

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

Acerca da organização atual da segurança nas empresas financeiras, especialmente no Banco do Brasil S.A. (BB), assinale a opção correta.

- Ⓐ A segurança na criação e na manutenção do processo negocial visa tornar os produtos financeiros rentáveis e agregar a percepção de confiança e segurança na experiência de relacionamento. Quando do lançamento de novos produtos financeiros, sua aplicação, além de garantir a plena rentabilidade dos produtos, depende basicamente da adoção de alternativas de soluções de segurança, envolvendo a gestão de riscos, de forma a evitar ou reduzir perdas com falhas, fraudes e roubos.
- Ⓑ O princípio “conheça o seu cliente” requer que os funcionários do BB colem informações acerca da atividade econômica dos clientes, por meio da monitoração da movimentação financeira, da verificação da compatibilidade entre o faturamento e a atividade econômica, entre outros aspectos, mesmo que esses procedimentos violem a privacidade do cliente, pois isso evita que a instituição seja usada para o crime de lavagem de dinheiro.
- Ⓒ Os amplos níveis de disponibilidade e o acesso aos clientes, existentes no *Internet Banking*, constituem o principal canal por meio do qual as organizações criminosas cometem crimes.
- Ⓓ A gestão da segurança nas empresas, um processo sistemático, integrado em todos os níveis e segmentos institucionais, avalia, periodicamente, de forma cíclica, dinâmica e flexível, os danos causados pelos riscos operacionais, de modo a compensar tais perdas por meio da adoção de controles.
- Ⓔ Os aspectos regulatórios da gestão da segurança no Brasil, amparados por leis criadas no século XX, incluem, entre outros, a atividade de segurança privada e sua fiscalização pela Polícia Federal, além da prevenção da utilização do sistema financeiro para o crime de lavagem de dinheiro.

QUESTÃO 2

Acerca da segurança corporativa, com foco na atividade do BB, assinale a opção correta.

- Ⓐ A estratégia prioritária da segurança corporativa tem por objetivo controlar fenômenos sociais, como crime e violência, de forma a influenciar aspectos sociais, econômicos, psicológicos, políticos e tecnológicos relacionados a estes fenômenos.
- Ⓑ A segurança corporativa é um processo vivo, dinâmico, multidisciplinar, embasado em ciências como sociologia, psicologia e administração, visando a integração com o negócio, as equipes de excelência, as tecnologias de ponta, a inteligência estratégica, a educação e a cultura.
- Ⓒ A segurança contra o crime e a violência na sociedade constitui o tema central da governança corporativa no BB.
- Ⓓ A segurança é um componente secundário na garantia de um ambiente saudável, ético, propício à motivação pessoal, à integração e à geração de resultados.
- Ⓔ As profundas mudanças que os governos sofreram recentemente tiveram como consequência a globalização, a rápida proliferação da Internet e a modernização do crime organizado.

QUESTÃO 3

Considerando o processo de gestão de segurança no BB, é correto afirmar que

- Ⓐ a proteção de ativos físicos e financeiros, como numerário, equipamentos e instalações físicas, possui prioridade secundária frente a outros valores, como imagem, informações e pessoas.
- Ⓑ a ausência de planejamento, de monitoramento e de controle nas ações de segurança, combinada com o despreparo dos funcionários da organização em segurança corporativa, tende a aumentar o risco e reduzir a incerteza acerca da ação dos criminosos.
- Ⓒ os criminosos especializados são atores externos e os funcionários e contratados do banco são atores internos das ocorrências ou incidentes de segurança, e ambos cometem erros de procedimento, de descumprimento de normas, negligência e dolo do ponto de vista dos negócios do banco.
- Ⓓ o exame dos processos de uma organização, o monitoramento do negócio, a percepção de cenários e a manutenção permanente das pessoas mobilizadas geram informações que podem ser usadas tanto para aprimorar a segurança da organização como para planejar ações criminosas contra ela.
- Ⓔ são três as estratégias que viabilizam o macroprocesso de gestão de segurança: a prevenção ou inibição, que consiste na criação de fatores que inibem ocorrências; a recuperação, que consiste na elaboração de planos de continuidade de negócios e de recuperação de atividades; e a pesquisa estratégica, que consiste na coleta de informações consideradas úteis para a segurança preventiva.

