PROJETO INTEGRADO INOVAÇÃO - CIBERSEGURANÇA

CIBERSEGURANÇA

PROJETO INTEGRADO

Prezado aluno,

Seja bem-vindo a este semestre!

A proposta de Projeto Integrado é possibilitar a aprendizagem interdisciplinar dos conteúdos desenvolvidos nas disciplinas desse semestre.

ORIENTAÇÕES DO PROJETO INTEGRADO

- O trabalho será realizado **individualmente**.
- **Importante:** Você deverá postar o trabalho finalizado no AVA, o que deverá ser feito na pasta específica da disciplina Projeto Integrado obedecendo ao prazo limite de postagem, conforme disposto no AVA. Não existe prorrogação para a postagem da atividade.
- Deve conter, depois de pronto, capa e folha de rosto padrão da Instituição, sendo organizado no que tange à sua apresentação visual (tipos e tamanhos de fontes, alinhamento do texto, espaçamentos, adentramento de parágrafos, apresentação correta de citações e referências, entre outros elementos importantes), conforme modelo disponível no AVA.
- A produção textual é um trabalho original e, portanto, não poderá haver trabalhos idênticos aos de outros alunos ou com reprodução de materiais extraídos da internet. Os trabalhos plagiados serão invalidados, sendo os alunos reprovados na atividade. Lembre-se de que a prática do plágio constitui crime, com pena prevista em lei (Lei n.º 9.610), e deve ser evitada no âmbito acadêmico.
- **Importante:** O trabalho deve ser enviado em formato Word. Não serão aceitos, sob nenhuma hipótese, trabalhos enviados em PDF.

A seguir, apresentamos a você alguns dos critérios avaliativos que nortearão a análise do Tutor a Distância para atribuir o conceito à produção textual:

- Normalização correta do trabalho, com atendimento ao número de páginas solicitadas.
- Apresentação de estrutura condizente com a proposta apresentada (com introdução, desenvolvimento e conclusão).
- Uso de linguagem acadêmica adequada, com clareza e correção, atendendo à norma padrão.
- Atendimento à proposta, contemplando todos os itens solicitados, com objetividade, criatividade, originalidade e autenticidade.
- Fundamentação teórica do trabalho, com as devidas referências dos autores eventualmente citados.

Lembre-se de que seu Tutor a Distância está à disposição para lhe atender em suas dúvidas e, também, para repassar orientações sempre que você precisar. Aproveite esta oportunidade para realizar um trabalho com a qualidade acadêmica de nível universitário.

- **Leitura proposta**

Para atingir os objetivos deste projeto integrado, você deverá seguir as instruções voltadas à elaboração do trabalho disponibilizadas ao longo do semestre, sob a orientação do Tutor a Distância.

ATIVIDADES

Situação Problema: Consultoria para desenvolver cibersegurança da SecureTech Solutions S.A, que é uma fintech que oferece serviços financeiros digitais.

Contexto

Você será consultor de cibersegurança contratados pela SecureTech Solutions S.A para desenvolver um plano integrado que resolva as vulnerabilidades atuais e permita o crescimento seguro da empresa.

Com o avanço das tecnologias digitais e o crescente número de ameaças cibernéticas, o campo da cibersegurança tornou-se essencial para a proteção de sistemas, dados e operações nas mais diversas organizações

A SecureTech Solutions S.A é uma fintech em rápido crescimento, oferece serviços financeiros digitais, incluindo pagamentos, empréstimos e investimentos, e está no centro da transformação digital do setor financeiro. Com operações que abrangem diversos países e uma base de clientes global, a SecureTech enfrenta desafios complexos relacionados à cibersegurança, privacidade e conformidade regulatória.

Hoje a infraestrutura da SecureTech combina sistemas legados com novas tecnologias, incluindo uma crescente adoção de soluções baseadas em nuvem e integração com APIs de parceiros. Com a expansão de seus serviços, a empresa registra um aumento nas tentativas de invasões, vazamentos de dados e fraudes financeiras. Adicionalmente, os requisitos regulatórios se tornaram mais rigorosos, especialmente com a aplicação da LGPD (Lei Geral de Proteção de Dados) no Brasil, GDPR (General Data Protection Regulation) na Europa e regulamentações específicas para fintechs em diversos mercados.

No último trimestre, a SecureTech enfrentou:

- Ataques de ransomware direcionados a sistemas internos de gestão financeira;
- Vazamento de dados de clientes devido a brechas de segurança em APIs;
- Problemas de escalabilidade e desempenho em sua rede, afetando a experiência dos usuários durante picos de demanda;
- Desalinhamento de políticas de governança de segurança, gerando dificuldades em auditorias internas e externas;
- Vulnerabilidades em aplicações web e móveis, exploradas por agentes maliciosos para realizar fraudes;

Para resolver os problemas, devemos alinhar alguns pontos com as disciplinas trabalhadas no semestre.

Teremos alguns passos para resolvermos esse desafio, que será:

- Redesenhar a infraestrutura de rede para melhorar a escalabilidade, desempenho e resiliência contra ataques.
- Propor soluções como segmentação de rede, firewalls avançados e sistemas de detecção e prevenção de intrusões (IDS/IPS).

Passo 1:

Um dos problemas que a SecureTech Solutions anda enfrentando é a vulnerabilidade do TCP/IP. Sabendo disso, desenvolva um relatório sobre as vulnerabilidades conhecidas no protocolo TCP/IP e apresentar possíveis soluções ou práticas de mitigação para cada uma delas.

Passo 2:

Estabelecer um framework de governança que inclua políticas, métricas e controles alinhados às normas internacionais (ISO 27001) e requisitos locais (LGPD, GDPR).

Propor um plano de resposta a incidentes cibernéticos e um programa de conscientização para colaboradores.

Passo 3:

Desenvolver estratégias para minimizar o risco de vazamentos de dados pessoais, incluindo criptografia, anonimização e controle de acesso.

Criar um plano de conformidade com as regulamentações aplicáveis, priorizando a transparência e o consentimento dos usuários.

Passo 4:

Como consultor de cibersegurança contratado pela SecureTech Solutions S.A, você deverá desenvolver um plano teórico focado na implementação de controles de acesso robustos. Este plano deve abordar as vulnerabilidades atuais e estabelecer uma base sólida para o crescimento seguro da empresa. Sua tarefa é identificar os desafios relacionados à permissão de acesso dentro do contexto da SecureTech, analisando como as soluções podem ser aplicadas para proteger dados, sistemas e garantir conformidade regulatória. Ao longo do processo, considere os fatores tecnológicos, humanos e regulatórios apresentados no problema.

Passo 5:

Projete um sistema de controle de acesso baseado no princípio do menor privilégio, onde cada colaborador, sistema ou API tem acesso apenas às informações e recursos necessários para executar suas funções específicas. Este sistema deve incluir a autenticação multifator (MFA) como requisito para todos os usuários, especialmente aqueles com permissões administrativas. Além disso, integre ferramentas de gestão de identidade e acesso (IAM) para unificar o controle sobre os diferentes níveis de autorização, independentemente do sistema ou tecnologia utilizada.

Como resultado desta atividade, você deverá apresentar uma proposta teórica detalhada para um plano de controle de acesso integrado que equilibre a proteção de dados, a eficiência operacional e a conformidade regulatória na SecureTech Solutions S.A.

Bons estudos!!!

Docentes do curso