

REVISÃO AV1 - SEGURANÇA até aula 10

1) Atualmente, qual o ativo mais importante para as empresas?

Informação

2) Quais os aspectos que tem influência direta na SI?

Pessoas, processos e tecnologias

3) Por que a segurança da informação é complexa?

Porque é preciso manter todos os itens seguros

4) Qual a maior dificuldade em se implementar a SI?

Pessoas, que são difíceis de agradar e querem fazer tudo de se jeito e com total liberdade

5) Qual a diferença de dados e informação?

Dados - itens isolados e que, sozinhos, não fazem sentido

Informação - conjunto de dados que tem sentido

6) Quais são as etapas do ciclo de vida da informação?

Manuseio, armazenamento, transporte e descarte

7) Quais são os itens do CIDAL?

Confidencialidade, integridade, disponibilidade, autenticidade e legalidade

8) Qual a primeira norma de segurança, que era voltada para SO's?

Orange book

9) Qual série de normas é uma evolução da ISO 17799?

ISO 27000

10) O que é análise de risco?

Processo de avaliar se um risco é aceitável ou não para uma empresa

11) O que é risco?

Probabilidade de uma ameaça explorar uma vulnerabilidade, gerando impactos negativos

12) Como classificamos as ameaças?

Naturais, físicas, intencionais e não intencionais

13) Quais são os 2 métodos de análise de risco estudados em sala de aula?

Matriz GUT e análise SWOT

14) O que é uma política de segurança?

Conjunto de normas normativas na empresa, que visa a proteção dos ativos

15) Quais são os itens que devem existir em cada uma das normas da PSI?

Descrição, objetivo, deveres do usuário, deveres do administrador, recomendações e penalidades

16) Diferencie custodiante e proprietário da informação

O proprietário é quem usa a informação pela necessidade e pode definir a importância da mesma, e o custodiante é quem tem a guarda da informação

17) Por que classificar a informação?

Para poder implementar os controles adequados a cada tipo de informação

18) Quais são os itens da classificação da informação do ponto de vista de acesso indevido?

Secreta, confidencial, restrita, interna e pública

10) O que deve ser usado para combate a incêndio no data center?

CO2 ou FM200

20) Defina engenharia social

Técnica usada por golpistas para ter acesso a informação sem uso de força bruta

21) Defina biometria

Uso de características físicas ou comportamentais para identificar um indivíduo

22) Cite 3 tecnologias de biometria

Impressão digital, face, assinatura, mãos e dedos, voz, digitação, íris e retina