ATIVIDADE 1

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 formulário a seguir:**
https://linktr.ee/ucs20232

2) **Atividades feitas individualmente ou entregues com atraso NÃO SERÃO CONSIDERADAS.**

3) **Todas as respostas devem ser escritas aqui no espaço destacado em COR AZUL abaixo.**

Grupo

Maria Clara Borges Rodrigues Santos RA: 82410853

Giovanna Araujo Thomazzini Codo RA: 824134072

Julia Zezilia Rodrigues RA: 824213803

1) Leia **Capítulo 1 – Introdução aos conceitos da Segurança da Informação** (pág. 9 até 25) do Livro disponível em: https://www.cefospe.pe.gov.br/images/media/1665420043_Apostila%20Introducao%20Seguranca%20Informacao%20Corporativa.pdf

   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 do **Capítulo 1** citado 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 ULIFE:

VÍDEO 1- https://player.vimeo.com/video/251621361

VÍDEO 1- https://player.vimeo.com/video/148906669

LIVRO NO ULIFE
https://integrada.minhabiblioteca.com.br/reader/books/9788502122185/pageid/20 (Ler da Página 1 até 18)

*TABELA PREENCHIDA NO FINAL DO DOCUMENTO

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

RESPOSTA DO ALUNO

Pergunta 01:

O Capítulo 1 da apostila de Introdução à Segurança da Informação Corporativa oferece uma visão abrangente sobre os conceitos fundamentais da segurança da informação e como eles se aplicam no contexto organizacional. Assim, o material começa destacando a importância de compreender o contexto onde os problemas de segurança da informação ocorrem, muitas vezes negligenciados no cotidiano das pessoas. Em seguida, introduz o conceito de sistemas, com base na Teoria Geral dos Sistemas de Ludwig Von Bertalanffy. Segundo essa teoria, um sistema é um conjunto de partes que interagem para alcançar objetivos específicos. Sistemas podem ser abertos, interagindo com o ambiente externo, ou fechados, operando apenas internamente. Essa compreensão é essencial para aplicar os princípios de segurança da informação em contextos organizacionais complexos.

Sob esse viés, as empresas são vistas como sistemas abertos que interagem com o ambiente externo, como sistemas tributário e legal. A integração de departamentos e setores visa atingir objetivos como lucro e crescimento. Então, para gerenciar eficazmente uma empresa, é crucial utilizar mecanismos de comunicação e controle, os quais se mostram fundamentais para a SI.

Ademais, a segurança da informação é baseada em três princípios fundamentais: confidencialidade, integridade e disponibilidade. A confidencialidade garante que apenas usuários autorizados possam acessar informações específicas e é comprometida quando informações são acessadas por pessoas não autorizadas. A integridade assegura que as informações permaneçam inalteradas e confiáveis, sendo comprometida por alterações não autorizadas e a disponibilidade garante que os usuários autorizados possam acessar e processar dados quando necessário, sendo comprometida pela falta de acesso a dados essenciais.

Além dos princípios fundamentais, existem princípios auxiliares como identificação e autenticação. A autenticação, em particular, é destacada pela

sua importância em garantir a segurança dos sistemas, começando pela escolha de senhas seguras. As senhas, quando combinadas com um nome de usuário, são um fator essencial de autenticação, proporcionando um nível elevado de segurança se forem bem construídas e implementadas. A complexidade da senha, caracterizada pela combinação de letras maiúsculas e minúsculas, números e símbolos, é crucial para dificultar a sua quebra, embora torne a senha mais difícil de memorizar. Além disso, práticas como evitar a reutilização de senhas e não anotá-las em locais inseguros são fundamentais para prevenir comprometimentos de segurança.

Assim, a biometria surge como uma alternativa à autenticação tradicional, utilizando características físicas ou comportamentais únicas de cada indivíduo. Embora os sistemas biométricos estejam se tornando mais comuns e acessíveis, sua eficácia depende de fatores como a universalidade e a singularidade das características escolhidas. No entanto, a biometria enfrenta desafios como a dificuldade de coleta de certos dados e a possibilidade de ser enganada por falsificações sofisticadas. Assim, a implementação de sistemas biométricos requer uma análise cuidadosa de aspectos como desempenho, aceitabilidade e segurança.

