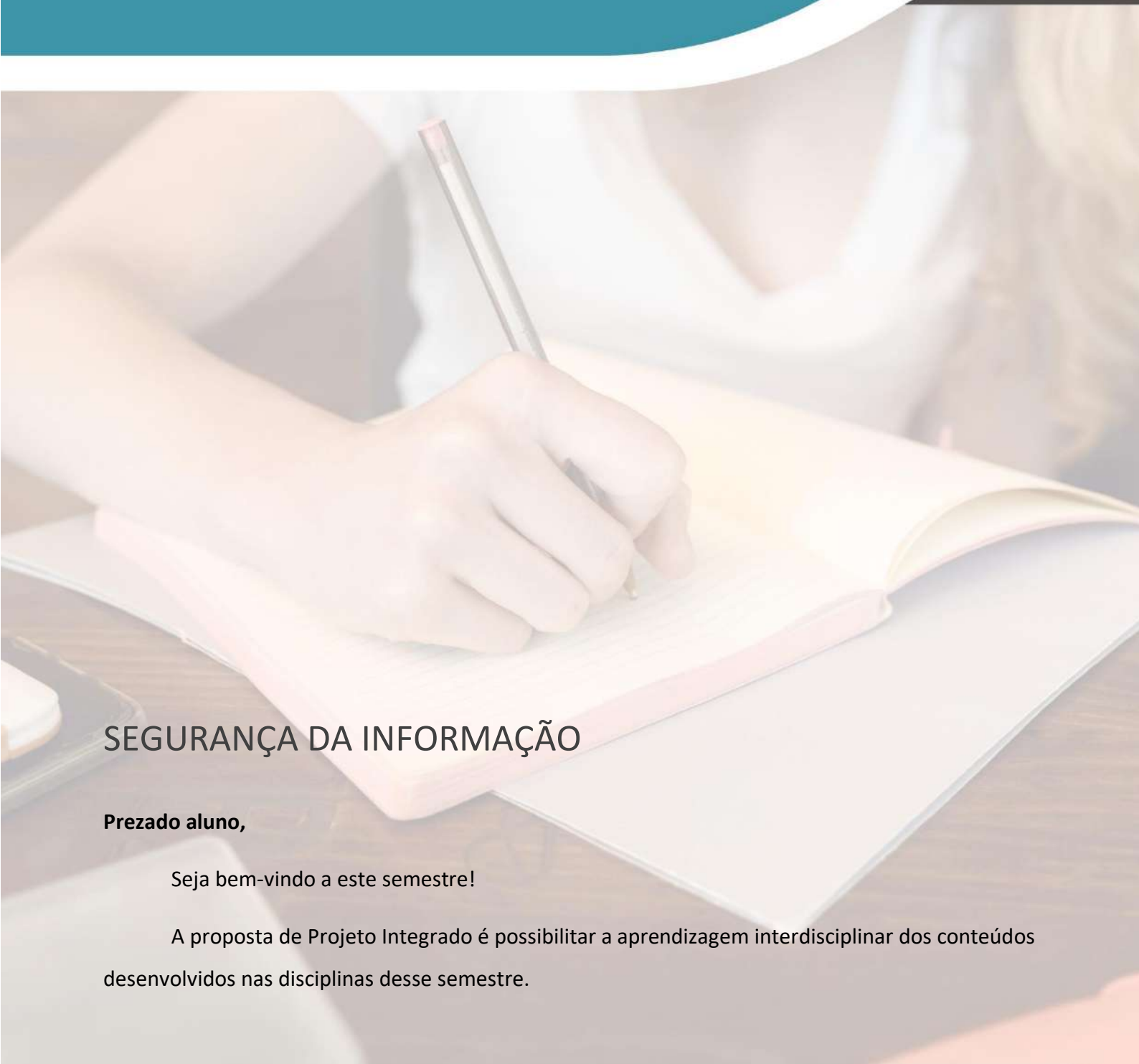


PROJETO INTEGRADO INOVAÇÃO – SEGURANÇA DA INFORMAÇÃO

A background image showing a close-up of a person's hand holding a pen and writing in an open notebook. The image is slightly blurred and has a warm, yellowish tint. The notebook is open to a page with horizontal lines. The person's hand is in the foreground, and the rest of their body is out of focus in the background.

SEGURANÇA DA INFORMAÇÃO

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: Desenvolvimento de nova plataforma de pagamento digital

Contexto:

A DataShield Corp é uma empresa global de soluções financeiras que lidera o mercado em serviços de pagamento eletrônico, gerenciamento de crédito e tecnologia blockchain para contratos inteligentes. Atuando em mais de 30 países, a companhia processa milhões de transações diárias, movimentando dados altamente sensíveis, como informações financeiras, dados pessoais de clientes e contratos empresariais.

Recentemente, a DataShield lançou o SafePay+, uma nova plataforma de pagamento digital que integra inteligência artificial para detecção de fraudes em tempo real. No entanto, o crescimento acelerado trouxe desafios significativos relacionados à segurança, conformidade regulatória e sustentabilidade operacional, ameaçando sua reputação e competitividade.

