Gestão de Risco

Total de pontos 210/450

Escolha atentamenta a resposta mais correcta!

Email *

belarminosimaojunior@gmail.com

185 de 415 pontos

✓ A gestão de risco é um processo que permite: * 5/5

- ○ identificar e reduzir as vulnerabilidades em activos e infraestrutura das organizações .
- ○ identificar e eliminar as ameaças sobre os activos e infraestrutura das organizações.
- ◉ identificar e reduzir o risco sobre os activos e infraestrutura das organizações. ✓
- ○ Nenhuma das alíneas anteriores está correcta.

✓ São objectivos de gestão de risco: * 5/5

- (●) garantir a confidencialidade, disponibilidade e integridade de informação nas organizações. ✓
- ( ) garantir a competitividade, lucrativdade e produtividade das organizações
- ( ) ambas alíneas anteriores estão correctas.
- ( ) Nenhuma das alíneas anteriores está correcta.

✗ São empreendimentos do processo de gestão de risco: * 0/5

- ( ) identificação, classificação e controlo de risco.
- ( ) identificação, medição e controlo de risco
- (●) identificação, avaliação e controlo de risco ✗
- ( ) Nenhuma das alíneas anteriores está correcta

Resposta correta

- (●) identificação, classificação e controlo de risco.

Seleccione o empreendimento mais conveniente aquando do processo de gestão de risco.

	Identificação do Risco	Avaliação do Risco	Controlo de Risco	Pontuação	
Avaliar a perda de valor se os ativos de informação forem comprometidos.	☐	☑	☐	0/10	✗
Avaliar a probabilidade de ataque sobre vulnerabilidades.	☐	☑	☐	10/10	✓
Desenvolver a estratégia e o plano do controlo.	☐	☐	☑	10/10	✓
Determinar a vantagem de cada controlo específico.	☐	☐	☐	0/10	✗
Identificar e priorizar as ameaças.	☑	☐	☐	10/10	✓
Inventariar categorizar, classificar e priorizar os activos.	☑	☐	☐	10/10	✓
Planificar e organizar o processo de gestão de risco.	☑	☐	☐	10/10	✓
Rever possíveis controlos					

Especificar as vulnerabilidades dos activos.	☐	☐	☑	0/10	✗
Documentar os resultados/conclusões.	☑	☐	☐	10/10	✓
Avaliar o valor dos activos	☐	☐	☑	0/10	✗
Atribuir valor ao ataque sobre os activos.	☐	☑	☐	0/10	✗
Medir o risco para o activo de informação.	☐	☑	☐	10/10	✓
Calcular o factor de risco relativo por activo.	☐	☑	☐	10/10	✓
Implementar o controlo de risco.	☐	☑	☐	10/10	✓
Categorizar os componentes do SI.	☐	☐	☑	10/10	✓
Aplicação de controlos para reduzir os riscos aos dados e sistemas de informação de uma organização	☑	☐	☐	10/10	✓
Exame e documentação de postura da infoSec da organização e dos	☐	☐	☑	10/10	✓

riscos que esta enfrenta					
Determinação da extensão/nível em que os activos de informação da organização estão expostos ou em risco	☑	☐	☐	0/10	✗
os activos de informação da organização estão expostos ou em risco	☑	☐	☐	10/10	✓

Respostas corretas

	Identificação do Risco	Avaliação do Risco	Controlo de Risco
Avaliar a perda de valor se os ativos de informação forem comprometidos.	☐	☐	☑
Rever possíveis controlos.	☐	☑	☐
Documentar os resultados/conclusões.	☐	☑	☐
Avaliar o valor dos activos	☑	☐	☐
Exame e documentação de postura da infoSec da organização e dos riscos que esta enfrenta	☐	☑	☐

que esta enfrenta

que esta enfrenta

Para cada descrição abaixo, faça corresponder com a respectiva estratégia decontrolo de risco *

