Trabalho segurança da informação

Comprovação da realização de atividades complementares.

Aluno: Lucas Vinicius Silveira (202402390562)

Questão 1

(2019 - Instituto UniFil - Prefeitura de Cambé/PR - psicólogo) A segurança da informação está relacionada à proteção de um conjunto de dados no sentido de preservar os valores que possuem para um indivíduo ou uma organização. O conceito se aplica a todos os aspectos de proteção de informações e dados. O conceito de segurança informática ou segurança de computadores está intimamente relacionado com ele, incluindo não apenas a segurança dos dados/informação, mas também a dos sistemas em si. Assinale a alternativa que não representa um dos princípios da segurança da informação.

A	Confidencialidade
B	Integridade
C	Permutabilidade
D	Disponibilidade
E	Irretratabilidade

Parabéns! A alternativa C está correta.

Os principais pilares da segurança da informação são a confidencialidade, integridade e disponibilidade. Há os complementares, como a autenticidade, a legalidade e o não repúdio.

Questão 2

(2019 - IDECAN - IF-AM - bibliotecário documentalista) A segurança da informação está baseada em três pilares: confidencialidade, integridade e disponibilidade. Com base nessa informação, analise as afirmativas a seguir.

I. Garantir o acesso por pessoa ou dispositivo devidamente autorizado a todo hardware, software e dados sempre que necessário.

II. As informações devem ser armazenadas da forma como foram criadas, de modo que não sejamcorrompidas ou danificadas.

III. As informações não poderão ser vistas ou utilizadas sem as devidas autorizações de acesso por pessoas ou dispositivos.

Assinale a alternativa que apresente a ordem correta de associação com os três pilares da segurança da informação.

A	I - Disponibilidade; II - Integridade; III - Confidencialidade.
B	I - Confidencialidade; II - Integridade; III - Disponibilidade.
C	I - Integridade; II - Confidencialidade; III - Disponibilidade.
D	I - Confidencialidade; II - Disponibilidade; III - Integridade.
E	I - Disponibilidade; II - Confidencialidade; III - Integridade.

Questão 3

(2020 - IDIB - Prefeitura de Colinas do Tocantins/TO - engenheiro civil) Em se tratando de segurança da informação, a literatura da área de tecnologia da informação elenca três prioridades básicas. Essas três prioridades também são chamadas de pilares da segurança da informação. Assinale a alternativa que indica corretamente o nome da prioridade básica relacionada ao uso de recursos que visam restringir o acesso às informações.

A	Inviolabilidade
B	Confidencialidade ✓
C	Acessibilidade
D	Invulnerabilidade
E	Indisponibilidade

Parabéns! A alternativa B está correta.

Os principais pilares da segurança da informação são a confidencialidade, integridade e disponibilidade. Há os complementares, como a autenticidade, a legalidade e o não repúdio.

Questão 4

A internet foi criada no final da década de 1990 nos laboratórios do CERN pelo físico britânico Tim Berns-Lee. Desde aquele tempo, diversas criações vieram moldando as gerações subsequentes. Atualmente, destacam-se as imagens na internet conhecidas como memes. Alguns deles têm um caráter educativo, ensinando, de forma lúdica, algumas práticas que não devem ser seguidas. Uma delas é o manuseio de senhas.

Na verdade, a ideia é ensinar ao usuário a manusear sua senha de forma correta, não a deixando, por exemplo, embaixo do teclado. No meme do tapete que fala, o objetivo é ensinar ao usuário como manejá-la corretamente. Marque o item que integra esse ensinamento.

A	Confidencialidade	✓
B	Disponibilidade	
C	Integridade	
D	Irretratabilidade	
E	Criptografia	

Parabéns! A alternativa A está correta.

A confidencialidade está relacionada à manutenção de uma informação passível de ser observada, lida ou acessada apenas por quem tem direito. Em outras palavras, é semelhante a deixar uma conta de e-mail aberta para que qualquer pessoa possa lê-la sem precisar da senha (chave embaixo do tapete, senha embaixo do teclado).

Questão 5

Alguns anos após sua aposentadoria, Bill resolve estudar para obter uma certificação de segurança. Ele e seu vizinho de porta, Steve, que também gostaria de tirar a tão sonhada certificação, resolvem criar mnemônicos para decorar os assuntos.