QUESTÃO 4

Acerca de risco operacional e segurança no BB, assinale a opção correta.

- A** Risco operacional é definido como a certeza da ocorrência de perdas resultantes de falha, deficiência ou inadequação de fatores de risco, como processos internos, pessoas e sistemas.
- B** Competências e carga de trabalho são exemplos de fatores externos que podem ser causadores de perdas operacionais.
- C** Nem todas as perdas que são medidas e quantificadas expressam prejuízos pecuniários.
- D** São classes de vulnerabilidades organizacionais no contexto da segurança corporativa: físicas, naturais, sociais, de *hardware*, de *software*, de meios de armazenamento e de comunicação.
- E** A exigência de capital, a conformidade e a inteligência estratégica são, respectivamente, responsabilidades da diretoria de gestão de risco, de controles internos e de gestão da segurança. Essas diretorias constituem parte da estrutura de gestão do risco operacional.

QUESTÃO 5

A respeito de segurança de pessoas e ambientes no BB, assinale a opção correta.

- A** A gestão de segurança de pessoas e ambientes protege, de forma preventiva, reativa e corretiva, os funcionários, os clientes, os ambientes das agências e os prédios administrativos, entre outros.
- B** A gestão de segurança de pessoas e ambientes aplica às mais diversas pessoas e ambientes as seguintes gradações de segurança: excepcional, elevada, mediana, rotineira e periférica.
- C** A gestão de segurança de pessoas e ambientes atualiza constantemente a matriz de vulnerabilidades de um ambiente como base para a indicação de procedimentos de segurança aplicáveis a esse ambiente.
- D** Os escritórios e as estações de trabalho de uma unidade estratégica são enquadrados usualmente no nível de segurança excepcional.
- E** Na elaboração da matriz de controles de uma dependência, são observados a região geográfica na qual se inserem a dependência, a localização da dependência no espaço urbano e os limites de numerário da dependência.

QUESTÃO 6

Com referência à gestão de segurança de pessoas e de ambientes no BB, assinale a opção correta acerca de procedimentos e recursos obrigatórios, bem como de soluções em segurança física.

- A** Conforme regulamentação da Polícia Federal, os estabelecimentos financeiros que realizam guarda de valores ou movimentação de numerário precisam implementar plano de segurança que detalhe condições e presença de contingente de vigilância armada com coletes à prova de bala, até mesmo na sala de autoatendimento, controle de acesso lógico, sistema de detecção de fumaça e de metais, sistema interno de televisão, fechadura eletrônica de tempo programável para cofre, entre outras medidas.
- B** A constatação pela comissão de vistoria de irregularidades nos quesitos de segurança do plano de segurança de uma dependência gera autuação do BB.
- C** A Comissão Consultiva para Assuntos de Segurança Privada é a instância colegiada composta pelo setor de segurança privada e pelas agências públicas envolvidas na regulação e no controle desta atividade, e é integrada por representantes do Departamento de Polícia Federal, do Comando do Exército, do Instituto de Resseguros do Brasil, da Federação Brasileira dos Bancos e da Confederação Nacional dos Bancários, entre outras.
- D** Entre os mecanismos de disparo do sistema de alarme, incluem-se sensores, senhas e acionadores. São exemplos de sensores, as botoeiras fixas, de senhas, de coação e de acionadores, e os sensores passivos, ativos, magnéticos e sísmicos.
- E** As correspondências entre solução de verificação de segurança e sua função primária são: fechadura eletrônica de tempo programável → identificar; circuito fechado de televisão → auditar; controle de acesso físico → inibir; vigilância armada → detectar; eclusas → deter ameaças.

QUESTÃO 7

Acerca dos procedimentos preventivos adotados pelo BB para segurança de pessoas e ambiente, assinale a opção correta.

- A** Vizinhos devem ser desencorajados a auxiliar na vigilância da residência de funcionário do banco que estiver viajando.
- B** Nos ambientes de tesouraria, bateria de caixas e processamento do Serviço de Atendimento Operacional, proíbe-se a entrada de prestadores de serviço.
- C** No trânsito, o funcionário do banco que suspeitar estar sendo seguido deve dirigir-se rapidamente a um posto policial.
- D** Os funcionários do banco devem divulgar suas rotinas e hábitos de deslocamento.
- E** Os funcionários do banco que atuam em agências devem verificar, periodicamente, se há obstrução de câmeras ou sensores na sala de autoatendimento.

