INSTITUTO POLITÉCNICO DE BEJA
Escola Superior de Tecnologia e Gestão
Mestrado em Engenharia de Segurança Informática
Fundamentos de Cibersegurança

Trabalho Individual

Martinho José Novo Caeiro - 23917

Beja, novembro de 2025

INSTITUTO POLITÉCNICO DE BEJA
Escola Superior de Tecnologia e Gestão
Mestrado em Engenharia de Segurança Informática
Fundamentos de Cibersegurança

Trabalho Individual

Martinho José Novo Caeiro - 23917

Orientadores: Rui Miguel Silva & Rogério Matos Bravo

Beja, novembro de 2025

Resumo

Este relatório descreve o desenvolvimento de uma aplicação de segurança informática, implementada em Python, uma linguagem de programação dinâmica. O objetivo é explorar conceitos fundamentais de segurança e demonstrar a aplicação prática desses conceitos. Esta aplicação é desenvolvida no âmbito da unidade curricular de Fundamentos de Cibersegurança IPBeja, 2025.

Keywords: mitre, att&ck, segurança informática, fundamentos de cibersegurança

Abstract

This report describes the development of a cybersecurity application implemented in Python, a dynamic programming language. The goal is to explore fundamental security concepts and demonstrate their practical application. This application is developed within the scope of the Fundamentals of Cybersecurity course IPBeja, 2025.

Keywords: mitre, att&ck, cybersecurity, fundamentals of cybersecurity

Índice

Índice de Figuras

1 Introdução

Este relatório apresenta o trabalho individual realizado para a unidade curricular de *Fundamentos de Cibersegurança* do *Mestrado em Engenharia de Segurança Informática* do *Instituto Politécnico de Beja*. O objetivo principal é a análise de conceitos e normas (*MITRE/ATT&CK*, *ISO 27000* e legislação nacional relevante).

O relatório foi elaborado de acordo com o *"Manual de Normas Obrigatórias para a Elaboração de Documentos Institucionais e Trabalhos Académicos"* do *Instituto Politécnico de Beja*.

Em termos de estrutura, o **Capítulo I (Grupo I)** aborda a área escolhida do MITRE, a análise detalhada de uma campanha do ATT&CK e a comparação de técnicas entre matrizes; o **Capítulo II (Grupo II)** discute os pilares da segurança da informação, as três dimensões principais e o conceito de **'Governança'**, com ligação à **Resolução do Conselho de Ministros**, quando pertinente.

A bibliografia e as fontes consultadas são apresentadas no final do documento e o relatório será disponibilizado no repositório GitHub (Martinho Caeiro, 2025).

2 Teoria

2.1 MITRE

O MITRE (MITRE Corporation, 2025a) é uma organização sem fins lucrativos que opera centros de pesquisa e desenvolvimento financiados pelo governo dos Estados Unidos.

2.2 Att&ck

O ATT&CK (MITRE Corporation, 2025b) é um framework desenvolvido pelo MITRE que documenta as táticas e técnicas utilizadas por adversários cibernéticos.

2.3 Segurança da Informação

A Segurança da Informação refere-se à prática de proteger informações e sistemas de informação contra acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição. Envolve a implementação de políticas, procedimentos e tecnologias para garantir a confidencialidade, integridade e disponibilidade dos dados.

3 Grupo I

O presente capítulo procede à análise detalhada de uma das áreas de cibersegurança do projecto *MITRE*, tendo sido escolhida a opção **c) -** *Cyber Intelligence Threat Analysis.* O objetivo desta secção é reproduzir e aprofundar a abordagem apresentada em aula para a área da Gestão de Vulnerabilidades, adaptando-a ao domínio da *Threat Analysis*, com ênfase nos sistemas de classificação, nas suas inter-relações e nas implicações operacionais para a deteção e mitigação de ameaças.

