CONHECIMENTOS ESPECÍFICOS

Acerca de gestão de segurança da informação, seus conceitos e definições, julgue os itens que se seguem.

51 A atividade de avaliação de riscos em segurança da informação consiste na identificação de fontes e estimativas de riscos por meio do uso sistemático de informações, obtidas mediante observação.

52 Um incidente, também conhecido como evento de segurança da informação, é definido como a ocorrência de uma situação inesperada, com a qual a organização não estava preparada para lidar.

53 A segurança da informação pode ser entendida como uma atividade voltada à preservação de princípios básicos, como confidencialidade, integridade e disponibilidade da informação.

54 Ativo, em segurança da informação, refere-se aos itens financeiros que precisam ser protegidos, pois representam valor para a organização e devem ser preservados.

A respeito de aspectos gerais da norma ABNT NBR ISO/IEC 27001, julgue os itens a seguir. Nesse sentido, considere que a sigla SGSI, sempre que empregada, refere-se a sistema de gestão da segurança da informação.

55 De acordo com a referida norma, a exclusão de qualquer critério de aceitação dos riscos deve ser feita mediante justificativa e evidências de que os riscos serão aceitos pelas pessoas responsáveis por eles.

56 A abordagem em processo tem como ponto de partida a visão da gestão da segurança como um ciclo PDCA.

57 A mencionada norma está voltada para criação de um SGSI, no entanto ela não possui alinhamento com as normas ISO 9001 ou 140001, visto que estas se referem a sistemas de gestão da qualidade.

58 Os requisitos propostos pela referida norma são especificados apenas para planejar e desenhar um SGSI em forma de projeto, pois sua implementação fica a cargo de outras normas mais específicas da série 27000.

59 A melhoria contínua do SGSI, assim como a análise crítica de sua implementação, faz parte da etapa DO (fazer) do PDCA aplicado ao processo.

60 A grande contribuição da norma citada é o fato de ela destinar-se a todos os tipos de organizações, em qualquer país, que possuam a tecnologia da informação como a sua atividade-fim.

Com relação aos requisitos para o SGSI, de acordo com a ABNT NBR ISO/IEC 27001, julgue os itens de **61** a **65**.

61 Para que a implementação e a operação do SGSI sejam feitas em conformidade com a norma em questão, as organizações devem definir como será medida a eficácia dos controles ou grupos de controles selecionados. Assim, será possível comparar ou reproduzir os resultados da implementação desses controles.

62 A documentação de um SGSI é um item de grande importância no processo, pois contém informações sobre todo o processo. Essa documentação é composta, entre outras, pela declaração da política e dos objetivos do SGSI, de seu escopo e dos procedimentos e controles que apoiam o SGSI.

63 Selecionar objetivos de controle e controles para o tratamento de riscos não é tarefa inerente ao estabelecimento do SGSI, pois essa atividade é própria do tratamento dos riscos, que é feito apenas após a ocorrência de eventos e incidentes.

64 A responsabilidade pela implantação do SGSI cabe exclusivamente aos profissionais da área de TI; a direção da organização apenas acompanha o processo.

65 O processo de melhoria do SGSI, previsto pela norma em apreço, consiste em identificar não conformidades potenciais e suas causas; avaliar a necessidade de ações para evitar a ocorrência de não conformidades; determinar e implementar ações preventivas necessárias.

No que se refere aos objetivos de controle, contidos no Anexo A (normativo) ABNT NBR ISO/IEC 27001, julgue os itens subsequentes.

66 Conforme prevê a norma em apreço, em acordo com terceiros referente à aquisição de produtos de TI, dispensa-se o controle do SGSI no que diz respeito a segurança da informação.

67 A violação da política de segurança da informação deve ser apurada por meio da aplicação de processo disciplinar formal: é o que estabelece o controle de processo disciplinar contido no grupo de controle de segurança em recursos humanos.

68 A integridade de informações disponibilizadas em sistemas acessíveis publicamente não precisa ser alvo da política de segurança, visto que são, por natureza, informações não confidenciais, ou seja, públicas.

69 Entre os controles referentes ao gerenciamento de acesso do usuário, tendo-se em vista assegurar o acesso autorizado e prevenir o não autorizado, o anexo em questão estabelece que a análise crítica de direitos de acesso dos usuários deve ser feita por meio de um processo formal e conduzida em intervalos regulares.

70 A referida norma é explícita ao afirmar que, em razão de seu caráter privativo, as políticas e procedimentos de segurança de uma organização não podem ser expostos à opinião de outros, o que impossibilita contatos com grupos de interesses especiais ou ainda a promoção de fóruns especializados de segurança da informação e associações profissionais.

