

INTRODUÇÃO A SEGURANÇA DA INFORMAÇÃO

1. Assinale a assertiva que representa um dos benefícios para a adoção da norma ABNT NBR ISO/IEC 27001:2013 por uma organização

- ☐ Mecanismo para eliminar o sucesso do sistema
- ☐ Fornece insegurança a todas as partes interessadas
- ☐ Não participação da gerência na Segurança da Informação
- ☐ Isola recursos com outros sistemas de gerenciamento
- ☒ Oportunidade de identificar e eliminar fraquezas

2. (Ano: 2009 Banca: FCC Órgão: TCE-GO Prova: FCC - 2009 - TCE-GO - Técnico de Controle Externo - Tecnologia da Informação)

Em relação à segurança da informação e aos controles de acesso físico e lógico, considere:

I. Se um usuário não faz mais parte de um grupo de acesso aos recursos de processamento da informação, é certo que o grupo seja extinto com a criação de um novo, contendo os usuários remanescentes.

II. Direitos de acesso (físicos e lógicos) que não foram aprovados para um novo trabalho devem ser retirados ou adaptados, incluindo chaves e qualquer tipo de identificação que associe a pessoa ao novo projeto.

III. O acesso às áreas em que são processadas ou armazenadas informações sensíveis deve ser controlado e restrito às pessoas autorizadas, preferencialmente por controles de autenticação, por exemplo, cartão de controle de acesso mais PIN (personal identification number).

Está correto o que se afirma em:

- ☐ III, apenas.
- ☒ II e III, apenas.
- ☒ I, II e III.
- ☐ I e III, apenas.
- ☐ I e II, apenas.

3. Assinale a assertiva que **NÃO** representa um dos benefícios para a adoção da norma ABNT NBR ISO/IEC 27001:2013 por uma organização:

- ☒ Isola recursos com outros sistemas de gerenciamento
- ☒ Participação da gerência na Segurança da Informação
- ☐ Oportunidade de identificar e eliminar fraquezas
- ☐ Fornece segurança a todas as partes interessadas
- ☐ Mecanismo para minimizar o fracasso do sistema

4. O item 12.2.1 da norma ABNT NBR ISO/IEC 27002:2013 diz respeito aos controles contra *malware*, cujas diretrizes para implementação recomendam a proteção contra códigos maliciosos baseada em softwares de detecção de *malware* e reparo, na conscientização da informação, no controle de acesso adequado e nos planos de continuidade de negócio.

Com base no acima exposto, e no seu conhecimento de segurança da informação e sistemas de computação, marque a alternativa que possui uma das diretrizes recomendadas

- ☐ Ignorar informalmente a presença de quaisquer arquivos não aprovados ou atualização não autorizada
- ✓ ☒ Estabelecer uma política formal para proteção contra os riscos associados com a importação de arquivos e softwares, seja de redes externas, ou por qualquer outro meio, indicando quais medidas preventivas devem ser adotadas
- ☐ Estabelecer uma política informal proibindo o uso de *softwares* autorizados
- ☐ Conduzir análises informais, esporádicas e descompromissadas dos softwares e dados dos sistemas que suportam processos críticos de negócio
- ☐ Instalar e atualizar regularmente softwares de detecção e remoção de *malware*, independentemente da fabricante, procedência e confiabilidade, para o exame de computadores e mídias magnéticas

5. Qual norma técnica possui o seguinte título: **“Tecnologia da informação e Técnicas de segurança e Sistemas de gestão da segurança da informação e Requisitos”**?

- ☐ ABNT NBR ISO/IEC 27002:2013
- ☐ ABNT NBR ISO 9001:2008
- ☐ ABNT NBR ISO 14001:2004
- ✓ ☒ ABNT NBR ISO/IEC 27001:2013
- ✗ ☐ ABNT NBR ISO/IEC 20000-1:2011

6. "O acesso é atribuído pelo administrador do sistema e é estritamente baseado na função do sujeito dentro da família ou organização e a maioria dos privilégios se baseia nas limitações definidas pelas responsabilidades do trabalho". Selecione a opção que corresponde a esse tipo de controle de acesso:

- ✗ ☐ Controle de acesso obrigatório (MAC).
- ☐ Controle de acesso total (TAC).
- ☐ Controle de acesso discricionário (DAC).
- ✓ ☒ Controle baseado em papéis (RBAC).
- ☐ Controle de acesso segregado (SAC).

7. Normalmente quando o assunto segurança da informação é discutido, as pessoas acabam associando o tema a *hackers*, vulnerabilidade em sistemas e vazamento de informações. E limitam-se a acreditar que é necessário **apenas** um bom antivírus e *firewalls* para proteger o ambiente tecnológico. No entanto, a segurança da informação não se limita apenas a estes pontos. Há outros aspectos que precisam ser considerados também.

Diante deste contexto, pode-se esclarecer que o ponto de partida de qualquer sistema de segurança é garantir o acesso a dados, equipamentos, demais sistemas e ambientes físicos e eletrônicos aos indivíduos autorizados. A esta característica dá-se o nome de (I) e a forma mais simples de oferecê-la é por meio do *login* e da senha de acesso.

No texto acima, (I) refere-se a:

- ✓ ☒ Autenticidade
- ☐ Disponibilidade
- ☐ Não repúdio.
- ☐ Confidencialidade
- ☐ Integridade

8. *“A informação em conjunto com recursos tecnológicos é uma necessidade para o funcionamento tático, estratégico e operacional de qualquer empresa. Para vencer no mundo dos negócios, é preciso saber obter a informação como ferramenta estratégica de competitividade. Precisamos saber onde encontrar a informação, como apresentá-la e como usá-la, assim como é fundamental conhecê-la. Precisamos estar sempre atentos ao que acontece fora e dentro das organizações.”* (Trecho consultado em 02/10/20, extraído de < <https://administradores.com.br/producao-academica/a-importancia-da-informacao>>)

O trecho acima reflete parte da relevância da informação no contexto organizacional. Mas sabemos que usualmente há equívoco na definição dos

conceitos de Dados, Informação e Conhecimento. Diante do exposto, assinale a alternativa que os elucida corretamente.

