(PREVIC 2011) De acordo com as normas NBR/ISO/IEC 27002/2005 e NBR/ISO/IEC 27001/2006 e com o modelo PDCA (plan, do, check, act), adotado por esta última para estruturar os processos do sistema de gestão da segurança da informação (SGSI), julgue os itens a seguir.

107 Na prática, os padrões 27001 e 27002 normalmente são usados em conjunto, embora seja possível o uso de outros controles de segurança da informação juntamente com o padrão 27001, até mesmo em substituição ao padrão 27002.

108 A organização deve fazer análises críticas com o objetivo de identificar tentativas e violações de segurança bem-sucedidas, sendo esta uma atividade verificada na fase check (checar).

No que se refere à classificação e controle de ativos da informação, segurança de ambientes físicos e lógicos e controle de acesso, julgue os itens que se seguem de acordo com as normas NBR/ISO/IEC 27001/2006 e 27002/2005.

109 Como forma de estabelecer um controle mais adequado da segurança da informação, segundo a norma NBR/ISO/IEC 27002/2005, convém considerar os controles de acesso lógico e físico de forma conjunta. As regras e os direitos para cada usuário ou grupo de usuários devem estar claramente expressos na política de controle de acesso.

110 Alcançar e manter a proteção adequada dos ativos da organização é um objetivo de controle estabelecido na norma NBR/ISO/IEC 27001/2006. Associado a esse objetivo, há o controle relativo à remoção de propriedade, o qual determina que um ativo não mais utilizado por um proprietário deverá ser dele desvinculado.

111 Um arquivo de texto, uma IDE para desenvolvimento em linguagem C e um pendrive são classificados como ativos de software, de serviço e físico, respectivamente.

112 Muitos serviços disponíveis na Internet enviam senhas temporárias aos seus usuários. De acordo com a norma NBR/ISO/IEC 27002/2005, essa prática é conveniente, desde que realizada de forma segura, procurando-se evitar o uso de correio eletrônico de terceiros ou sem criptografia.

Acerca da definição, implantação e gestão de políticas de segurança e auditoria, julgue os itens subsequentes.

113 Registros ou logs de auditoria podem conter dados pessoais confidenciais e de intrusos; por isso, é importante que medidas de proteção adequadas sejam tomadas, como, por exemplo, não permitir, quando possível, que administradores de sistemas não tenham permissão de exclusão ou desativação de registros de suas próprias atividades.

114 Uma política de segurança eficaz parte da premissa do uso efetivo de um conjunto de ferramentas de segurança, como firewalls, sistemas de detecção de intrusos, validadores de senha e criptografia forte.

De acordo com as normas NBR/ISO/IEC 15999 e 27005, julgue os próximos itens.

115 De acordo com a norma NBR/ISO/IEC 27005, a comunicação de riscos visa assegurar que as informações sobre os riscos sejam compartilhadas entre os tomadores de decisão e outros stakeholders, buscando-se, assim, alcançar um entendimento de todos sobre como os riscos serão gerenciados.

116 Uma ameaça pode causar impacto em vários ativos ou apenas
em parte de um deles, podendo ter efeitos imediatos (operacionais) ou futuros (negócios).

A respeito de planejamento, identificação e análise de riscos, julgue os itens subsecutivos.

117 Riscos residuais referem-se aos riscos para os quais ainda não foram estabelecidos controles dentro do tratamento de riscos.

118 A transferência de riscos envolve a decisão de transferir o ônus de determinados riscos para terceiros, deixando a cargo destes a atividade de monitoração dos riscos transferidos.

Em relação a plano de continuidade de negócio, julgue os itens seguintes.

119 As análises/avaliações de risco do plano de continuidade do negócio devem envolver os responsáveis pelos processos e recursos do negócio. É importante que essas análises/avaliações não se limitem aos recursos de processamento da informação, mas incluam os resultados específicos da segurança da informação.

120 Os planos de continuidade de negócio devem ser testados e atualizados regularmente, de forma a assegurar que os membros da equipe de recuperação, bem como outros envolvidos, tenham ciência desses planos e de suas responsabilidades para a continuidade do negócio quando um plano for realmente acionado.

(BRB 2011 – Cargo 2) Determinada empresa efetuou, de acordo com a norma ISO/IEC 27002, análise crítica da sua política de segurança, iniciando-a por uma área específica. Uma equipe interna de auditoria, composta por pessoas não relacionadas à área objeto de análise, foi montada especialmente para essa finalidade. Considerando essa situação hipotética e o que dispõe a referida norma, julgue os itens a seguir.

112 Segundo a norma mencionada, as informações de saída geradas pela análise crítica devem conter, entre outras, tendências relacionadas a ameaças e vulnerabilidades, assim como relatos acerca de incidentes de segurança ocorridos na área analisada.

113 Suponha que a equipe de auditoria, por meio da análise do documento de política de segurança da informação e dos controles estabelecidos para a área avaliada, tenha observado que a referida área estava provendo novos serviços disponibilizados via Web sem avaliação/análise de risco nem detalhamento dos controles de segurança relativos a tais serviços. Nesse caso, é correto afirmar que o procedimento adotado pela área avaliada não atende ao que dispõe a norma em questão.

De uma lanchonete na Georgia (EUA), um ex-funcionário de uma empresa farmacêutica norte-americana conseguiu apagar a maior parte da infraestrutura de computadores dessa companhia. Usando uma conta de usuário, o ex-funcionário acessou a rede da empresa e disparou o console de gerenciamento vSphere Vmware instalado secretamente por ele próprio na rede da companhia algumas semanas antes da sua demissão. Pelo vSphere, ele apagou 88 servidores dos sistemas de hospedagem VMware da empresa, um a um.