3.1 Cyber Intelligence Threat Analysis

3.2

3.3

4 Grupo II

O presente capítulo tem como objetivo abordar os principais conceitos estruturantes da **Segurança da Informação**, tal como definidos no âmbito da unidade curricular de *Fundamentos de Cibersegurança*. São analisados os pilares, vetores e princípios de governança que sustentam a proteção da informação e a gestão de riscos no contexto das organizações modernas, com particular atenção às normas da família *ISO/IEC 27000* e à legislação nacional aplicável.

4.1 Os Quatro Pilares da Segurança da Informação

A segurança da informação, de acordo com uma visão abrangente e integrada, assenta em quatro pilares fundamentais: **Tecnologias**, **Pessoas**, **Organizações** e **Segurança Física**. Estes elementos, interdependentes entre si, formam a base sobre a qual as normas da família *ISO/IEC 27000* (incluindo as versões mais recentes da *ISO/IEC 27001:2022* e *ISO/IEC 27002:2022*) estruturam a gestão da segurança da informação.

4.1.1 Tecnologias

Este pilar corresponde ao conjunto de ferramentas, sistemas e mecanismos técnicos implementados para proteger a informação. Inclui medidas como o controlo de acessos, a encriptação, a gestão de vulnerabilidades, os sistemas de deteção e prevenção de intrusões, bem como políticas de *backup* e recuperação. O foco é garantir que os recursos tecnológicos oferecem **confidencialidade**, **integridade** e **disponibilidade**, de acordo com os objetivos organizacionais e as boas práticas definidas pela *ISO/IEC 27002:2022*.

4.1.2 Pessoas

As pessoas representam simultaneamente o **maior ativo** e o **elo mais vulnerável** da segurança da informação. A consciencialização, a formação contínua e a definição clara de responsabilidades são essenciais para reduzir o risco humano. De acordo com as normas ISO, a cultura organizacional deve promover comportamentos seguros e uma compreensão clara das políticas internas de segurança, prevenindo negligência, erro humano ou engenharia social.

4.1.3 Organizações (processos e procedimentos)

Este pilar abrange a estrutura organizacional, os processos e os procedimentos formais que sustentam o **Sistema de Gestão da Segurança da Informação (SGSI)**. Inclui políticas, planos de gestão de incidentes, auditorias, avaliação de riscos e conformidade com a legislação (como o RGPD e a legislação nacional aplicável). A norma *ISO/IEC 27001:2022* reforça este pilar ao definir requisitos para a implementação e manutenção de controlos de segurança eficazes, sustentados em documentação e melhoria contínua.

4.1.4 Segurança Física

A segurança física visa proteger as infraestruturas, equipamentos e suportes de informação contra ameaças físicas — como acesso não autorizado, incêndios, inundações ou sabotagem. Abrange o controlo de acessos a edifícios, a vigilância, a gestão ambiental e a proteção dos dispositivos de armazenamento. Sem segurança física, qualquer sistema técnico ou processo organizacional fica vulnerável, comprometendo os restantes pilares.

4.1.5 Pilar mais importante

Apesar da sua interdependência, o **pilar das pessoas** é frequentemente considerado o mais determinante. As tecnologias, políticas e infraestruturas só são eficazes se forem corretamente compreendidas e aplicadas pelos utilizadores. O comportamento humano é o fator crítico que pode tanto reforçar como comprometer os restantes pilares, tornando a formação e a sensibilização indispensáveis à eficácia global da segurança da informação.

4.1.6 Ligação à Intervenção Digital Forense

A **intervenção digital forense** — responsável pela recolha, preservação e análise de evidências digitais — relaciona-se diretamente com vários destes pilares, mas de forma especial com as **tecnologias** e as **organizações (processos e procedimentos)**.

- **Tecnologias:** a recolha e preservação de evidências requerem ferramentas técnicas adequadas, como software de aquisição forense e mecanismos de hashing, que asseguram a integridade dos dados.

