Plano Analítico: Segurança Informática em Redes e Sistemas

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 (Nuclear)
- **Ano:** 4º | **Semestre:** 2º (8º Semestre)
- **Créditos:** 8.0 UC
- **Carga Horária Total:** 120 Horas (90h de Contacto | 30h de Trabalho Complementar)

2. Apresentação e Justificação

A disciplina aborda os princípios de confidencialidade, integridade e disponibilidade (Tríade CID) aplicados a infraestruturas tecnológicas. Num cenário de crescentes ciberataques, o engenheiro de informática deve dominar técnicas de criptografia, segurança em redes sem fios, firewalls e sistemas de deteção de intrusão. A UC justifica-se pela necessidade de projetar sistemas resilientes e conformes com as normas internacionais de segurança, em linha com o **Decreto Presidencial 193/18**.

3. Competências a Desenvolver (Decreto 193/18)

3.1 Competências Instrumentais (Saber)

- Compreender os fundamentos da criptografia simétrica e assimétrica.
- Conhecer as principais vulnerabilidades em redes e sistemas (OWASP, CVE).
- Entender os protocolos de comunicação segura (SSL/TLS, IPsec, SSH).

3.2 Competências Técnicas e Operacionais (Saber Fazer)

- **Segurança de Perímetro:** Configurar Firewalls, IDS/IPS e VPNs para proteção de tráfego.
- **Auditoria:** Realizar testes de vulnerabilidade e análise de logs para identificação de incidentes.
- **Hardening:** Aplicar técnicas de endurecimento de sistemas operativos e servidores.

3.3 Competências Atitudinais (Saber Ser/Estar)

- Atuar com ética profissional e conformidade legal na manipulação de dados sensíveis.
- Demonstrar proatividade na gestão de riscos e resposta a incidentes de segurança.

4. Conteúdo Temático (Estrutura de 120 Horas)

1. **Fundamentos de Segurança:** Ameaças, vulnerabilidades, riscos e a Tríade CID.
2. **Criptografia:** Algoritmos (AES, RSA), funções de hash (SHA-256), assinaturas digitais e infraestrutura de chaves públicas (PKI).
3. **Segurança em Redes:** Ataques comuns (Spoofing, DoS/DDoS, MitM) e defesa com Firewalls (Stateful vs Stateless).

4. **Protocolos Seguros e VPNs:** Implementação de IPsec e tunelamento seguro para acesso remoto.
5. **Segurança em Sistemas Operativos:** Controlo de acessos, autenticação multifator (MFA) e segurança de privilégios.
6. **Segurança Aplicacional e Web:** Proteção contra SQL Injection, XSS e segurança em APIs.
7. **Gestão de Incidentes e Forense:** Planos de continuidade de negócio e introdução à análise forense digital.

5. Regime de Avaliação (Disciplina Específica)

- **Avaliação Contínua (40%):**
    - 1ª Frequência (Criptografia e Fundamentos): 13%
    - 2ª Frequência (Segurança de Redes e Aplicações): 14%
    - **Laboratório Prático:** Simulação de defesa e ataque controlado (Capture The Flag - CTF): 13%
- **Exame Normal (60%):** Prova global teórica e prática em laboratório.

6. Referências Bibliográficas (APA 7ª Ed.)

- Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson.
- Tanenbaum, A. S., & Wetherall, D. J. (2021). *Redes de computadores* (6ª ed. - Cap. de Segurança). Pearson.
- Kaufman, C., Perlman, R., & Speciner, M. (2002). *Network security: Private communication in a public world*. Prentice Hall.
- Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley.