indica o processo de gestão de riscos de segurança da informação que prevê a identificação dos riscos, bem como sua priorização qualitativa, quando se usam como entradas, por exemplo, seu escopo e seus limites.

A aceitação do risco de segurança da informação
B tratamento do risco de segurança da informação
C análise/avaliação de riscos de segurança da informação
D comunicação do risco de segurança da informação

Questão 56

Conforme a NBR ISO/IEC 27001:2013, no cumprimento dos requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação (SGSI), a organização deve determinar os limites e a aplicabilidade do SGSI para estabelecer o seu escopo, devendo, assim, considerar

A os métodos aplicáveis para monitoramento, medição, análise e avaliação, a fim de assegurar resultados válidos.
B o processo pelo qual a comunicação será realizada.
C implicações da não conformidade com os requisitos do sistema de gestão de segurança da informação.
D interfaces e dependências entre as atividades desempenhadas pela organização e as desempenhadas por outras organizações.

Questão 57

Na gestão de riscos, o tratamento de riscos

A corresponde à seleção e implementação de medidas para modificar determinado risco.
B identifica e estima riscos, considerando o uso sistemático de informações, além de englobar a análise de ameaças, vulnerabilidades e impactos.
C compreende todas as ações tomadas para controlar os riscos em uma organização, incluindo-se análise/avaliação, tratamento, aceitação e comunicação de riscos.
D compara o risco estimado na análise com critérios predefinidos, com o objetivo de identificar a importância do risco para a organização.

Questão 58

No tratamento de riscos, as medidas de segurança são classificadas em

A corretivas e preventivas, apenas.
B preventivas, orientativas e informativas.
C orientativas e informativas, apenas.
D corretivas, preventivas e orientativas.

Questão 59

A virtualização em que o mesmo *hardware* é utilizado de modo isolado e simultâneo por vários servidores, de forma consolidada, é a

A de aplicativos.
B assistida por *hardware*.
C do sistema operacional.
D de *storage*.

Questão 60

Assinale a opção correspondente ao comando que apresenta a relação de todas as contas de determinado usuário em um servidor Windows.

A `NetUserGetGroups`
B `NetUserEnum`
C `NetUserAdd`
D `NetUserGetInfo`

Questão 61

Para que apenas pessoas autorizadas tenham acesso aos dados pessoais de clientes das organizações, é correto

A fazer o gerenciamento apropriado do ciclo de vida dos dados pessoais do cliente, incluindo-se coleta, distribuição e encerramento de atributos.
B recorrer a técnicas de autenticação robustas, como as autenticações multifatoriais, o que torna dispensável a checagem da identidade do usuário.
C aplicar o princípio de maximização de dados, limitando-se a poucos indivíduos o direito de acesso aos sistemas relativos a dados pessoais.
D monitorar as sessões dos usuários que lidam com dados pessoais dos clientes, o que dispensa a realização de análise concreta no caso de um incidente.

Questão 62

No que se refere a perfis de negócio em gestão de acessos e identidades, assinale a opção correta.

A Caso o principal motivador seja aumentar a segurança, deve-se começar pela sequência dos perfis de consulta, passar aos perfis com poder de aprovação em fluxos de trabalho e, por fim, chegar aos perfis que aprovam transações financeiras e que fornecem acesso a dados sensíveis.
B Para o aumento da agilidade e da produtividade, devem-se focar, primeiramente, os perfis dos cargos de maior quantidade na empresa; em seguida, os perfis cujos cargos tenham maior rotatividade; e, por fim, os perfis mais propensos a gerar erros manuais.
C As soluções de SSO (*single sign-on*) não podem envolver uso de um servidor de diretório do padrão LDAP (Lightweight Directory Access Protocol).
D A automação do provisionamento de perfis padrão é uma das funcionalidades que mais contribui para aumentar a agilidade, a satisfação dos usuários de TI e erros operacionais.

Questão 63

Quanto ao monitoramento, à detecção e à resposta a incidentes de segurança, assinale a opção correta.

A Na etapa detecção, percebe-se um comportamento fora do padrão do sistema, razão por que se busca identificar o problema e coletar o máximo de informações possíveis para auxiliar na solução.
B A etapa preparação ocorre durante um ataque e nela se inserem ferramentas de verificação e criam-se políticas de segurança para evitar novos ataques e vazamentos de informações.
C A etapa restauração ocorre após um ataque bem-sucedido e geralmente com perda de dados e(ou) indisponibilidade de serviços, atuando na restauração sem o uso de *backups*.
D Na etapa contenção, atua-se para minimizar danos, buscando-se a prevenção a novos ataques a curto prazo e soluções para o problema a longo prazo.