QUESTÃO 8

Com relação à segurança da informação, assinale a opção correta.

- A** Ativos de valor para a segurança da informação, tais como bancos de dados e arquivos, programas de aplicação, equipamentos computacionais, serviços, pessoas, reputação e imagem, estão relacionados aos sistemas de informação.
- B** Todos os ativos de informação realizam o ciclo da informação, que é composto pelas seguintes fases: criação, uso, armazenamento, transporte e descarte.
- C** Em geral, a maximização de retorno sobre investimentos e oportunidades não está relacionada à segurança da informação.
- D** Confidencialidade, integridade e disponibilidade são atributos fundamentais da segurança da informação. Cada sistema de informação apresenta níveis de segurança particulares e iguais para cada um desses três atributos.
- E** A quebra de sigilo bancário configura um tipo de incidente mais diretamente relacionado à integridade do que à confidencialidade de um sistema.

QUESTÃO 9

A respeito da política de segurança da informação no BB, assinale a opção correta.

- A** A exposição de sistemas críticos a ataques criminosos constitui uma das formas mais eficientes para o reconhecimento e a compreensão integral das consequências de violação da política de segurança.
- B** A fim de evitar a variabilidade dos processos organizacionais, as medidas de segurança não devem ser implementadas sem a definição prévia de uma política de segurança.
- C** Constituem atributos de uma boa cadeia normativa de políticas de segurança da informação: a abrangência, de iniciativa das instâncias inferiores da estrutura hierárquica organizacional, e a implantação monolítica, orientada para o aproveitamento de oportunidades, concentrada em questões punitivas e proibitivas.
- D** Os normativos que apresentam os passos para a realização de uma atividade de nível operacional são considerados norma.
- E** Para garantir a segurança da cadeia normativa das políticas de segurança da informação, deve-se priorizar a confidencialidade em detrimento da disponibilidade.

QUESTÃO 10

Com base nos modelos de classificação da informação e de controle de acesso no BB, assinale a opção correta.

- A** A classificação da informação deve ser efetuada pelo custodiante que atua em unidade estratégica (diretoria gestora), com base nos controles estabelecidos pelo proprietário da informação e mediante a fixação de rótulo no documento que a contém.
- B** O esquema de classificação da informação organiza a informação nas categorias pública, interna e confidencial. As classes \$ 10 e \$ 20 pertencem à categoria de informação pública; a classe \$ 30 pertence à categoria interna e a classe \$ 40, à confidencial.
- C** O proprietário é o responsável por assegurar que as informações estejam protegidas de acordo com a classificação estabelecida pelo custodiante.
- D** A fim de prevenir eventual violação de informação rotulada, deve-se monitorá-la continuamente.
- E** Cada área de negócios deve estabelecer sistema próprio de classificação da informação.

QUESTÃO 11

Com referência aos controles lógicos de acesso aos sistemas, redes e aplicativos do BB, assinale a opção correta.

- Ⓐ Um sistema de controle de acesso lógico deve assegurar que apenas usuários identificados, autenticados, autorizados e monitorados tenham acesso a determinado recurso crítico.
- Ⓑ A autorização do usuário é baseada em três fatores: o que a pessoa sabe, o que a pessoa tem e quem é a pessoa.
- Ⓒ Entre as tecnologias de autenticação disponíveis atualmente no mercado, o *smartcard* e o *token* USB apresentam em comum elevada incidência de falsos positivos, algo que não ocorre com a tecnologia de biometria por impressão digital.
- Ⓓ Conheça o seu cliente, privilégio mínimo e minimização da superfície de ataque são princípios aplicados, de forma geral, na criação de mecanismos de autorização seguros, com elevada usabilidade e custo-efetividade.
- Ⓔ As antigas dificuldades e inconveniências operacionais durante a geração e atualização de senhas (ou *passwords*) hoje são facilmente resolvidas por meio da adoção de senhas formadas por mais de dez caracteres — combinando-se letras, números e caracteres de pontuação — e com prazo de validade de uma semana.

