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 A afirmativa 1 é a única falsa

b A afirmativa 3 é a única verdadeira

c As afirmativas 1 e 3 são verdadeiras

d As afirmativas 2 e 3 são falsas

e As afirmativas 1 e 2 são verdadeiras

Pontuação: 1

2 A segurança também deve ser aplicada na gestão de recursos humanos. Em relação a este tópico, analise as afirmativas e marque a alternativa correta:

Num	Afirmativa
1	Equipamentos pessoais usados dentro da rede da empresa, como celulares e notebooks não devem ser tratados na PSI, pois são de uso pessoal
2	De acordo com a norma 27002 o papel de um colaborador diz respeito às funções que este exerce dentro da empresa
3	A norma 27002 define o termo responsabilidade como o prejuízo gerado por um ataque cibernético

a As afirmativas 2 e 3 são verdadeiras

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

c As afirmativas 1 e 2 são falsas

d As afirmativas 1 e 2 são verdadeiras

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

Pontuação: 1

3 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:

Num	Afirmativa
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 A afirmativa 3 é a única falsa

b As afirmativas 2 e 3 são verdadeiras

c As afirmativas 1 e 2 são falsas

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

e A afirmativa 3 é a única verdadeira

Pontuação: 1

4 O cálculo de riscos é uma função matemática que leva em conta alguns fatores. Analise as afirmativas relacionadas e marque a alternativa correta:

Num	Afirmativa
1	Em geral, em relação à gestão de risco uma organização reativa possui um planejamento menos efetivo que uma organização proativa
2	A comunicação do risco, sugerida pela norma ABNT 27005 serve para indicar os culpados pelos prejuízos trazidos pela concretização do risco
3	De acordo com a norma 27005, a etapa de "Análise do Risco" precede e fornece requisitos para a etapa de "Avaliação do Risco"

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

b As afirmativas 2 e 3 são falsas

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

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

e A afirmativa 1 é a única 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:

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

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 Todas as alternativas são verdadeiras

Pontuação: 1

6 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 A afirmativa 2 é a única verdadeira

b As afirmativas 1 e 2 são verdadeiras

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

d A afirmativa 3 é a única falsa

e As afirmativas 2 e 3 são falsas

Pontuação: 1

7 A Análise de Impactos nos Negócios (AIN) faz parte do Ciclo de Vida da Gestão de Continuidade de Negócios (GCN) recomendado pela norma ABNT ISO/IEC 27002. A norma recomenda que em algumas situações o risco deve ser aceito e não tratado. Descreva um exemplo no qual a organização deve simplesmente aceitar o risco e a ameaça que este representa, justificando o porquê desta medida.

A empresa pode optar pela aceitação do risco quando o custo para reparar é maior que o benefício. Neste caso, deve tomar as medidas necessárias para mitigar os danos e do cumentar a decisão com a ciência da alta direção. Por exemplo, se o custo de substituiç ão de um hardware for excessivamente alto, a empresa evitar a compra e optar por faze r backups frequentes de modo a minimizar o dano. A empresa também pode evitar a co mpra de um Gerador de Energia se na sua localidade o risco de queda de energia é mín imo. Após uma análise de risco a empresa pode concluir que riscos residuais devem ser aceitos. Em qualquer caso deve-se sempre registar a decisão e ter o aval da direção da empresa.

Conceito: Certo - Pontuação: 4
Explicação:
Muitas vezes a reparação de um risco representa um custo maior que o prejuízo causado pela ameça. Por exemplo, em uma organização que tem poucos problemas de indisponibilidade elétrica, não há necessidade da compra de um gerador que garanta o fornecimento ininterrupto de energia. Principalmente se a indisponibilidade ocasional não representar um prejuízo significativo para a empresa.

Legenda:
Alternativa correta

Resposta do aluno

Pontuação total: **10**