Questão 64

Atualmente, as empresas de telefonia lidam com incidentes de segurança que contemplam ameaças cada vez mais populares, como ataques de *ransomware* e DDoS, os quais podem ser executados por meio de *kits* facilmente encontrados na Internet. A fim de mitigar esse tipo de problema, é recomendado

A integrar os produtos de segurança para visualizar o cenário completo e, assim, evitar que uma violação seja perdida.
B conhecer o ambiente de rede para determinar o impacto e o alcance de um incidente de segurança, o que não implica saber quantos servidores, aplicativos e dispositivos existem na organização.
C garantir que as entidades conectadas ao ambiente de rede, salvo raras exceções, estejam alinhadas aos protocolos de políticas de segurança.
D adotar uma postura reativa com relação à segurança, já que esse é o único modo de proteger o negócio.

Questão 65

As vulnerabilidades relativas à área de segurança do tipo *hardware* incluem

A ausência de um controle eficiente de mudança de configuração.
B ausência de uma trilha de auditoria.
C tabelas de senhas desprotegidas, sem criptografia.
D procedimentos de recrutamento inadequados.

Questão 66

A respeito de criptografia e de anonimização de dados, assinale a opção correta.

A A criptografia é o processo de codificação de uma informação legível para uma informação indecifrável para terceiros.
B O uso da anonimização dos dados não permite que ferramentas como *machine learning*, inteligências artificiais e IoT (Internet of Things) realizem manipulações nos dados sem que haja quebra de privacidade.
C O processo de criptografia realiza a codificação das informações por meio de seu descarte no conjunto final de dados criptografados.
D A anonimização dá origem ao dado anonimizado, que, por sua vez, é sinônimo de dado pessoal, caracterizado como aquele capaz de identificar uma pessoa.

Questão 67

Tendo como referência o plano de conscientização de segurança, assinale a opção correta.

A Com o referido plano, espera-se diminuir os riscos associados à divulgação de dados confidenciais e aumentar a exploração de vulnerabilidades no que se refere tanto a empregados quanto a sistemas computacionais, circunstâncias em que o fator humano é decisivo.
B Nos sistemas de informação em uma empresa, as pessoas (funcionários e colaboradores) são a parte mais forte no que se refere à proteção dos ativos de informação da empresa.
C Em uma organização, compreende-se que somente a área de TI pode tornar obrigatórios os esforços de conscientização de segurança.
D O plano referido objetiva minimizar os riscos relacionados à segurança da informação, por meio de processo de conscientização e aprendizado sobre diversos mecanismos que possam causar problemas.

Questão 68

Um funcionário de uma universidade, ao visualizar um anexo de *email*, possibilitou que um *software* mal-intencionado tivesse acesso a dados sigilosos armazenados em seu computador.

Tendo como referência inicial essa situação hipotética, assinale a opção correta, a respeito do plano de conscientização de segurança.

A A universidade necessita de uma política de segurança cibernética, viabilizada por meio de treinamentos, campanhas de conscientização e outros métodos educacionais que alcancem todos os setores, a fim de prevenir incidentes e proporcionar o uso responsável das tecnologias.
B Um programa de conscientização de segurança não será significativamente menos dispendioso do que outras medidas de segurança, como aquisição de tecnologias específicas de proteção ou contratação de uma empresa externa para conduzir treinamentos de segurança.
C Para evitar o tipo de caso em tela, seria pouco profícuo desenvolver um programa eficiente de treinamento, já que esse recurso é um meio pouco econômico de reduzir riscos, especialmente quando foca na conscientização sobre segurança cibernética.
D Investir no desenvolvimento de um programa de treinamento de conscientização sobre segurança não é uma prioridade no que se refere a processos de identificação e de prevenção do tipo de ataque em questão.

Questão 69

A respeito da política de segurança da informação (PSI), assinale a opção correta.

A Acordos, contratos, convênios e outros instrumentos congêneres celebrados por empresas que adotam políticas de segurança da informação não necessariamente têm de estar de acordo com a PSI.
B A PSI deve ser avaliada periodicamente, a fim de garantir o cumprimento dos requisitos de segurança da informação e o respeito à cláusula de responsabilidade e sigilo.
C A PSI não pode conter informações dos tipos de bloqueio e restrições a *sites* e acesso à Internet.
D A PSI é um documento restrito e acessível somente à alta direção das organizações, a qual o acessa para nortear suas ações.

