

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

5 – GESTÃO DE SEGURANÇA

Para responder às questões de 1 a 4, considere que a situação abaixo descrita tenha transcorrido em agência do Banco do Brasil S.A. (BB).

Uma ação de inteligência levou policiais dos estados X e Y a interceptarem um plano de sequestro seguido de assalto a uma agência bancária no interior do estado X. Os assaltantes foram capturados em um município, a 375 km da capital do estado Y, durante operação montada por agentes da Coordenadoria de Inteligência da Secretaria de Segurança Pública e Defesa Social e por inspetores da Delegacia de Narcóticos.

Segundo a polícia, o grupo planejou sequestrar a gerente da agência bancária e sua família, a fim de praticar o crime conhecido como sapatinho: com a família da gerente em cativeiro, a quadrilha levaria a funcionária à agência e roubaria o dinheiro do cofre e dos terminais eletrônicos.

As investigações revelaram ainda que, caso o sequestro da gerente não desse certo, o plano B dos ladrões era invadir a agência com maçaricos e outros utensílios e arrombar os caixas. A polícia, porém, agiu mais rápido.

Internet: <www.cratonoticias.wordpress.com> (com adaptações).

QUESTÃO 1

Tendo o texto como referência inicial, assinale a opção correta no que concerne a segurança, especialmente em instituições financeiras.

- Ⓐ Para ser eficaz, o processo de segurança de uma empresa depende do envolvimento de um grupo restrito de pessoas que nela trabalham.
- Ⓑ Tanto o crime quanto a violência, no contexto apresentado, são fenômenos sociais que podem ser mais bem controlados por meio da adequada troca de informações entre as instituições financeiras e os agentes de segurança pública.
- Ⓒ Em empresas financeiras que busquem garantir boa posição no mercado e tranquilidade aos acionistas e clientes, a gestão de riscos é de uso opcional.
- Ⓓ A facilidade e a disponibilidade de ambientes tecnológicos criados pelas empresas geram conforto para os usuários e auxiliam a mantê-los afastados dos agentes do crime.
- Ⓔ A confiança depositada por acionistas e clientes em uma instituição financeira depende do conhecimento íntimo que eles tenham dos procedimentos de segurança realizados pela instituição.

QUESTÃO 2

Considerando a situação descrita no texto, assinale a opção correta acerca dos fatores do processo de gestão de segurança no BB.

- Ⓐ A situação em apreço poderia impactar de forma direta os valores ou objetos de proteção no processo de gestão de segurança do BB, a saber: pessoas, incluídos os familiares dos empregados, que poderiam ter sido sequestradas; ativos físicos e financeiros, que poderiam ter sido perdidos; imagem da instituição, que poderia ter sido afetada pela veiculação de notícia de caráter negativo; informações de rotinas de serviço e funções específicas de empregados.
- Ⓑ De acordo com as informações do texto em questão, apenas os atores externos contribuíram para a ocorrência noticiada.
- Ⓒ A ação policial apresentada associa-se mais diretamente à estratégia adotada no processo de gestão de segurança do BB — operação de prevenção ou de inibição — que à de pesquisa estratégica.
- Ⓓ Da estratégia de recuperação faz parte a utilização, estabelecida e obrigatória, de fechadura eletrônica de tempo programável, com função de retardo, a qual visa dificultar a ação planejada pelos assaltantes.
- Ⓔ A estratégia de correção inclui um plano de continuidade de negócios, que seria ativado caso o sinistro planejado fosse materializado com a destruição de terminais de autoatendimento.

QUESTÃO 3

Acerca das implicações do cenário descrito no texto, no contexto de gestão do risco do BB, assinale a opção correta.

