

Nas questões a seguir, marque, para cada uma, a única opção correta, de acordo com o respectivo comando. Para as devidas marcações, use a **Folha de Respostas**, único documento válido para a correção das suas respostas.

## 5 – GESTÃO DE SEGURANÇA

### QUESTÃO 1

Assinale a opção correspondente à propriedade que **não** é alcançada com o uso de técnicas da criptografia para proteção da informação.

- A integridade
- B autenticidade
- C irretratabilidade (não-repúdio)
- D confidencialidade
- E disponibilidade

### QUESTÃO 2

Os cheques são confeccionados em papel especial e um conjunto de itens de segurança, físicos e eletrônicos, são usados para a verificação da autenticidade do documento, juntamente com a assinatura do emitente, na sua liquidação ou pagamento. Os quesitos de segurança física do cheque **não** incluem

- A marca d'água.
- B leiaute e cores.
- C caracteres pequenos.
- D ausência de barras divisórias.
- E caracteres numéricos vazados com repetição em negativo.

### QUESTÃO 3

Assinale, entre as senhas apresentadas nas opções a seguir, a que é considerada mais segura, segundo as regras e os cuidados especiais pertinentes.

- A 2210Carlos, de Carlos Silva que faz aniversário em 22 de outubro
- B 139002, de um usuário cuja conta é 13900-2
- C Acvnd12d03, a partir da frase “A conta venceu no dia 12 de março”
- D Flamengo2009
- E 1122334455

### QUESTÃO 4

Com relação à classificação das informações no Banco do Brasil (BB), assinale a opção correta.

- A Informações sensíveis públicas são aquelas que podem ser divulgadas sem restrição ou por imposição legal que não expõe o BB a riscos.
- B Informações sensíveis críticas são as que devem ter suas propriedades preservadas para a continuidade dos negócios e objetivos do BB; divulgá-las indevidamente expõe a instituição a riscos elevados.
- C Informações não sensíveis restritas são aquelas que não podem ser divulgadas porque expõem o BB a riscos.
- D Informações sensíveis internas são aquelas que podem ser divulgadas sem restrição ou por imposição legal.
- E Informações sensíveis externas são aquelas que não podem ser divulgadas sem restrição ou por imposição legal.

### QUESTÃO 5

Acerca da política de segurança da informação de uma empresa, analise as asserções do seguinte enunciado.

A política de segurança e as diretrizes, as normas e os procedimentos dela decorrentes, em uma empresa, devem ser simples e de fácil compreensão,

**porque**

estão alinhados com as estratégias de negócios da empresa, padrões e procedimentos.

Assinale a opção correta a respeito desse enunciado.

- A As duas asserções são verdadeiras, e a segunda justifica a primeira.
- B As duas asserções são verdadeiras, mas a segunda não justifica a primeira.
- C A primeira asserção é falsa, e a segunda é verdadeira.
- D A primeira asserção é verdadeira, e a segunda é falsa.
- E Tanto a primeira asserção quanto a segunda são falsas.

### QUESTÃO 6

Assinale a opção que relaciona corretamente uma vulnerabilidade presente nas organizações com a respectiva classificação.

- A ausência de recursos para o combate a incêndios – vulnerabilidade natural
- B conservação inadequada de equipamentos – vulnerabilidade física
- C disposição desorganizada dos cabos de energia e de rede – vulnerabilidade de *hardware*
- D programas que permitem a execução de códigos maliciosos – vulnerabilidade de *software*
- E proximidade de rios propensos a inundação – vulnerabilidade de meios de armazenamento

**QUESTÃO 7**

O BB aplica, em suas ações de segurança de pessoas e ambientes, a teoria dos círculos concêntricos. Assinale a opção correta de acordo com essa teoria.

- A** A segurança rotineira aplica-se a áreas isentas de sensibilidade ou periculosidade, que integram os limites físicos da unidade ou instalação.
- B** Áreas de altíssima sensibilidade ou periculosidade, cujo acesso é restrito a pessoas institucionalmente envolvidas nas atividades ali desenvolvidas, estão no escopo da segurança excepcional.
- C** O controle de acesso classificado como ultrassecreto caracteriza as áreas de uma organização consideradas como de segurança elevada.
- D** São consideradas como áreas de segurança mediana os centros de processamento de dados de uma organização.
- E** O saguão das agências, nas organizações, é exemplo de área considerada como de segurança periférica.

**QUESTÃO 8**

A respeito da segurança de ambientes no BB, assinale a opção **incorreta**.

- A** O uso de ambientes como tesouraria ou bateria de caixas é vedado para finalidades que não sejam as específicas desses ambientes.
- B** O uso de alarme e CFTV é obrigatório para ambientes como o corredor de abastecimento do terminal de autoatendimento.
- C** Prestadores de serviço podem acessar áreas internas desde que estejam acompanhados por um funcionário autorizado.
- D** O acesso a ambientes internos deve ser vedado ao público, sendo, portanto, dispensável o controle de acesso efetivo a alguns deles.
- E** Salas de telecomunicação requerem controle de acesso, para que se permita a entrada apenas de pessoas que trabalhem nesses locais.