Com base nos aspectos gerais da norma ABNT NBR ISO/IEC 27002, que estabelece o código de prática para a gestão da segurança da informação, julgue os itens que se seguem.

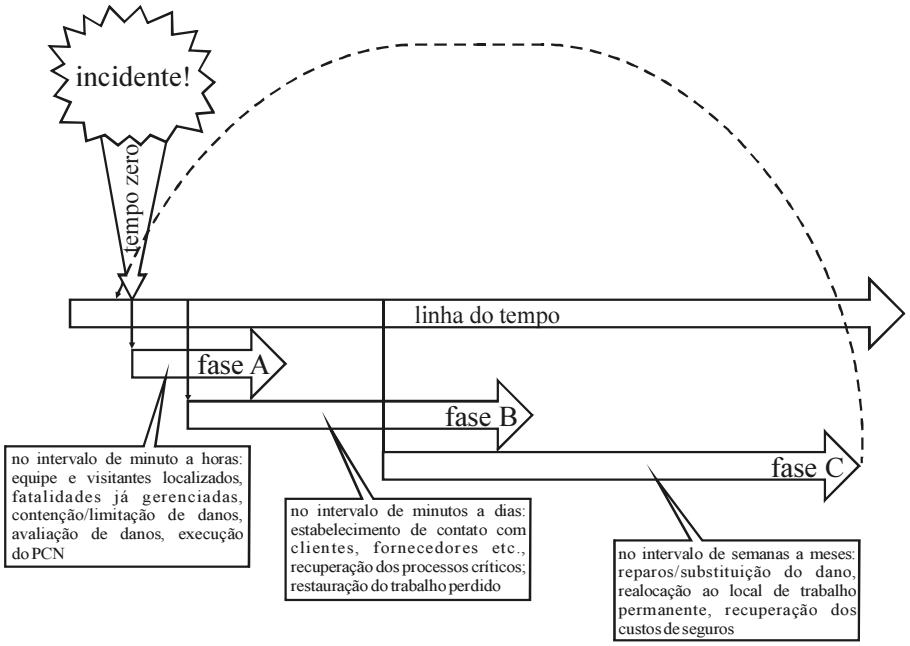
71 A conformidade não é um dos conteúdos da referida norma, pois não visa à obtenção de certificação, já que essa incumbência fica a cargo de empresas privadas responsáveis pala análise de conformidade da prática de empresas às práticas recomendadas tanto pela NBR 27002 quanto pela NBR 27001.

72 Uma análise de riscos deve ser realizada periodicamente em um ambiente computacional, principalmente quando houver a mudança nos requisitos de segurança ou quando surgirem novas ameaças ou vulnerabilidades que ponham em risco a segurança.

73 Requisitos de segurança da informação podem ser obtidos a partir da análise/avaliação dos riscos da organização com base nos seus objetivos estratégicos; a partir da legislação vigente; e, finalmente, a partir dos requisitos do negócio para o processamento da informação que a organização desenvolve para realizar suas operações.

74 A proteção de dados e privacidade de informações pessoais, de registros organizacionais e os direitos de propriedade intelectual muitas vezes são vistos erroneamente como controles essenciais para uma organização.

75 A norma em apreço estabelece diretrizes e princípios para a segurança da informação, no entanto a implementação de seus objetivos de controles e dos controles não garante o atendimento aos requisitos de segurança da informação, pois a implementação é de responsabilidade do SGSI.



Norma ISO 15999-1, p. 25, item 8.2.4 – Nota Técnica.

A partir da figura acima, que ilustra as fases de tempo de um incidente, julgue os próximos itens.

76 A fase C corresponde à continuidade de negócios.

77 Em alguns casos, a ativação dos planos das fases A, B e C pode ocorrer em rápida sucessão ou simultaneamente.

78 Em organizações pequenas, a responsabilidade pelas fases A e B pode ser atribuída um único indivíduo.

Com relação a conteúdo prático, objetivos de controles e diretrizes para implementação recomendados pela norma ABNT NBR ISO/IEC 27002, julgue os itens de **79** a **88**.

79 Cabe exclusivamente aos gestores e administradores a coordenação da segurança da informação dentro de uma organização.

80 A responsabilidade por um ativo de informação na organização deve ser atribuída às equipes de suporte estabelecidas e nomeadas. De acordo com a norma vigente, veda-se, por exemplo, responsabilizar um usuário por um ativo inventariado.

81 Em gestão da segurança da informação, só devem ser classificadas as informações que possuam algum valor para a organização, ou seja, aquelas cuja divulgação traga algum malefício financeiro ou de imagem a qualquer indivíduo que nela trabalhe.

82 Uma informação deve ser classificada de acordo com os seus requisitos de confidencialidade, integridade e disponibilidade, não havendo, nessa norma, indicação de parâmetros para outros tipos de requisitos a serem considerados.

