ATIVIDADE 2

ATENÇÃO:

1) **Esta Atividade deverá ser feita em GRUPO DE PELO MENOS 04 ALUNOS E DE NO MÁXIMO 08 ALUNOS embora a entrega deverá ser feita INDIVIDUALMENTE .**
2) **Atividades feitas individualmente ou entregues com atraso NÃO SERÃO CONSIDERADAS..**

Grupo

Maria Clara Borges Rodrigues Santos RA:82410853

Giovanna Araujo Thomazzini Codo RA:824134072

Julia Zezilia Rodrigues RA:824213803

1) LIVRO NO ULIFE: Leia **Análise de Vulnerabilidades em Serviços de Informação (**pág. 73 até 84) do Livro disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788595025875/pageid/72

   Faça um Resumo comentando detalhadamente os principais conceitos abordados neste tópico.

2) Crie um Jamboard colocando o que cada membro do seu Grupo achou de mais importante na Leitura citada na questão anterior. Compartilhe o link do Jamboard criado aqui. (A resposta desta questão é apenas o link do Jamboard com os tópicos/conceitos que cada membro do Grupo escolheu ao ler o Capítulo citado).

3) Leia **Material 1** anexo e redija um parágrafo resumindo o conteúdo dele.

4) Pesquise os materiais abaixo e preencha a Tabela abaixo:

   VÍDEOS DISPONÍVEIS NO YOUTUBE:

   VÍDEO 1- https://www.youtube.com/watch?v=AWUhXq4FDNo

VÍDEO 2- https://www.youtube.com/watch?v=DkhUBSlDuOo

LIVRO NO ULIFE
Normas de Segurança em TI
https://integrada.minhabiblioteca.com.br/reader/books/9788595025875/pageid/164 (Ler da Página 165 até 176)

MATERIAL	RESUMO DO SEU CONTEÚDO
VÍDEO 1	
VÍDEO 2	
LIVRO NO ULIFE	

*TABELA PREENCHIDA NO FINAL DO DOCUMENTO

RESPOSTA DO ALUNO

Pergunta 01:

A evolução tecnológica e a crescente dependência da internet têm transformado a maneira como indivíduos e organizações interagem, realizam negócios e armazenam informações. No entanto, com essa dependência, surge uma preocupação crítica: a segurança da informação. A proteção dos dados e a garantia de que serviços essenciais permaneçam disponíveis e confiáveis são desafios constantes para a área de segurança da informação (SI). Neste contexto, a análise de vulnerabilidades em serviços de informação desempenha um papel vital, permitindo a identificação de fraquezas que podem ser exploradas por agentes mal-intencionados.

Assim, a segurança da informação é ancorada em três pilares fundamentais: disponibilidade, confidencialidade e autenticidade. A disponibilidade refere-se à capacidade de um sistema manter seus serviços operacionais e acessíveis pelo máximo de tempo possível, resistindo a falhas de hardware, software e energia. A confidencialidade assegura que informações sensíveis sejam acessadas apenas por indivíduos ou máquinas autorizadas, enquanto a autenticidade garante a verificação da identidade de quem acessa esses dados. Esses elementos, quando comprometidos, podem resultar em sérias vulnerabilidades que ameaçam a integridade dos sistemas de informação.

Sob esse viés, é possível dizer que uma vulnerabilidade é qualquer fraqueza que reduz a segurança de um sistema, tornando-o suscetível a ataques. Essas vulnerabilidades podem envolver falhas em software,

configuração inadequada de sistemas ou até mesmo erros humanos. Quando exploradas, podem levar à perda de dados, interrupção de serviços ou à exposição de informações sensíveis. Entre as ameaças mais comuns decorrentes de vulnerabilidades em serviços de informação estão vírus, cavalos de Troia, worms, phishing, spyware, roubo de informações, fraudes financeiras e, notavelmente, ataques de negação de serviço (DoS).

Ademais, os ataques de negação de serviço (DoS) representam uma das ameaças mais significativas para a segurança da informação. Visto que esses ataques têm como objetivo sobrecarregar sistemas ou redes, tornando-os inacessíveis para usuários legítimos. Existem dois tipos principais de ataques de negação de serviço: o ataque DoS convencional e o ataque distribuído (DDoS). O ataque DoS tradicional envolve o uso de uma única máquina para enviar um grande volume de solicitações para o servidor alvo, sobrecarregando-o e impedindo que ele responda a novos pedidos. Já o ataque DDoS é mais sofisticado, utilizando uma rede de máquinas zumbis, controladas por um computador máster, para realizar o ataque de forma distribuída e em larga escala. Esse tipo de ataque é particularmente perigoso porque as máquinas zumbis podem estar espalhadas por diversas localidades, tornando difícil a detecção e a mitigação do ataque.

Outrossim, os ataques de negação de serviço podem ser classificados em subcategorias, como ataques por inundação, reflexivos, na infraestrutura da rede, exploração de vulnerabilidades e ataques de protocolo. Cada tipo de ataque explora diferentes aspectos da infraestrutura e dos protocolos de comunicação, dificultando a defesa contra essas ameaças. Por exemplo, o ataque reflexivo utiliza intermediários para amplificar o tráfego de ataque, tornando a origem do ataque difícil de rastrear. Já o ataque na infraestrutura da rede visa os servidores que traduzem nomes de sites, causando a interrupção do acesso aos mesmos.