- ☒ ☐ Dado é um fato bruto não lapidado; II. Informação depende da interpretação pessoal de cada indivíduo sobre dados agrupados; III. Conhecimento é representado pelo agrupamento dos dados.
- ☒ ☐ Dado é um fato bruto não lapidado; II. Informação é a junção de dados que foram contextualizados; III. Conhecimento é pessoal, isto é, depende da interpretação das informações juntamente com as vivências/experiências pessoais.
- ☐ ☐ Dado é um fato bruto não lapidado; II. Informação depende da interpretação pessoal de cada indivíduo; III. Conhecimento é a junção de dados que foram contextualizados.
- ☐ ☐ Dado depende da interpretação pessoal aliada às vivências de cada indivíduo; II. Informação é a junção de dados que foram contextualizados; III. Conhecimento é a junção de informações não lapidadas.
- ☐ ☐ Dado é formado por um conjunto de informações contextualizadas; II. Informação é um fato bruto não lapidado; III. Conhecimento é pessoal, isto é, depende da interpretação das informações juntamente com as vivências/experiências pessoais.

9. O Plano de Continuidade de Negócios (PCN), determinado pela norma **ABNT NBR 15999 Parte 1**, visa contemplar importantes aspectos, dentre os quais observamos subsequentemente:

I. O Plano de Continuidade de Negócios (PCN) descreve como a empresa deve atuar diante da identificação das ameaças e dos impactos nas operações a fim de garantir a preservação do negócio.

II. O Plano de Continuidade de Negócios (PCN) visa maximizar os problemas advindos das interrupções nas atividades de negócios e proteger os processos críticos dos defeitos de grandes falhas ou desastres.

III. O Plano de Continuidade de Negócios (PCN) tem como objetivo estabelecer as diretrizes e as responsabilidades a serem observadas no Sistema de Gestão de Continuidade de Negócios.

IV. O Plano de Continuidade de Negócios (PCN) visa especificar as ameaças e riscos identificados na organização e analisar os impactos no negócio, caso eles se concretizem.


Após a leitura, analise as asserções acima e, a seguir, assinale a alternativa correta:

- ☒ ☐ Somente as asserções I, III e IV estão corretas
- ☐ ☐ Somente as asserções I, II e III estão corretas;
- ☐ ☐ Somente as asserções III e IV estão corretas.
- ☐ ☐ Somente as asserções I, II e IV estão corretas;
- ☒ ☐ Somente as asserções II e IV estão corretas;

10. O Risco é um conceito importante quando se trata do Plano de Continuidade de Negócios (PCN). A respeito do Risco, selecione a opção correta:


- ☐ ☐ Normalmente não podem ser controlados.
- ☐ ☐ Não pode ser analisado em termos probabilísticos, uma vez que sempre está presente.
- ☒ ☐ Possível evento que pode causar perdas ou danos, ou dificultar o atingimento de objetivos.
- ☒ ☐ Evento súbito e imprevisto que provoca grandes perdas ou danos a uma organização.
- ☐ ☐ É um conceito abstrato e com baixa chance de se transformar em um desastre.

11- A alteração dos dados por pessoa/software/processo não autorizado em um data center, por exemplo, pode ser considerada uma ameaça da:


- ☐ Confidencialidade
- ☐ Lealdade
- ☐ Disponibilidade
- ☐ Autenticidade
- ☒  Integridade

12- Um funcionário estava passando na sala de equipamentos de computação quando esbarrou em um servidor web que estava posicionado no canto de uma mesa e o derrubou no chão, parando a operação do mesmo.


Segundo a norma ABNT NBR ISO/IEC 27002:2013, o responsável pela segurança do servidor deixou de colocar em prática o controle relacionado à

- ☐ Segregação de funções
- ☐ Gerenciamento de senha de usuário
- ☒  Localização e proteção do equipamento
- ☐ Acordo de confidencialidade
- ☐ Inventário dos ativos


13- Um funcionário de uma empresa concluiu que existe uma probabilidade de 67% de sobrecarga e problemas no serviço de distribuição de conteúdo de vídeo em um eventual aumento na demanda do servidor. Dentro da GR, essa conclusão pode ser obtida na etapa de:

- ☐ Aceitação do risco (residual)
- ☐ Monitoramento e controle de riscos
- ☐ Terminação de riscos
- ☒  Processo de avaliação de riscos
- ☐ Definição do contexto

14- Houve um superaquecimento em um roteador, que, por isso, parou de funcionar. O plano de tratamento para esse caso, definido como risco alto, será colocado em prática imediatamente, porque esse risco é considerado:

- ☐ Não identificado
- ☒  Prioritário
- ☐ Resolvido
- ☐ Residual
- ☐ Informalmente identificado

15- Em relação à biblioteca ITIL (Information Technology Infrastructure Library), selecione a opção correta:

- ☒  Concentra-se no alinhamento de serviços de TI com as necessidades dos negócios
- ☐ Não pode ser aplicada em nenhum aspecto do plano de continuidade dos negócios.
- ☐ Aborda todas as necessidades dos negócios da empresa.
- ☐ É aplicada apenas no plano de continuidade dos negócios.
- ☐ Junto com o plano de recuperação de desastres, tem um papel reativo quando ocorrem problemas.