83 A ação de se evitar um risco, de modo a eliminar a ocorrência de suas consequências e, naturalmente, a realização da atividade que o ocasionaria, não faz parte do tratamento do risco, pois o tratamento refere-se ao risco que se toma, não ao que se evita.

84 As consequências da violação da política de segurança devem ser incluídas em um plano de tratamento de riscos, mas não devem fazer parte do documento da política em si.

85 Segundo a citada norma, convém que a política de segurança seja analisada crítica e periodicamente, à luz do resultado do desempenho do processo e de acordo com a política de segurança da informação.

86 A norma em questão recomenda que sejam incluídas, na política de segurança da informação, declarações que esclareçam termos e condições de trabalho de recursos humanos, incluindo até responsabilidades que se estendam para fora das dependências da organização e fora dos horários normais de trabalho.

87 Recuperação de erros, procedimentos de reinicialização e planos de contingência, apesar de serem bem específicos ao processo de aceitação de sistemas, devem ser considerados para minimizar os riscos de falhas de sistemas, no gerenciamento de operações e comunicações preconizado pela norma 27002.

88 A norma referida recomenda que se realizem treinamento, educação e conscientização de pessoas apenas antes da contratação, para assegurar que os novos recursos humanos saibam agir com segurança diante das atividades a serem desenvolvidas por eles.

Acerca de ataques maliciosos a redes de computadores, julgue os itens seguintes.

89 Normalmente, no planejamento de um ataque, o invasor determina o caminho e os filtros de acesso implementados nos roteadores e *firewalls*.

90 A coleta de informações e dados sobre o sítio ou os servidores do alvo é um dos principais pontos de partida de um ataque a redes de computadores.

91 O invasor que idealiza um ataque a redes de computadores interessa-se, entre outros aspectos, pela topologia de rede, pelas informações úteis para ataques por meio de engenharia social, pelos tipos de serviços disponíveis, pelo cadastro da empresa na Internet e pelos ataques executados contra a empresa no passado.

92 De forma geral, os ataques a redes de computadores compõem-se das seguintes fases: planejamento, coleta de dados, aproximação, invasão e exploração.

93 A técnica de *spoofing* é normalmente utilizada na fase de invasão a redes de computadores.

A respeito de prevenção e tratamento de incidentes, julgue os itens que se seguem.

94 Convém que as organizações adotem uma estrutura simples, que permita uma rápida reestruturação e a confirmação da natureza e da extensão do incidente, além de possibilitar o controle da situação e do incidente e a comunicação com as partes interessadas.

95 Um plano de gerenciamento de incidentes cria condições para que a organização gerencie todas as fases de um incidente.

96 O plano de recuperação de negócios visa, entre outros objetivos, prevenir maiores perdas ou indisponibilidade de atividades críticas e dos recursos que as suportam.

Com base na NBR ISO/IEC 15999, julgue os itens de **97** a **104**.

97 As apólices de seguro são estratégias eficazes e suficientes para o tratamento de risco, pois garantem recompensa financeira para as perdas mais significativas da organização.

98 A gestão de riscos de uma organização só será considerada eficiente se conseguir eliminar todos os riscos internos e também os externos.

99 A organização deve manter e melhorar a eficiência e a eficácia do SGCN por meio de ações corretivas e preventivas, quando assim determinar a análise crítica da direção.

100 Define-se a análise de impacto nos negócios — do inglês *business impact analysis* (BIA) — como o processo de análise das funções de negócio e dos possíveis efeitos causados nessas funções por uma interrupção.

101 A política de gestão da continuidade de negócios (GCN), proposta pela direção administrativa da empresa, deve ser aprovada pela alta direção e, em seguida, comunicada somente aos empregados da área de TI, já que o sigilo é imprescindível para o seu sucesso.

102 O plano de continuidade de negócios deve ser testado, de forma que se garanta sua correta execução a partir de instruções suficientemente detalhadas. Adotado esse plano, não convém que a organização providencie auditoria externa, já que essa auditoria poderá comprometer os dados sigilosos da organização.

103 A alta direção deve participar da análise crítica da capacidade de gestão da continuidade do negócio da organização, de forma a garantir sua aplicabilidade, adequação e funcionalidade.

104 O tempo objetivado de recuperação (*recovery time objective*) é o tempo-alvo para a retomada da entrega de produtos, serviços ou atividades após a ocorrência de um incidente.

De acordo com a NBR ISO/IEC 27005, julgue os próximos itens.

105 A conscientização dos gestores a respeito dos riscos, da natureza dos controles aplicados para mitigá-los e das áreas definidas como de interesse pela organização auxilia a organização na gestão dos incidentes e eventos previstos, porém não influencia no tratamento dos incidentes não previstos.