Para decorar os pilares da segurança da informação, eles criam o seguinte mnemônico: "Cresci vendo televisão. Sempre achei o CID muito seguro ao narrar as reportagens". Bill e Steve criaram vários mnemônicos. No dia seguinte, houve a prova de certificação. Sua primeira questão versava sobre os pilares. A ideia do mnemônico deu certo, mas eles esqueceram o que representava cada letra.

Você resolve explicar para eles o significado de cada uma. Marque a alternativa que apresenta os termos corretos.

A	Confidencialidade, integridade e disponibilidade.	✓
B	Confiabilidade, integridade e disponibilidade.	
C	Confiabilidade, integridade e disponibilidade.	
D	Confiabilidade, integridade e dedutibilidade.	
E	Confidencialidade, disponibilidade e integridade.	

Parabéns! A alternativa A está correta.

C é de confidencialidade: a capacidade do acesso à informação apenas por aqueles que possuem autorização; I, de integridade: a possibilidade de alteração da informação por

Questão 1

Ao realizarmos o download de uma ISO de um software, normalmente usamos as funções de hash. Marque a alternativa que apresenta o pilar da segurança da informação que corresponde ao uso dessas funções.

A	Confidencialidade
B	Integridade ✓
C	Disponibilidade
D	Legalidade
E	Integralidade

Parabéns! A alternativa B está correta.

As funções de *hash* criam um conjunto de valores alfanuméricos que representa a informação. Alterando-se um bit da informação, normalmente todo o conjunto de valores é alterado. Dessa forma, assegura-se de que não haverá alteração da informação.

Questão 2

Constitui um dever de todo cidadão elaborar anualmente o imposto de renda. Com o advento da internet, a nossa declaração agora pode ser enviada diretamente para os servidores do governo. No início dessa metodologia, era comum haver notícias nos telejornais sobre os servidores não aguentaram e se desligarem sozinhos. Marque a alternativa que apresenta o pilar da segurança da informação que denomina perfeitamente tal situação.

A	Confidencialidade
B	Integridade
C	Disponibilidade
D	Conformidade
E	Confiabilidade

Parabéns! A alternativa C está correta.

Quando os servidores foram desligados, pararam de funcionar; com isso, tornaram-se indisponíveis.

Questão 1

(2019 - IF-BA - assistente em administração) A respeito dos conceitos que envolvem a segurança da informação, analise as afirmativas a seguir.

I.Os mecanismos de segurança podem ser lógicos ou físicos.
II. A perda de confidencialidade, integridade e disponibilidade é um exemplo dos eventos que comprometem a segurança da informação.
III. Assinatura digital, encriptação e firewall são exemplos de mecanismos lógicos de segurança.

Assinale:

A	Se somente as afirmativas I e II estiverem corretas.
B	Se somente a afirmativa II estiver correta.
C	Se somente a afirmativa I estiver correta.
D	Se todas as afirmativas estiverem corretas. ✓
E	Se nenhuma das afirmativas estiver correta.

Parabéns! A alternativa D está correta.

Mecanismos ou controles de segurança podem ser lógicos e físicos. A segurança da informação é baseada em três aspectos fundamentas: confidencialidade, integridade e disponibilidade. Desse modo, a perda de qualquer um dos três aspectos já impacta na segurança. A pior situação ocorre quando perdemos os três juntos: trata-se praticamente

Questão 2

(2019 - Comperve - UFRN - analista de tecnologia da informação) A segurança computacional possui uma terminologia própria. Uma padronização na utilização dessa terminologia garante o correto entendimento entre os diferentes agentes envolvidos. Em relação a isso, considere as seguintes afirmações sobre a segurança computacional.

I. A segurança física visa providenciar mecanismos para restringir o acesso às áreas críticas da organização a fim de garantir a integridade e a autenticidade dos dados.
II. Uma ameaça pode ser definida como algum evento que pode ocorrer e acarretar algum perigo a algum ativo da rede. As ameaças podem ser intencionais ou não intencionais.
III. São ameaças mais comuns às redes de computadores o acesso não autorizado, o reconhecimento (ex.: PortScan) e a negação de serviço (ex.: DoS ou DDoS).
IV. O "tripé da segurança" é formado de pessoas, processos e políticas de segurança. De nada adianta uma política do tipo se as pessoas e os processos não forem considerados.