QUESTÃO 12

De acordo com a Lei Complementar n.º 105/2001, as situações que configuram quebra de sigilo bancário **não** incluem o(a)

- Ⓐ troca de informações sobre transações bancárias de clientes por intermédio de centrais de risco.
- Ⓑ troca de informações sobre transações bancárias de clientes inadimplentes ou emitentes de cheques sem provisão de fundos.
- Ⓒ comunicação às autoridades competentes sobre suposta prática de ilícitos fiscais, quaisquer que sejam as fontes de recursos dos clientes.
- Ⓓ revelação de informações bancárias sigilosas com o consentimento expresso dos interessados.
- Ⓔ vazamento de dados bancários de um cliente por meio de um computador do BB infectado por um *malware*.

QUESTÃO 13

Considere que um funcionário do BB, ao utilizar um computador em seu ambiente de trabalho, tenha recebido um *e-mail* não solicitado com as seguintes características.

- remetente: encomendas@correios.com.br
- assunto: encomenda SEDEX
- texto: devido à greve, consta nos Correios de sua cidade uma encomenda postada como SEDEX, na qual o remetente nos passou seu *e-mail*, se possível comparecer a uma agência dos Correios com seus documentos para resgatar a encomenda
- ao final do referido *e-mail* aparece a informação abaixo, contendo um *hiperlink*:
<http://correios.com.br/encomendas/sedex10.asp?go=postBR5977598323>

Essa situação hipotética indica que, provavelmente,

- Ⓐ o computador utilizado pelo funcionário acaba de receber um *spam*.
- Ⓑ o funcionário está sofrendo um ataque de *scam* ou *phishing*.
- Ⓒ há um *backdoor*, *worm*, *trojan*, *adware* ou *spyware* instalado no computador utilizado pelo funcionário.
- Ⓓ o computador utilizado pelo funcionário está sofrendo um ataque de engenharia social que tenta inserir vírus nesse computador.
- Ⓔ um *e-mail* legítimo dos Correios foi enviado para esse funcionário.

QUESTÃO 14

A respeito de criptografia, assinatura e certificação digital e seus usos no BB, assinale a opção correta.

- Ⓐ O uso de criptografia simétrica garante aos seus usuários integridade, autenticidade, disponibilidade, não repúdio e confidencialidade.
- Ⓑ Quando um cliente do BB faz uso de um certificado digital para acesso aos serviços do Internet *Banking*, os sistemas do banco recebem por intermédio do cliente as seguintes informações: indicação da autoridade certificadora que emitiu o certificado, chave privada da autoridade certificadora e dados que identificam e autenticam o cliente.
- Ⓒ O BB usa serviços da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) e é também uma de suas autoridades certificadoras raiz.
- Ⓓ Quando um cliente do BB, pessoa física, faz uso de um certificado digital, as informações do certificado são armazenadas em um *smartcard*.
- Ⓔ Abertura de contas, videoconferência e autenticação biométrica realizadas por meio de certificados digitais são alguns serviços e soluções usados no BB.

QUESTÃO 15

Um indivíduo apresentou ao funcionário que atua no caixa do BB a carteira nacional de habilitação (CNH). Na oportunidade, o funcionário constatou visualmente que não existiam microcaracteres e fibras coloridas no documento apresentado.

A respeito dessa situação, assinale a opção correta.

- A** O documento apresentado não é autêntico quanto à integridade e à integralidade.
- B** O documento apresentado não é autêntico quanto à origem.
- C** Ocorreu falha no acolhimento do documento apresentado.
- D** A agência deve manter contato com a regional de segurança e com o serviço jurídico jurisdicionário para confirmar a autenticidade do documento.
- E** Na hipótese de a CNH ser autêntica, o documento deve ser usado para exame de assinatura.

QUESTÃO 16

A respeito de procedimentos de guarda, movimentação e encaixe de numerário no banco, são considerados procedimentos inadequados

- A** a citação do nome do colega que vai abrir o cofre e a ativação da fechadura de retardo após o cofre ser trancado.
- B** o controle de saldo da unidade e o reforço ou alívio do numerário.
- C** o abastecimento de envelopes dos terminais por um único funcionário, sob o alerta da vigilância, e o trancamento do cofre após duas horas do encerramento do expediente externo.
- D** o rodízio das chaves e do segredo do cofre e a desatenção ao controle de acesso e à guarda do numerário.
- E** a manutenção das chaves e do segredo do cofre sob a guarda de uma única pessoa e a distribuição do numerário nas várias prateleiras do cofre.