	Defender	Transferir	Mitigar	Aceitar	Encerrar	Pontuação	
Baseia-se na conclusão de que o custo de proteger um atvo não justifica os gastos com segurança.	○	○	○	◉	○	5/5	✓
Direciona aorganização a evitar as actividades de negócios que apresentam riscos incontroláveis.	○	○	○	○	◉	5/5	✓
É a escolha de não fazer nada para proteger uma vulnerabilidade e aceitar o resultado de sua exploração	○	○	○	◉	○	5/5	✓
É realizada por meio do combate às ameaças, removendo vulnerabilidades de ativos, limitando oacesso a ativose adicionandomedidas de proteção	○	○	◉	○	○	0/5	✗

inclui aplicação de política,tecnologia, educação e treinamento de pessoal.	○	○	◉	○	○	0/5	✗
Previlegia o outsourcing	○	◉	○	○	○	5/5	✓
Requer a criação de três tipos de planos: planos de resposta a incidente, plano de recuperação de desastres e o plano de continuidade de negócios	○	○	◉	○	○	5/5	✓
Tenta impedir a exposição da vulnerabilidade	○	○	◉	○	○	0/5	✗
Tenta reduzir o impacto causado pela exposição da vulnerabilidade por meio de planeamento e preparação	○	○	◉	○	○	5/5	✓
Tenta transferir o risco para outros activos, outros processos ou outras organizações	○	◉	○	○	○	5/5	✓

processos ou outras organizações

Respostas corretas

	Defender	Transferir	Mitigar	Aceitar	Encerrar
É realizada por meio do combate às ameaças, removendo vulnerabilidades de ativos, limitando oacesso a ativose adicionandomedidas de proteção.	◉	○	○	○	○
inclui aplicação de política,tecnologia, educação e treinamento de pessoal.	◉	○	○	○	○
Tenta impedir a exposição da vulnerabilidade	◉	○	○	○	○

✓ Qual é a fórmula usada para calcular a espectativa de perda anual? * 10/10

- ○ ALE=ARO*EF
- ○ ALE=AV*ARO
- ◉ ALE=AV*EF*ARO ✓
- ○ ALE+EF*ARO
- ○ Nenhuma das alíneas anteriores está correcta

✕ Suponha que a empresa XYZ Software tenha um novo projeto de desenvolvimento de aplicativo, com orçamento projetado de US $ 1.200.000. Use as informações da tabela abaixo e calcule: ARO (Taxa de Ocorrência Anualizada) e ALE (Expectativa de Perda Anualizada): [Dê a resposta de seguinte maneira - (ARO1,ALE1) = (valorX,$valorY), ..., (ARO6,ALE6) = (valorW, valorZ) Por exemplo: (ARO1,ALE1) = (2, $2000)]. *···/50

Categoria de ameaça	Custo por Incidente (SLE)	Frequência de Ocorrência	ARO	ALE
Ataque de DoS	$ 2,500.00	1/trimestre		
Cheias	$ 25,000.00	1/10 anos		
Desfiguração do sítio Web	$ 500.00	1/mês		
Erros do Programador	$ 5,000.00	1/semana		
Fogo	$ 500,000.00	1/10 anos		
Perda de PI	$ 75,000.00	1/ano		

(ARO1, ALE1) = (4, $10.000)
(ARO2, ALE2) = (0,1, $2.500)
(ARO3, ALE3) = (12, $6.000)
(ARO4, ALE4) = (52, $260.000)
(ARO5, ALE5) = (0,1, $50.000)
(ARO6, ALE6) = (1, $75.000)

✕ Suponha que um ano passou e XYZ melhorou a segurança aplicando uma série de controlos. Usando as informações da alínea anterior e a tabela a seguir, calcule ARO e ALE pós-controlo para cada categoria de ameaça listada e preencha as células vazias. (Dê a resposta de seguinte maneira - (ARO1,ALE1) = (valorX,$valorY), ..., (ARO6,ALE6) = (valorW, valorZ). *···/50

Categoria de ameaça	Custo por Incidente (SLE)	Frequência de Ocorrência	ARO	ALE
Ataque de DoS	$ 2,500.00	1/semestre		
Cheias	$ 25,000.00	1/10 anos		
Desfiguração do sítio Web	$ 500.00	1/trimestre		
Erros do Programador	$ 5,000.00	1/mês		
Fogo	$ 500,000.00	1/10 anos		
Perda de PI	$ 75,000.00	1/ 2 anos		

(ARO1, ALE1) = (0,5, $1.250)
(ARO2, ALE2) = (0,1, $2.500)
(ARO3, ALE3) = (4, $2.000)
(ARO4, ALE4) = (12, $60.000)
(ARO5, ALE5) = (0,1, $50.000)
(ARO6, ALE6) = (0,5, $37.500)

✗ Na tabela abaixo, indique o CBA para a abordagem planeada de controlo de risco para cada categoria de ameaça e determine se o controle proposto vale os custos. Preencha as células vazias (Dê a resposta de seguinte maneira - (CBA1,custos1) = (valorX,SIM/NÃO), ..., (CBA6,custos6) = (valorZ,SIM/NÃO). *···/50