Em relação à segurança computacional, estão corretas as afirmativas:

A	III e IV.
B	II e IV.
C	II e III. ✓
D	I e II.
E	I e III.

Questão 3

(2016 - CESPE /Cebraspe - TRT - 8ª Região - analista judiciário - tecnologia da informação) Correspondem a itens capazes de oferecer controle ou proteção no âmbito da segurança física preventiva:

A	As chaves públicas criptográficas.
B	Os dispositivos de autenticação biométrica. ✓
C	Os sistemas de autenticação por senhas *single sign on*.
D	Os certificados digitais.
E	Os sistemas de Firewall.

✓

Parabéns! A alternativa B está correta.

A segurança física está relacionada ao acesso às dependências das instalações; a lógica, aos algoritmos que protegem os dados.

Questão 4

(2013 - FCC - TRT - 9ª Região - técnico judiciário – segurança) Convém que sejam utilizados perímetros de segurança (barreiras, como paredes, portões de entrada controlados por cartão ou balcões de recepção com recepcionistas) para proteger as áreas que contenham informações e instalações de processamento da informação. Além disso, que sejam levadas em consideração e implementadas as seguintes diretrizes para perímetros de segurança física, quando apropriado:

I. Os perímetros de segurança devem ser claramente definidos, assim como a localização e capacidade de resistência de cada perímetro precisam depender dos requisitos de segurança dos ativos existentes no interior do perímetro e dos resultados da análise/avaliação de riscos.
II. Os perímetros de um edifício ou de um local que contenha instalações de processamento da informação precisam ser fisicamente sólidos (ou seja, o perímetro não deve ter brechas nem pontos onde poderia ocorrer facilmente uma invasão).
III. Deve-se implantar uma área de recepção ou outro meio para controlar o acesso físico ao local ou ao edifício. Esse acesso deve ficar restrito somente ao pessoal autorizado.
IV. Devem ser construídas barreiras físicas para impedir o acesso físico não autorizado e a contaminação do meio ambiente.

Está correto o que se afirma em:

A	II, III e IV.
B	I, II e III.
C	II e III.
D	I, II, III e IV. ✓
E	I e III.

Questão 5

Ao projetar uma rede, é comum adotar um firewall para proteger uma rede interna. Com relação ao papel do firewall, marque a opção que apresenta uma forma correta de classificar esse ativo de TIC.

A	Segurança lógica
B	Segurança física
C	Segurança patrimonial
D	Segurança empresarial
E	Nenhuma das alternativas

Parabéns! A alternativa A está correta.

O firewall é um importante ativo de rede; desse modo, encontrá-lo em um projeto de rede torna-se imprescindível. Ele protege uma rede interna analisando e bloqueando, por meio de algoritmos proprietários de cada marca, o acesso e o transporte de dados para dentro dela. Por manipulá-los, este ativo é classificado como segurança lógica.

Questão 6

A partir da pandemia ocorrida em 2020, os sistemas de acesso evoluíram para o uso de reconhecimento facial. Muitos desses sistemas possuem slogans bem criativos, como este: "Um sistema de acesso com reconhecimento facial permite levar a sua empresa diretamente para o mundo da alta tecnologia por meio do uso desta importante ferramenta de segurança: _____".

Marque a alternativa que apresenta o termo que completa o slogan anterior de forma mais satisfatória.

A	Lógica
B	Física ✓
C	Mista
D	Empresarial
E	Patrimonial

Parabéns! A alternativa B está correta.

Um sistema de acesso, independentemente do tipo de chave (senha) criado, permite o bloqueio físico a determinado local. Esta chave (senha), com o passar do tempo, vem evoluindo bastante: cartões com códigos de barra, tarja magnética, digital, veias da mão e, agora, reconhecimento facial.