Atualmente a infraestrutura de redes é híbrida, combinando servidores locais e ambientes em nuvem pública. Existem gargalos de desempenho devido à falta de segmentação eficiente e políticas inconsistentes de controle de acesso. Filiais internacionais enfrentam problemas de latência e comunicação segura, especialmente em regiões com infraestrutura limitada.

Em um ataque recente, um grupo de hackers explorou uma vulnerabilidade em uma API, comprometendo dados de um pequeno grupo de clientes. Apesar de ter evitado um impacto maior, a empresa identificou a falta de ferramentas modernas e de uma equipe forense capacitada para investigar o incidente e identificar a origem da ameaça.

Embora transações financeiras usem padrões avançados de criptografia (TLS 1.3), sistemas internos ainda dependem de métodos antiquados, como SSL. Dados críticos estão armazenados sem criptografia em backups locais, aumentando a exposição a ataques de ransomware.

A empresa segue parcialmente o framework ISO 27001, mas não possui um programa de governança bem definido para alinhamento entre os objetivos de segurança e negócios. Falta de KPIs claros para monitorar a eficácia das políticas e práticas de TI.

Os data centers consomem grande quantidade de energia, sendo muitos baseados em fontes não renováveis. O aumento no descarte de equipamentos obsoletos sem práticas adequadas de reciclagem está em desacordo com os objetivos de ESG (Environmental, Social, and Governance).

Novos Desafios:

Com o lançamento da SafePay+ e a meta de expandir sua base de clientes em 50% nos próximos dois anos, a DataShield está enfrentando os seguintes desafios adicionais, que desenvolveremos em alguns passos:

Passo 1

Garantir uma infraestrutura de rede escalável e resiliente para suportar o aumento no tráfego. Implementar políticas de segurança mais rigorosas para proteger APIs e sistemas internos.

Passo 2

Pensando na criptografia da DataShield Corp analise o cenário atual e elabore um relatório para justificar mudanças nos métodos de criptografia utilizados, considerando os seguintes pontos: a substituição do SSL por protocolos mais seguros como o TLS 1.3 em sistemas internos, a implementação de criptografia para os dados armazenados em backups locais e o uso de criptografia assimétrica em pontos críticos para evitar acessos não autorizados. Para realizar a análise, você deve fundamentar cada recomendação com base em vulnerabilidades identificadas e melhores práticas do mercado, explicando os benefícios técnicos, como maior proteção contra ataques de *ransomware* e interceptações de dados. Ao final, discuta como essas mudanças podem contribuir para a conformidade regulatória e o fortalecimento da reputação da empresa no mercado global.

Passo 3

Durante o processamento de transações, a equipe de segurança detectou comportamentos anômalos associados a um possível ataque. Como parte da equipe de análise forense digital, sua tarefa é investigar os logs capturados para identificar o tipo de ataque, os possíveis objetivos do invasor e propor medidas para prevenir ocorrências futuras. Você recebeu um log capturado durante o período de uma atividade suspeita. O log contém informações como endereços IP, *timestamps*, URLs acessadas, respostas do servidor e status de autenticação. Sua tarefa é:

1. Analisar o log fornecido para:

- Identificar o tipo de ataque (ex.: SQL Injection, Cross-Site Scripting, Brute Force, entre outros).
- Localizar os IPs suspeitos e o comportamento padrão.
- Apontar os possíveis impactos desse ataque para a SafePay+.

- Propor medidas para prevenir ataques similares no futuro.

Log:

```
[2023-12-03 14:22:10] IP: 192.168.15.10 | URL: /login | Method: POST | Status: 401 |
User-Agent: Mozilla/5.0
[2023-12-03 14:22:12] IP: 192.168.15.10 | URL: /login | Method: POST | Status: 401 |
User-Agent: Mozilla/5.0
[2023-12-03 14:22:15] IP: 192.168.15.10 | URL: /login | Method: POST | Status: 401 |
User-Agent: Mozilla/5.0
[2023-12-03 14:23:00] IP: 203.0.113.5 | URL: /contract?id=1%20OR%201=1 | Method: GET
| Status: 200 | User-Agent: Python-urllib/3.9
[2023-12-03 14:23:30] IP: 203.0.113.5 | URL:
/contract?id=2%20UNION%20SELECT%20password%20FROM%20users | Method: GET | Status:
500 | User-Agent: Python-urllib/3.9
[2023-12-03 14:24:10] IP: 198.51.100.25 | URL: /admin | Method: POST | Status: 403 |
User-Agent: Mozilla/5.0
[2023-12-03 14:25:00] IP: 198.51.100.25 | URL: /admin | Method: POST | Status: 403 |
User-Agent: Mozilla/5.0
[2023-12-03 14:26:15] IP: 198.51.100.25 | URL: /admin | Method: POST | Status: 403 |
User-Agent: Mozilla/5.0
```

Passo 4:

Construir um programa de governança bem definido para alinhamento entre os objetivos de segurança e negócios.

Passo 5:

Adotar práticas de Green IT para melhorar sua reputação e reduzir custos operacionais.

Bons estudos!!!

Docentes do curso