CONHECIMENTOS ESPECÍFICOS

Acerca de gestão, risco e conformidade, julgue os itens a seguir.

51 O ciclo de vida da informação, inclui as etapas de manuseio, de armazenamento, de transporte e de uso, mas não a de descarte, uma vez que esta, mesmo no caso de ser descarte inadequado, não é fonte de vulnerabilidade.

52 Caso não disponha de recursos para o desenvolvimento de plano de gestão de continuidade do negócio próprio, a organização pode, alternativamente, adquirir um plano padrão, que pode ser personalizado conforme as características da instituição.

53 A ISO/IEC n.º 17799 originou-se da adoção, pela ISO (*International Organization for Standardization*), da norma britânica BS 7799, anteriormente seguida de forma ampla.

54 Entre as formas de abordagem do risco inclui-se a transferência do risco, atividade que não se confunde com a abstenção do tratamento do risco.

55 Gestão de risco consiste no conjunto de procedimentos que permitem a proteção, de forma absoluta, contra quebras de confidencialidade.

No que se refere à equipe de resposta e tratamento a incidentes (ETIR) e aos incidentes de segurança, julgue os itens que se seguem.

56 As diretrizes do trabalho da ETIR e o planejamento da estratégia de resposta a incidentes devem ser traçados pelo agente responsável e pelos membros da equipe, sem o envolvimento do gestor de segurança da informação, que tem a função de atuar como analista de conformidade do processo.

57 Incidente de segurança refere-se a qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores, incluindo aqueles decorrentes de conduta maliciosa, denominados ataques.

58 Um processo seguro e tempestivo de notificação de incidentes de segurança é um componente crítico de qualquer programa de segurança no que se refere à gestão e ao tratamento de incidentes.

59 Entre os modelos de formação do time de resposta a incidentes previstos pela ISACA, *Central*, *Distributed*, *Coordinating* e *Outsourced*, apenas o último não foi incorporado ao regramento do DSIC (NC 05/IN01/DSIC/GSIPR) para a administração pública, haja vista que, no âmbito dessa administração, a escolha preferencial, na formação da equipe, deve recair sobre servidor público ocupante de cargo efetivo ou militares de carreira.

60 A equipe de resposta e tratamento a incidentes pode ser formada por uma única pessoa.

61 A implementação do monitoramento de uso do sistema dispensa a prévia análise de riscos.

Julgue os próximos itens, relativos ao uso de soluções criptográficas.

62 As soluções criptográficas, ainda que possam ser quebráveis, são empregadas para tornar o ataque custoso, em termos econômicos e procedimentais, e, consequentemente, inviabilizar o objetivo malicioso.

63 A *colisão de hashes* ocorre quando duas entradas de mensagens idênticas resultam em dois valores diversos de *message digest* ou *hash*, e pode decorrer, por exemplo, de exploração do tipo força bruta (ataque de dicionário).

64 O algoritmo AES, em relação ao DES, seu antecessor, apresenta as seguintes vantagens: maior tamanho de blocos, uso de chaves de tamanho variável e variabilidade do número de *rounds*.

65 O *criptex*, sistema supostamente desenvolvido por Leonardo Da Vinci, não consiste em exemplo de criptografia aplicada a um texto-em-claro, mas de criptologia aplicada a controle de acesso.

A respeito de segurança da informação e continuidade do negócio, julgue os itens seguintes.

66 As etapas necessárias à adequada construção de uma garantia de continuidade do negócio são identificação da crise, análise de impactos no negócio, planejamento, política de continuidade, definição de estratégias de contingência e elaboração dos planos de contingência para os diversos perímetros.

67 O BIA (*business impact analysis*) fundamenta todo o planejamento geral e os planos específicos da gestão de continuidade, sendo uma ferramenta empregada para realizar a identificação, a quantificação e a qualificação de perda, bem como a suspensão ou a interrupção dos processos de negócio. Além disso, mediante esse instrumento são estabelecidas as datas a partir das quais as estratégias de continuidade terão início.

68 O RPO (*recovery point objective*) é o ponto no tempo em que o reinício das operações após um desastre é desejável, considerando-se os custos da recuperação em face dos custos da interrupção.

69 O RTO (*recovery time objective*) representa o último ponto, na linha de tempo, anterior ao desastre e posterior ao último becape realizado que foi julgado como aceitável, em termos de custo, e considerando-se a avaliação de todas as circunstâncias do negócio em questão.

