Seminário - Tema 01: Alicerces da Proteção Digital (Apresentação: 01/09 a 05/09)

Equipe: Amanda da Silva Brito, Henrique Batista Dias & Laviny Vasconcelos

Assunto: Esta é a fundação de todo o nosso curso. O objetivo é construir a base que sustentará todos os outros conhecimentos. Vocês irão explorar os três pilares sagrados da segurança (Confidencialidade, Integridade e Disponibilidade) e a diferença crucial entre proteger os dados (Segurança Lógica) e proteger os equipamentos que os guardam (Segurança Física). Ao final, a turma deverá ser capaz de identificar os ativos de informação de uma empresa e entender os controles básicos de acesso que definem quem pode ver e fazer o quê, aplicando o princípio do menor privilégio.

Tópicos:

- Os Pilares da Segurança da Informação: Confidencialidade, Integridade e Disponibilidade (Tríade CIA).
- Conceito de Ativo de Informação.
- Segurança Física: Controle de acesso a ambientes (salas, prédios), proteção contra ameaças ambientais.
- Segurança Lógica: Autenticação (senhas, biometria, tokens...), autorização e perfis de acesso.
- O Princípio do Menor Privilégio.

Dicas do professor:
Este é um tema fundamental e denso, e por serem um trio, vocês podem dividir as tarefas de forma muito eficaz. **Henrique**, você poderia se concentrar na pesquisa profunda dos conceitos da Tríade CIA e da Segurança Lógica, estruturando a base do texto didático. **Laviny** poderia pesquisar exemplos práticos e casos reais de falhas de segurança física e lógica para ilustrar a apresentação, tornando o conteúdo mais palpável. **Amanda**, você pode ser a grande organizadora, monte os slides garantindo que a mensagem final seja clara e coesa para a turma.

Seminário - Tema 02: O Campo de Batalha Invisível (Apresentação: 08/09 a 12/09)

Equipe: Edna Ines de Assis & Daiana Ferreira dos Santos

Assunto: Para se defender, é preciso conhecer as armas do inimigo. O foco aqui são as ameaças que exploram tanto a tecnologia quanto a mente humana. Vocês irão mapear os tipos mais comuns de software malicioso (Malware) e, principalmente, desvendar as táticas de Engenharia Social, onde a manipulação psicológica é a principal ferramenta do atacante. A meta é que a turma desenvolva um "sexto sentido" para desconfiar de links, e-mails e abordagens suspeitas, compreendendo que o elo humano é frequentemente o mais vulnerável.

Tópicos:

- Tipos de Malware: Vírus, Worms, Trojans e o temido Ransomware.
- O que é Engenharia Social?

- Técnicas de Phishing e Spear Phishing.
- Outras táticas de manipulação: Pretexting e Baiting.
- Ataques de Negação de Serviço (DoS).

Dicas do professor:
Este tema é perfeito para uma abordagem prática e humana. **Edna**, poderia mergulhar na pesquisa sobre a psicologia por trás da Engenharia Social, explicando por que essas táticas funcionam tão bem e estruturando o texto didático. **Daiana**, você poderia focar em como esses ataques afetam os pequenos negócios, criando uma apresentação visualmente impactante com exemplos reais de e-mails de phishing e histórias que conectem com a realidade dos colegas.

Seminário - Tema 03: A Rede de Segurança Corporativa (Apresentação: 15/09 a 19/09)

Equipe: Tomas Augusto Oliveira Quintao & Ingrid Nicole Vasconcelos Leles

Assunto: O que uma empresa faz quando o pior acontece? Este seminário aborda o plano de sobrevivência digital. O objetivo é explicar como as organizações garantem a Continuidade Operacional mesmo diante de um desastre, como uma falha grave de sistema ou um ataque. Vocês irão detalhar as estratégias de Backup (as cópias de segurança) e os Planos de Contingência, que são os manuais de instrução para reerguer os sistemas. Ao final, a turma entenderá que a prevenção é ideal, mas a preparação para a recuperação é essencial.

Tópicos:

- Conceito de Continuidade Operacional.
- Tipos de Backup: Completo, Incremental e Diferencial.
- Estratégia de Backup 3-2-1.
- O que é um Plano de Contingência e quais seus componentes.
- Diferença entre Recuperação de Desastres (DR) e Continuidade de Negócios (BC).

Dicas do professor:
Aqui temos um tema muito prático e processual. **Tomas** poderia pesquisar e explicar as diferentes tecnologias e métodos de backup, talvez até criando um pequeno tutorial em vídeo ou uma demonstração de como um software de backup funciona. **Ingrid** poderia focar na parte de planejamento, estruturando como se monta um Plano de Contingência, quais perguntas devem ser respondidas e como isso se conecta com a biologia de um "organismo" empresarial que precisa sobreviver.

