



Quadros Normativos

Controlos tecnológicos para conformidade
com o Regulamento Geral sobre a
Proteção de Dados

Introdução

- Conjunto de políticas e procedimentos que regulam a implementação e gestão contínua da segurança de uma organização
- Inclui os planos ou quadro de referência para a cibersegurança de uma organização
- Não indica/obriga à conformidade
- Não significa que uma organização está automaticamente segura

Necessidade de um quadro normativo

- É considerado as melhores práticas da industria
- Permite que as organizações tenham a informação organizada de acordo com os requisitos de conformidade
- Ajuda as organizações a comunicar com outras organizações utilizando o mesmo vocabulário
- Assegura que as organizações são capazes de garantir a sua própria segurança e criam um quadro de referência para introduzir melhorias

Quadros normativos

Regulamentos:

- RGPD (UE 2016/679), Lei 58/2019,
- Processamento de dados pelas autoridades (UE 2016/680), Lei 59/2019
- RJSC (UE 2016/1148), Lei 46/2018
- Resolução de conselho de ministros 41/2018

Normas:

- Família ISO 27000
- NIST Cyber Security Framework
- NIST SP800-53
- NIST SP800-37
- ITIL
- Quadro nacional de referência para a Cibersegurança (QNRCS)

Boas práticas:

- Manual de boas práticas sobre o RGPD do GNS
- MITRE ATT&CK

Regulamento geral sobre a proteção de dados

Tecnologia

- Artigo 5º – Princípios relativos ao tratamento de dados pessoais
- Artigo 15º – Direito de acesso do titular dos dados
- Artigo 16º – Direito de retificação
- Artigo 17º – Direito ao apagamento dos dados («direito a ser esquecido»)
- Artigo 18º – Direito à limitação do tratamento
- Artigo 19º – Obrigação de notificação da retificação ou apagamento dos dados pessoais ou limitação do tratamento
- Artigo 20º – Direito de portabilidade dos dados
- Artigo 21º – Direito de oposição
- Artigo 22º – Decisões individuais automatizadas, incluindo definição de perfis
- Artigo 24º – Responsabilidade do responsável pelo tratamento
- Artigo 25º – Proteção de dados desde a conceção e por defeito
- Artigo 32º – Segurança do tratamento
- Artigo 33º – Notificação de uma violação de dados pessoais à autoridade de controlo
- Artigo 35º – Avaliação de impacto sobre a proteção de dados

Regulamento geral sobre a proteção de dados

Artigo 5º - Princípios relativos ao tratamento de dados pessoais

1. Os dados pessoais são:

(...)

c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»);

(...)

f) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas («integridade e confidencialidade»);

2. O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo («responsabilidade»).

Regulamento geral sobre a proteção de dados

Artigo 24º - Responsabilidade do responsável pelo tratamento

1. Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades.

Regulamento geral sobre a proteção de dados

Artigo 25º - Proteção de dados desde a conceção e por defeito

1. (...) o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados.
2. O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por definição, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por definição, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares.

Regulamento geral sobre a proteção de dados

Artigo 32º - Segurança do tratamento

1. (...) o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado:

- a) A pseudonimização e a cifragem dos dados pessoais;
- b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;
- c) A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico;
- d) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

Regulamento geral sobre a proteção de dados

Artigo 32º - Segurança do tratamento

2. Ao avaliar o nível de segurança adequado, devem ser tidos em conta, designadamente, os riscos apresentados pelo tratamento, em particular devido à destruição, perda e alteração acidentais ou ilícitas, e à divulgação ou ao acesso não autorizados, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.
4. O responsável pelo tratamento e o subcontratante tomam medidas para assegurar que qualquer pessoa singular que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratante, tenha acesso a dados pessoais, só procede ao seu tratamento mediante instruções do responsável pelo tratamento, exceto se tal lhe for exigido pelo direito da União ou de um Estado-Membro.

Regulamento geral sobre a proteção de dados

Artigo 33º – Notificação de uma violação de dados pessoais à autoridade de controlo

1. Em caso de violação de dados pessoais, o responsável pelo tratamento notifica desse facto a autoridade de controlo competente nos termos do artigo 55.º, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares. Se a notificação à autoridade de controlo não for transmitida no prazo de 72 horas, é acompanhada dos motivos do atraso.

