



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 apresenta uma análise crítica e aplicada de conceitos fundamentais de cibersegurança, centrada no framework MITRE/ATT&CK e na sua aplicação prática para identificação, deteção e resposta a ameaças. O documento inclui uma revisão teórica, um estudo de caso detalhado sobre a campanha *Operation MidnightEclipse* (ID C0048), e uma comparação de técnicas entre as matrizes Enterprise, Mobile e ICS. Complementarmente, aborda os pilares e vetores da segurança da informação e o conceito de governança, alinhando controlos e práticas com a família *ISO/IEC 27000* e a legislação nacional relevante. O relatório encerra com recomendações operacionais para deteção, mitigação, investigação forense e partilha de informação de ameaças, visando reforçar a postura de segurança em contextos organizacionais.

Keywords: mitre, att&ck, segurança informática, governança, investigação forense

Abstract

This report delivers a critical and practical analysis of core cybersecurity concepts, focused on the MITRE/ATT&CK framework and its operational use for threat identification, detection and response. It contains a theoretical overview, a detailed case study of the *Operation MidnightEclipse* campaign (ID C0048), and a comparison of techniques across Enterprise, Mobile and ICS matrices. The work also examines information security pillars and governance, aligning relevant controls with the *ISO/IEC 27000* family and applicable national legislation. The document concludes with operational recommendations for detection, mitigation, forensic investigation and threat information sharing to strengthen organisational security posture.

Keywords: mitre, att&ck, cybersecurity, governance, forensic investigation

Índice

1	Introdução	1
2	Revisão Teórica	2
2.1	MITRE	2
2.2	Att&ck	2
2.3	Segurança da Informação	2
3	Grupo I	3
3.1	Cyber Threat Information Sharing	3
3.1.1	TAXII	4
3.1.2	STIX	4
3.2	Campanha <i>Operation MidnightEclipse</i>	5
3.3	Tática Collection	6
3.3.1	Enterprise	6
3.3.2	Mobile	6
3.3.3	ICS	7
3.3.4	Exemplos	7
4	Grupo II	8
4.1	Os Quatro Pilares da Segurança da Informação	8
4.1.1	Tecnologias	8
4.1.2	Pessoas	8
4.1.3	Organizações (processos e procedimentos)	9
4.1.4	Segurança Física	9
4.1.5	Pilar mais importante	9
4.1.6	Ligação à Intervenção Digital Forense	10
4.2	Os Três Vetores da Segurança da Informação	11
4.2.1	Segurança Física	11
4.2.2	Segurança Humana	11

4.2.3	Segurança Lógica	12
4.2.4	Ligação à SEGNA4	12
4.3	O conceito de ‘Governança’	13
4.3.1	Conteúdo e Aplicação Prática	13
4.3.2	Importância para a Cibersegurança e o Combate ao Cibercrime	14
4.3.3	Correspondência com a RCM n.º 41/2018	14
5	Conclusão	15
	Bibliografia	16

1 Introdução

Este relatório apresenta o trabalho individual realizado para a unidade curricular de *Fundamentos de Cibersegurança* (IPBeja, 2025) 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).

Em termos de estrutura, o relatório organiza-se em dois blocos complementares. O **Grupo I** explora em detalhe a área seleccionada do MITRE/ATT&CK, incluindo análise de campanhas representativas, identificação de táticas, técnicas e procedimentos (TTPs) e comparação de técnicas entre as matrizes Enterprise, Mobile e ICS. O **Grupo II** analisa os fundamentos da segurança da informação - pilares, vetores e o conceito de **Governança** - estabelecendo ligações práticas às normas *ISO/IEC* e à legislação nacional quando pertinente, e propondo recomendações operacionais para deteção, mitigação, resposta a incidentes e gestão de risco.

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

2 Revisão Teórica

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, 2025f) 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 (Wikipedia, 2025) 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 das áreas selecionadas do MITRE/ATT&CK, com especial foco na transformação da informação técnica em inteligência acionável para operações de defesa. Pretende-se identificar e descrever as táticas, técnicas e procedimentos (TTPs) mais relevantes, analisar campanhas representativas e comparar técnicas entre as diferentes matrizes (Enterprise, Mobile e ICS). O capítulo integra estudos de caso, avaliação de ferramentas e recomendações práticas para deteção, mitigação e resposta a incidentes, promovendo a ligação entre a análise de ameaças e as medidas operacionais.