Questão 1

(2019 - FCC - TRF - 4ª Região - analista judiciário - sistemas de tecnologia da informação) Suponha que um analista do Tribunal Regional Federal da 4ª Região se depare com uma situação em que deve implantar mecanismos de proteção interna voltados à segurança física e lógica das informações no ambiente do tribunal. Para isso, ele levantou os seguintes requisitos:

I. Não instalar em áreas de acesso público equipamentos que permitam o acesso à rede interna do tribunal.
II. Os usuários não podem executar transações de TI incompatíveis com sua função.
III. Apenas usuários autorizados devem ter acesso ao uso dos sistemas e aplicativos.
IV. É necessário proteger o local de armazenamento das unidades de backup e restringir o acesso a computadores e impressoras que possam conter dados confidenciais.

O analista classificou correta e respectivamente os requisitos de I a IV como uma segurança:

A	física, física, lógica e física.
B	física, lógica, lógica e física. ✓
C	lógica, física, lógica e física.
D	lógica, física, física e lógica.
E	física, lógica, lógica, lógica.

Parabéns! A alternativa B está correta.

Questão 2

(2018 - Cesgranrio - Transpetro - analista de sistemas júnior - processos de negócio) Para proteger as redes de dados, as empresas criam perímetros de segurança formados por componentes que avaliam o tráfego de ingresso e egresso. O componente que utiliza listas de controle de acesso formadas por regras que determinam se um pacote pode ou não atravessar a barreira é a(o):

A	firewall.	✓
B	proxy.	
C	DMZ.	
D	IPS.	
E	roteador.	

Parabéns! A alternativa A está correta.

O firewall usa as regras para criar barreiras e políticas relacionadas.

Questão 1

(IADES – 2019 – CRF-TO – Analista de TI) "[...] é uma fraqueza de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças" (HINTZBERGEN, 2018). A definição apresentada refere-se ao conceito de:

A	Exposição
B	Salvaguarda
C	Vulnerabilidade ✓
D	Risco
E	Impacto

Parabéns! A alternativa C está correta.

Como pudemos verificar neste módulo, "vulnerabilidades" e "fraquezas" são conceitos que estão intimamente relacionados.

Questão 2

Considere o ataque às torres gêmeas ocorrido em Nova York. Marque a opção que não apresenta uma possível classificação àquela ameaça.

A	Lógica
B	Humana
C	Infraestrutura
D	Terrorista
E	Física

Parabéns! A alternativa A está correta.

O ataque às torres gêmeas ocorreu quando aviões comerciais foram sequestrados por grupos terroristas; assim, foi uma ameaça física, humana, que nesse contexto é sinônimo de terrorista e infraestrutura.

Questão 1

(IBFC – 2018 – Câmara de Feira de Santana-BA – Técnico de Suporte em Informática) É um software nocivo do tipo spyware, cuja finalidade é registrar tudo o que é digitado, quase sempre a fim de capturar senhas, números de cartão de crédito e afins. Essa é a descrição técnica do:

A	Datalogger
B	Keycutter
C	Datacutter
D	Keylogger ✓
E	Trashing hash

Parabéns! A alternativa D está correta.

As letras B e C não existem e Datalogger e Trashing hash não está relacionado com segurança.

Questão 2

(CESGRANRIO – 2018 – Transpetro – Analista de Sistemas Júnior – Infraestrutura) O código malicioso que visa criptografar os dados das vítimas e cobrar pagamento de resgate pela chave e pelo código de decriptação é classificado como um:

A	Worm
B	Spyware
C	Ransomware
D	Trojan Horse
E	Wardriving

Parabéns! A alternativa C está correta.

Worm é um malware que se prolifera sozinho através de compartilhamentos de rede. Spyware captura o comportamento do usuário e envia para um atacante. Cavalo de Troia, ou trojan horse, é uma técnica em que um software malicioso se faz passar por outro software.

Questão 1

Qual palavra é citada frequentemente na Norma ISO/IEC 27001, que constitui sua característica marcante?

A	Convém
B	Recomenda
C	Deve
D	Espera
E	Sugere

Parabéns! A alternativa C está correta.

Orientações do que **deve** ser feito. Os requisitos definidos nesta norma são genéricos e é pretendido que sejam aplicáveis a todas as organizações, independentemente de tipo, tamanho e natureza. A exclusão de quaisquer dos requisitos especificados nas seções de 4 a 10 na versão 2013 não é aceitável quando uma organização reivindica conformidade com esta norma.