Seminário - Tema 04: O Manual de Regras do Jogo (Apresentação: 22/09 a 26/09)

Equipe: Rafaela Vitória Ferreira & Rian Freitas Silva Dias

Assunto: Segurança sem regras claras é apenas uma intenção. A Política de Segurança da Informação (PSI) é o documento que transforma a intenção em ação, servindo como a "lei" da

segurança dentro de uma empresa. A missão de vocês é explicar o que é a PSI, por que ela é vital e como ela é estruturada. A turma precisa entender que este documento define as responsabilidades de todos, desde o uso aceitável da internet até o descarte seguro de informações, sendo a espinha dorsal de uma cultura de segurança.

Tópicos:

- O que é e qual a importância de uma Política de Segurança da Informação (PSI).
- Estrutura de uma PSI: Seções comuns (Objetivos, Escopo, Papéis e Responsabilidades).
- Exemplos de políticas específicas: Política de Senhas, Política de Uso Aceitável, Política de Mesa Limpa.
- O processo de criação, aprovação e divulgação da PSI.

Dicas do professor:
Este tema exige clareza e boa comunicação. **Rian** poderia focar na estrutura e na "sintaxe" da PSI, explicando como as regras são escritas e organizadas para não deixar brechas, e talvez montar o esqueleto do texto didático. **Rafaela**poderia pesquisar exemplos de políticas de segurança em hospitais e outras áreas, trazendo casos reais que mostrem o impacto da PSI na proteção de dados sensíveis e montando uma apresentação clara e objetiva.

Seminário - Tema 05: A Arte de Esconder Segredos (Apresentação: 29/09 a 03/10)

Equipe: Júlio Silva Freitas & Davi Martins de Oliveira

Assunto: Como garantir que uma mensagem enviada pela internet só seja lida pelo destinatário? A resposta está na Criptografia, a antiga arte de embaralhar informações. Vocês irão introduzir os conceitos fundamentais da criptografia simétrica e assimétrica, que são a base de quase toda a segurança digital moderna. Além disso, explicarão o que são os Certificados Digitais, que funcionam como o "RG" de um site, garantindo sua autenticidade. A meta é que a turma entenda como essas tecnologias protegem desde o "cadeado" no navegador até as transações financeiras.

Tópicos:

- O que é Criptografia: Conceitos de Chave, Cifrar e Decifrar.
- Criptografia Simétrica (Chave Secreta).
- Criptografia Assimétrica (Chave Pública e Privada).
- O que é e como funciona um Certificado Digital (SSL/TLS).
- Infraestrutura de Chaves Públicas (PKI) e Autoridades Certificadoras (AC).

Dicas do professor:
Este é um tema que pode parecer abstrato, então o desafio é torná-lo concreto. **Davi**, que tomou gosto em HTML e CSS, pode usar essa familiaridade para explicar o lado visível da criptografia: como o "cadeado" (HTTPS) funciona no navegador e qual o papel do Certificado Digital, criando uma apresentação visualmente clara. **Júlio** poderia trazer analogias como a criptografia como diferentes tipos de chaves e cadeados usados para proteger um local, estruturando essa lógica no texto de apoio.

Seminário - Tema 06: O Padrão Ouro da Segurança (Apresentação: 20/10 a 24/10)

Equipe: Edmilson Araújo Castro Filho & Igor Santos Castro

Assunto: Como uma empresa pode provar que suas práticas de segurança são boas? Seguindo padrões internacionais. O foco deste seminário é a norma ISO/IEC 27002, que funciona como um grande catálogo de boas práticas para a Gestão da Segurança da Informação. A tarefa de vocês é apresentar essa norma não como um documento chato, mas como um guia estratégico que ajuda as organizações a cobrir todas as bases da segurança, desde os recursos humanos até a gestão de ativos.

Tópicos:

- O que são padrões e normas de segurança e por que são importantes.
- Introdução a norma ISO/IEC 27002
- Apresentação da estrutura da ISO/IEC 27002: as principais seções de controle.
- Exemplos práticos de controles (Ex: Controle de Acesso, Segurança Física, Gestão de Ativos).
- A diferença entre certificação (ISO 27001) e boas práticas (ISO 27002).

Dicas do professor:
Este tema pode ser muito teórico, então o segredo é o dinamismo. **Igor** poderia explicar como as seções e controles se organizam de forma lógica, como se fosse a arquitetura de um grande sistema. **Edmilson**, você pode ser o responsável por "traduzir" esses controles para o mundo real, pesquisando exemplos de como empresas como a Riot (League of Legends) aplicam esses padrões para proteger os dados de milhões de jogadores, tornando a apresentação mais dinâmica e conectada aos interesses da turma.