Além da prevenção, a reação a ataques também é essencial. O CERT recomenda um processo estruturado que envolve preparação, identificação, contenção, remediação, recuperação e análise pós-ataque. Ferramentas automatizadas de varredura e análise de tráfego são fundamentais para identificar anomalias e responder rapidamente a incidentes, minimizando os prejuízos e restaurando os serviços afetados.

Portanto, a análise de vulnerabilidades em serviços de informação é um processo crucial para garantir a segurança e a continuidade das operações em um mundo cada vez mais digitalizado. Compreender os tipos de vulnerabilidades, como os ataques DoS e DDoS, e utilizar as ferramentas apropriadas para mitigá-las, permite que organizações protejam seus dados e sistemas contra ataques potencialmente devastadores. Embora a erradicação completa das vulnerabilidades seja um desafio, a implementação de

estratégias robustas de segurança pode minimizar os riscos e assegurar que os serviços de informação permaneçam confiáveis e disponíveis, mesmo diante das ameaças mais sofisticadas.

Pergunta 02:

https://jamboard.google.com/d/1ELnhntzSlncf5j-laAasXOFnPlvQeYhFJtRPYihS318/edit?usp=sharing

Pergunta 03:

O artigo de Ronan Leandro Coelho dos Santos e Mário Rubens W. Sott destaca a relevância crucial da segurança da informação para o funcionamento eficaz e a continuidade das empresas. O artigo apresenta explicações detalhadas de termos e subtemas importantes para garantir o pleno entendimento do tema, como as definições de segurança, informação, a importância da segurança física e lógica, as principais ameaças e vulnerabilidades, além de dicas de como proteger seu negócio. O texto aborda a necessidade de políticas de segurança para proteger dados, enfatizando que as ameaças muitas vezes se originam dentro da própria organização, seja de forma intencional ou não. Além disso, apresenta uma série de etapas que, se seguidas fielmente, levam a uma boa política de segurança. A segurança da informação é fundamental para garantir a integridade, confidencialidade, disponibilidade e não repúdio dos dados, aspectos essenciais para a tomada de decisões que afetam diretamente o lucro e prejuízo da empresa.

Tabela:

MATERIAL	RESUMO DO SEU CONTEÚDO
VÍDEO 1	O vídeo mostra que para ter risco precisa ter vulnerabilidade e ameaça; ativos é qualquer item de valor para a organização; ameaça é uma condição que pode causar problema a um ativo, para solucionar o cibernético precisa mitigar; vulnerabilidade é uma falha no design do sistema. A avaliação de risco: Identificar ameaças ex: enchente e ataques de hackers, identificar vulnerabilidade, determinar a probabilidade, determinar o impacto, determinar o risco, que são de duas maneiras a quantitativa e a qualitativa que é por tabelas, se for por números tem uma conta chamada Annul loss expeciany que ajuda a determinar quando aceitar, evitar, transferir ou mitigar o risco, ALE = Custo X Ocorrências Ex: 3 milhões = 1 milhão X 3
VÍDEO 2	Identificação e Avaliação: Ameaças: Identifique potenciais ameaças, como ataques de hackers, malwares, falhas de sistema ou desastres naturais. Avalie a probabilidade de cada ameaça ocorrer Vulnerabilidade: Realize auditorias de segurança e testes de penetração para identificar vulnerabilidade nos sistemas, softwares, redes e processos Riscos: Com base nas ameaças e vulnerabilidade identificadas, determine os riscos para o negócio. Avalie a gravidade do impacto de cada risco. Priorização: Classifique as vulnerabilidades e riscos com base na probabilidade de ocorrência e no impacto potencial. Use uma matriz de risco para ajudar na priorização Mitigação e Controle: Ameaças: Implante controles para prevenir ou reduzir o impacto das ameaças. Isso pode incluir

	firewalls, sistemas de detecção de intrusão, criptografia, backup de dados, etc. Vulnerabilidades: Aplique correções (patches) de segurança, atualize softwares, revise configurações de sistemas e implemente práticas de codificação segura. Riscos: Desenvolva implemente políticas de segurança da informação, planos de contingência e procedimentos de recuperação de desastres para mitigar os riscos. Monitoramento e Resposta: Monitore continuamente os sistemas para detectar e responder a incidentes de segurança em tempo real. Tenha um plano de resposta a incidentes bem definido. Treinamento e Conscientização: Eduque a equipe sobre práticas de segurança e como reconhecer ameaças, como phishing ou engenharia social. A conscientização é crucial para reduzir as vulnerabilidades. Revisão e Melhoria Contínua: Regularmente revise as estratégias de segurança, faça auditorias e revise os riscos e vulnerabilidades de TI. Atualize as políticas e procedimentos conforme necessário.
LIVRO NO ULIFE	As normas de segurança em TI (Tecnologia da informação) são conjuntos de diretrizes e melhores práticas estabelecidas para proteger informações e sistemas contra ameaças. Elas visam garantir a confidencialidade, integrida e disponibilidade dos dados. Algumas das principais normas incluem: ISO/ IEC 27001: Define requisitos para um Sistema de Gestão de Segurança da informação (SGSI), protegendo informações sensíveis de uma organização. NIST SP 800-53: Catálogo de controles de segurança e privacidade. NIST Cybersecurity Framework: Ajuda na gestão e redução de riscos de cibersegurança.

	PCI- DSS: Conjunto de requisitos de segurança para empresas que processam, armazenam ou transmitem dados de cartões de crédito, protegendo essas informações. Essas normas ajudam as organizações a implementar práticas seguras e a cumprir regulamentos, reduzindo o risco de incidentes de segurança.