ATIVIDADE 3

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 no Classroom.**
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 **Criptografia e Certificação Digital** (145-164) do Livro disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788536531212/pageid/145

   Escreva pelo menos 8 parágrafos comentando detalhadamente os principais conceitos abordados.

2) Crie um Jamboard colocando o que cada membro do seu Grupo achou de mais importante na leitura do **ARTIGO 1** e **ARTIGO 2**. 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 o vídeo disponibilizado no link: https://www.youtube.com/watch?v=uJ4tIHzQT5M . Tenha certeza de que você compreendeu como é construída a Matriz de Risco. Em seguida, faça o exercício solicitado no último slide do Material 1.

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

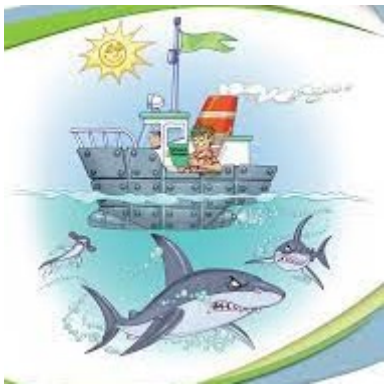
   VÍDEOS DISPONÍVEIS NO YOUTUBE:

VÍDEO 1- https://www.youtube.com/watch?v=hKlNCWDUaZ0

VÍDEO 2- https://www.youtube.com/watch?v=xCV0ecVybgA

VÍDEO 3- https://www.youtube.com/watch?v=RwvwSqN_lto

LIVRO LINK ABAIXO



Cartilha de Segurança para Internet (capa na imagem acima) disponível em: https://sites.google.com/site/myalvarenga/livros?authuser=0
(Ler da Página 67 até 84 – Capítulos 9 e 10)

*TABELA PREENCHIDA NO FINAL DO DOCUMENTO

MATERIAL	RESUMO DO SEU CONTEÚDO
VÍDEO 1	
VÍDEO 2	
VÍDEO 3	
LIVRO	

RESPOSTA DO ALUNO

Pergunta 01:

A criptografia é uma prática essencial no campo da segurança da informação, utilizada para proteger dados, proporcionando ao transformá-los em textos cifrados, incompreensíveis para qualquer pessoa ou sistema não autorizado. Essa prática se desenvolveu ao longo dos séculos, com suas raízes na palavra grega que significa "escrita oculta". Inicialmente, a privacidade era focada principalmente no sigilo, garantindo que mensagens importantes permanecessem secretas. No entanto, à medida que as necessidades de segurança evoluíram, a criptografia passou a abranger também a autenticação, integridade e não-repúdio das informações, tornando-se uma ferramenta multifacetada e necessária.

No cerne da criptografia estão os conceitos de criptografia simétrica e assimétrica, que envolvem o uso de chaves para codificar e decodificar informações. Assim, a criptografia simétrica utiliza a mesma chave para ambos os processos, o que, embora eficiente, apresenta desafios na distribuição segura dessa chave, especialmente em redes amplas. Por outro lado, a criptografia assimétrica utiliza um par de chaves — uma pública e outra privada —, resolvendo alguns dos problemas de distribuição enfrentados pela simétrica. Essa abordagem é fundamental para sistemas de chave pública, como o algoritmo RSA, amplamente utilizado para proteger a confidencialidade das informações em transações online e comunicações sensíveis.