Questão 2

Marque a alternativa correta quanto à afirmação sobre a Norma ISO/IEC 27002.

A	A palavra-chave que determina a sua principal característica é DEVE.
B	A relevância de qualquer controle deve ser determinada segundo os riscos específicos a que uma organização está exposta. ✓
C	Todos os controles são importantes e devem ser considerados.
D	Eventuais controles adicionais e recomendações que a comissão de segurança da organização deseja implementar, mas que não estejam incluídos na norma, devem ser desconsiderados.
E	Controles são definidos por empresas especializadas.

Parabéns! A alternativa B está correta.

A norma contém orientações do que **convém** ser feito. Embora todos os controles sejam importantes e devam ser considerados, a relevância de qualquer controle deve ser determinada segundo os riscos específicos a que uma organização está exposta. Nem todos os controles e diretrizes contidos na norma podem ser aplicados, e controles adicionais e recomendações não incluídos podem ser necessários. Ela possui 35 objetivos de controles e 114 controles básicos distribuídos em 14 seções.

Cenas/Ocorrência	Registro de não conformidade (NC)		
	Req. ISO/IEC 27001	Existe NC?	Descrição da NC e da evidência objetiva ou indicação do que fazer a seguir
Um dos auditores internos é responsável pela administração do banco de dados em um setor. Como na auditoria metade da equipe da empresa viajou para treinamento do novo sistema, ele acabou auditando também a sua área, incluindo partes do seu trabalho.		( ) Sim ( ) Não ( ) Simples Obs. ( ) Falta informação	

Marque a alternativa que representa o parecer mais adequado do auditor para a descrição da cena.

A	Existe não conformidade, os auditores não devem auditar seu próprio trabalho.
B	A descrição é uma simples observação para uma descrição importante que ainda não foi feita.
C	A prática está em conformidade com a norma, tendo em vista a possibilidade de a equipe ser pequena e o funcionário possuir competência para tal.
D	Faltam as informações se esse fato estava previsto nos critérios dessa auditoria e se a imparcialidade foi assegurada.
E	É preciso aprimorar a prática para se adequar à norma.

Parabéns! A alternativa D está correta.

Na realidade, todas as respostas podem estar corretas, mas conforme já informado, iremos analisar com as sugestões e premissas estabelecidas no primeiro exemplo.

Questão 2

Leia a notícia a seguir extraída de um site da web, para aplicação dos itens da Norma ABNT NBR ISO/IEC 27002:2013:

Quando o Deutsche Bank perdeu seus escritórios nos ataques de 11 de setembro, os funcionários puderam acessar o e-mail corporativo no dia seguinte para que pudessem se conectar com clientes e colegas de trabalho em casa. "Tivemos acesso aos nossos arquivos, embora a TI estivesse na Torre Dois do World Trade Center", diz uma fonte. "Tivemos backup em Jersey City. Não perdemos nada. Tenho amigos que trabalham em empresas menores que não ficaram dois meses sem poder ir ao escritório. O escritório de advocacia de um amigo faliu" (DEUTSCHE BANK, 2009).

Este relato de adoção de medidas de proteção, nestes termos, poderá ser melhor enquadrado no item da Norma ISO/IEC 27002:2013.

A	7.1: Antes da contratação, dentro do item 7, *Segurança em Recursos Humanos*.
B	9.2: Gerenciamento de acesso do usuário, dentro do item 9, *Controle de Acesso*.
C	10.1: Controles criptográficos, dentro do item 10, *Criptografia*.
D	17.1: Continuidade da segurança da informação, dentro do item 17, *Aspectos da segurança da informação na Gestão da Continuidade do Negócio*.
E	9.4.1: Restrição de acesso à informação.

Parabéns! A alternativa D está correta.