Seminário - Tema 07: Em Busca das Brechas (Apresentação: 27/10 a 31/10)

Equipe: Bruno Aparecido Dias & Grazielle Moreira Barros Pinto

Assunto: A melhor defesa começa com um bom ataque... a si mesmo. Este seminário introduz a prática da Análise de Vulnerabilidades, um processo proativo onde um profissional de segurança age como um detetive, usando ferramentas para "escanear" redes e sistemas em busca de falhas conhecidas. O objetivo é encontrar e catalogar essas brechas (como softwares desatualizados ou portas abertas) para que possam ser corrigidas antes que um invasor real as encontre. A turma precisa entender isso como um "check-up" de segurança.

Tópicos:

- Diferença entre Ameaça, Vulnerabilidade e Risco.
- O que é Análise de Vulnerabilidades (Scanning).
- Tipos de Scanners e como funcionam.
- Interpretando um relatório de vulnerabilidades: Falsos positivos e priorização.

- O ciclo de gerenciamento de vulnerabilidades: Identificar, Classificar, Corrigir, Verificar.

Dicas do professor:
Este tema une teoria e prática. **Grazielle**, pode focar na parte prática, pesquisando sobre as ferramentas de scanning (como o OpenVAS ou Nessus), mostrando suas interfaces e como os relatórios são gerados, tornando o processo bem visual. **Bruno** explicaria os conceitos teóricos de forma clara e didática, como se estivesse contando uma história sobre como os "detetives" digitais encontram as vulnerabilidades de um sistema, existem vários vídeos desse no Youtube procure pelo Pato.

Seminário - Tema 08: Vestindo o Chapéu do Invasor (Ético) (Apresentação: 03/11 a 07/11)

Equipe: Jonas Torres Mendes Quintao & Mary Anne Quintão Nascimento

Assunto: Se a Análise de Vulnerabilidades é encontrar a porta destrancada, o Teste de Invasão (Pentest) é tentar abri-la e ver até onde se consegue chegar. A missão de vocês é explicar como os hackers éticos trabalham, simulando um ataque real de forma controlada e autorizada para testar a eficácia das defesas de uma empresa. É crucial abordar as fases de um pentest e, acima de tudo, a ética por trás dessa prática. A turma deve entender que o objetivo não é quebrar, mas fortalecer.

Tópicos:

- O que é um Pentest (Teste de Invasão) e por que ele é realizado.
- A diferença fundamental entre Análise de Vulnerabilidades e Pentest.
- As fases de um Pentest: Reconhecimento, Varredura, Ganho de Acesso, Manutenção de Acesso, Limpeza de Rastros.
- Tipos de Pentest (White box, Grey box, Black box).
- A importância da ética e do contrato (escopo do teste).

Dicas do professor:
Este é um tema que gera muita curiosidade. **Jonas** poderia se aprofundar na pesquisa das fases técnicas do Pentest, estruturando o passo a passo de como um teste acontece e montando o texto didático de forma bem detalhada. **Mary Anne** poderia ser a responsável por encontrar estudos de caso e exemplos (sempre de forma ética) para a apresentação, além de criar um quiz (Kahoot!) que desafie os colegas a pensar como um pentester.

Seminário - Tema 09: Quando o Alarme Soa (Apresentação: 10/11 a 14/11)

Equipe: Késia de Medeiros Moreira & Náthaly Vieira Miranda

Assunto: Um incidente de segurança aconteceu. O pânico não resolve. O que resolve é um plano. O objetivo de vocês é apresentar o Plano de Resposta a Incidentes como um "manual de primeiros socorros" para crises digitais. O foco deve ser em um passo a passo claro e simples, mostrando o que uma equipe de segurança faz desde o momento em que descobre um ataque até a recuperação

total. A meta é que a turma entenda que ter um processo organizado é o que separa um pequeno susto de um desastre completo. Norma: NIST 800-61

Tópicos:

- **Passo 1: Preparação:** O que ter pronto ANTES do incidente.
- **Passo 2: Identificação:** Como saber que estamos sob ataque?
- **Passo 3: Contenção:** Como "isolar o fogo" para não se espalhar.
- **Passo 4: Erradicação:** Como remover a ameaça do sistema.
- **Passo 5: Recuperação:** Como voltar à normalidade com segurança.
- **Passo 6: Lições Aprendidas:** O que fazer para não acontecer de novo.

Dicas do professor:
Este é o grande final, e o segredo aqui é a clareza e a organização. **Késia** crie os slides que definem cada um dos 6 passos de forma muito clara e objetiva, e elaborando as questões do quiz. **Náthaly**, encontre um caso simples e real de um ataque e usar essa história para guiar toda a apresentação, mostrando como cada um dos 6 passos se aplicou àquele caso. Isso vai te ajudar a manter o foco e a tornar a aula super interessante para todos.