Questão 1

Continuando com o exemplo do estudo de caso para aplicação dos itens da Norma ABNT NBR ISO/IEC 27001:2013 da empresa de web hosting que busca a conformidade para o seu Sistema de Gestão de Segurança da Informação, e considerando as mesmas sugestões e premissas definidas no início dos conceitos deste módulo, veja a seguinte descrição da cena/ocorrência:

	Registro de não conformidade (NC)		
Cenas/Ocorrência	Req. ISO/IEC 27001	Existe NC?	Descrição da NC da evidência objetiva ou indicação do qu fazer a seguir
Um dos auditores internos é responsável pela administração do banco de dados em um setor. Como na auditoria metade da equipe da empresa viajou para treinamento do novo sistema, ele acabou auditando também a sua área, incluindo partes do seu trabalho.		( ) Sim ( ) Não ( ) Simples Obs. ( ) Falta informação	

Marque a alternativa que representa o parecer mais adequado do auditor para a descrição da cena.

A Existe não conformidade, os auditores não devem auditar seu próprio trabalho.

B A descrição é uma simples observação para uma descrição importante que ainda não foi feita.

C A prática está em conformidade com a norma, tendo em vista a possibilidade de a equipe ser pequena e o funcionário possuir competência para tal.

D Faltam as informações se esse fato estava previsto nos critérios dessa auditoria e se a imparcialidade foi assegurada. check_circle

E É preciso aprimorar a prática para se adequar à norma.

check_circle

Parabéns! A alternativa D está correta.

Na realidade, todas as respostas podem estar corretas, mas conforme já informado, iremos analisar com as sugestões e premissas estabelecidas no primeiro exemplo.

Essa cena será enquadrada no item 9.2, *Auditoria Interna*.

A letra A estaria correta se estivéssemos utilizando a norma ABNT NBR ISO/IEC 27001:2006, que cita exatamente que os auditores não devem auditar seu próprio trabalho. Essa frase deixou de existir na versão 2013, embora ainda seja uma boa prática.

Na letra B, pode até ser que venha uma descrição mais importante, mas iremos nos ater apenas à descrição, que já é suficiente para o auditor analisar na norma ou fazer questionamentos ao auditado.

A letra C não está correta, pois faltam informações sobre algumas frases do item da norma.

Enfim, na letra D, o auditor realizará exatamente as perguntas sobre as informações faltantes descritas, e ainda cabe mais uma, se esse acontecimento (auditar o próprio trabalho) está previsto no programa de auditoria.

Questão 2

Leia a notícia a seguir extraída de um site da web, para aplicação dos itens da Norma ABNT NBR ISO/IEC 27002:2013:

Quando o Deutsche Bank perdeu seus escritórios nos ataques de 11 de setembro, os funcionários puderam acessar o e-mail corporativo no dia seguinte para que pudessem se conectar com clientes e colegas de trabalho em casa. "Tivemos acesso aos nossos arquivos, embora a TI estivesse na Torre Dois do World Trade Center", diz uma fonte. "Tivemos backup em Jersey City. Não perdemos nada. Tenho amigos que trabalham em empresas menores que não ficaram dois meses sem poder ir ao escritório. O escritório de advocacia de um amigo faliu" (DEUTSCHE BANK, 2009).

Este relato de adoção de medidas de proteção, nestes termos, poderá ser melhor enquadrado no item da Norma ISO/IEC 27002:2013.

A 7.1: Antes da contratação, dentro do item 7, *Segurança em Recursos Humanos*.

B 9.2: Gerenciamento de acesso do usuário, dentro do item 9, *Controle de Acesso*.

C 10.1: Controles criptográficos, dentro do item 10, *Criptografia*.

D 17.1: Continuidade da segurança da informação, dentro do item 17, *Aspectos da segurança da informação na Gestão da Continuidade do Negócio*. check_circle

E 9.4.1: Restrição de acesso à informação.

check_circle

Parabéns! A alternativa D está correta.

Este é um relato jornalístico que carece de detalhes, mas usaremos para fins didáticos. Também faltam os subitens de cada uma das subseções citadas, mas a análise do exercício ficaria muito extensa.

Para melhor enquadramento a um item da Norma ISO/IEC 27002:2013, vamos analisar o objetivo de controle de cada item:

Letra a) 7.1: Antes da contratação. Objetivo: Assegurar que funcionários e partes externas entendem as suas responsabilidades e estão em conformidade com os papéis para os quais eles foram selecionados.
Letra b) 9.2: Gerenciamento de acesso do usuário. Objetivo: Assegurar acesso do usuário autorizado e prevenir acesso não autorizado a sistemas e serviços.
Letra c) 10.1: Controles criptográficos. Objetivo: Assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou integridade da informação.
Letra d) 17.1: Continuidade da segurança da informação. Objetivo: Convém que a continuidade da segurança da informação seja contemplada nos sistemas de gestão da continuidade do negócio da organização.