Regime jurídico de segurança do ciberespaço

- NIS (Network Information Security)
- Segurança das Redes de Informação (Directiva SRI)
- Garantir um elevado nível comum de segurança das redes e da informação em toda a União (2016/1148)
- Transposto na Lei n.º 46/2018 de 13 de agosto
- Cibersegurança das redes e sistemas de operadores de:
 - Serviços essenciais
 - Água,
 - Banca
 - Energia
 - Infraestrutura digital
 - Mercado financeiro
 - Saúde
 - Transportes
 - Serviços digitais
 - Mercados online
 - Motores de pesquisa
 - Serviços de computação na nuvem

Regime jurídico de segurança do ciberespaço

- Equipas de resposta a incidentes de segurança informática a nível nacional (CSIRT)
 - Centro Nacional de Cibersegurança (autoridade nacional de cibersegurança)
- Grupos de coordenação internacional
 - Para coordenação estratégica e troca de informações
- Cada Estado-Membro define a estratégia de segurança em conjunto com os operadores através de medidas políticas e regulamentares
- Cada Estado-Membro designa as autoridades nacionais competentes, os pontos de contacto únicos e os CSIRT nacionais
 - CERT.pt
- Obriga à notificação de incidentes
- Aplicação de boas práticas

Resolução do Conselho de Ministros n.º 41/2018

- Define orientações técnicas para a Administração Pública em matéria de arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais
- Define requisitos técnicos divididos entre:
 - *Front-end*
 - Camada aplicacional
 - Camada de dados
- Boas práticas para desenvolvimento seguro
- Capacidade de autenticar e autorizar todos os utilizadores, dispositivos e sistemas
- Restrições de acesso à informação
- Sistemas de armazenamento redundantes, de alta disponibilidade, sem pontos de falha únicos
- Todas as redes e sistemas de informação devem ser capazes de classificar, priorizar, pesquisar, editar e apagar dados pessoais

ISO 27000

- Família de normas ligadas à segurança da informação
- Implementação de um Sistema de Gestão de Segurança de Informação (SGSI)
- ISO 27001 – Especifica o SGSI
- ISO 27002 – Catalogo de controlos geridos pelo SGSI
- Quadro normativo mais relevante
- Aproximação baseada no levantamento do risco e independente das tecnologias
- Define um planeamento baseado em seis pontos:
 - Definir uma política de segurança
 - Definir o âmbito do Sistema de Gestão da Segurança de Informação
 - Realizar um levantamento de riscos
 - Gerir os riscos identificados
 - Definir controlos a ser implementados
 - Definir a Declaração de Aplicabilidade

ISO 27000

Família

- ISO/IEC 27000, Information security management systems — Overview and vocabulary
- ISO/IEC 27001, Information security management systems — Requirements
- ISO/IEC 27002, Code of practice for information security controls
- ISO/IEC 27003, Information security management system implementation guidance
- ISO/IEC 27004, Information security management — Measurement
- ISO/IEC 27005, Information security risk management
- ISO/IEC 27006, Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27007, Guidelines for information security management systems auditing
- ISO/IEC TR 27008, Guidelines for auditors on information security controls
- ISO/IEC 27009, Sector-specific application of ISO/IEC 27001 — Requirements
- ISO/IEC 27010, Information security management for inter-sector and inter-organizational
- ISO/IEC 27011, Information security management guidelines for telecommunications organizations communications based on ISO/IEC 27002
- ISO/IEC 27013, Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- ISO/IEC TR 27015, Information security management guidelines for financial services