106 A existência de vulnerabilidade, ainda que não se verifique ameaça a ela relacionada, requer, necessariamente, a implementação de controle apropriado.

107 Na fase "planejar" de um SGSI, define-se o contexto, procede-se à avaliação de riscos, desenvolve-se o plano de tratamento do risco e definem-se os critérios de aceitação do risco.

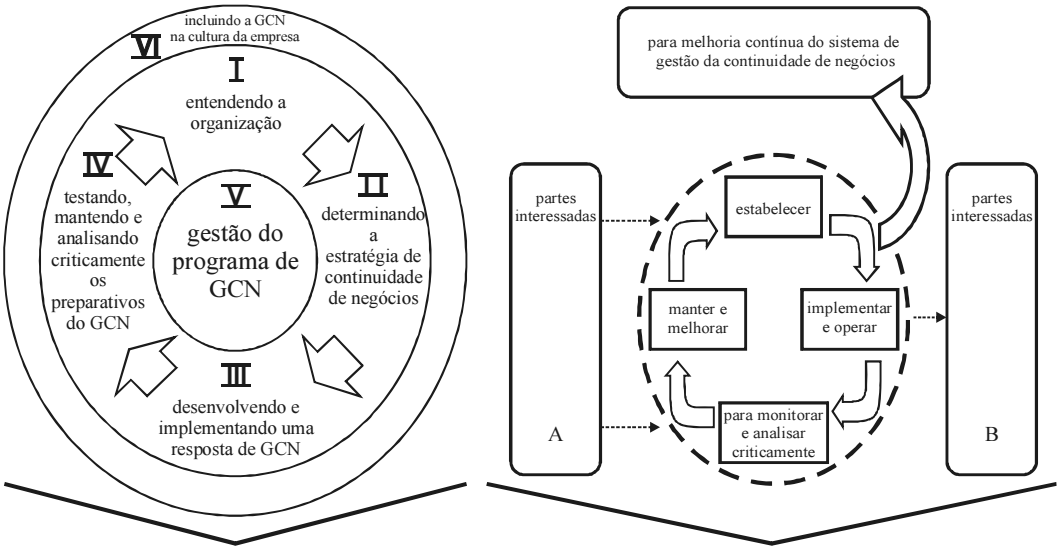
108 No processo de identificação das ameaças, devem-se considerar o não atendimento à legislação, agentes de danos físicos ou tecnológicos, ações não autorizadas e aspectos culturais.

109 A definição, pela organização, dos critérios para aceitação do risco depende de suas políticas, metas e objetivos. Uma vez definidos, esses critérios devem ser utilizados para todas as classes de risco.

110 O nível de detalhamento da identificação dos ativos de uma organização pode influenciar na quantidade de informações reunidas durante a avaliação de riscos.

111 Define-se evento como a combinação das consequências advindas da ocorrência de uma situação indesejada com a probabilidade de essa situação ocorrer.

112 A integração de novos controles de risco à infraestrutura existente e a interdependência entre controles existentes são fatores constantemente ignorados pelos gestores de segurança da informação.



Norma ISO 15999-2, p. vii

Tendo como referência a figura acima, julgue os itens que se seguem, a respeito do ciclo de vida da GCN.

113 Na figura, I corresponde ao elemento que garante que o programa de GCN esteja alinhado aos objetivos, às obrigações e às responsabilidades legais da organização.

114 Na figura, o elemento do ciclo de vida de GCN cujo objetivo é garantir a continuidade das atividades críticas e o gerenciamento dos incidentes é indicado por III.

115 O período máximo de interrupção tolerável da atividade crítica é indicado, na figura, por IV.

116 É fundamental, para que o processo de GCN seja corretamente introduzido na organização e se estabeleça como parte de sua cultura, a participação da alta direção. Na figura em apreço, a participação da alta direção corresponde à gestão do programa de GCN.

117 O elemento A da parte 2 da figura ilustra a possibilidade de que, em um sistema de gestão de continuidade de negócios (SGCN), a entrada corresponda às necessidades da continuidade de negócios e às expectativas das partes interessadas.

118 Na parte 2 da figura, o elemento B corresponde aos resultados da continuidade de negócios que atendem aos requisitos e às expectativas iniciais das partes interessadas, como, por exemplo, a continuidade de negócios gerenciada.

119 A parte 2 da figura, que representa o ciclo de vida da continuidade de negócios, não pode ser incluída em nenhuma atividade da parte 1 da figura, que representa o modelo PDCA (*plan do check act*).

120 É necessário que as partes interessadas da organização confiem na capacidade de ela sobreviver a interrupções. Na figura, o elemento responsável por garantir essa confiança é representado por V.