Questão 70

Na elaboração de políticas, diretrizes e procedimentos de segurança da informação, é correto

A assegurar que as contínuas avaliações de riscos de segurança da informação produzam resultados únicos, não comparáveis, válidos e consistentes.
B estabelecer e manter critérios de aceitação do risco, de acordo com os padrões mundiais, independentemente do tipo da cultura da empresa.
C realizar o processo de avaliação do risco de segurança da informação para identificar os riscos associados à perda de confidencialidade, integridade e disponibilidade da informação.
D avaliar a probabilidade realística da ocorrência dos riscos não identificados.

Questão 71

Entre as diretrizes para a implementação da segurança de perímetro, utilizada para proteger instalações de processamento de informação, inclui-se

A implantar uma área de recepção para controlar o acesso físico.
B fazer a manutenção de equipamentos em intervalos recomendados pelos fabricantes.
C segregar cabeamento de comunicação de dados do cabeamento de energia.
D manter os equipamentos de telecomunicação em conformidade com a especificação de fabricantes.

Questão 72

Uma área de escritório de determinada empresa é definida como de alta criticidade, tal que somente uma pequena parte de funcionários deve ter acesso às informações confidenciais utilizadas nesse ambiente.

Nessa situação, para controlar a segurança física na área em questão, é correto

A utilizar instalação física discreta com a menor indicação possível, fora ou dentro do edifício, sobre as atividades do escritório.
B eliminar o uso de fotocopiadoras e máquinas fotográficas.
C identificar e autorizar claramente os funcionários e fornecedores que podem remover ativos desse local.
D utilizar equipamentos com proteção contra a exposição a campos eletromagnéticos intensos.

Questão 73

Em relação a controles de segurança em uma organização, assinale o requisito aderente a uma arquitetura de *zero trust*.

A Os acessos concedidos devem ser registrados e revisados em intervalo mínimo de seis meses.
B As comunicações de maior criticidade devem ser identificadas, para que seja implementada a proteção na comunicação exclusivamente dessa rede objetivando melhor eficiência.
C Os acessos a recursos empresariais individuais devem ser feitos com o mínimo de privilégios e concedidos por sessão.
D Os privilégios de acesso a recursos podem ser feitos com base em modelos previamente definidos ou replicados das permissões de outros usuários já existentes.

Questão 74

Em uma arquitetura *zero trust* para proteção de perímetro, o elemento lógico que tem a função de tomar a decisão final de acesso a um recurso para determinada ação denomina-se

A *policy engine.*
B *policy administrator.*
C *continuous diagnostics and mitigation*.
D *policy enforcement point.*

Questão 75

Com base na NBR ISO/IEC 27002, ao elaborar uma política de becape para se proteger contra a perda de dados, uma organização deve considerar

A o *software* de automação dos becapes.
B o tamanho da mídia para armazenamento.
C a proteção com encriptação dos dados.
D a identificação do usuário dono dos dados.

Questão 76

De acordo com a NBR ISO/IEC 27002, uma política de becape que busque validar a integridade dos dados copiados deve

A registrar a lista de mídias com dados de cópia de segurança.
B armazenar as mídias com temperaturas definidas pelo fabricante.
C armazenar as cópias em localidade física diferente de onde se encontram os dados originais.
D testar a restauração dos dados em intervalos de tempo planejados.

Questão 77

Em uma política de becape que considere a abrangência e a frequência na geração de cópias para determinado volume de dados, o formato que proporciona o menor tempo de cópia e espaço para armazenamento é o

A incremental.
B parcial.
C completo.
D diferencial.

Questão 78

Determinado serviço está sendo publicado e necessita de elevada disponibilidade; por isso, foram instalados servidores adicionais para que, em caso de falhas, o serviço seja instantaneamente alternado para eles, garantindo-se a continuidade do funcionamento. Nessa situação, foi utilizado o mecanismo de

A *failover*.
B elasticidade.
C rede definida por *software*.
D balanceamento de carga.

Questão 79

Um certificado digital foi compartilhado para troca de *emails* entre duas pessoas de forma segura; antes da comunicação, o certificado precisou de um canal seguro para ser compartilhado entre os participantes da comunicação, a fim de que ambos pudessem ter o mesmo certificado.

Nessa situação, é correto afirmar que

A faltou mecanismo para garantir integridade da comunicação.
B foi utilizada criptografia simétrica.
C aconteceu decodificação na origem e codificação no destino.
D faltou a chave pública ser compartilhada.

Questão 80

Se um documento recebeu assinatura digital, então essa ação

A comprova a autenticidade da informação.
B garante a confidencialidade do documento.
C permite codificar o documento, por meio de uma chave pública.
D permite que todos os visualizadores do documento codifiquem a informação.