Além disso, a criptografia assimétrica também desempenha um papel crucial nas assinaturas digitais, que são mecanismos de segurança utilizados para garantir a proteção e integridade de uma mensagem. Uma assinatura digital é criada criptografando um valor hash exclusivo da mensagem original com a chave privada do remetente. O destinatário pode, então, usar a chave pública correspondente para decodificar o hash e compará-lo com o hash da mensagem recebida, verificando se a mesma foi alterada ou adulterada durante a transmissão. Isso não apenas protege contra fraudes, como também garante saber se a mensagem realmente foi gerada pelo remetente declarado

Portanto, para garantir a confiança nas chaves públicas utilizadas em assinaturas digitais e outras formas de criptografia assimétrica, são utilizados certificados digitais emitidos por autoridades (ACs) confiáveis. Esses certificados digitais funcionam como identidades eletrônicas, atestando a validade das chaves públicas e garantindo que elas pertencem de fato às partes que as possuíam. Isso impede que invasores usem chaves falsas para interceptar ou modificar comunicações, adicionando uma camada extra de segurança em transações on-line e outras interações digitais que desbloqueiam alta confiabilidade.

Assim, a integração de certificados digitais com assinaturas digitais é particularmente relevante em contextos corporativos e governamentais, onde a integridade e a retenção das informações são críticas. Por exemplo, na comunicação corporativa, o uso de e-mails assinados digitalmente garante que as informações trocadas entre funcionários e parceiros sejam seguras e invioláveis. Ademais, o gerenciamento adequado das chaves públicas e a conformidade com normas rigorosas de segurança são essenciais para proteger a proteção da empresa e evitar possíveis consequências legais decorrentes da má utilização das ferramentas de segurança.

Sob esse viés, a criptografia, em conjunto com a certificação digital, não apenas protege os dados previstos, mas também garante que as partes envolvidas em uma transação ou comunicação possam confiar na integridade e na proteção das informações. Essa combinação é crucial para o funcionamento seguro de inúmeras atividades no mundo moderno, desde transações financeiras até o envio de documentos eletrônicos que substituem documentos financeiros tradicionais. A confiança nas transações digitais, portanto, não depende apenas da criptografia em si, mas também dos certificados de garantia e verificação

Visto isso, em um cenário global cada vez mais interligado, onde a troca de informações é constante e em grande escala, a criptografia e a certificação digital se destacam como fundamentos da segurança cibernética. Eles permitem que indivíduos e organizações se comuniquem e realizem transações com confiança, sabendo que suas informações estão protegidas contra

interceptação, adulterações e fraudes. Ao garantir que apenas os destinatários pretendidos possam acessar e modificar as informações, essas tecnologias fortalecem a confiança nas interações digitais e direcionadas para a construção de um ambiente digital mais seguro e confiável.

Em suma, a criptografia e a assinatura digital são duas faces de uma mesma moeda, ambos fundamentais para a proteção da integridade e confidencialidade das informações no mundo digital. Juntas, elas não apenas protegem dados contra acessos não autorizados, mas também garantem que as comunicações e transações digitais sejam realizadas com total segurança e confiança. À medida que a dependência de soluções digitais cresce, a importância dessas tecnologias continuará a se expandir, consolidando-se como elementos essenciais na infraestrutura.

Pergunta 02:

https://jamboard.google.com/d/1V4WkyGSRwrlUrc6ZaXsmvGpBQHGC9C8AldLPX3LHmTA/edit?usp=sharing

Pergunta 03:

Ativo	Probabilidade	Impacto	Cálculo do Risco	Risco Avaliado
Infraestrutura de Nuvem	High	High	4x5	20 - VH
Servidores Administrativos	Medium	Medium	3x3	9 - M
Sistemas Operacionais	Low	Medium	2x3	6 - L
Antivírus	Very Low	Low	1x2	2 - VL
Dados Corporativos	High	High	4x5	20 - VH
Conectividade de Rede	Medium	Medium	3x3	9 - M

Colaboradores de TI	High	Medium	4x4	16 - H
Colaboradores Terceirizados	Medium	Medium	3x3	9 - M

Pergunta 04:

MATERIAL	RESUMO DO SEU CONTEÚDO
VÍDEO 1	A criptografia é uma técnica fundamental para garantir a segurança da informação, permitindo que dados confidenciais sejam protegidos contra acessos não autorizados. Ela envolve a codificação de informações de uma forma que apenas partes autorizadas possam decifrá- las e compreendê- las. A confidencialidade só é acessível apenas para quem tem autorização, a criptografia transforma os dados em um formato ilegível, como o texto cifrado que só pode ser revertido ao seu formato original, em um texto claro por meio de um chave criptográfica; A integridade garante que a informação não foi alterada durante o trânsito, técnicas criptográficas como hash modifica o conteúdo que será detectada; Autenticidade verifica a identidade que envolve na comunicação, provando que a informação tenha uma fonte legítima; O não- repúdio é uma parte não possa negar ter enviado, estes são os princípios básicos da criptografia. A criptografia simétrica usa a mesma chave tanto para criptografar quanto para descriptografar os dados, já a criptografia assimétrica usa um par de chaves, uma pública para criptografar os dados e a outra para descriptografá- los; A criptográfica de hash forma um valor fixo a partir de dados de qualquer tamanho, esse valor é único para conjunto de dados e é usado para ver a integridade da informação. As Comunicações seguras serve para proteger os dados transmitidos; Armazenamento de Dados é para prevenir acessos não autorizados; Assinaturas digitais garantem a autenticidade e a integridade dos documentos digitais; A

	autenticação protege senhas e credenciais em sistemas de login, essas são as aplicações.
VÍDEO 2	Uma VPN tem uma conexão segura e criptografada entre o dispositivo do usuário e um servidor remoto operado pelo serviço de VPN. Conexão com o servidor VPN quando conecta a uma VPN, estabelece uma conexão com um servidor VPN em outra localização; Criptografia dos dados são todos os dados que envia e recebe pela internet são criptografados pelo software da VPN antes de sair do dispositivo; Encaminhamento de dados são os criptografados são enviados pelo túnel VPN até o servidor VPN. Alteração do Endereço IP quando usa uma VPN, o endereço IP do seu dispositivo é substituído pelo endereço IP do servidor VPN tanto que o IP permanece oculto, esse são os funcionamento básico de uma VPN- Parte I.
VÍDEO 3	Estenografia é a arte e ciência de esconder informações de forma que o receptor sabe que a mensagem está lá, mas um terceiro não consegue perceber. Os princípios básicos da esteganografia em imagens é a técnica de LSB, ela modifica os bits menos significativos dos pixels da imagem para armazenar os dados do texto; funciona da seguinte forma, cada pixel em uma imagem digital é representado por valores de cor, geralmente em formato RGB; em uma imagem de 24 bits, cada uma das cores é representada por 8 bits; alterar o último bit de cada cor original, mas permite armazenar informações. Imagine quem tenha uma imagem e deseja esconder a mensagem “OI’’; primeiro convertemos o texto em binária; seguida usamos a técnica LSB para esconder esses bits dentro dos pixels da imagem, essa é a técnica LSB. Ferramentas e Linguagens Usadas serve para implementar esteganografia, linguagens como Python, com bibliotecas como PIL permite fácil manipulação de imagens e implementação de técnicas de esteganografia.

LIVRO	O capítulo 9. Criptografia fala que é a pratica de proteger informações ao converter em um formato ilegível para qualquer pessoa que não tenha a chave de decodificação; O objetivo é garantir o sigilo e a integridade dos dados durante a transmissão ou armazenamento; A criptografia utiliza algoritmos matemáticos para cifrar e decifrar informações; Existem dois tipos principais de criptografia: simétrica, onde a mesma chave é usada para cifrar e decifrar os dados, e assimétrica, que utiliza um par de chaves, uma pública para cifrar e uma privada para decifrar. O capítulo 10. Uso seguro da internet envolve adotar práticas que protejam sua privacidade, dados pessoais e dispositivos contra ameaças cibernéticas; alguns exemplos são: senhas fortes, autenticação de dois fatores (2FA), atualizações regulares, cuidado com phishing, rede wi- fi seguras, compartilhamento consciente e downloads seguros.