Atividade:

**1) O que você entende por ativo de uma empresa? Explique.**

**R=** Ativo é qualquer recurso de valor que a empresa possui e que pode ser convertido em dinheiro ou utilizado para gerar lucro. Os ativos podem ser tangíveis ou intangíveis.

**2) Os incidentes em uma empresa ocorrem quando uma e/ou várias ameaças exploram os pontos fracos da mesma, seja intencionalmente ou não. Cite os princípios da segurança da informação foram violados.**

**R=** Dentre os principais princípios da segurança que são violados são:

Confidencialidade devido ao vazamento de informações sigilosas são acessadas por pessoas não autorizadas.

Violação da Integridade com alterações das informações através de manipulações de dados.

Autenticidade, também pode ser violado quando a identidade de usuários ou sistemas é falsificada, como no caso de phishing ou spoofing.

**3) Quando um ativo da informação sofre um ataque potencial podemos entender como ameaça. Esse ataque poderá ser efetuado por agentes externos ou internos diante das vulnerabilidades apresentadas no sistema da empresa. Como as ameaças podem ocorrer?**

**R=** Ameaças físicas envolvem danos ou perda de ativos tangíveis, como edifícios, equipamentos, devido a eventos naturais, como incêndios, inundações, terremotos, ou até mesmo causado pelas pessoas.

Ameaças cibernéticas envolvem ataques a sistemas de informação, havendo a perda dos ativos intangíveis redes e dados digitais de uma empresa, como malware, hacking e ataques de negação de serviço. Esses ataques podem resultar em perda de dados, roubo de informações confidenciais, interrupção dos negócios e danos severos a empresa.

Ameaças internas envolvem funcionários ou colaboradores da empresa que, intencionalmente, comprometem os ativos da empresa. Isso pode incluir roubo de informações confidenciais, ou até mesmo erros humanos que levam à perda ou dano de ativos.

**4) Cite algum risco aos quais as pessoas estão sujeitas ao utilizar a internet.**

**R=** Roubo de identidade como informações pessoais, números de cartão de crédito, senhas, números de identidade e outros dados pessoais.

As pessoas podem ser levadas a instalarem softwares maliciosos podem danificar seu computador ou dispositivos, roubar informações pessoais ou espioná-lo.

Golpes online são comuns, e as pessoas podem ser enganadas a enviar dinheiro ou outras informações pessoais para pessoas.

A internet pode ser um lugar onde a privacidade pode ser invadida, coletando dados e acessando informações pessoais sem permissão.

**5) Leia as afirmações e assinale a alternativa correta:**

Alternativa: D

**6) Explique a importância de um Plano de Recuperação de Desastres para as empresas.**

**R=** Um plano de recuperação de desastres pode ajuda a minimizar o tempo de inatividade em caso de interrupção podendo salvar grandes perdas financeiras.

Este plano de também é capaz de minimizar os custos associados à desastres naturais erro humano, incluindo perda de receita e custos de recuperação. Também a identificação de vulnerabilidades no sistema da empresa, permitindo que elas sejam abordadas antes que ocorram problemas.