

Arquitetura Digital Segura e Tolerante a Falhas

Módulo 8: Engenharia de Software

– RESUMO EXECUTIVO

Este módulo capacita estudantes a analisar, projetar e simular arquiteturas de software robustas, com foco em táticas de escalabilidade, de segurança, de tolerância a falhas, de desempenho, entre outros.

Durante 10 semanas, uma turma dedicada de alunos e seus professores irá entender o seu desafio e propor soluções utilizando metodologias ágeis. Ao final do cronograma, sua empresa receberá até 5 protótipos funcionais, permitindo que você acelere e valide ideias.

O módulo integra competências em estruturas de dados avançadas, segurança de sistemas e algoritmos com conhecimentos de governança corporativa, gestão de pessoas e gestão do conhecimento, formando profissionais preparados para decisões arquiteturais de alto impacto.

– O DESAFIO

Sistemas digitais modernos precisam operar de forma contínua, segura e resiliente, ou seja, o digital e o *business* se confundem e um não existe sem o outro. Falhas de segurança, indisponibilidade e perda de dados geram prejuízos financeiros, danos à reputação e riscos regulatórios. Organizações de todos os setores enfrentam a necessidade de construir arquiteturas que antecipem e resistam a falhas, sem comprometer a experiência do usuário.

Muitas empresas operam com arquiteturas frágeis, sem redundância, monitoramento inadequado e sem processos claros de recuperação de desastres. A complexidade crescente dos sistemas exige profissionais capazes de tomar decisões arquiteturais informadas, considerando trade-offs entre desempenho, segurança e custo.

– OBJETIVO DO MÓDULO

Analisar, projetar e validar uma arquitetura de software segura, escalável e tolerante a falhas que atenda aos requisitos da empresa parceira, demonstrando decisões de design fundamentadas e impacto mensurável na confiabilidade e segurança do sistema, ou seja, blindagem e continuidade de negócios.

– PROBLEMAS QUE PODEMOS RESOLVER

1. Resiliência e Continuidade Operacional

- Projeto de arquiteturas tolerantes a falhas com mecanismos de recuperação automática.
- Análise e mitigação de pontos únicos de falha em sistemas críticos.
- Simulação de cenários de falha e validação de estratégias de contingência.
- Controle em malha fechada nos moldes da automação digital.

2. Segurança e Conformidade

- Implementação de políticas de segurança da informação alinhadas à ISO/IEC 27001, ISO/IEC 10746 e ISO/IEC 25010.
- Análise de vulnerabilidades e auditoria de sistemas.
- Proteção de dados e conformidade com LGPD e regulamentações setoriais.

3. Escalabilidade e Desempenho

- Otimização de arquiteturas para suportar crescimento de carga e volume de dados.
- Decisões de design baseadas em táticas arquiteturais de desempenho e manutenibilidade.
- Análise de complexidade e otimização de algoritmos críticos.

– POSSÍVEIS CASOS DE APLICAÇÃO

1. Casos de Sucesso Reais (O que já entregamos)

- **Tecnologia e Redes Sociais:** Projetamos com a **Meta** (Facebook/Instagram) uma arquitetura escalável e segura para o processo de contratação de serviços e fornecedores.
- **Serviços Financeiros:** Desenvolvemos com o **Bank of America** o projeto de arquitetura para sistemas de negociação e transações com alta disponibilidade, garantindo segurança reforçada contra ataques e conformidade regulatória contínua.
- **Mobilidade e Transporte:** Estruturamos para o **Metrô-SP** a arquitetura de sistemas críticos de controle e monitoramento de infraestrutura, garantindo tolerância a falhas e estabilidade de operação em tempo real.
- **Pesquisa e Inovação:** Criamos para o **IPT (Instituto de Pesquisas Tecnológicas)** uma plataforma de processamento de dados com arquitetura distribuída e blindada, garantindo integridade e rastreabilidade total das informações.

2. Outras Aplicações Possíveis (Onde mais podemos gerar valor)

A necessidade de arquiteturas blindadas contra quedas e vazamentos de dados é universal. Nossos alunos podem atuar como um "laboratório de testes de estresse" seguro para sua empresa, identificando vulnerabilidades e propondo melhorias de arquitetura em setores como:

- **Saúde e Hospitais:** Arquitetura para sistemas de prontuário eletrônico e telemedicina que exigem alta disponibilidade (zero *downtime*) e segurança máxima de dados sensíveis para conformidade rigorosa com a LGPD.
- **Varejo e E-commerce:** Redesenho e testes de arquiteturas transacionais para suportar o hiper crescimento de volume de usuários e transações simultâneas em datas críticas (como Black Friday), sem lentidão ou queda de servidores.
- **Indústria e Manufatura:** Plataformas de monitoramento industrial contínuo com detecção de anomalias em rede e mecanismos de recuperação automática (*disaster recovery*) para evitar paradas milionárias em linhas de produção.
- **Setor Público e GovTech:** Sistemas de infraestrutura de dados governamentais que precisam de proteção robusta contra ataques cibernéticos e auditoria constante de segurança.

– POSSÍVEIS ENTREGÁVEIS

Os grupos desenvolvem uma arquitetura de software validada e documentada, podendo incluir:

- Documento de arquitetura de software com decisões de design fundamentadas.
- Simulação de cenários de falha com relatório de resiliência.
- Implementação de protótipo funcional com mecanismos de segurança e tolerância a falhas.
- Análise de segurança e auditoria de vulnerabilidades.
- Dashboard de monitoramento com storytelling de dados.
- Documentação técnica e de negócios com análise de governança corporativa.

– **PREMISSAS E REQUISITOS**

1. Da Empresa Parceira:

- Disponibilização de informações sobre arquitetura atual, requisitos de segurança e cenários de falha.
- Acesso a especialistas do negócio e especialistas técnicos para reuniões quinzenais.
- Definição clara dos requisitos não funcionais e critérios de sucesso.
- Abertura para testar e validar as soluções propostas ao longo do desenvolvimento.

2. Do Projeto:

- Foco em problemas que envolvam segurança, resiliência ou escalabilidade de sistemas.
- Complexidade arquitetural compatível com o escopo de 10 semanas.
- Potencial de impacto mensurável na confiabilidade ou segurança da operação.
- Alinhamento com práticas éticas, LGPD e normas de segurança da informação.

– **ESCOPO E RESTRIÇÕES**

1. Escopo Incluído:

- Análise e projeto de arquitetura de software com foco em segurança e resiliência.
- Simulação de cenários de falha e validação de mecanismos de recuperação.
- Implementação de protótipo funcional com componentes de segurança.
- Documentação técnica completa e documentação de governança.
- Validação funcional com cenários reais do parceiro.

2. Fora do Escopo:

- Implementação em ambiente de produção (deployment final).
- Testes de penetração (pentest) em ambiente de produção da empresa.
- Manutenção e suporte pós-projeto.
- Certificações de segurança ou compliance.

– **POSSÍVEIS TECNOLOGIAS / ARQUITETURA / FERRAMENTAS DE NEGÓCIOS**

Tecnologias e Arquitetura:

- Padrões arquiteturais (microserviços, event-driven, CQRS).
- Frameworks de segurança e criptografia.
- Ferramentas de monitoramento e observabilidade.
- Algoritmos em grafos e estruturas de dados avançadas.
- Programação funcional.
- Ferramentas de simulação de falhas (chaos engineering).

Ferramentas de Negócios:

- Frameworks de governança corporativa.
- Ferramentas de gestão do conhecimento.
- Modelos de gestão de pessoas e mudança organizacional.
- Ferramentas de storytelling de dados e dashboards.