

 (resultados.cfm?action=list)

## 2301 - SEGURANÇA E AUDITORIA DE SISTEMAS DE INFORMAÇÃO - Resultados

- 1 Processos de auditoria podem ser entendidos como serviços de segurança que buscam rastrear, entender, analisar eventos (maliciosos ou não) em sistemas, redes, equipamentos ou corporações. Analise as afirmativas a respeito das formas de auditoria e marque a alternativa correta:



Num Afirmativa

- 1 O processo de verificação se um processo está sendo seguido é uma forma de auditoria
- 2 Não se aplicam processos de auditoria em eventos inesperados como incidentes de segurança
- 3 Quando se usam logs de diversas fontes/origens é muito importante que haja sincronia entre os horários dos registros

a As afirmativas 1 e 2 são verdadeiras

b A afirmativa 1 é a única falsa

c As afirmativas 2 e 3 são falsas

  d As afirmativas 1 e 3 são verdadeiras

e A afirmativa 3 é a única verdadeira



**Pontuação: 1**

- 2 O ambiente físico também precisa estar adequado às normas e práticas de segurança. Leia as afirmativas e marque a alternativa correta em relação aos cuidados com o ambiente físico:

Num Afirmativa

- 1 Um perímetro de segurança física é uma área criada para garantir a segurança dos ativos
- 2 São exemplos de perímetro de segurança: calçadas e áreas externas da empresa
- 3 O termo barreiras múltiplas diz respeito ao uso de múltiplos controles de acesso físico em um determinado perímetro de segurança

a A afirmativa 3 é falsa, enquanto a 1 é verdadeira

  b As afirmativas 3 e 1 são verdadeiras

c A afirmativa 1 é falsa, enquanto a 2 é verdadeira

d A afirmativa 2 é a única verdadeira

e A afirmativa 2 é verdadeira, enquanto a 3 é falsa

**Pontuação: 1**



- 3** A preocupação com a segurança deve começar bem antes de um sistema entrar em operação. Já no desenvolvimento ou aquisição ações que garantam a segurança devem ser implementadas. Analisando as afirmativas, marque a alternativa correta:

Num Afirmativa

- 1 Entre as validações de segurança exigidas em Sistemas Gerenciadores de Banco de Dados está a verificação se uma informação é pública
- 2 Um Buffer Overflow (estouro de capacidade) ocorre, por exemplo, quando um campo ou endereço de memória recebe uma quantidade de dados acima de sua capacidade máxima
- 3 Um exemplo de validação de dados na entrada é a checagem e correção dos dados que serão enviados a um usuário

**a** As afirmativas 2 e 3 são falsas

**b** A afirmativa 1 é verdadeira, enquanto a 3 é falsa

  **c** A afirmativa 2 é a única verdadeira

**d** As afirmativas 1 e 2 são verdadeiras

**e** A afirmativa 3 é a única falsa

**Pontuação: 1**

- 4** Uma PSI bem elaborada é vital para que a empresa adote e divulgue boas práticas de segurança. Marque a alternativa correta em relação às afirmativas apresentadas:

Num Afirmativa

- 1 Uma PSI é composta por regras que não precisam estar de acordo com a lei, pois são de uso interno
- 2 A norma 27001 sugere que haja um setor responsável pela segurança. Porém, a criação da PSI pode contar com outros setores participantes
- 3 Uma PSI deve focar exclusivamente assuntos tecnológicos quando elaborada pelo responsável pela segurança

**a** A afirmativa 3 é a única falsa

**b** A afirmativa 2 e 3 são falsas

**c** A afirmativa 1 é verdadeira, enquanto a 2 é falsa

**d** A afirmativa 3 é verdadeira, enquanto a 1 é falsa

  **e** A afirmativa 3 é falsa, enquanto a 2 é verdadeira

**Pontuação: 1**

- 5** A gestão de incidentes é um conjunto bastante amplo de atividades que busca garantir a continuidade dos negócios quando ocorrem incidentes ou eventos inesperados capazes de impactar negativamente a empresa. Analisando as afirmativas, marque a alternativa correta:

NumAfirmativa

- 1 Para o estabelecimento da GCN é necessário o envolvimento da direção para imbutir em toda a empresa a cultura da gestão de continuidade
- 2 A conformidade é o processo responsável por controlar a quantidade de incidentes que ocorrem em um período de tempo
- 3 Um dos cinco passos da GCN é o Entendimento da Organização, que está diretamente vinculado à Análise de impactos nos Negócios (AIN)

**a** Todas as alternativas são verdadeiras



**b** A afirmativa 2 é a única falsa

**c** As afirmativas 1 e 2 são verdadeiras

**d** As afirmativas 3 e 2 são falsas

**e** A afirmativa 3 é verdadeira, enquanto a 1 é falsa

**Pontuação: 1**

- 6** As empresas compartilham informações sobre suas operações constantemente. É necessário que a gestão das operações e das comunicações garanta a eficiência das operações e a segurança dos dados compartilhados. Analise as afirmativas relacionadas e marque a alternativa correta:

NumAfirmativa

- 1 Uma das formas de "planejar sistemas" é dimensionar recursos e escalabilidade ainda na fase de projeto destes sistemas
- 2 Um código malicioso inserido em uma rede por um elemento interno (funcionário, por exemplo) não tem a capacidade de afetar a integridade de um sistema
- 3 Um teste sobre as cópias de segurança busca checar a integridade e efetividade dos backups antes de uma eventual restauração

**a** As afirmativas 1 e 2 são falsas

**b** As afirmativas 2 e 3 são verdadeiras



**c** A afirmativa 2 é falsa, enquanto a 1 é verdadeira

**d** A afirmativa 3 é a única falsa

**e** A afirmativa 3 é a única verdadeira

**Pontuação: 1**

**7 A segurança da informação**, portanto, é a proteção da informação contra vários tipos de **ameaças**, de modo a garantir a **continuidade do negócio**, minimizar **riscos**, maximizar o **retorno sobre os investimentos** e as **oportunidades** de negócio.

Ao analisarmos essa definição, precisamos definir alguns pontos-chave, para o correto entendimento de toda essa definição. Inicialmente, a definição nos trás o conceito de que a segurança da informação é a proteção contra vários tipos de **ameaças**. Relacione quais são estas ameaças :

Estas ameaças são:

A falta de treinamento em segurança de TI, colaboradores sem comprometimento com a organização, risco de ataques cibernéticos como hack, phishing e outros, risco a desastres naturais, entre outros.

**Conceito: Certo - Pontuação: 4**

**Explicação:**

Descontentamento ou desmotivação de colaboradores;

Baixo nível de conscientização dos colaboradores sobre assuntos relacionados à segurança;

Inexistência de políticas e procedimentos para acesso, manipulação e armazenagem da informação;

Hacking, vírus, spam, e-mails maliciosos;

Falta de um plano de recuperação a desastres;

Desastres naturais, tais como incêndio, inundação, terremoto etc.

**Legenda:**

 Alternativa correta

 Resposta do aluno

---

**Pontuação total: 10**