Desse modo, os tokens de hardware oferecem uma camada adicional de segurança, atuando como um segundo fator de autenticação além das senhas. Esses dispositivos, variam desde simples chaveiros até tokens com recursos avançados, sendo eficazes ao exigirem a posse do token para acessar sistemas. No entanto, eles não são invulneráveis, uma vez que roubados, podem colocar a segurança das credenciais associadas em risco.

Outrossim, a autorização e o controle de acesso são fundamentais para garantir que apenas usuários devidamente autenticados possam acessar determinados recursos ou informações. A autorização é a aplicação de políticas que definem quais usuários têm permissão para realizar determinadas ações, enquanto o controle de acesso envolve a implementação de tecnologias e processos para limitar o acesso. Princípios como menor privilégio, precisa saber e segregação de funções são críticos para garantir que o acesso seja restrito ao necessário, reduzindo o risco de acesso não autorizado.

Além disso, a auditoria complementa esses mecanismos, monitorando e registrando as atividades dos usuários para garantir que as políticas de segurança sejam seguidas. A rastreabilidade das ações é crucial para responsabilizar os usuários, detectar e prevenir fraudes e outras violações, e proteger a organização contra possíveis consequências legais e financeiras decorrentes de incidentes de segurança. Assim, a auditoria assegura que os sistemas continuem protegidos e em conformidade com as diretrizes de segurança da organização.

Pergunta 02:

https://jamboard.google.com/d/1wwd93mN5NBuxfbtfkyoPqHKfP-W2rTp4KWVeKYv6TYg/edit?usp=sharing

Pergunta 03:

O texto aborda a importância e os aspectos da segurança da informação nas organizações, destacando que, com a transição das informações de mídias físicas para digitais, surgiram novos desafios para proteger dados valiosos. Inicialmente, o texto enfatiza que, enquanto a segurança de informações digitais é crucial para a sobrevivência e sucesso das empresas, as informações armazenadas digitalmente são mais vulneráveis a roubos e perdas em comparação com as físicas. O artigo define conceitos centrais como segurança e informação, e detalha a SI através de seus quatro princípios fundamentais: confidencialidade, integridade, disponibilidade e não repúdio. A segurança da informação é abordada tanto em termos físicos, com controle de acesso e proteção de equipamentos, quanto lógicos, com o uso de senhas e ferramentas de segurança cibernética. Além disso, o material diferencia ameaças internas e externas, oferecendo exemplos e sugerindo medidas para mitigação, como treinamento de funcionários e uso de antivírus. Políticas de segurança são apresentadas como essenciais para a gestão de riscos, incluindo a definição de normas e a criação de planos de contingência para garantir a proteção contínua das informações.

Pergunta 04:

MATERIAL	RESUMO DO SEU CONTEÚDO

VÍDEO 1	Vídeo Indisponível
VÍDEO 2	Vídeo Indisponível
LIVRO NO ULIFE	A informação é um bem único e valioso no mundo atual, diferente dos bens materiais tradicionais de suas características particulares e disputas. Isso significa que pode ser usada coincidentemente por diversas pessoas sem perder valor ou qualidade. Além disso, a informação é facilmente reproduzida e distribuída, especialmente com as tecnologias digitais, gerando desafios relacionados à propriedade intelectual. Seu valor depende do contexto em que é usada, sendo essencial para decisões planejadas e o desenvolvimento econômico e social A segurança da informação nas organizações contém a proteção de dados e informações contra acessos não autorizados, uso indevido, divulgação, alteração ou destruição. Essa segurança é importante para garantir o sigilo, integridade e disponibilidade das informações, elementos importantes para o funcionamento correto e seguro das áreas das empresas. Para isso, as organizações criam políticas, procedimentos, controles tecnológicos e treinamentos, pretendendo proteger seus ativos de informação, prevenir riscos e conter possíveis impactos de acidente de segurança, como ataque cibernético e violações de dados