- Ⓐ Veiculada a notícia do sequestro, o banco ficou exposto, em especial, aos riscos de crédito, de liquidez, de mercado e ao risco legal.
- Ⓑ As ameaças, as vulnerabilidades e os riscos que ocorreram no contexto analisado são de origem essencialmente involuntária.
- Ⓒ Cabe à Diretoria de Gestão de Riscos, entre as três diretorias que compõem a estrutura específica de gerenciamento de risco operacional definida pelo BB, a identificação dos fatores de risco operacional aos quais se encontra exposto o banco, conforme o cenário descrito no texto.
- Ⓓ Caso ficasse configurada forte conexão entre o crime praticado e os crimes de lavagem de dinheiro, tal possibilidade remeteria ao envolvimento de ações da Diretoria de Gestão de Riscos, pois os assaltantes estariam usando o banco para lavagem de dinheiro.
- Ⓔ As ações da Diretoria de Gestão de Segurança refletem-se diretamente na prevenção do tipo de crime citado no texto.

QUESTÃO 4

Considere que, após a divulgação da notícia do sequestro, o BB decida aprimorar o processo de segurança de uma unidade em condições similares à descrita. Nesse caso,

- A o nível de segurança da unidade deverá ser alterado para elevado.
- B o posicionamento dos vigilantes deverá ser incluído no plano de segurança da unidade.
- C o plano de segurança deverá ser vistoriado pela polícia militar.
- D a matriz de vulnerabilidade deverá ser atualizada.
- E o sistema de alarme não deverá ser alterado.

QUESTÃO 5

Considerando o emprego de controles de acesso ou de lista de verificação de segurança em uma unidade do BB, assinale a opção correta.

- A Em caso de sequestros, o uso de leitores de características biométricas torna mais fácil o acionamento de alarmes em situação de coação que o uso de teclados para coletar senhas.
- B A conjugação de critérios para elevar o nível de identificação em sistemas de controle de acesso permite a criação de autenticação por múltiplos fatores.
- C O uso de *tags* é comum para o controle de identificação de veículos, mas não, de objetos como *notebooks*.
- D A lista de verificação de segurança não é elemento do processo de garantia da funcionalidade dos equipamentos de segurança.
- E A lista de verificação de segurança facilita diretamente a formulação do plano de segurança da unidade.

QUESTÃO 6

Com relação a aspectos gerais do modelo de segurança da informação adotado no BB, assinale a opção correta.

- A A necessidade de equipes cada vez mais especializadas para implantação e gerenciamento de segurança da informação depende da preponderância da necessidade de controle de acesso físico, em contraposição ao controle de acesso lógico.
- B A informação a ser protegida é apenas aquela que é capaz de ser processada por um computador.
- C Além da informação propriamente dita, é necessário proteger demais ativos associados a sistemas de informação, como ambientes físicos, serviços de comunicação, pessoas e bens intangíveis.
- D Toda a informação a ser protegida se desenvolve em um ciclo que envolve as seguintes etapas: criação, armazenamento, criptografia, distribuição e destruição.
- E Independentemente do nível de proteção exigido, é necessário empregar o maior conjunto disponível de mecanismos de proteção para qualquer informação.

QUESTÃO 7

Assinale a opção correta acerca da aplicação de princípios e de políticas de segurança da informação no BB.

- A A confidencialidade é um princípio que se sobrepõe à disponibilidade e à integridade da maioria das informações necessárias ao funcionamento dos negócios do BB.
- B Diretrizes e normas de segurança da informação são as bases para a definição dos princípios e da política de segurança da informação.
- C A relação entre custos e benefícios decorrentes da implantação de mecanismos de segurança não é, a princípio, relevante para a definição de uma política de segurança da informação.
- D A inflexibilidade é uma das características que garantem o sucesso de uma política de segurança da informação.
- E Durante a realização das etapas para implantação de uma política de segurança da informação, o desenvolvimento do conteúdo deve preceder à elaboração dos procedimentos de segurança da informação.

QUESTÃO 8

Constitui procedimento adequado ao modelo adotado no BB para a classificação de informações

- A estabelecer o grau de importância da informação com base no criador e na data de criação.
- B designar empregado recém-integrado à área de negócios para responder pela classificação das informações da área.
- C identificar os requisitos legais que se aplicam à manipulação da informação.
- D atribuir ao proprietário a responsabilidade por assegurar a proteção da informação sob custódia de terceiros.
- E criar sistema de classificação de sigilo específico para a unidade de negócios.

QUESTÃO 9

A respeito do controle de acesso a sistemas, redes e aplicativos no BB, assinale a opção correta.

- A A limitação e a desabilitação de acessos são as principais funções do controle de acesso a sistemas.
- B O uso de biometria com impressão digital viabiliza o transporte seguro de credenciais e chaves de usuários.
- C O administrador, para decidir se uma pessoa, programa ou dispositivo tem permissão para acessar determinado dado, programa de computador ou serviço, deve adotar o princípio da maximização de privilégios.
- D A disponibilização ao usuário, após sua entrada no sistema, de relatório com as últimas tentativas de acesso malsucedidas em sua conta permite identificar tentativas de uso não autorizado.
- E Quanto mais longa for uma senha, maior será a segurança de seu uso.

QUESTÃO 10

Com relação ao emprego de ferramentas de proteção da informação no contexto da segurança da informação, assinale a opção correta.

- A As tentativas de acessos indevidos a um computador de uso pessoal conectado à Internet podem ser bloqueadas com o emprego de *firewall* pessoal.
- B Desabilitar a atualização automática de programas produz impacto negativo maior em uma ferramenta *antispam* que em uma ferramenta antivírus.
- C Para se obter assinatura digital eficaz por meio de criptografia, deve-se utilizar, obrigatoriamente, criptografia simétrica e, opcionalmente, criptografia assimétrica.
- D Por oferecer maior facilidade na distribuição de chaves, o emprego da criptografia simétrica é mais vantajoso que o uso da criptografia assimétrica.
- E Navegação na Web, envio e recebimento de correio eletrônico e assinatura digital em contratos de câmbio são operações cuja efetivação depende do emprego de certificados digitais.

QUESTÃO 11

No que concerne aos ataques de engenharia social a instituições como o BB, assinale a opção correta.

- A Independentemente do total de recursos investidos em tecnologia da informação, enquanto as falhas do ciclo de engenharia de *software* não forem sanadas, os ataques de engenharia social continuarão a existir.
- B Apenas os empregados de nível estratégico e tático da instituição precisam ter conhecimento de que as informações por eles manuseadas têm valor e de que seu vazamento, em decorrência da engenharia social, pode causar grandes prejuízos à instituição.
- C Atitudes de violência, arrogância e egoísmo adotadas por uma pessoa não são usualmente empregadas em ataques de engenharia social.
- D A casa e a rua são os locais onde mais comumente ocorrem ataques de engenharia social que afetam o BB e seus empregados.
- E Formalização de política de segurança, classificação da informação e controle de acessos físicos são medidas que pouco contribuem para a redução de ataques de engenharia social.

QUESTÃO 12

A respeito da segurança em produtos, serviços e processos do BB, assinale a opção correta.

- A A identificação da integralidade de um documento depende da prévia verificação de sua autenticidade e origem.
- B Para se estabelecer limite de crédito a clientes, deve-se ter acesso, sempre que necessário, aos documentos originais do cliente.
- C Quando efetuado em agências, o acolhimento de carta precatória independe de apoio de serviço jurídico.
- D Para que uma procuração particular seja acatada pelo BB, é necessário que o cliente a revigore anualmente.
- E A custódia e o saneamento do numerário para as demais instituições financeiras, à ordem do Banco Central do Brasil (BACEN), são processos de movimentação de numerário mais vulneráveis que o abastecimento de caixa eletrônico.

QUESTÃO 13

Assinale a opção correta com relação ao pagamento de valores elevados, cheques e contestação de débito no BB.

- A Nas agências, compete ao gerente a definição dos limites operacionais para liquidação de cheques oriundos da compensação e para pagamento no caixa.
- B Caracteres holográficos e fibras de papel coloridas são itens de segurança física do cheque emitido pelo BB.
- C Os quesitos eletrônicos de segurança visam obstar modalidades de fraude, como raspagem, colagem e banho químico.
- D A validade da banda CMC-7 e o controle de contraordem são quesitos eletrônicos de segurança de cheque do BB observados na liquidação ou pagamento.
- E O uso de senhas e códigos de acesso por clientes do BB tem por principal finalidade a prevenção de fraudes documentais.

QUESTÃO 14

A gestão de continuidade de negócios (GCN)

- A concentra-se na prevenção de fenômenos que poderiam provocar interrupções, em larga escala, em uma empresa, tais como atividades terroristas, mudanças climáticas drásticas e falhas ou danos nas instalações físicas.
- B prepara as empresas para superar os desafios de uma interrupção, qualquer que seja a sua causa.
- C focaliza, primariamente, a adoção de medidas de recuperação.
- D não contempla medidas reativas a serem adotadas após a ocorrência de um incidente.
- E ignora o fato de que as famílias dos empregados da organização podem ser atingidas pela mesma ocorrência que deu origem a algum tipo de interrupção.

QUESTÃO 15

Acerca da GCN nas organizações financeiras, assinale a opção correta.

- A O interesse dos órgãos de supervisão bancária concentra-se no aumento da capacidade individual de resiliência de cada membro do sistema financeiro frente a grandes interrupções, arrefecendo-se no plano da resiliência coletiva.
- B A implantação da GCN por instituições financeiras no Brasil faz que interrupções repetidas ou prolongadas no funcionamento de alguns agentes do sistema financeiro não tenham capacidade de minar a confiança e resultar em uma retirada de capital que afetaria o Sistema Financeiro Nacional.
- C As empresas do sistema financeiro, embora profundamente dependentes da automatização, desenvolvem, por meio da GCN, completa independência da infraestrutura física que dá suporte à automatização, tal como telecomunicações e energia.
- D A gestão eficaz da continuidade de negócios concentra-se na origem da interrupção, o que fornece à indústria financeira e às autoridades financeiras maior flexibilidade para tratar amplo leque de interrupções.
- E Entre os impactos a serem avaliados no escopo da GCN incluem-se os danos ambientais, a deterioração da qualidade de produtos ou serviços, os danos à viabilidade financeira, os danos à reputação da instituição, o não cumprimento de deveres ou regulamentações e o dano ou a perda de instalações, tecnologias ou informação.

QUESTÃO 16

Com relação a aspectos legais, a governanças e a melhores práticas no âmbito da GCN, assinale a opção correta.

- A** O Acordo de Basileia II recomenda que as instituições financeiras mantenham planos de continuidade de negócios para minimização dos riscos operacionais.
- B** O BACEN recomenda às instituições financeiras brasileiras, por meio da Resolução n.º 3.380, a implantação de estrutura de gerenciamento de risco de segurança da informação, o que indiretamente subsidia a formulação de planos de continuidade de negócios.
- C** As NBRs 15999-1 e 15999-2 abordam o processo, os princípios e a terminologia da gestão da continuidade de negócios para instituições financeiras no Brasil.
- D** As NBRs ISO/IEC 27001 e 27002 são especificamente voltadas para a definição de métodos de gerenciamento de continuidade de negócios em instituições financeiras.
- E** A Lei Sarbanes Oxley determina a obrigatoriedade da adoção da gestão de continuidade de negócios por empresas financeiras, o que afeta dezenas de empresas brasileiras que mantêm ADRs (*american depositary receipts*) negociadas na NYSE, entre elas, o BB.

QUESTÃO 17

A respeito da metodologia de GCN, adotada no BB, assinale a opção correta.