QUESTÃO 17

Assinale a opção que apresenta procedimento inadequado acerca do pagamento de valores elevados e de cheques, especialmente os emitidos pelo BB.

- A** A definição, pelo administrador de uma agência, dos limites operacionais para liquidação de cheques oriundos da compensação.
- B** O levantamento e apuração de eventuais irregularidades no pagamento de valores elevados pela análise dos *logs*, que contém registro do usuário, dependência, data e horário de acesso às transações realizadas.
- C** A entrega de cheques a um cliente mediante coleta de sua assinatura ou do uso de senha.
- D** Na ausência de administradores em uma unidade, o uso de lateralidade definida para produtos e serviços a fim de identificar quem seria o responsável por liberar o pagamento de valores elevados.
- E** A autorização, pelo administrador, de transações que extrapolem a alçada estabelecida para o nível três.

QUESTÃO 18

Considerando a contestação de débitos, as fraudes e seus mecanismos de controle no BB, assinale a opção correta.

- A** Para os três segmentos, pessoa física, pessoa jurídica e governo, utilizam-se senhas numéricas, alfanuméricas e alfabéticas.
- B** O banco classifica as fraudes como eletrônicas ou documentais, adotando, conforme a situação, distintos procedimentos junto ao cliente.
- C** O cadastramento de computador para uso no *Internet Banking* depende da efetiva aceitação do cliente e permite a realização de transações envolvendo limites mais elevados, bem como alterações de cadastro em ambiente *online*.
- D** Recorte e colagem, com adulteração de campos referentes ao valor numérico, extenso e favorecido; banho químico, com retirada da escrita original; raspagem usando borracha, lâmina metálica ou lixa são fraudes pouco comuns encontradas nos cheques.
- E** Quanto aos requisitos de segurança, para que ocorra a liquidação ou pagamento de um cheque, é suficiente que este seja cadastrado e que sua banda magnética (CMC-7) seja válida.

QUESTÃO 19

Constitui princípio norteador da gestão de continuidade de negócios no BB

- A** a realização cíclica de um conjunto tarefas, tais como conhecer a organização e identificar suas necessidades estratégicas, atividades essenciais e níveis de resiliência apropriados, adotar estratégia de continuidade que avalia o tempo de retomada em relação aos objetivos de recuperação e ao custo da estratégia, desenvolver, implementar, testar e manter respostas de continuidade que estabeleçam papéis e aloquem responsabilidades.
- B** a ação reativa no estabelecimento de fundamentos estratégico-operacionais para desenvolver resiliência organizacional.
- C** o explícito comprometimento do corpo operacional em garantir a continuidade das funções de negócio, a qualquer tempo e em qualquer circunstância.
- D** o caráter opcional de implementação, de acordo as normas do sistema financeiro estabelecidas no Acordo de Basileia II, na Lei Sarbanes-Oxley e na Resolução n.º 3.380/2006 do BACEN.
- E** a concentração da resposta nas origens da interrupção.

QUESTÃO 20

Com relação aos planos e procedimentos de continuidade de negócios, assinale a opção correta.

- A** A vinculação do plano de continuidade a recursos como pessoas, instalações, tecnologia, informação, fornecedores de suprimentos ou serviços é opcional.
- B** Os procedimentos de natureza preventiva devem ser excluídos do plano de continuidade de negócios.
- C** Devido à pouca quantidade e variedade de planos de continuidade e áreas envolvidas, a criação de mecanismos de planejamento e controle da realização de testes e exercícios dispensa o uso de uma agenda corporativa.
- D** As avaliações dos planos de continuidade devem ser realizadas por meio de testes, cujos resultados são considerados oficiais, e exercícios que simulem um cenário de interrupção e acionamento do mecanismo alternativo de funcionamento.
- E** A estimativa de recursos, para cada atividade prevista no plano, deve contemplar minimamente recursos de pessoal, localização dos postos de trabalho e instalações necessárias, tecnologia, equipamentos e instalações físicas, informação, eletrônica ou em papel, suficientemente atualizada e precisa sobre trabalhos anteriores ou em andamento, serviços e fornecedores externos.