Este é um relato jornalístico que carece de detalhes, mas usaremos para fins didáticos. Também faltam os subitens de cada uma das subseções citadas, mas a análise do exercício ficaria muito extensa. Para melhor enquadramento a um item da Norma ISO/IEC

Questão 1

Um funcionário de uma organização resolveu adotar o número de sua matrícula como senha. Marque a alternativa que apresenta a postura que deve ser adotada pela empresa para evitar essa situação:

A	A organização deve sugerir um padrão de senhas.
B	A organização não deve fazer nada, pois a responsabilidade pela senha é do funcionário.
C	A organização deve implementar um sistema que verifique se a senha atende a determinados pré-requisitos. ✓
D	A organização deve obrigar que os funcionários mudem suas senhas periodicamente.
E	Criar mais de uma matrícula para cada um dos funcionários.

✓

Parabéns! A alternativa C está correta.

O responsável pelo cadastro das senhas pode implementar um programa para evitar

Questão 2

Selecione a opção que apresenta algumas das recomendações de treinamento em conscientização de segurança que podem ser implementadas nas organizações:

A	Escolher indivíduos específicos para treinar.
B	A responsabilidade pela segurança da informação é apenas dos funcionários, portanto a organização não deve fazer nada.
C	A responsabilidade pela segurança da informação é apenas da diretoria, portanto a organização não deve fazer nada.
D	Desenvolver treinamentos e exercícios de simulação. ✓
E	Selecionar funcinários para treinamentos mediante técnicas de amostragem.

Parabéns! A alternativa D está correta.

Algumas recomendações de treinamento são:

Questão 1

Quais são os recursos que o controle de acesso visa proteger?

A	Apenas dados pessoais.
B	Apenas dados organizacionais.
C	Todos os programas da organização.
D	Todos os recursos que possam fornecer informação sobre a organização, seus funcionários, clientes e parceiros. ✓
E	Softwares estratégicos para a organização.

Parabéns! A alternativa D está correta.

Aplicativos, arquivos de dados, utilitários e sistema operacional, arquivos de senha e arquivos de log. O objetivo do controle de acesso não é proibir ou dificultar o acesso, mas

Questão 2

(Adaptado de CESPE – Polícia Federal – Papiloscopista – 2018) “São exemplos de vírus contidos em programas aparentemente inofensivos. Além disso, as suas ações são disfarçadas pelas funcionalidades do programa hospedeiro”. Considere a definição dada e selecione a opção que corresponde a esse tipo de vírus:

A	Cavalo de Troia.	✓
B	Polimórfico.	
C	Vírus *stealth*.	
D	Vírus blindado.	
E	Wardriving.	

Parabéns! A alternativa A está correta.

Questão 1

Marque a alternativa que apresenta os tipos de criptografias:

A	Chave simétrica, chave assimétrica e função Hash. ✓
B	Quântica e Hash.
C	SHA, MD5 e PCK.
D	Firewall e antivírus.
E	Criptografia transsimétrica

✓

Parabéns! A alternativa A está correta.

Criptografia de chave simétrica, criptografia de chave assimétrica e função Hash. O motivo da existência de três tipos de criptografia é que cada esquema é otimizado para alguma aplicação específica. As funções de hash, por exemplo, são adequadas para garantir a

Questão 2

Selecione a opção que apresenta todos os itens que compõem um certificado digital:

A	Nome do titular do certificado, biometria, o indivíduo ou a entidade identificada pelo certificado, datas de expiração, cópia da chave pública do detentor de certificado.
B	Nome do titular do certificado, número de série usado para identificar exclusivamente um certificado, o indivíduo ou a entidade identificada pelo certificado, datas de expiração, cópia da chave pública do detentor de certificado. ✓
C	Nome do titular do certificado, número de série usado para identificar exclusivamente um certificado, o indivíduo ou a entidade identificada pelo certificado, datas do envio do certificado, cópia da chave pública do detentor de certificado.
D	Nome do titular do certificado, número de série usado para identificar exclusivamente um certificado, o indivíduo ou a entidade identificada pelo certificado, datas de expiração, trechos criptografados da mensagem.
E	Nome do titular do certificado, chave criptográfica, data de nascimento, nome da mãe, datas deenvio do certificado, entidade identificada pelo certificado.

Parabéns! A alternativa B está correta.