70 A aprovação do plano de continuidade do negócio pelo nível executivo da organização (CEO e CSO) é dispensável.

71 Os princípios da confidencialidade, integridade e disponibilidade são objetivos da segurança da informação, entre os quais se incluem o da autoria, o de não repúdio, o da auditabilidade e o da legalidade.

Com relação aos princípios gerais de controle de acesso, julgue os itens subsecutivos.

72 Os métodos de autenticação comumente empregados fundamentam-se na clássica divisão entre o que você sabe (senha ou número PIN); o que você tem (*token* ou um *smart card*); e o que você é (íris, retina e digitais).

73 O controle de acesso RBAC (*role-based access control*) indica, com base em uma engenharia de papéis, o método de acesso, de modo que o nível de acesso de um colaborador, por exemplo, possa ser determinado a partir do tipo de atividade que este exerce.

74 Separação de tarefas, privilégio mínimo e necessidade de saber são conceitos que identificam os três principais tipos de controle de acesso.

Acerca de controle de acesso e certificação digital, julgue os itens a seguir.

75 Em uma PKI (*public key infrastructure*), utiliza-se uma solução mista de troca de conteúdo encriptado, em que são manejadas soluções de criptografia simétrica, criptografia assimétrica e funções *hash*, para se garantir a disponibilidade das informações.

76 Um dispositivo do tipo IDS (*intrusion detection system*) atua com proatividade, prevendo ataques e antecipando-se a explorações de vulnerabilidades, a partir de assinaturas frequentemente atualizadas.

Acerca da análise de vulnerabilidades, julgue os itens seguintes.

77 Um computador com programa antivírus desatualizado é exemplo de vulnerabilidade.

78 Um funcionário mal remunerado e insatisfeito com a instituição onde trabalha não constitui fator de vulnerabilidade porque os recursos humanos são fatores excluídos da análise de vulnerabilidades.

79 A falta de auditorias periódicas ou de um plano de continuidade do negócio, dado estes serem fatores internos de controle, não constitui exemplo de vulnerabilidade.

80 A análise de vulnerabilidades integra as atividades da gestão de riscos e, por meio dela, identificam-se fragilidades ou pontos fracos em ativos que possam ser explorados por ameaças.

O tribunal de justiça de determinado estado da Federação iniciou processo licitatório para a aquisição de geradores de energia elétrica, para evitar danos causados por eventuais falhas no fornecimento por parte da companhia elétrica responsável.

Com referência a essa situação hipotética, julgue os itens que se seguem.

81 Atividades como testes e revisões dos geradores integram o plano de continuidade do negócio, embora não estejam vinculados ao ciclo de gestão da continuidade do negócio.

82 No que diz respeito à segurança da informação, a compra dos geradores atende à gestão da continuidade do negócio do tribunal.

Acerca dos procedimentos de segurança da informação, julgue os seguintes itens.

83 Caso uma empresa decida pôr em prática controle da implementação de mudanças no sistema de informação que utiliza em suas operações, é correto afirmar que essa decisão se deu pela necessidade da empresa em minimizar riscos de falha de becape.

84 Os procedimentos de segurança da informação são componentes táticos da política de segurança da informação.

85 Considere que uma empresa tenha introduzido sistema de autenticação biométrica como controle de acesso de seus funcionários às suas instalações físicas. Nessa situação, o uso desse tipo de controle é um procedimento de segurança da informação.

No contexto da segurança da informação, as informações são ativos da organização e podem ser classificadas de diferentes maneiras. A respeito desse assunto, julgue os próximos itens.

86 A informação deve ser classificada de acordo com o seu valor, seus requisitos legais e sua sensibilidade ou criticidade.

87 É responsabilidade da equipe de segurança da informação da instituição a classificação de um ativo ou de uma informação.

88 Com a classificação das informações, busca-se assegurar níveis adequados de proteção das informações.

Acerca de auditoria e conformidade, julgue os itens subsequentes, a respeito de segurança da informação.

89 Em uma auditoria, para a verificação dos sistemas operacionais, os processos do negócio seguem seu fluxo sem interrupções.

90 Conformidade é um conceito relacionado à adesão dos sistemas de informação às políticas e às normas organizacionais de segurança da informação.

91 Atividades de usuários, exceções e outros eventos são registros ou *logs* de eventos produzidos e mantidos pela instituição, mas, por constituírem eventos qualitativos, não são objetos apropriados para futuras investigações ou auditorias.

92 A regulamentação de controles de criptografia obriga a conformidade do uso de criptografia com leis, acordos e regulamentações pertinentes.