**QUESTÃO 9**

Com relação aos conceitos de gestão de segurança, assinale a opção **incorreta**.

- A** Um incidente é um fato decorrente da ação de uma ameaça que explora uma ou mais vulnerabilidades, levando a perdas.
- B** Ameaças são agentes ou condições que causam incidentes que comprometem os ativos da organização por meio da exploração de vulnerabilidades, causando impacto aos negócios.
- C** O impacto diz respeito à abrangência dos danos causados por um incidente de segurança sobre um ou mais processos de negócio.
- D** Vulnerabilidades são fragilidades presentes ou associadas a ativos que, quando exploradas por ameaças, levam à ocorrência de incidentes de segurança.
- E** Os fatores de risco operacionais permitem a quantificação da incerteza, possibilitando à empresa lidar, de forma racional, com problemas que envolvem o imprevisível.

**QUESTÃO 10**

Acerca das estratégias que viabilizam a gestão de segurança no BB, assinale a opção correta.

- A** A disseminação de instruções e cultura de segurança e a realização de análises de risco são exemplos de atividades de prevenção ou inibição de incidentes de segurança.
- B** A atualização de sistemas e equipamentos e o monitoramento de tendências são atividades que se incluem no escopo da estratégia de recuperação.
- C** A recuperação tem por objetivo corrigir erros e falhas, de forma a evitar a ocorrência de incidentes em uma empresa.
- D** A correção é indispensável para a recuperação da continuidade de negócios após incidente de segurança ocorrido em uma empresa.
- E** A definição de especificações de ferramentas e equipamentos de segurança está entre as atividades referentes à estratégia de correção.

**QUESTÃO 11**

Com relação aos quesitos de segurança bancária, assinale a opção correta.

- A** A presença da vigilância armada é obrigatória durante o horário comercial.
- B** A aprovação do plano de segurança é expressa por meio da emissão de portaria de aprovação pela secretaria de segurança pública.
- C** O plano de segurança é um requisito legal e aborda itens como vigilância armada e sistema de alarme.
- D** Os sensores passivos dos sistemas de alarme compõem-se de duas partes de metal e geralmente são utilizados em portas e janelas.
- E** Os sensores ativos dos sistemas de alarme são sensores de choque que emitem vibrações.

**QUESTÃO 12**

Com relação à segurança e ao risco operacional de uma instituição, julgue os itens a seguir.

- I Acidente automobilístico de menor importância é exemplo de fator de risco externo.
- II A qualidade de vida no trabalho, as competências e a carga de trabalho estão relacionadas aos riscos referentes às pessoas.
- III A segurança lógica e a disponibilidade de dados e sistemas estão associadas aos riscos referentes a processos.

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.
- E** Todos os itens estão certos.

**QUESTÃO 13**

A respeito de procedimentos que envolvem transações financeiras no BB, especialmente pagamentos de valores elevados, julgue os seguintes itens.

- I O autorizador de transações que ultrapassam os limites operacionais para o nível três é corresponsável pelo exame dos documentos e das assinaturas, bem como das possíveis ocorrências apontadas pelo sistema.
- II As transações que extrapolam a alçada estabelecida para o nível dois são autorizadas exclusivamente pelo administrador.
- III Na ausência dos administradores das unidades, as autorizações referentes a pagamentos de valores elevados serão efetuadas somente pela Unidade Alta Renda.
- IV Para acompanhamento e eventual apuração de irregularidades, os sistemas corporativos mantêm registro do usuário, da data e do horário de acesso às transações realizadas.

Estão certos apenas os itens

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

**QUESTÃO 14**

Acerca dos quesitos de segurança do cheque, no BB, que devem ser observados na liquidação ou pagamento, assinale a opção **incorreta**.

- A Os cheques fornecidos para os clientes têm a numeração cadastrada para a respectiva conta.
- B Os cheques cadastrados têm sua situação controlada pelo sistema eletrônico; se apresentados após liquidados, geram a ocorrência correspondente.
- C O sistema eletrônico realiza o controle de contraordem, verificando se há alguma para o cheque apresentado.
- D Todos os campos da banda magnética do cheque apresentado são verificados no caixa, não se permitindo o pagamento em caso de divergência.
- E O sistema eletrônico do BB verifica o leiaute dos cheques, identificando possíveis adulterações como raspagem nos campos preenchíveis e supressão de linhas.

**QUESTÃO 15**

Quanto ao sigilo bancário, analise as asserções do seguinte enunciado.

Deve-se comunicar às autoridades competentes as informações sobre operações referentes à prática de ilícitos administrativos dentro dos prazos estipulados, **porque** constitui crime o retardamento na prestação de informações sigilosas requeridas por autoridades requisitantes competentes.