Categoria de ameaça	Custo do Controlo (ACS)	**Tipo de controlo**	CBA	Vale os custos?
Ataque de DoS	$10000	Firewall		
Cheias	$10000	Seguros/Backup		
Desfiguração do sítio Web	$10000	Firewall		
Erros do Programador	$20000	Treinamento		
Fogo	$10000	Seguros/Backup		
Perda de PI	$15000	Firewall/IDS		

Tecnologia de Informação: Controle de Acesso 25 de 35 pontos

Leia atentamente as perguntas e responda acertadamente

✗ São tipos de controle de acesso EXCEPTO. * 0/5

- [ ] Directivo
- [ ] Compensatório
- [ ] Correctivo
- [x] Identificação ✓
- [ ] Autenticação
- [ ] Preventivo
- [ ] Autorização
- [ ] Recuperação
- [ ] Prestação de contas (Accountability)
- [ ] Dissuasivo
- [ ] Detectivo
- [ ] Todos
- [ ] Nenhum

Resposta correta

- [x] Identificação
- [x] Autenticação
- [x] Autorização

- [x] Prestação de contas (Accountability)

✗ Geralmente, o controle de acesso segue que os seguintes passos: * 0/5

- [ ] Directivo
- [ ] Compensatório
- [ ] Correctivo
- [x] Identificação ✓
- [x] Autenticação ✓
- [ ] Preventivo
- [x] Autorização ✓
- [ ] Recuperação
- [ ] Prestação de contas (Accountability)
- [ ] Dissuasivo
- [ ] Detectivo
- [ ] Todos
- [ ] Nenhum

Resposta correta

- [x] Identificação
- [x] Autenticação
- [x] Autorização

- [x] Prestação de contas (Accountability)

✓ É o processo de verificar ou de testar se uma identidade proclamada é válida. *5/5

- (•) Autenticação ✓
- ( ) Autorização
- ( ) Identificação
- ( ) Prestação de contas
- ( ) Nenhuma

✗ Tem basicamente três factos, nomeadamente: algo que você sabe; algo que você tem e, finalmente, algo que você é. *

- ○ Autorização
- ○ Autenticação
- ◉ Identificação ✗
- ○ Prestação de contas

Resposta correta

- ◉ Autenticação

✓ Usa rótulos para regular o acesso a activos organizacionais e é maioritariamente usado pelos militares. *5/5

- ◉ MAC - Mandatory Access Control - Controle de acesso obrigatório ✓
- ○ DAC - Discretionary Access Control - Controle de acesso discricionário
- ○ RBAC - Role Based Access Control - Controle de acesso baseado em função
- ○ Centralizado (Ex: Single Sign On - SSO)
- ○ Descentralizado

✓ Cada objecto (pasta ou ficheiro) tem um proprietário e este define os direitos e privilégios; Usado em empresas e é difícil de restrear os objectos. *5/5

- ○ MAC - Mandatory Access Control - Controle de acesso obrigatório
- ◉ DAC - Discretionary Access Control - Controle de acesso discricionário ✓
- ○ RBAC - Role Based Access Control - Controle de acesso baseado em função
- ○ Centralizado (Ex: Single Sign On - SSO)
- ○ Descentralizado

✗ controlam actividades em um único sistema de computador, especialmente, observando as trilhas de auditoria, logs de eventos el ogs de aplicação. *

- ○ IDS baseado em rede
- ○ IDS baseado em Host
- ○ IDS baseado em conhecimento
- ◉ IDS baseado em comportamento ✗

Resposta correta

- ◉ IDS baseado em Host

✓ É também conhecido por detecção baseada em assinatura ou ainda detecção baseada em padrão, utiliza uma base de dados de assinaturas cujo conteúdo tenta fazer corresponder com os eventos monitorados. *5/5

- ○ IDS baseado em rede
- ○ IDS baseado em Host
- ◉ IDS baseado em conhecimento ✓
- ○ IDS baseado em comportamento

✓ Emite falsos alarmes e pode bloquear actividades autorizadas não conhecidas. *5/5

- ○ IDS baseado em rede
- ○ IDS baseado em Host
- ○ IDS baseado em conhecimento
- ◉ IDS baseado em comportamento ✓

O que achou desses quizzes?

Interessantes e desafiadores. Contudo, foram úteis para a preparação.