Plano Analítico: Auditoria Informática

1. Identificação da Unidade Curricular

- **Instituição:** Instituto Superior Politécnico de Ciências e Tecnologia (INSUTEC)
- **Curso:** Engenharia de Informática e Sistemas de Informação (EISI)
- **Classificação:** Disciplina Específica / Gestão de Sistemas
- **Ano:** 5º | **Semestre:** 1º (9º Semestre)
- **Créditos:** 6.0 UC
- **Carga Horária Total:** 90 Horas (60h de Contacto | 30h de Trabalho Complementar)

2. Apresentação e Justificação

A Auditoria Informática é o processo de recolha e avaliação de evidências para determinar se um sistema de informação protege os ativos, mantém a integridade dos dados e utiliza os recursos de forma eficiente. No contexto atual de cibersegurança e conformidade legal (como a Lei de Proteção de Dados de Angola), o auditor de sistemas desempenha um papel vital na mitigação de riscos operacionais e reputacionais, assegurando o cumprimento do **Decreto Presidencial 193/18**.

3. Competências a Desenvolver (Decreto 193/18)

3.1 Competências Instrumentais (Saber)

- Compreender os conceitos, normas e metodologias de auditoria de sistemas (ISACA/COBIT).
- Conhecer o ciclo de vida de uma auditoria, desde o planeamento ao relatório final.
- Entender a importância dos controlos internos em ambientes de IT.

3.2 Competências Técnicas e Operacionais (Saber Fazer)

- **Avaliação de Risco:** Identificar vulnerabilidades e ameaças em infraestruturas e aplicações.
- **Execução de Testes:** Aplicar testes de conformidade e testes substantivos para validar controlos.
- **Elaboração de Relatórios:** Redigir pareceres técnicos e recomendações para a correção de deficiências.

3.3 Competências Atitudinais (Saber Ser/Estar)

- Atuar com total independência, objetividade e sigilo profissional.
- Demonstrar rigor ético e ceticismo profissional na avaliação de evidências digitais.

4. Conteúdo Temático (Estrutura de 90 Horas)

1. **Fundamentos de Auditoria de TI:** Definições, tipos de auditoria (interna vs externa) e o papel do auditor.
2. **Normas e Frameworks:** O uso do COBIT como guia de auditoria e as normas ITAF (Information Technology Assurance Framework).

3. **Gestão de Risco e Planeamento:** Identificação de riscos de IT e definição do plano de auditoria baseado no risco.
4. **Auditoria de Infraestrutura e Redes:** Avaliação de centros de dados, segurança perimetral e administração de sistemas.
5. **Auditoria de Aplicações e Dados:** Verificação de controlos de entrada, processamento, saída e integridade de bases de dados.
6. **Continuidade de Negócio e Disaster Recovery:** Avaliação da resiliência organizacional perante falhas catastróficas.
7. **Relatório de Auditoria:** Estrutura do relatório, classificação de achados e acompanhamento (*follow-up*).

5. Regime de Avaliação (Disciplina Específica)

- **Avaliação Contínua (40%):**
    - 1ª Frequência (Metodologia e Planeamento): 13%
    - 2ª Frequência (Auditoria Técnica e Aplicações): 14%
    - **Projeto Prático:** Simulação de uma auditoria técnica a um sistema real ou hipotético: 13%
- **Exame Normal (60%):** Prova global teórica sobre normas internacionais e resolução de casos de estudo.

6. Referências Bibliográficas (APA 7ª Ed.)

- ISACA. (2019). *CISA Review Manual* (27th ed.).
- Senft, S., Gallegos, F., & Manson, A. (2012). *Information technology control and audit* (4th ed.). CRC Press.
- Sousa, C. R. (2015). *Auditoria de sistemas de informação*. FCA.
- Cascarino, R. E. (2012). *Auditor's guide to IT auditing* (2nd ed.). Wiley.