93 A execução correta dos procedimentos de segurança da informação, em conformidade com normas e com a política de segurança da empresa, deve ser garantida pelos vários gestores, cada um em sua área.

Julgue os seguintes itens, com base na NBR ISO/IEC 15408.

94 O TSF (TOE (*target of evaluation*) *security functions*) representa as funções de segurança de um TOE que serão avaliadas.

95 O PP (*protection profile*) compõe os requisitos de auditoria para a avaliação do sistema.

Considerando o que dispõe a NBR ISO/IEC 27001, julgue os próximos itens.

96 A exclusão de controles considerados necessários deve ser justificada por meio do fornecimento de evidências a respeito da aceitação dos riscos pelas pessoas responsáveis.

97 Um evento de segurança da informação inesperado e que pode comprometer uma operação do negócio da organização é denominado incidente de segurança da informação.

98 Denomina-se declaração de riscos a declaração documentada que contém informações referentes aos objetivos de controle e controles pertinentes ao sistema de gestão de segurança da informação da organização.

99 Essa norma aborda o processo que estabelece, implementa, opera, monitora, analisa criticamente, mantém e melhora o sistema gestão de segurança da informação de uma organização.

No que se refere às políticas de segurança da informação, julgue os itens subsequentes, de acordo com a NBR ISO/IEC 27002.

100 Para que haja confiabilidade, o documento de política de segurança da informação deve permanecer inalterado ao longo do tempo.

101 O documento de política de segurança da informação de uma empresa deve definir as políticas dessa área, com base nos objetivos do negócio, na legislação e na regulamentação pertinente.

102 O principal objetivo das políticas de segurança da informação é colaborar com a gestão da segurança da informação, orientando-a e apoiando-a administrativamente.

Ainda acerca de política de segurança da informação, julgue os itens a seguir, com base na NBR ISO/IEC 27002.

103 A situação de ações preventivas é uma saída da análise crítica da política de segurança da informação.

104 Comprometimento e apoio visível dos colaboradores do nível gerencial fazem parte dos fatores críticos de sucesso para a implementação de segurança da informação dentro da organização.

105 O documento de política de segurança da informação deverá conter a definição das responsabilidades gerais da gestão de segurança da informação. As responsabilidades específicas, como a gestão de incidentes de segurança da informação, devem ser contempladas em manuais de procedimentos.

106 A política de segurança da informação de uma organização deve ser comunicada de maneira acessível e relevante a todos os usuários.

107 A política de segurança da informação de uma organização não pode fazer parte de uma política geral da empresa, devendo ser contemplada em um documento específico, com versões controladas, contendo especificamente as diretrizes de segurança da informação.

108 Realimentação das partes interessadas é uma entrada da análise crítica da política de segurança da informação.

Com base na NBR ISO/IEC 27004, julgue os itens que se seguem.

109 As métricas de um programa de medição de segurança da informação devem ser quantificáveis com base nos objetivos do sistema de gestão de segurança da informação.

110 Para se identificarem as necessidades de informação, é necessário definir o escopo e selecionar as métricas de medição.

111 É recomendável coletar, analisar e desenvolver os resultados de medições.

112 Um programa de medição de segurança da informação deve contemplar análise e avaliação dos riscos.

113 A estrutura operacional de um programa de medição de segurança da informação é determinada de acordo com a complexidade do sistema de gestão de segurança da informação, sendo necessário que as métricas estejam diretamente relacionadas à operação do sistema de gestão de segurança da informação.

114 O desempenho dos processos implementados no sistema de gestão de segurança da informação pode ser um objeto de medição.

115 O estabelecimento de um programa de medição de segurança da informação dentro da organização é de responsabilidade da área responsável pela tecnologia da informação.

Considerando o que dispõe a NBR ISO/IEC 27005, julgue os itens subsecutivos.

116 Requisitos legais e regulatórios a serem necessariamente atendidos pela organização devem fazer parte do escopo da gestão de riscos de segurança da informação.

117 Deve ser recebida como entrada do processo de avaliação de riscos uma lista de cenários de incidentes identificados como relevantes, com as respectivas consequências para os processos de negócio.

118 A perda de uma oportunidade de negócio devido a um evento de segurança da informação é considerada um critério de impacto.

119 Na definição da metodologia de avaliação dos riscos, devem ser identificadas as ameaças que podem afetar os ativos de informação que serão avaliados.

120 Para o tratamento dos riscos, a referida norma estabelece as seguintes opções: reter, reduzir, evitar ou transferir o risco.

cespeUnB
Centro de Seleção e de Promoção de Eventos