1 Ma	rcar para revisão
Um ataque de negação de serviço tenta afetar a disponibilidade de um ativo, por exemplo, inundando um servidor rede com mais dados do que é capaz de processar por unidade de tempo.	le aplicação em
Se existe uma ferramenta, dentro do domínio do servidor, que reage a um ataque de negação de serviço, ela é classi uma medida de controle:	ficada como
A Preventiva	
B Recuperadora	
C Limitadora	
D Reativa	
E Detectora	
2 Ma	rcar para revisão
Un combinada cominão de comunicación de la CD. Ele complete de CD.	

Um membro da comissão de segurança precisa saber informações sobre cada um dos processos da GR. Ele consultará uma dentre as normas da família ISO/IEC 27000, que definem uma série de normas relacionadas à segurança da informação. Ele precisa obter a norma:

A ISO/IEC 27005

B ISO/IEC 31000

C ISO/IEC 27002

D ISO/IEC 27001

E ISO/IEC 27000

Pontos de falha na segurança da informação são áreas ou componentes de um sistema, rede, processo ou organização que apresentam vulnerabilidades.

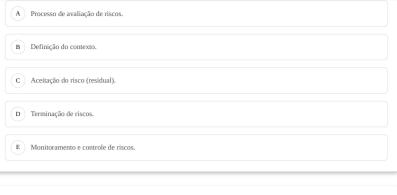
Qual é a definição de "vulnerabilidade" na segurança da informação?

A Uma causa potencial de um incidente indesejado.

B Uma mudança não desejável nos objetivos de negócios.

D Uma fragilidade de um ativo que pode ser explorada por ameaças.	
E Um evento indesejado que compromete a segurança da informação.	
4	Marcar para revisão
A proteção de informações, também conhecida como segurança da informação, é un informação desempenha um papel fundamental nos negócios e na sociedade como u impedir a divulgação não autorizada, a alteração indesejada e a indisponibilidade de	ım todo. A proteção de informações visa
Qual dos seguintes termos se refere à proteção de informações contra acesso não au	torizado?
A Integridade.	
B Disponibilidade.	
C Vulnerabilidade.	
D Confidencialidade.	
E Ameaça.	
5	Marcar para revisão
ouve um superaquecimento em um roteador, que parou de funcionar. O plano de trata to", será colocado em prática imediatamente, porque esse risco é considerado:	mento para esse caso, definido como "risco
	mento para esse caso, definido como "risco
to", será colocado em prática imediatamente, porque esse risco é considerado:	mento para esse caso, definido como "risco
to", será colocado em prática imediatamente, porque esse risco é considerado:  A Residual	mento para esse caso, definido como "risco
to", será colocado em prática imediatamente, porque esse risco é considerado:  A Residual  B Não identificado	mento para esse caso, definido como "risco
to", será colocado em prática imediatamente, porque esse risco é considerado:  A Residual  B Não identificado  C Resolvido	mento para esse caso, definido como "risco

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:



A gestão de riscos de segurança da informação é um processo fundamental para proteger ativos de informação contra ameaças e vulnerabilidades que podem comprometer a confidencialidade, integridade e disponibilidade dos dados. Ela envolve a identificação, avaliação, tratamento e monitoramento dos riscos de segurança da informação em uma organização.

O que são riscos residuais na gestão de riscos de segurança da informação?

A Riscos que não podem ser tratados.

C Riscos que não foram identificados.

D Riscos que foram aceitos pela organização.

E Riscos que foram transferidos para terceiros.