- **Organizações:** a existência de procedimentos normalizados (cadeia de custódia, registos de auditoria, políticas de acesso e conservação) garante que a prova digital é admissível e fidedigna.
- **Pessoas:** os peritos forenses e os técnicos de segurança devem agir de forma ética e tecnicamente rigorosa, assegurando a imparcialidade e a rastreabilidade das suas ações.

Assim, a intervenção digital forense concretiza a aplicação prática dos pilares da segurança da informação, garantindo que a gestão de incidentes e a produção de prova digital são realizadas de forma segura, controlada e conforme às normas internacionais.

4.2 Os Três Vetores da Segurança da Informação

A segurança da informação pode ser analisada segundo três vetores principais, também designados como as **três dimensões operacionais da segurança**: **Segurança Física**, **Segurança Humana** e **Segurança Lógica**. Estes vetores formam uma estrutura integrada que assegura a proteção da informação em todas as suas formas — material, humana e tecnológica — e encontram correspondência direta no enquadramento da **Segurança da Informação Classificada (SIC)**, conforme definido pela **Resolução do Conselho de Ministros n.º 5/1990**, que aprova a **SEGNAC4** (Sistema de Segurança Nacional de Classificação, Codificação e Salvaguarda de Informação Classificada).

4.2.1 Segurança Física

A segurança física tem como objetivo proteger as instalações, equipamentos e suportes de informação contra ameaças de natureza física, acidental ou intencional. Inclui medidas como o controlo de acessos a edifícios e zonas restritas, vigilância eletrónica, barreiras físicas, proteção ambiental (contra incêndios, inundações, etc.) e a salvaguarda de documentos em cofres ou armários classificados. No contexto da **SEGNAC4**, a segurança física é indispensável para garantir que a informação classificada, em suporte material, não é acedida, copiada ou destruída sem autorização.

4.2.2 Segurança Humana

A segurança humana refere-se à gestão dos riscos associados ao fator humano, reconhecendo que as pessoas podem ser tanto a maior defesa como a maior vulnerabilidade da segurança da informação. Abrange procedimentos de seleção, credenciação e formação de pessoal, garantindo que apenas indivíduos devidamente autorizados e conscientes das suas responsabilidades têm acesso a informação classificada. A **SEGNAC4** estabelece regras específicas sobre credenciação de segurança, dever de sigilo e responsabilidade disciplinar ou penal em caso de violação das normas de proteção da informação classificada.

4.2.3 Segurança Lógica

A segurança lógica, também designada **segurança tecnológica ou digital**, incide sobre os sistemas informáticos e redes de comunicação. Compreende o conjunto de medidas destinadas a proteger a informação processada ou armazenada em formato eletrónico, incluindo autenticação, controlo de acessos, encriptação, gestão de vulnerabilidades, auditorias de segurança e registos de atividade. Na **SIC**, a segurança lógica é essencial para assegurar que a informação classificada mantida em sistemas digitais cumpre os níveis de proteção definidos, prevenindo o acesso não autorizado ou a exfiltração de dados.

4.2.4 Ligação à SEGNAC4

A **Resolução do Conselho de Ministros n.º 5/1990** define o modelo nacional de proteção da informação classificada, estabelecendo que a segurança deve ser assegurada de forma global, integrando os três vetores mencionados. A eficácia da **Segurança da Informação Classificada** depende, assim, da articulação entre as dimensões física, humana e lógica - cada uma cobrindo diferentes fases e contextos da proteção da informação. Quando devidamente coordenadas, estas três dimensões garantem a **confidencialidade**, **integridade** e **disponibilidade** da informação classificada, em conformidade com as exigências nacionais e internacionais de segurança.

4.3 O conceito de 'Governança'

O conceito de **Governança** da Segurança da Informação e da Cibersegurança, conforme apresentado no âmbito deste curso e nas normas da família *ISO/IEC 27001*, representa o conjunto de práticas, responsabilidades e processos que asseguram que a gestão da segurança é conduzida de forma estruturada, mensurável e alinhada com os objetivos estratégicos da organização.