3.1 Cyber Threat Information Sharing

A área *Cyber Threat Information Sharing* (MITRE Corporation, 2025e) foca-se nos processos e mecanismos utilizados para partilhar informação sobre ameaças cibernéticas entre equipas, organizações e entidades externas. O objetivo principal é aumentar a capacidade coletiva de deteção, prevenção e resposta, garantindo que os indicadores de ataque, técnicas utilizadas pelos adversários e outros elementos relevantes chegam rapidamente aos intervenientes que deles necessitam.

A partilha de informação de ameaças pode incluir **IOCs** (Indicators of Compromise), padrões de comportamento observados, artefactos recolhidos em incidentes, ou relatórios de análise produzidos por equipas de *Cyber Threat Intelligence*. Esta partilha deve seguir formatos estruturados e normalizados que permitam interoperabilidade e automatização.

Entre os sistemas e padrões mais utilizados destacam-se o seguintes:

3.1.1 TAXII

O **Trusted Automated eXchange of Indicator Information** (Taxii Project, 2025) é uma framework comunitária que define conceitos, protocolos e formatos de mensagem para a partilha segura, eficiente e automatizada de informação de ameaças. O TAXII especifica a forma como dados estruturados podem ser enviados e recebidos entre plataformas, permitindo que organizações consumam e disponibilizem inteligência de forma padronizada.

Existem dois modelos principais de operação no TAXII:

- *Collections* - repositórios lógicos onde conjuntos de dados de ciberameaças são armazenados e disponibilizados.
- *Channels* - mecanismos de comunicações pub/sub que permitem fluxos contínuos de informação.

Além disso, o TAXII suporta autenticação, controlo de acesso e transportes seguros, garantindo que apenas entidades autorizadas podem aceder à informação partilhada.

3.1.2 STIX

O **Structured Threat Information eXpression** (STIX Project, 2025) é uma linguagem desenvolvida para representar informação de ameaças de forma estruturada, permitindo interoperabilidade entre sistemas e facilitando a automatização de processos de deteção e resposta.

O STIX permite descrever não apenas IOCs, mas também:

- **TTPs (Tactics, Techniques and Procedures)** - modelos que representam comportamentos e padrões de ataque.
- **Entidades envolvidas** - como atores de ameaça, campanhas e intrusões conhecidas.
- **Relações entre objetos** - possibilitando análises avançadas, como correlação de indicadores e identificação de cadeias de ataque.

A versão mais recente, STIX 2.x (OASIS Open, 2025b), foi otimizada para compatibilidade com TAXII 2.x (OASIS Open, 2025c) e para simplificar o modelo de dados, permitindo uma representação mais clara e eficiente da inteligência partilhada, estas são agora geridas pela OASIS (OASIS Open, 2025a).

3.2 Campanha *Operation MidnightEclipse*

A campanha **Operation MidnightEclipse - ID C0048** (MITRE Corporation, 2025g) decorreu entre março e abril de 2024. Esta explorou a vulnerabilidade CVE-2024-3400 no módulo GlobalProtect de firewalls Palo Alto, permitindo execução remota de código com privilégios de root. O ator associado, identificado como UTA0218, realizou um ataque direcionado, combinando exploração de zero-day, implantação de backdoor e exfiltração de dados críticos.

As técnicas e TTPs observadas incluem:

- T1190 - Exploit Public-Facing Application: exploração da vulnerabilidade no firewall.
- T1059.004 - Command and Scripting Interpreter: Unix Shell: execução de comandos via bash.
- T1105 - Ingress Tool Transfer: download de ferramentas adicionais.
- T1053.003 - Scheduled Task/Job: Cron: persistência com tarefas agendadas.
- T1078.002 - Valid Accounts: Domain Accounts: uso de credenciais válidas para movimentação lateral.
- T1090 - Proxy: comunicação C2 via túnel com GOST.

O software/ferramentas usadas incluiu:

- UPSTYLE: backdoor Python para execução remota.
- GOST: criação de túneis reversos para comunicação com servidores de comando e controle.

A campanha visou roubo de credenciais, dados de configuração do firewall e movimentação lateral dentro da rede, mantendo persistência com cron jobs e backdoors. A mitigação recomendada incluiu patches do PAN-OS, monitorização de tráfego, análise de logs e recolha de evidências forenses.

3.3 Tática Collection

A tática *Collection* descreve a recolha de dados realizada por um adversário após comprometer um sistema. Embora a tática seja comum às matrizes *Enterprise*, *Mobile* e *ICS*, as técnicas associadas diferem significativamente devido às particularidades de cada ambiente.

3.3.1 Enterprise

No ambiente *Enterprise - TA0009* (MITRE Corporation, 2025b), a recolha de dados centra-se em artefactos típicos de sistemas operativos tradicionais, como ficheiros locais, credenciais, histórico de navegação, processos, memória e dados de aplicações corporativas. As técnicas focam mecanismos amplamente presentes em sistemas Windows, Linux e macOS, refletindo um conjunto de ativos essencialmente digitais.

3.3.2 Mobile

Na matriz *Mobile - TA0035* (MITRE Corporation, 2025c), a recolha é condicionada por mecanismos de segurança próprios de dispositivos móveis, tais como *sandboxing*, permissões de aplicações e acesso limitado ao sistema de ficheiros. Assim, as técnicas incidem sobre dados pessoais e de aplicações, nomeadamente localização, contactos, mensagens, fotos, sensores e dados armazenados por aplicações móveis.

3.3.3 ICS

No domínio *ICS - TA0100* (MITRE Corporation, 2025d), a recolha de informação está relacionada com processos industriais e sistemas de controlo. As técnicas visam obter dados operacionais provenientes de PLCs, sensores, actuadores, sistemas SCADA e parâmetros de controlo. Estes dados são críticos para compreender e manipular processos físicos.

3.3.4 Exemplos

Alguns exemplos de técnicas específicas para cada matriz incluem:

- **Enterprise:** a técnica *T1005 - Data from Local System*: permite recolher ficheiros e credenciais armazenadas num sistema.
- **Mobile:** a técnica *T1409 - Access Stored Application Data*: foca-se na recolha de dados de aplicações móveis, como mensagens ou bases de dados internas.
- **ICS:** a técnica *T0887 - Operation Information*: permite ao adversário recolher dados operacionais de dispositivos industriais, como leituras de sensores ou estados de PLCs.

Estas diferenças demonstram que, embora a tática seja comum, as técnicas variam devido à natureza distinta dos ambientes e dos dados relevantes em cada matriz.

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* (ISO, 2025a) 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* (ISO, 2025b) e *ISO/IEC 27002:2022* (ISO, 2025c)) 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 (EUR-Lex, 2025) 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** (Diário da República, 2025b), 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, accidental 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 SEGNA C4

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** (Diário da República, 2025a), 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

Neste relatório procurei integrar teoria e prática no domínio da cibersegurança, explorando o framework MITRE/ATT&CK, mecanismos de partilha de informação (STIX/TAXII), conceitos de governança e princípios de investigação forense. Ao longo do trabalho aprendi a mapear táticas, técnicas e procedimentos (TTPs) para contextos operacionais distintos, a analisar campanhas reais - como a *Operation MidnightEclipse* - e a correlacionar controlos técnicos com normas da família *ISO/IEC 27000* e enquadramentos nacionais (SEGNAC4, ENSCE).

O desenvolvimento deste projeto reforçou competências práticas e metodológicas: recolha e organização de bibliografia, análise crítica de artefactos técnicos, formulação de recomendações de deteção e mitigação, e a importância da cadeia de custódia em intervenções forenses. Aprendi também a traduzir dados técnicos em inteligência acionável e a considerar as diferenças entre matrizes Enterprise, Mobile e ICS ao propor medidas de defesa.

Em termos pessoais, este trabalho aprofundou a minha capacidade de síntese, o pensamento crítico e a literacia técnica necessária para comunicar resultados técnicos de forma estruturada e justificada.

Em suma, o relatório constitui uma base sólida que consolida os conhecimentos adquiridos e abre caminho para a sua aplicação prática continuada e para investigação complementar em ciberinteligência.