Assinale a opção correta a respeito desse enunciado.

- A As duas asserções são verdadeiras, e a segunda justifica a primeira.
- B As duas asserções são verdadeiras, mas a segunda não justifica a primeira.
- C A primeira asserção é falsa, e a segunda é verdadeira.
- D A primeira asserção é verdadeira, e a segunda é falsa.
- E Tanto a primeira asserção quanto a segunda são falsas.

**QUESTÃO 16**

Assinale a opção correspondente ao tópico que **não** é abrangido pela Avaliação de Processos Estratégicos no BB.

- A vinculação de recursos humanos, sistemas e serviços terceirizados
- B avaliação do impacto da indisponibilidade dos processos
- C estabelecimento de fluxos específicos de informação
- D vinculação de estratégias para os cenários definidos
- E classificação dos processos estratégicos

**QUESTÃO 17**

Acerca dos testes e exercícios dos planos de continuidade de negócios realizados no contexto da gestão da continuidade de negócios (GCN), no BB, julgue os itens seguintes.

- I Os testes envolvem avaliações de situações reais de cenários de interrupção e acionamento dos mecanismos alternativos de funcionamento.
- II Nos exercícios, os resultados obtidos não são considerados oficiais ou válidos.
- III Os testes e exercícios devem ser documentados para servirem de fonte de consulta para a melhoria dos planos de continuidade e correção de estratégias.
- IV Os testes e exercícios podem adiantar um resultado previsto.

Estão certos apenas os itens

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

**QUESTÃO 18**

Considere que todas as dependências de uma instituição financeira passem a adotar um modelo de segurança de pessoas e ambientes embasado na teoria dos círculos concêntricos, na adoção de planos de segurança, em procedimentos preventivos e em demais princípios da gestão de segurança, como propostos pelo BB. Nessa situação, estaria em conformidade com o modelo de segurança adotado

- A a ênfase no uso de escudos blindados para melhor posicionamento dos vigilantes em uma agência bancária.
- B a adoção do nível de segurança excepcional para a área de escritórios de uma unidade estratégica da instituição.
- C a programação de abertura do cofre das agências com um tempo de retardo inferior a quinze minutos, em horário de expediente.
- D a confecção do plano de segurança de pessoas e ambientes de uma dependência, conforme normas da polícia federal, pela empresa de vigilância que atende a essa dependência.
- E dar preferência, durante a elaboração de uma matriz de vulnerabilidades, aos dados relativos ao perfil da clientela de determinada agência, em detrimento do conhecimento do limite de numerário dessa dependência.

**QUESTÃO 19**

A classificação da informação e o controle de acesso lógico são práticas e processos comuns em ambientes de tecnologia da informação no BB. É condizente com as práticas e os processos de segurança da informação no BB

- A produzir documento que recebe o rótulo de sigilo \$40 e repassá-lo para um grupo de clientes.
- B o uso de *token* USB para armazenamento e movimentação da chave privada de uma entidade de uma infraestrutura de chave pública.
- C permitir a criação de senhas de acesso de funcionários a sistemas internos da instituição formadas exclusivamente por letras, sem o uso de caracteres numéricos ou de controles.
- D adotar, para a redução da disseminação, respectivamente, de vírus, *phishing* e *spyware*, recursos de criptografia, autenticação e autorização e *firewall* pessoal.
- E a adoção de distintos conjuntos de controles para cada uma das várias fases do ciclo de vida de uma mesma informação.

**QUESTÃO 20**

A GCN compreende uma abordagem de gerenciamento de riscos do negócio que envolve o comprometimento do corpo diretivo de uma organização, para garantir as funções do negócio, a qualquer tempo e circunstância. Em organizações financeiras, a GCN é uma exigência legal. Assinale a opção em que a situação hipotética apresentada corrobora a existência de uma percepção adequada da GCN, em uma instituição financeira.

- A Um auditor externo delegou a avaliação da eficácia de um programa de testes de continuidade de negócios para a área de tecnologia do cliente.
- B Adotou-se um plano de continuidade para um banco que considera essencial a manutenção da continuidade no nível estratégico e secundária a manutenção da continuidade nos níveis tático e operacional.
- C Um representante de entidade ou agência reguladora considerou que o fator preponderante para a criação da GCN, na instituição financeira que está visitando, era a redução dos riscos de perda de rentabilidade e consequentes prejuízos aos acionistas dessa instituição.
- D Um membro da diretoria do banco promoveu a formalização das estratégias de continuidade por meio da divulgação de planos e procedimentos de continuidade de negócios.
- E Foram realizadas as seguintes atividades durante o teste e manutenção dos planos de continuidade: estabeleceram-se níveis para os serviços prestados; alocaram-se papéis e responsabilidades para pessoas chave; e estimaram-se os tempos máximos toleráveis para uma interrupção.