Questão 1

Imagine que uma pessoa não autorizada conseguiu invadir o datacenter de uma organização corporativa que possui roteadores e servidores. Dentro dos termos relacionados à segurança da informação, esta pessoa, para a corporação, pode ser considerada:

A	Impacto
B	Vulnerabilidade
C	Controle
D	Ameaça ✓
E	Stakeholder

Parabéns! A alternativa D está correta.

A norma ABNT NBR ISO/IEC 27002:2013 diz que "ativos são objeto de ameaças tanto acidentais como deliberadas. [...] em função das várias maneiras nas quais as ameaças podem se aproveitar das vulnerabilidades para causar dano à organização, os riscos de segurança da informação estão sempre presentes. Uma segurança da informação eficaz reduz esses riscos, protegendo a organização das ameaças e vulnerabilidades e, assim,

Questão 2

Segundo a norma ABNT NBR ISO/IEC 27001:2013, uma organização, para entender as necessidades e as expectativas das partes interessadas, "deve determinar: a) As partes interessadas que são relevantes para o sistema de gestão de segurança da informação; e b) Os requisitos dessas partes interessadas relevantes para a segurança da informação".

As partes interessadas em um sistema de gestão de segurança da informação podem ser entendidas como:

A	As pessoas que não possuem interesse na organização.
B	Os indivíduos ou grupos que se interessam pelo desempenho ou sucesso da organização. ✓
C	Pessoas que possuem interesses estritamente pessoais.
D	Outras empresas que realizam as próprias análises de risco.
E	Indivíduos promotores dos eventos de risco.

Parabéns! A alternativa B está correta.

As partes interessadas são pessoas, grupos ou organizações que podem gerar um impacto ou ser impactados pelo desempenho da organização.

Analise as afirmativas a seguir:

I - Uma vez que uma ameaça explora vulnerabilidade(s) de um ativo e causa um incidente de segurança da informação, este, por sua vez, poderá causar um impacto não desejável à organização, ou seja, uma mudança não desejável nos objetivos de negócios.
II - Se uma organização adotar o conjunto mais econômico de medidas para controlar os riscos, pode-se afirmar com toda a certeza que ela pode dispensar a utilização das etapas da gerência de riscos, pois toda a organização irá obter o nível de risco no patamar "inexistente".
III - Uma típica matriz de risco consegue apresentar graus para a medição qualitativa ou quantitativa da probabilidade, mas fica inviável apresentar graus para a medição do impacto.

Marque a alternativa que possui somente as afirmativas verdadeiras:

A	Somente II.
B	Somente I. ✓
C	I e III.
D	I, II e III.
E	I e II.

Parabéns! A alternativa B está correta.

Tabela: STALLINGS, 2015, p. 412.

Mostramos acima um levantamento das consequências de algumas ameaças para um grupo de aspectos de segurança. Na gestão de riscos, este tipo de tabela, sem levar em consideração a tomada de decisão feita após sua elaboração, pode ser um dos frutos da atividade da seguinte etapa:

A	Estabelecimento do contexto.
B	Análise dos riscos. ✓
C	Tratamento do risco.
D	Aceitação do risco residual.
E	Matriz de probabilidade *versus* impacto.

Parabéns! A alternativa B está correta.

A análise ou estimativa de riscos faz parte da etapa de processo de avaliação deles. Os objetivos desta etapa são identificar os riscos e definir o que deve ser feito para diminuí-los até um nível aceitável. Esta tabela mostra o levantamento realizado na etapa de identificação deles. Após isso, é possível realizar sua estimativa e avaliação.

Questão 1

O Plano de Continuidade de Negócios (PCN) descreve como a empresa deve atuar diante da identificação das ameaças e dos impactos nas operações a fim de garantir a preservação do negócio. Portanto, ele é essencial para a minimização das possíveis perdas. Nesse sentido, é correto afirmar sobre o PCN que:

A	É um processo corretivo.
B	É um processo preventivo. ✓
C	Apenas profissionais de determinados segmentos da organização devem participar da sua elaboração.
D	Nem sempre é necessário, pois é rara a ocorrência de desastres.
E	Considera aspectos externos e internos da organização e seu planejamento estratégico.

Parabéns! A alternativa B está correta.