Acerca da situação descrita no texto acima e considerando o disposto na norma ISO/IEC 27002, julgue os itens subsequentes.

114 Considerando-se as recomendações da norma ISO/IEC 27002, infere-se que houve falha da empresa na implementação dos controles relativos à segurança de recursos humanos.

115 Na situação descrita, houve violações de confidencialidade, integridade e disponibilidade nos ativos da empresa.

Com relação a mecanismos de segurança, julgue os itens que se seguem.

116 Honeypots são mecanismos de segurança, geralmente isolados e monitorados, que aparentam conter informação útil e valiosa para a organização. São armadilhas para enganar agentes invasores como spammers ou crackers.

117 Conforme disposto na norma ISO/IEC 27002, sistemas biométricos podem ser utilizados como mecanismos de controle de acesso. Considerando-se essa informação, é correto afirmar que uma porta com dispositivo biométrico de leitura de impressão digital para se acessar uma sala de servidores caracteriza um controle de acesso lógico.

Um banco inglês informou a 34 mil investidores que seus dados pessoais podem ter sido roubados durante o encaminhamento de material para o departamento fiscal do governo. As informações estavam em dois CD-ROMs protegidos com senhas, mas não criptografados. O porta-voz do banco disse que, apesar de o pacote ter chegado intacto ao escritório do governo, quando chegou ao setor correto, os CDs não estavam mais lá.

Com relação à situação apresentada no texto acima, no que se refere a gerenciamento de segurança da informação e considerando o disposto na norma ISO/IEC 27002, julgue os próximos itens.

119 Na situação descrita, foram violados os controles associados à segurança física.

120 Na situação em apreço, não foram devidamente implementados os controles referentes à segurança lógica.

(TRE-ES 2011 – Análise de Sistemas) Com base na ABNT NBR ISO/IEC 17799/2005, que trata de questões de segurança da informação nas organizações, julgue os próximos itens.

88 O documento relativo à política de segurança da informação deve ser aprovado pela direção da empresa, publicado e comunicado a todos os funcionários e às partes externas relevantes.

89 As instalações de processamento da informação gerenciadas pela organização podem permanecer fisicamente juntas das que são gerenciadas por terceiros, desde que o acesso ao local seja devidamente controlado.

90 As ações que minimizam o risco de vazamento de informações mediante o uso e a exploração de covert channels incluem a varredura do envio de mídias e comunicações, para verificação da presença de informação oculta; o mascaramento e a modulação do comportamento dos sistemas e das comunicações, a fim de evitar que terceiros subtraiam informações dos

sistemas; e o monitoramento regular do uso dos recursos computacionais e das atividades do pessoal.

91 A autenticação de usuários remotos pode ser alcançada com o emprego de técnicas de criptografia, hardware tokens ou protocolo de desafio/resposta. Essas técnicas são utilizadas em várias soluções de Virtual Private Network.

92 Nessa norma, são estabelecidos as diretrizes e os princípios gerais para o início, a implementação, a manutenção e a melhoria da gestão de segurança da informação em uma organização.

(MEC 2011 – Gerente de Segurança) Julgue os próximos itens, relativos a sistema de gestão de segurança da informação (SGSI).

81 No estabelecimento do SGSI, deve-se definir seu escopo e seus limites, junto com uma política específica, a qual deve estar alinhada às metas de negócio.

82 A formulação de um plano de tratamento de riscos é uma das atividades que ocorre após a implementação e operação de um SGSI.

83 O controle dos registros referentes ao SGSI restringe-se aos aspectos referentes aos eventos de natureza técnica.

84 A rastreabilidade de decisões, remetendo a políticas e decisões da direção superior, é um dos requisitos de um SGSI.

85 O SGSI adota o modelo PDCA (plan-do-check-act), que estrutura todos os processos, visando proporcionar melhoria contínua.

Com relação aos controles a serem implementados em um SGSI, julgue os itens seguintes.

86 Os usuários devem ser conscientizados e educados no que diz respeito à segurança da informação, uma vez que recai sobre eles a responsabilização pelos eventos em que venham a se envolver, como quebras de segurança e erros de operação.

87 O código fonte de programas é um bem informacional que requer proteção adequada, podendo até conter segredos de negócio; assim, seu acesso deve ser restrito e sujeito a controles de acesso.

88 Acordos de não divulgação que reflitam as necessidades da organização para proteção da informação devem ser revisados sempre que houver vazamento de informação.

89 Os controles relativos a movimentação de equipamentos, informações ou software são similares aos controles patrimoniais relativos a outros bens; assim, esses itens só devem ser removidos com autorização prévia e devido registro.

90 As responsabilidades pela segurança da informação devem estar claramente definidas, oferecendo-se, como contrapartida, aos responsáveis os poderes necessários para implementação e operação dos controles, de forma a viabilizar o atendimento aos requisitos de segurança específicos.

Julgue os itens a seguir, relativos à gestão de continuidade de negócio (GCN).

91 A política de GCN define os processos relativos às atividades de preparação para estabelecer a capacidade de continuidade de negócios e o gerenciamento contínuo dessa capacidade.

92 Admite-se que o tempo planejado para a recuperação da normalidade de funcionamento do negócio seja maior que o tempo máximo de interrupção desse funcionamento.

93 Na documentação relativa à GCN, devem estar incluídos, entre outros, documentos relativos à política de GCN, à análise de impacto nos negócios e à avaliação de riscos e ameaças.

94 A GCN não tem relação com o gerenciamento de riscos.