1

Marcar para revisão

Um ataque de negação de serviço tenta afetar a disponibilidade de um ativo, por exemplo, inundando um servidor de aplicação em rede com mais dados do que é capaz de processar por unidade de tempo.

Se existe uma ferramenta, dentro do domínio do servidor, que reage a um ataque de negação de serviço, ela é classificada como uma medida de controle:

A Preventiva

B Recuperadora

C Limitadora

D Reativa

E Detectora

2

Marcar para revisão

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

3

Marcar para revisão

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.

C Uma medida que pode modificar o risco.

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 uma área crítica na era digital, na qual a informação desempenha um papel fundamental nos negócios e na sociedade como um todo. A proteção de informações visa impedir a divulgação não autorizada, a alteração indesejada e a indisponibilidade de dados e sistemas.

Qual dos seguintes termos se refere à proteção de informações contra acesso não autorizado?

A Integridade.

B Disponibilidade.

C Vulnerabilidade.

D Confidencialidade.

E Ameaça.

5

Marcar para revisão

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

A Residual

B Não identificado

C Resolvido

D Prioritário

E Informalmente identificado

6

Marcar para revisão

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 Processo de avaliação de riscos.

B Definição do contexto.

C Aceitação do risco (residual).

D Terminação de riscos.

E Monitoramento e controle de riscos.

7 Marcar para revisão

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.

B Riscos que não foram identificados.

C Riscos que foram totalmente eliminados.

D Riscos que foram aceitos pela organização.

E Riscos que foram transferidos para terceiros.

8 Marcar para revisão

O acesso não autorizado é uma das principais ameaças à segurança da informação e ocorre quando uma pessoa ou entidade obtém acesso a sistemas, dados, redes ou informações confidenciais sem a devida permissão ou autorização.

Qual dos seguintes termos se refere à proteção de informações contra acesso não autorizado?

A Confidencialidade.

B Integridade.

C Ameaça.

D Disponibilidade.

E Vulnerabilidade.

9 Marcar para revisão

O sistema de monitoramento de *nobreak* detectou uma variação na tensão elétrica na entrada dos aparelhos, mas essa variação não foi o suficiente para causar danos aos equipamentos de computação a eles conectados.

Conforme os termos relacionados à segurança da informação, o que ocorreu pode ser classificado como:

A Evento

B Tensionamento

C Eletricidade

D Dano

E Variação

10 Marcar para revisão

A gestão de riscos de segurança da informação é uma prática essencial para proteger os ativos de informação e garantir a continuidade dos negócios em um ambiente cada vez mais digital e sujeito a ameaças.

Qual dos seguintes elementos é essencial na gestão de riscos de segurança da informação?

A Medidas de controle.

B Vulnerabilidades identificadas.

C Comunicação do risco.

D Ativos de informação.

E Aceitação do risco.

Questão **1** de 10

1 2 3 4 5

6 7 8 9 10

○ Em branco **(10)**