Exercícios sobre a norma ISO 27000 e suas derivadas:

1) A respeito da norma ISO/IEC 27002/2005 julgue os itens seguintes:

1. Para se obter uma certificação segundo a norma ISO/IEC 27002/2005 será necessário, entre outros controles, proteger dados pessoais e privacidade das pessoas, Os registros da organização, e, os direitos de propriedade intelectual.

2. São fontes de requisitos de SI , segundo a supracitada norma, a análise de riscos, a legislação pertinente e os princípio organizacionais.

3. Para estar em conformidade com supracitada norma, todos os controles nela previstos devem ser implantados em qualquer tipo de Organização.

4. Segundo a supracitada norma, a delegação de responsabilidades, e o treinamento formal dos usuários nos princípios de SI são considerados requisitos “essenciais”de SI.

Assinale a opção que se refere corretamente aos quatro itens acima.

A) As afirmativas 1, 3, 4 estão corretas.
B) Apenas as afirmativas 2 e 3 não estão corretas.
C) Apenas a afirmativa 2 está correta.
D) A afirmativa 4 é verdadeira e a 2 é falsa.
E) Todas as afirmativas são falsas.

2) Segundo os fundamentos da norma iso/iec 27002/2005 analise as afirmativas e associe as colunas.

1) Comitê de segurança da informação.

2) Controle.

3) Funções de software e hardware.

4) Deve ser analisado criticamente.

5) Política.

( ) Controle.

( ) Firewall.

( ) estrutura organizacional.

( ) Permissão de acesso a um servidor.

( ) Ampla divulgação das normas de segurança da informação.

A) 4-3-1-2-5.

B) 1-2-4-3-5.

C) 5-1-4-3-2.

D) 4-3-5-2-1.

E) 2-3-1-5-4.

3) Conforme as normas ABNT NBR 27001, 27002 e 27005, um documento da política de segurança da informação deve:

A) conter o registro dos incidentes de segurança da organização.revelar informações sensíveis da organização.

B) ser aprovado pela direção, bem como publicado e comunicado para todos que tenham contato com a organização.

C) conter uma declaração de comprometimento elaborada por todos aqueles que atuam na organização, inclusive pela direção.

D) apresentar uma declaração de aplicabilidade dos controles de segurança da informação, além de definir como será o processo de gestão de riscos.

4) Ao se identificar quais seriam as informações que, caso percam a confiabilidade, a integridade e a disponibilidade, trariam prejuízos à organização, e, ao se localizar onde tais informações são processadas e armazenadas, as áreas críticas de informação e os locais que precisam ser protegidos serão determinados.

A) Certo.

B) Errado.

5) Sobre a estrutura, objetivos e conceitos gerais da Norma NBR ISO/IEC 27002, é correto afirmar:

A) Contém 21 seções de controles de segurança da informação, que juntas totalizam 59 categorias principais que abordam a análise/avaliação e o tratamento de riscos.

B) Define avaliação de riscos como um conjunto de atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos. Geralmente inclui o tratamento de riscos, a aceitação de riscos e a comunicação de riscos.

C) Define política como sendo as intenções e diretrizes globais formalmente expressas pela direção e define risco como sendo a combinação da probabilidade de um evento e de suas consequências.

D) Define segurança da informação como forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.

E) Tem como objetivo geral especificar os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto dos riscos de negócio globais da organização.

6) De acordo com a Norma ABNT NBR ISO/IEC 27002:2005, convém que o processo de planejamento da continuidade de negócios considere uma série de itens, EXCETO:

A) Implementação dos procedimentos que permitam a recuperação e restauração das operações do negócio e da disponibilidade da informação nos prazos necessários.

B) Identificação da perda aceitável de informações e serviços

C) Educação adequada de pessoas nos procedimentos e processos definidos, incluindo o gerenciamento de crise.

D) Documentação dos processos e procedimentos acordados.

E) Avaliação da gestão da continuidade de negócios, tendo como referência o grau da inserção da mesma na gestão corporativa.

7) A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização. Sobre os ativos, segundo a Norma ABNT NBR ISO/IEC 27002:2005, é correto afirmar:

A) Alguns ativos de informação, como documentos em forma eletrônica, não podem ser fisicamente rotulados, sendo necessário usar um rótulo eletrônico.

B) O inventário do ativo deve incluir apenas seu tipo, formato e localização, pois essas são as únicas informações relevantes para o caso da recuperação de um desastre.

C) A implementação de controles específicos não pode ser delegada pelo proprietário do ativo, mesmo sendo ele o único responsável pelos controles e pela proteção adequada de seus ativos.

D) Todos os ativos devem ter um alto nível de proteção pois, independentemente da sua importância, possuem valor para o negócio.

E) O processo de compilação de um inventário de ativos é importante, mas não é pré-requisito no gerenciamento de riscos.

8) Com relação a conteúdo prático, objetivos de controles e diretrizes para implementação recomendados pela norma ABNT NBR ISO/IEC 27002, julgue os itens:

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.

A) Certo

B) Errado