Bibliografia

- Diário da República. (2025a). *Resolução do Conselho de Ministros n.º 41/2018* [Página Oficial da Resolução do Conselho de Ministros n.º 41/2018]. Obtido novembro 19, 2025, de <https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/41-2018-114937034>
- Diário da República. (2025b). *Resolução do Conselho de Ministros n.º 5/1990* [Página Oficial da Resolução do Conselho de Ministros n.º 5/1990]. Obtido novembro 19, 2025, de <https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/5-1990-307435>
- EUR-Lex. (2025). *Regulamento (UE) 2016/679* [Página Oficial do Regulamento Geral sobre a Proteção de Dados (RGPD)]. Obtido novembro 19, 2025, de <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679>
- IPBeja. (2025). *Disciplina: Fundamentos de Cibersegurança / IPBeja* [Página FC]. Obtido novembro 13, 2025, de <https://cms.ipbeja.pt/course/view.php?id=1164>
- ISO. (2025a). *ISO/IEC 27000 Information security management systems — Overview and vocabulary* [Página Oficial da Norma ISO/IEC 27000]. Obtido novembro 19, 2025, de <https://www.iso.org/standard/73906.html>
- ISO. (2025b). *ISO/IEC 27001 Information security, cybersecurity and privacy protection — Information security management systems — Requirements* [Página Oficial da Norma ISO/IEC 27001]. Obtido novembro 19, 2025, de <https://www.iso.org/standard/27001>
- ISO. (2025c). *ISO/IEC 27002 Information security, cybersecurity and privacy protection — Code of practice for information security controls* [Página Oficial da Norma ISO/IEC 27002]. Obtido novembro 19, 2025, de <https://www.iso.org/standard/75652.html>
- 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). *Collection, Tactic TA0009 - Enterprise / MITRE ATT&CK®* [Página Oficial da Tática Collection na Matriz Enterprise]. Obtido novembro 26, 2025, de <https://attack.mitre.org/tactics/TA0009/>

MITRE Corporation. (2025c). *Collection, Tactic TA0035 - Mobile / MITRE ATT&CK®* [Página Oficial da Tática Collection na Matriz Mobile]. Obtido novembro 19, 2025, de <https://attack.mitre.org/tactics/TA0035/>

MITRE Corporation. (2025d). *Collection, Tactic TA0100 - ICS / MITRE ATT&CK®* [Página Oficial da Tática Collection na Matriz ICS]. Obtido novembro 19, 2025, de <https://attack.mitre.org/tactics/TA0100/>

MITRE Corporation. (2025e). *Making Security Measurable - Cyber Threat Information Sharing* [Página Oficial sobre Cyber Threat Information Sharing]. Obtido novembro 19, 2025, de <https://makingsecuritymeasurable.mitre.org/directory/areas/threatsharing.html>

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

MITRE Corporation. (2025g). *Operation MidnightEclipse / MITRE ATT&CK®* [Página Oficial da Campanha Operation MidnightEclipse]. Obtido novembro 19, 2025, de <https://attack.mitre.org/campaigns/C0048/>

OASIS Open. (2025a). *OASIS Cyber Threat Intelligence (CTI) Technical Committee* [Página Oficial da OASIS Open]. Obtido novembro 26, 2025, de https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti

OASIS Open. (2025b). *OASIS STIX Version 2.x Specification* [Página Oficial da Especificação OASIS STIX v2.x]. Obtido novembro 26, 2025, de <https://oasis-open.github.io/cti-documentation/stix/intro>

OASIS Open. (2025c). *OASIS TAXII Version 2.x Specification* [Página Oficial da Especificação OASIS TAXII v2.x]. Obtido novembro 26, 2025, de <https://oasis-open.github.io/cti-documentation/taxii/intro>

STIX Project. (2025). *STIX - Structured Threat Information Expression* [Página Oficial do STIX Project]. Obtido novembro 26, 2025, de <https://stixproject.github.io/>

Taxii Project. (2025). *TAXII - Trusted Automated eXchange of Indicator Information* [Página Oficial do TAXII Project]. Obtido novembro 26, 2025, de <https://taxiiproject.github.io/>

Wikipedia. (2025). *Information security - Wikipedia* [Página Wikipedia sobre Segurança da Informação]. Obtido novembro 13, 2025, de https://en.wikipedia.org/wiki/Information_security