

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 Limitadora☐ C Detectora☒ D Reativa☐ E Recuperadora**Resposta correta**

Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado

A ferramenta descrita no enunciado é classificada como uma medida de controle reativa porque ela responde a um ataque de negação de serviço depois que ele ocorre. As medidas de controle reativas são projetadas para responder a um incidente de segurança em andamento, ao contrário das medidas preventivas, que são projetadas para prevenir incidentes de segurança antes que eles ocorram. As medidas limitadoras, por outro lado, são projetadas para limitar o impacto de um incidente de segurança, enquanto as medidas detectoras são projetadas para detectar incidentes de segurança. As medidas recuperadoras são projetadas para recuperar de um incidente de segurança.

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 27000☐ B ISO/IEC 27001☐ C ISO/IEC 27002☒ D ISO/IEC 27005☐ E ISO/IEC 31000**Resposta correta**

Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado

A norma ISO/IEC 27005 é a mais adequada para o membro da comissão de segurança que precisa saber informações sobre cada um dos processos da GR. Esta norma é parte da família ISO/IEC 27000 e fornece diretrizes para a gestão de riscos de segurança da informação, o que inclui detalhes sobre todos os processos envolvidos.

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.**Resposta correta**

Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado

Uma vulnerabilidade é uma fragilidade de um ativo que pode ser explorada por uma ou mais ameaças, comprometendo 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.

5 C Ameaça.

D Vulnerabilidade.

E Confidencialidade.



Resposta correta

Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado

A confidencialidade está relacionada à proteção de informações contra acesso não autorizado. Ela é um dos pilares da segurança da informação.

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 Prioritário

B Não identificado

C Informalmente identificado

D Residual

E Resolvido



Resposta correta

Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado

Na situação apresentada no enunciado, um roteador superaqueceu e parou de funcionar, sendo classificado como um "risco alto". Isso significa que a situação é crítica e precisa ser tratada imediatamente. Portanto, esse risco é considerado "Prioritário", o que justifica a resposta correta ser a alternativa A. Os riscos prioritários são aqueles que exigem ação imediata para prevenir ou mitigar danos significativos.

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 Definição do contexto.

B Monitoramento e controle de riscos.

C Processo de avaliação de riscos.

D Terminação de riscos.

E Aceitação do risco (residual).



Resposta correta

Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado

A etapa em que um funcionário de uma empresa pode concluir a probabilidade de sobrecarga e problemas no serviço de distribuição de conteúdo de vídeo, em um eventual aumento na demanda do servidor, é durante o "Processo de avaliação de riscos". Esta etapa envolve a identificação e análise dos riscos que podem afetar um projeto ou uma operação. Neste caso, o risco identificado é a sobrecarga do servidor devido ao aumento da demanda. A probabilidade de 67% foi determinada como parte dessa avaliação de risco.

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 foram aceitos pela organização.

C Riscos que foram totalmente eliminados.

D Riscos que não foram identificados.

E Riscos que foram transferidos para terceiros.



Resposta correta

Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado

Riscos residuais são aqueles que foram aceitos pela organização após o tratamento, pois podem ser considerados pequenos ou de alguma forma inevitáveis.

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 Integridade.

B Disponibilidade.

C Ameaça.

D Vulnerabilidade.

E Confidencialidade.

✓ **Resposta correta**
Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado

A confidencialidade está relacionada à proteção de informações contra acesso não autorizado. Ela é um dos pilares da segurança da informação.

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

✓ **Resposta correta**
Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado

No contexto da segurança da informação, um "evento" é qualquer ocorrência que seja significativa para a gestão da informação. Neste caso, a variação na tensão elétrica detectada pelo sistema de monitoramento do nobreak é um evento, pois é uma ocorrência que pode ter implicações para a segurança da informação, mesmo que não tenha causado danos aos equipamentos de computação.

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 Comunicação do risco.

B Aceitação do risco.

C Medidas de controle.

D Vulnerabilidades identificadas.

E Ativos de informação.

✓ **Resposta correta**
Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado

As medidas de controle desempenham um papel fundamental na gestão de riscos de segurança da informação, pois são usadas para reduzir a probabilidade e o impacto de incidentes de segurança.

Questão 1 de 10

1

2

3

4

5

6

7

8

9

10

○ Corretas (10)

○ Em branco (0)