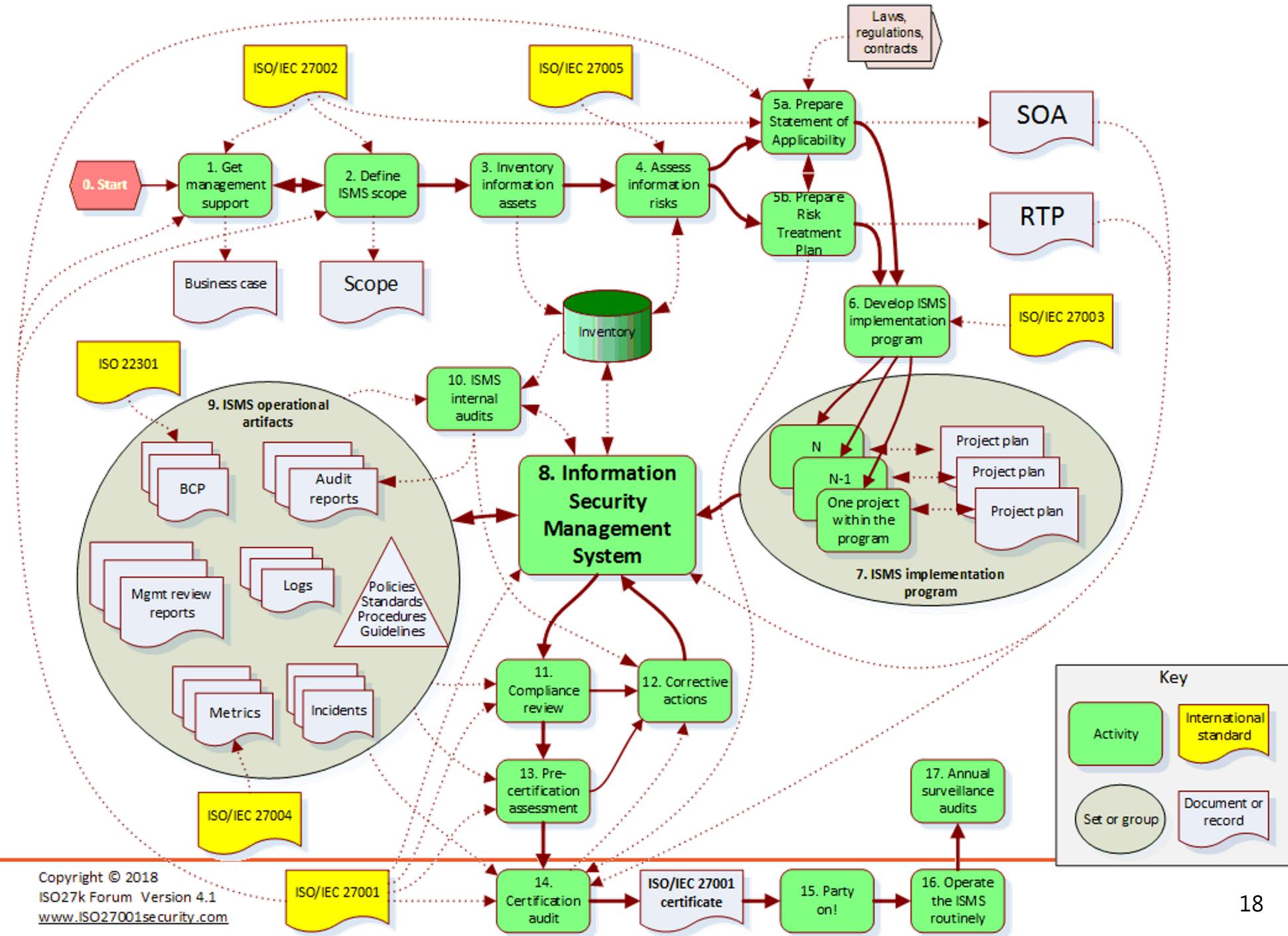
ISO 27000

Família

- ISO/IEC TR 27016, Information security management — Organizational economics
- ISO/IEC 27017, Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018, Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 27019, Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry
- ISO 27799, Health informatics — Information security management in health using ISO/IEC 27002
- ISO 27034, Information technology — Security techniques — Application security
- ISO 27035, Information technology — Security techniques — Information security incident management
- ISO 27039, Information technology — Security techniques — Selection, deployment and operations of intrusion detection systems (IDPS)
- ISO 27040, Information technology — Security techniques — Storage security
- ISO 27041, Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative methods
- ISO 27042, Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence
- ISO 27043, Information technology — Information technology — Security techniques — Incident investigation principles and processes
- ISO 27050, Information technology — Security techniques — Electronic discovery

ISO 27001 Roadmap

© ISO27k Forum



ISO 27000

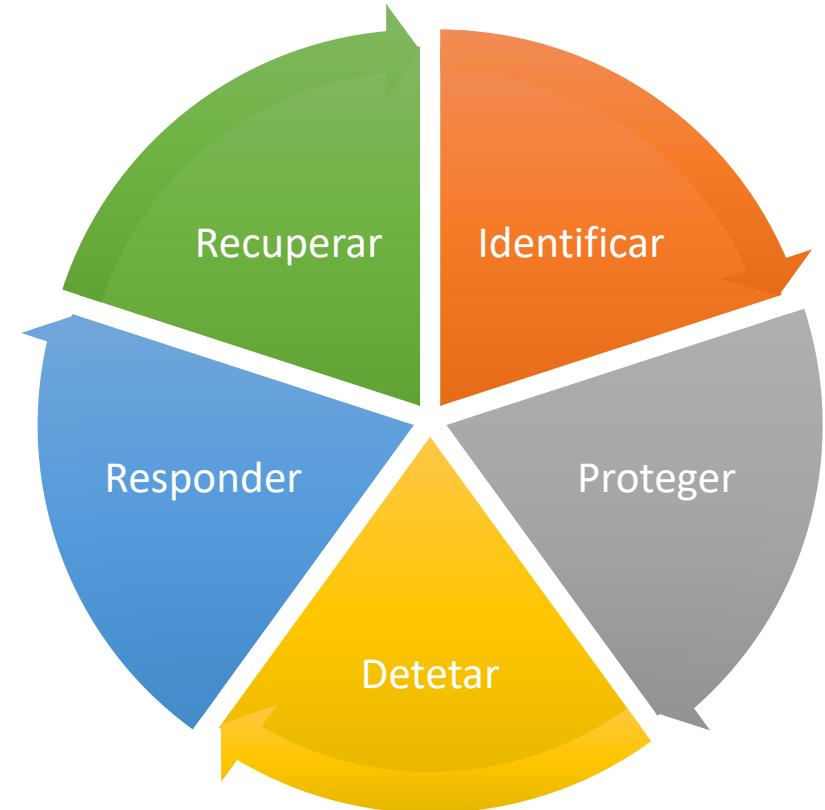
As boas notícias:

- O SGSI (ISMS) pode ser utilizado para atingir a manter a conformidade com o RGPD
- Existe mapeamento direto entre a maioria das cláusulas do RGPD para o ISO 27000
- ISO 27701 apresenta um conjunto de boas práticas de alinhamento com o RGPD e sua aplicação

NIST – National Institute of Standards and Technology

Cyber Security Framework

- Encorajado pelo NIST a ser aplicado em organizações privadas e infraestruturas críticas
 - Processo de 7 passos
 - Prioridades e âmbito
 - Orientação
 - Perfil atual
 - Levantamento de riscos
 - Perfil alvo
 - Determinar, analisar e priorizar lacunas
 - Implementar um plano de ação
- Não considera a certificação
- Os controlos usados podem vir de outro quadro normativo: ISO 27000 por exemplo



NIST – National Institute of Standards and Technology

Risk Management Framework (SP 800-37)

- Quadro normativo de gestão de risco
- Define a segurança de informação dos sistemas de informação desde a sua conceção
- Foca-se na definição de controlos de segurança e na sua implementação
- Processo para atingir a segurança dos sistemas de informação:
 - **Categorização** de segurança, baseada em análises de impacto
 - **Seleção** dos controlos de segurança
 - **Implementação** dos mecanismos de controlo
 - **Avaliação** dos controlos
 - **Autorização** do sistema de informação (para funcionamento)
 - **Monitorização** dos controlos de segurança

NIST – National Institute of Standards and Technology

Risk Management Framework (SP 800-53)

- SP 800-53 define os controlos de segurança a usar no RMF para satisfazer os requisitos de segurança
 - Catalogo de controlos publicados online no site do NIST
 - Aproximação de gestão de risco multicamada
 - Define uma base de referência em termos de controlos a ser usados
 - Mais burocrático que o CSF

Quadro Nacional de Referência para a Cibersegurança

- Referência para identificar normas, padrões e boas práticas
- Gestão do ciclo de vida da gestão da cibersegurança
 - Orientado à gestão do risco
- Processo contínuo de identificação, diagnóstico e resposta
- Clarifica melhor o papel do CISO, CSIRT e SOC
 - Baseado na Lei 46/2018 (RJSC, diretiva SRI)
- Enquadra outros quadros normativos no panorama nacional
- Aplica controlos muito próximos do NIST SP800-53 (RMF)



Manual de boas práticas sobre o RGPD do GNS

- Boas práticas ≠ quadro normativo
- 3 partes:
 - Deveres e responsabilidades das organizações
 - Resumo das diferentes estratégias, abordagens e procedimentos para a segurança dos dados, endereçando as tecnologias, processos e pessoas
 - Contributos para políticas e procedimentos
 - Definição de políticas e procedimentos endereçando os diferentes controlos tecnológicos
 - Subcontratação
 - Planos de emergência e continuidade de negócio
 - Segurança física
 - Medidas de defesa e segurança física
 - Áreas seguras

MITRE ATT&CK

Adversarial Tactics , Techniques, and Common Knowledge

- É uma base de dados catalogada de táticas e técnicas usadas por atacantes categorizada num modelo
- É baseada em observações realistas de comportamentos observados
- Focada nos atacantes e nos seus comportamentos, nas suas ferramentas e nas suas ações
- Atualizada trimestralmente a partir de observações da comunidade
- **Técnicas** são aquilo que se pretende detetar ou mitigar, ou emular em cenários de penetração
- Normalmente está disposta em matriz

MITRE ATT&CK

Utilização

- Alimentar sistemas de deteção de intrusões ou de análise de registos
- Avaliar os controlos de segurança existentes
- Avaliar novos controlos (se são capazes de mitigar riscos descritos no MITRE ATT&CK)
- Correlacionar novos ataques com informação já existente
- Exemplo:
 - https://resources.fox-it.com/rs/170-CAK-271/images/201912_Report_Operation_Wocao.pdf
 - <https://seguranca-informatica.pt/targeting-portugal-a-new-trojan-lampion-has-spread-using-template-emails-from-the-portuguese-government-finance-tax>