Por se tratar de um plano, é imprescindível a sua elaboração prévia, além da realização de treinamentos com as pessoas envolvidas nas

Questão 2

O processo de elaboração do Plano de Continuidade de Negócios (PCN) de uma organização é complexo. Nesse sentido, selecione a opção correta a respeito do PCN.

A	Depois de elaborado, não é necessário fazer revisões.
B	É importante para o bem-estar dos membros da organização, mas não tem impacto financeiro concreto.
C	Deve passar por revisões periodicamente para adequar-se a novos cenários. ✓
D	Como faz parte da estratégia da organização, apenas poucos membros devem ter acesso a ele.
E	Estabelece metas de emergência baseadas nos desastres previstos.

Parabéns! A alternativa C está correta.

Devido à característica dinâmica dos diversos cenários aos quais a organização é exposta e ao modo como evolui a maturidade dos processos para tratar tais cenários, o PCN deve ser revisto

Questão 1

O modelo PDCA (Plan-Do-Check-Act) é focado na melhoria contínua dos processos de uma organização. Selecione a opção que apresenta, resumidamente, como ele atinge seu objetivo:

A	Faz um mapeamento minucioso das unidades de negócios e, a partir disso, descreve detalhadamente como os processos devem ser realizados.
B	A partir da análise dos desvios do comportamento de um processo com as suas metas predefinidas, direciona quais medidas corretivas devem ser adotadas. ✓
C	Define as melhores estratégias para o negócio da organização.
D	Faz a documentação dos planos da organização baseado nos melhores padrões de mercado.
E	Contribui para o planejamento estratégico da organização estabelecendo pontos de controle e ações de efeito.

✓

Parabéns! A alternativa B está correta.

O PDCA é um modelo que considera a dinâmica em que os processos estão inseridos e como são compreendidos pelos responsáveis das

Questão 2

O Plano de Recuperação de Desastres (PRD) é um documento que define os recursos, as ações, as tarefas e os dados requeridos para administrar o processo de recuperação e de restauração dos componentes que suportam os Processos de Negócio. Selecione a opção correta em relação ao PRD.

A	Trata de ações a longo prazo.
B	Como trata de situações emergenciais, não há como medir a efetividade do seu desempenho.
C	O ponto objetivo de recuperação é a quantidade mínima de dados que uma organização está disposta a perder, caso ocorra um desastre.
D	O tempo objetivo de recuperação é o período máximo que uma organização está disposta a permitir até a retomada das suas atividades no caso de um desastre.
E	Trata das ações de emergência com uma visão prospectiva.

Parabéns! A alternativa D está correta.

O PRD é um componente do PCN. Dado um cenário de desastre, a ideia

Questão 1

Qual o propósito da Política de Gestão de Continuidade de Negócios (PGCN)?

A	Definir funções e responsabilidades das equipes envolvidas com o acionamento das ações de contingência antes, durante e após a ocorrência.
B	Determinar o planejamento para que, uma vez controlada a contingência e passada a crise, a empresa retome seus níveis originais de operação.
C	Restabelecer o funcionamento dos principais ativos que suportam as operações de uma organização, reduzindo o tempo de queda e os impactos provocados por um eventual incidente.
D	Fornecer uma base para que se possa entender, desenvolver e implementar a continuidade de negócios em uma organização. ✓
E	Realizar o alinhamento entre o plano de gerenciamento de TI e a estratégia do negócio.

Parabéns! A alternativa D está correta.

A PGCN é o conjunto dos processos e das atividades que uma

Questão 2

A respeito do Gerenciamento de Continuidade na biblioteca ITIL, é correto afirmar que:

A	Concentra-se no alinhamento de serviços de TI com as necessidades dos negócios.
B	Tem os mesmos objetivos do Plano de Continuidade de Negócios.
C	Concentra-se, principalmente, nos aspectos físicos da organização que são essenciais para dar continuidade aos negócios.
D	Sua eficácia está vinculada ao uso da tecnologia utilizada pela organização.
E	Realizar o alinhamento entre o plano de gerenciamento de TI e a estratégia do negócio.

Parabéns! A alternativa A está correta.

A biblioteca ITIL dá suporte para que as organizações atinjam seus objetivos alinhados com os serviços de tecnologia da informação mediante descrição das diversas etapas do ciclo de vida deles.