- A** A elevada profundidade de acompanhamento e o controle das ações em cada etapa são premissas que norteiam a adoção da metodologia de GCN.
- B** A Diretoria de Controles Internos, responsável por disponibilizar regras, modelos e padrões para a gestão da continuidade de negócios, busca, junto às unidades estratégicas, identificar e classificar os processos, considerando o impacto e o risco de sua indisponibilidade para, a partir dos resultados obtidos, assessorá-las na proposição e implantação de testes das medidas para manter os processos operacionais.
- C** Para a adoção da GCN no BB, definiram-se atribuições e responsabilidades de implementação — pelas áreas gestoras de produtos, serviços e sistemas — de mecanismos e soluções para manter os processos operacionais, exceto nos casos de cenários de interrupção ou de crise corporativa.
- D** A avaliação de processos estratégicos visa obter informações quantitativas acerca das características fundamentais de todos os processos táticos do BB.
- E** Bloqueio de acesso, indisponibilidade de serviços terceirizados e indisponibilidade da infraestrutura de tecnologia da informação são cenários de ameaça de continuidade de negócios adotados pelo BB para a elaboração dos planos de continuidade de negócios.

QUESTÃO 18

Constitui atribuição dos membros de um grupo coordenador de continuidade do BB

- A** identificar as principais vulnerabilidades dos processos estratégicos do banco.
- B** testar os planos de continuidade da dependência.
- C** manter toda a documentação relativa aos planos de continuidade da dependência, incluindo-se os normativos e listas de acionamento, em local seguro e acessível somente aos integrantes do Grupo Coordenador de Continuidade e aos executores dos procedimentos previstos.
- D** elaborar os planos de continuidade de fornecedores e prestadores de serviço.
- E** realizar a auditoria interna de planos de continuidade.

QUESTÃO 19

No que se refere a estratégias para a garantia da continuidade de negócios no BB, assinale a opção correta.

- A** As estratégias de continuidade, detalhadas nos planos de continuidade de negócios, devem ser ativadas quando ocorrerem os cenários de interrupção.
- B** Após analisar a relação entre custo e benefício da adoção das estratégias possíveis, o gestor deve baixar a mitigação, isto é, deve providenciar ações para adotar cada uma das estratégias.
- C** Para clientes, fornecedores de suprimentos ou serviços, e para os recursos de tecnologia de informação, instalações e pessoas, pode ser necessário o desenvolvimento de estratégia de continuidade específica.
- D** As principais informações que devem figurar nos planos de continuidade de negócios no BB incluem o plano de tratamento de riscos e a indicação dos cenários para os quais o plano se aplica.
- E** Com a finalidade básica de ofertar subsídios à auditoria, convém que os resultados dos testes e exercícios de planos de continuidade sejam amplamente documentados.

QUESTÃO 20

Acerca da função exercida pelas pessoas, consideradas elemento central de um sistema de segurança, inclusive no BB, assinale a opção correta.

- A** As ações de conscientização, educação e treinamento em segurança são restritas aos empregados do BB; os demais, incluindo-se os colaboradores que prestam serviços à instituição, devem receber treinamento apropriado e atualizações regulares acerca de políticas e normas por meio das empresas prestadoras de serviço, contratadas para tal fim.
- B** A atitude das pessoas frente à segurança deve ser tratada como objeto de controle e repressão da cultura organizacional, evitando-se que passe a ser vista como instrumento de autoproteção.
- C** Uma atitude positiva em relação à segurança, fruto de processo educativo que envolve mudança de comportamento, pode ser alcançada por meio de campanhas isoladas, devendo, entretanto, ser reavaliada sempre que necessário.
- D** Em todo o processo de formação da cultura de segurança, é necessário o envolvimento da alta direção da instituição.
- E** A seleção e a ordenação de conteúdos de conscientização, treinamento e educação devem privilegiar o uso de metodologia conceitualmente sólida e uniforme, atingindo, de forma contundente, indistinta e aprofundada, todos os públicos do banco.