Mais especificamente, os controlos **8.15** e **8.16** da *ISO/IEC 27001:2022* estabelecem as bases da governança, determinando que as organizações devem **monitorizar, rever e melhorar continuamente** os mecanismos de segurança, assegurando que as medidas implementadas permanecem eficazes e adequadas ao contexto operacional e às ameaças em evolução.

4.3.1 Conteúdo e Aplicação Prática

A **Governança da Segurança da Informação** implica:

- **Definir a granularidade dos acessos e dos "assets críticos"**, determinando níveis de privilégio e identificando os recursos cuja proteção é prioritária;
- **Avaliar e testar** regularmente a eficácia dos controlos e políticas de segurança;
- **Monitorizar** o comportamento dos sistemas e dos utilizadores, através de mecanismos de auditoria, registos e indicadores de desempenho;
- **Testar e rever os SOP (Standard Operating Procedures)**, garantindo que os procedimentos operacionais estão atualizados, coerentes e eficazes na mitigação de riscos.

Estas atividades asseguram que a segurança da informação é gerida de forma sistemática e não meramente reativa, promovendo uma cultura de responsabilidade, conformidade e melhoria contínua.

4.3.2 Importância para a Cibersegurança e o Combate ao Cibercrime

No domínio da **Cibersegurança**, a Governança é essencial para transformar políticas e orientações estratégicas em práticas concretas e auditáveis. Permite estabelecer mecanismos de responsabilização, definir papéis claros (por exemplo, CISO, gestores de risco, auditores) e integrar a gestão da segurança com os objetivos institucionais.

No **combate ao cibercrime**, a governança contribui para a capacidade de resposta organizada a incidentes, garantindo rastreabilidade, preservação de evidências digitais e cumprimento de obrigações legais — aspetos fundamentais em processos de investigação e cooperação entre entidades públicas e privadas.

4.3.3 Correspondência com a RCM n.º 41/2018

A **Resolução do Conselho de Ministros n.º 41/2018**, que aprova a **Estratégia Nacional de Segurança do Ciberespaço (ENSCE)**, apresenta um enquadramento convergente com o conceito de governança definido nas normas ISO. Ambos os documentos enfatizam:

- A necessidade de **estruturas organizacionais de coordenação** e de **responsabilidade partilhada**;
- A importância da **monitorização e avaliação contínua** das políticas de segurança;
- A criação de **mecanismos de supervisão e reporte** de incidentes e vulnerabilidades;
- A promoção de uma **cultura de segurança** transversal ao setor público, privado e académico.

Assim, pode afirmar-se que existe uma **correspondência direta** entre o conceito de Governança, tal como definido nas normas *ISO/IEC 27001:2022 (8.15/8.16)*, e os princípios orientadores da **RCM n.º 41/2018**, sendo ambos instrumentos complementares na consolidação da cibersegurança e na prevenção e combate ao cibercrime em Portugal.

5 Conclusão

Bibliografia

IPBeja. (2025). *Disciplina: Fundamentos de Cibersegurança | IPBeja* [Página FC]. Obtido novembro 13, 2025, de https://cms.ipbeja.pt/course/view.php?id=1164

Martinho Caeiro. (2025). *MITRE-Report - Repositório de Código* [Repositório da Aplicação MITRE-Report]. Obtido novembro 13, 2025, de https://github.com/MartinhoCaeiro/MITRE-Report

MITRE Corporation. (2025a). *About MITRE | MITRE* [Página Oficial do MITRE]. Obtido novembro 13, 2025, de https://www.mitre.org/

MITRE Corporation. (2025b). *MITRE ATT&CK® | MITRE ATT&CK®* [Página Oficial do MITRE ATT&CK]. Obtido novembro 13, 2025, de https://attack.mitre.org/