# ACADEMIA MILITAR

**Mestrado em Ciências Militares na Especialidade de Infantaria**

# Base de Dados Relacional de Controlos de Segurança da Informação

**Autor: Aspirante de Infantaria Tiago André Ferreira Gaspar.**

**Orientador: Tenente-Coronel de Infantaria José Carlos Lourenço Martins (Doutor).**

**Relatório Científico Final do Trabalho de Investigação Aplicada**

**Lisboa, junho de 2016**

# ACADEMIA MILITAR

**Mestrado em Ciências Militares na Especialidade de Infantaria**

# Base de Dados Relacional de Controlos de Segurança da Informação

**Autor: Aspirante de Infantaria Tiago André Ferreira Gaspar.**

**Orientador: Tenente-Coronel de Infantaria José Carlos Lourenço Martins (Doutor).**

**Relatório Científico Final do Trabalho de Investigação Aplicada**

**Lisboa, junho de 2016**

# EPÍGRAFE

*"Private information is practically the source of every large modern fortune."*

Fonte: Oscar Wilde (1854–1900)

# DEDICATÓRIA

À minha família e meus amigos que sempre me

apoiaram em todo o meu percurso.

Muito obrigado a todos.

# AGRADECIMENTOS

Não poderia deixar de demonstrar a minha mais sincera gratidão a todos aqueles que de forma direta ou indireta contribuíram e colaboraram para a realização deste trabalho de investigação.

Desta forma quero expressar palavras de apreço e agradecimento:

Ao Tenente Coronel Lourenço Martins pela sua disponibilidade para orientar o meu trabalho, pelo tempo despendido e por esclarecer todas as dúvidas que surgiram durante a realização do trabalho.

Ao Tenente Coronel Silva, pela sua disponibilidade sempre que necessitei na construção da base de dados.

Ao Tenente Coronel Pinto da Silva, pela sua recetividade sempre que foi necessário no que concerne à metodologia.

Ao Tenente Coronel Oliveira, Diretor de Curso de Infantaria, pela sua constante preocupação ao longo da elaboração deste trabalho.

A todos os Oficiais que me possibilitaram a realização de entrevistas, nomeadamente Major Pessoa Dinis, Major Nuno Gois e Major Salvador, contribuindo com conhecimentos factuais e credíveis para o trabalho de investigação.

Ao Aspirante de Infantaria Rui Torres, Aspirante de Infantaria Fábio Teles, Aspirante de Infantaria Cyril Lagoa, Aspirante de Infantaria José Santos e Aspirante de Infantaria Rafael Amador, pelos testes desenvolvidos na Base de Dados.

À Academia Militar e a todos os que nela servem, pela sua formação e por me terem feito crescer.

Aos meus camaradas de Curso Geral e em especial aos de Infantaria, por tudo aquilo que vivemos e passámos ao longo desta jornada.

À minha família e amigos por estarem sempre presentes no meu percurso, terem feito tudo para que nada me faltasse e por me terem feito crescer como pessoa.

Por último, a minha mais sincera gratidão à minha mãe por me corrigir o trabalho vezes sem conta.

# RESUMO

No desenvolvimento deste Trabalho de Investigação Aplicada, pretende-se responder à questão: Quais os requisitos necessários a implementar numa base de dados relacional de controlos de segurança da informação para Unidades, Estabelecimentos ou Órgãos militares do Exército Português? Deste modo, para se responder a esta questão central, houve necessidade de subdividir esta em quatro questões derivadas, sendo elas:

1. Quais as principais dimensões de segurança da informação ao nível organizacional?
2. Quais as principais categorias de segurança da informação ao nível organizacional?
3. Quais os principais controlos de segurança da informação a implementar numa organização militar?
4. Quais os requisitos funcionais necessários a implementar numa base de dados de controlos de segurança da informação a implementar numa organização militar?

Para responder a estas questões de investigação, este trabalho assenta numa investigação aplicada, com o objetivo de desenvolver uma aplicação prática para os conhecimentos adquiridos, materializando-se assim numa base de dados. Ainda, quanto ao objetivo da investigação, este é descritivo, explicativo e exploratório, uma vez que, tem o objetivo de descrever as principais dimensões, categorias e controlos da segurança da informação, assim como o objetivo de explicar quais são os requisitos funcionais necessários a implementar numa base de dados de controlos de segurança da informação. Por último, tem ainda o objetivo de efetuar um estudo exploratório, comprovando a eficácia da base de dados. Esta investigação assenta no método indutivo, partindo de premissas particulares para chegar a conclusões gerais, isto é, a partir de análise de documentos e de inquéritos por entrevista, identificar-se-ão quais são os requisitos funcionais necessários a implementar, generalizando para todas as Unidades, Estabelecimentos ou Órgãos militares do Exército Português. No que corresponde ao método de procedimentos, usar-se-á o método comparativo, com vista a identificar qual é a norma internacional de gestão de segurança de informação mais indicada a registar na base de dados. Por último, como referido anteriormente, no que concerne às técnicas de investigação, será usado o inquérito por entrevista, identificando os requisitos necessários a implementar, e a análise de documentos, identificando as principais dimensões, categorias

ou controlos necessários a implementar numa base de dados de controlos de segurança da informação.

Posto isto, numa primeira fase da investigação, através da análise de documentos, percecionam-se as principais dimensões, categorias e controlos de segurança da informação necessários a aplicar nas Unidades, Estabelecimentos ou Órgãos militares do Exército Português, por forma a contribuir para o sucesso na gestão da segurança da informação militar. Ainda, através de entrevistas a especialistas da área de segurança da informação e dos Sistemas de Informação nas unidades militares, identificar-se-ão quais os requisitos funcionais necessários a implementar numa base de dados de controlos de segurança da informação a implementar numa organização militar.

Por último, numa segunda fase, através do modelo de desenvolvimento de *software* em cascata revisto, pretende-se desenvolver uma base de dados relacional, em Microsoft Access, de controlos de segurança da Informação a fim de implementar em Unidades, Estabelecimentos ou Órgãos militares do Exército Português. Posteriormente, após o desenvolvimento da base de dados, pretende-se efetuar um estudo exploratório com vista a validar a mesma, de modo a comprovar se esta responde às necessidades[1] para a qual foi desenvolvida.

**Palavras chave:** Requisitos Funcionais, Segurança da Informação, Controlos de Segurança da Informação, Gestão da Segurança da Informação Militar, Base de Dados Relacional.

[1] Requisitos identificados, com base em entrevistas conduzidas a especialistas da área da segurança da informação.

# ABSTRACT

In the development of this Applied Research Work, it is intended to answer the question: What are the requirements necessary to implement in a relational database of information security controls for military units of the Portuguese army? Thus, to answer this central question, it was necessary to subdivide this into four derivative issues, which are:

1. What are the main dimensions of information security at the organizational level?
2. What are the main categories of information security at the organizational level?
3. What are the main controls of information security to implement in a military organization?
4. What are the functional requirements needed to implement in a database of information security controls to implement in a military organization?

To answer these investigations issues, this work is based on an applied research with the aim of finding a practical application for their knowledge, thus developing a database. Still, as the purpose of the investigation, this is descriptive, explanatory and exploratory, since, aims to describe the main dimensions, categories and information security controls, as well the aim of explain what are the functional requirements needed to implement a database of information security controls. Finally, it also has the purpose of conducting an exploratory study, demonstrating the effectiveness of the database. This research is based on the inductive method, from private premises to reach general conclusions, that is, from analysis of documents and interview surveys, will identify which are which are the functional requirements to implement, generalizing to all military units of the Portuguese army. As corresponds to the procedures method, we shall be use the comparative method, to identify what is the most appropriate international Norm for information security management to implement the database. Finally, as mentioned above, in regard to research techniques, will be the interview survey, identifying the requirements to implement, and document analysis, identifying the main dimensions, categories or controls necessary to implement a database security controls information.

In a first phase of research through the analysis of documents, the main dimensions, categories and controls of information security required to be applied in military units of

the Portuguese Army was understood order to contribute to the success in the safe management of military information. Still, through interviews with experts from the information security and information system area in military units, will identify what functional requirements necessary to implement a database of information security controls to implement a military organization.

Finally, in a second stage, through the software development model "revised cascade", it is intended to develop a relational database in Microsoft Access, of information security controls to implement in military units of the Portuguese Army. Subsequently, after the development of the database, it is intended to make an exploratory study to validate it, in order to ascertain that it meets the needs[2] for which it was developed.

**Key words:** Functional Requirements, Information Security, Information Security Controls, Safety Management of Military Information, Relational Database.

[2] Identified requirements, based on interviews conducted with experts in information security area.

# ÍNDICE GERAL

# ÍNDICE DE FIGURAS

# ÍNDICE DE TABELAS

# LISTA DE ANEXOS E APÊNDICES

# LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

| | |
|---|---|
| **1FN** | **P**rimeira **F**orma **N**ormal. |
| **2FN** | **S**egunda **F**orma **N**ormal. |
| **3FN** | **T**erceira **F**orma **N**ormal. |
| **4FN** | **Q**uarta **F**orma **N**ormal. |
| **5FN** | **Q**uinta **F**orma **N**ormal. |
| **AM** | **A**cademia **M**ilitar. |
| **BD** | **B**ase de **D**ados. |
| **CE** | **C**have **E**strangeira. |
| **CP** | **C**have **P**rimária. |
| **DEA** | **D**iagrama **E**ntidade-**A**ssociação. |
| **DF** | **D**ependência **F**uncional. |
| **E-R** | **E**ntidade-**R**elação. |
| **ENISA** | *European Union Agency for Network and Information Security*. |
| **EUA** | **E**stados **U**nidos da **A**mérica. |
| **FM** | ***F**ield **M**anual.* |
| **FNBC** | **F**orma **N**ormal de ***B**oyce/**C**odd*. |
| **GDH** | **G**rupo **D**ata **H**ora. |
| **HUMINT** | ***Hum**an **Int**elligence.* |
| **IMINT** | ***Im**agery **Int**elligence.* |
| **INFOSEC** | ***Info**rmation **Sec**urity*. |
| **MASINT** | ***M**easurement **a**nd **S**ignatures **Int**elligence.* |
| **N/D** | **N**ão **D**efinido. |

| | |
|---|---|
| **NATO** | *North Atlantic Treaty Organization.* |
| **NIF** | **N**úmero de **I**dentificação **F**iscal. |
| **NIST** | *National Institute of Standards and Technology*. |
| **OPSEC** | ***Sec**urity **Op**erations.* |
| **OSINT** | ***O**pen **S**ource **Int**elligence.* |
| **OTAN** | **O**rganização do **T**ratado do **A**tlântico **N**orte. |
| **SANS** | **S**ystem **A**dministration, **N**etworking and **S**ecurity. |
| **SBD** | **S**istema de **B**ase de **D**ados. |
| **SF** | **S**istemas de **F**icheiros. |
| **SGBD** | **S**istema de **G**estão de **B**ase de **D**ados. |
| **SGSI** | **S**istema de **G**estão de **S**egurança da **I**nformação. |
| **SI** | **S**istemas de **I**nformação. |
| **SIGINT** | ***Sig**nals **Int**elligence.* |
| **TECHINT** | ***Tech**nical **Int**elligence.* |
| **TIA** | **T**rabalho de **I**nvestigação **A**plicada. |
| **U/E/O** | **U**nidades, **E**stabelecimentos ou **Ó**rgãos. |
| **UML** | ***U**nified **M**odelling **L**anguage.* |

# INTRODUÇÃO

A Organização do Tratado do Atlântico Norte (OTAN) define segurança da informação como "objetivo de proteger a informação armazenada, processada ou transmitida, bem como os sistemas que a suportam, contra a perda de confidencialidade, integridade e disponibilidade, por meios de uma variedade de controlos processuais, técnicos e administrativos" (AAP-6, 2008, pp. 2-I-1).

Atualmente, segundo os novos paradigmas, o que se pretende garantir é a *Information Assurance*, que é definida pelos processos desenvolvidos para obter superioridade de informação em relação ao adversário (FM3-13, 2003).

*Information Assurance* é um conceito multifacetado que pretende constantemente manter os Sistemas de Informação (SI) contra a perda de Disponibilidade, Confidencialidade, Integridade, Autenticação e o Não-Repúdio (Howard, 2013).

Presentemente, um grande desafio que é necessário vencer é o crescente nível de competição pela obtenção de informação entre as várias instituições (Martins, Santos, Nunes, & Silva, 2012a). Este paradigma remete para a elevada necessidade de gerir os sistemas de gestão de segurança da informação.

Em suma, a garantia da segurança da informação é realizada através da implementação de um conjunto de controlos de segurança físicos, técnicos, humanos e administrativos que visam garantir a confidencialidade, a disponibilidade e a integridade da informação (Martins, Santos, Rosinha & Valente, 2013).

Segundo uma revisão de literatura e um *focus group*, não se identificou a existência ou a aplicação de um modelo ou método de segurança, que apresente uma visão integrada de gestão de segurança da informação e dos SI, para as unidades militares de acordo com o desafio anteriormente descrito (Martins, Santos, Nunes, & Silva, 2012b).

Devido a não se identificar a existência de um modelo, ou método de segurança da informação para as unidades militares, torna-se necessário planear e implementar uma *baseline* de controlos de segurança, os quais devem ser monitorizados e auditados após a sua implementação, de modo a simultaneamente garantir a obtenção e a partilha de lições aprendidas.

Esta *baseline* de controlos de segurança da informação pretende materializar-se numa base de dados (BD) relacional de controlos de segurança da informação. Consequentemente, esta BD visa gerir toda a informação relacionada com os controlos de segurança da informação implementados nas Unidades, Estabelecimentos ou Órgãos (U/E/O) militares do Exército Português.

A elaboração deste Trabalho de Investigação Aplicada (TIA) reconhece a fase de Análise, de Desenho, de Implementação dos requisitos funcionais, e, por último a fase da Testagem do Projeto.

Como objetivo geral de estudo, pretende-se identificar os requisitos necessários a implementar numa BD relacional de controlos de segurança da informação para U/E/O militares do Exército Português. No que concerne aos objetivos específicos de investigação, pretende-se identificar as principais dimensões, categorias e controlos de segurança da informação, assim como identificar os requisitos funcionais necessários a implementar numa BD de controlos de segurança da informação a implementar numa organização militar.

Esta investigação tem como finalidade criar uma base de dados relacional, em *Microsoft Access*, de controlos de segurança da Informação a fim de implementar em U/E/O militares do Exército Português.

A problemática de investigação tem por base a resposta à seguinte questão central: Quais os requisitos necessários a implementar numa base de dados relacional de controlos de segurança da informação para U/E/O militares do Exército Português?.

Derivadas da questão central, surgem outras questões cujas respostas são indispensáveis para solucionar a problemática levantada, nomeadamente:

1. Quais as principais dimensões de segurança da informação ao nível organizacional?
2. Quais as principais categorias de segurança da informação ao nível organizacional?
3. Quais os principais controlos de segurança da informação a implementar numa organização militar?
4. Quais os requisitos funcionais necessários a implementar numa base de dados de controlos de segurança da informação a implementar numa organização militar?

Em suma, para responder à questão central de investigação, o TIA está dividido em cinco capítulos. No primeiro capítulo faz-se uma primeira abordagem ao tema, apresentando-se uma revisão de literatura onde se expõe as principais definições, conceitos

e normas. No segundo capítulo, faz-se referência à metodologia da Investigação utilizada no estudo, nomeadamente no que diz respeito à natureza da investigação, ao objetivo da investigação, ao método de abordagem, ao método de procedimentos e por último às técnicas de investigação (recolha de dados). Relativamente ao terceiro capítulo, expõe-se o método, isto é, o processo de desenvolvimento de *software* utilizado. No quarto capítulo identificam-se as dimensões, categorias e controlos de segurança da informação, assim como os requisitos funcionais necessários a implementar na BD a desenvolver. No que respeita ao quinto e último capítulo, faz-se a modelação, análise e desenvolvimento da estrutura da BD, com vista a responder aos requisitos identificados anteriormente, assim como a descrição do desenvolvimento da mesma.

No final deste Relatório Científico Final do Trabalho de Investigação Aplicada, apresentam-se as conclusões, as limitações e possíveis trabalhos futuros no âmbito desta temática.

# CAPÍTULO 1. REVISÃO DE LITERATURA

## 1.1. Segurança da Informação e dos Sistemas de Informação

Segundo o *Field Manual* FM3-13 (2003), a Informação classifica-se como, todos os dados existentes, em qualquer meio e forma, aos quais é atribuído um significado numa forma útil de modo a transmitir uma mensagem com significado para os destinatários.

Contudo, com vista a garantir a segurança da informação anteriormente descrita, o FM3-13 (2003) define segurança da informação como:

> "a proteção e a defesa da informação e dos Sistemas de Informação contra o acesso ou a modificação não autorizada da informação quer seja no processamento, armazenamento ou na transmissão e o evitar a negação de serviços a utilizadores autorizados. A segurança da informação inclui as medidas necessárias para detetar, documentar e contrariar tais ameaças. A segurança da informação é composta pela segurança dos computadores e das comunicações" (tradução pelo próprio de (FM3-13, 2003, pp. 1-2)).

Em comparação, a OTAN define segurança da informação como "objetivo de proteger a informação armazenada, processada ou transmitida, bem como os sistemas que a suportam, contra a perda de confidencialidade, integridade e disponibilidade, por meios de uma variedade de controlos processuais, técnicos e administrativos" (AAP-6, 2008, pp. 2-I-1).

Contudo, com a evolução dos SI, atualmente o que se pretende garantir é a *Information Assurance*, definida como:

> "as ações desenvolvidas para obter superioridade de informação afetando a informação do adversário, os processos baseados em informação, os Sistemas de Informação e as redes baseadas em computadores de um adversário enquanto se defende a nossa própria informação, os processos baseados em informação, os Sistemas de Informação e as redes baseadas em computadores" (traduzido pelo próprio de (FM3-13, 2003, p.1-12)).

A *Information Assurance* é um conceito multifacetado que pretende constantemente manter os SI contra a perda de Disponibilidade, Confidencialidade, Integridade, Autenticação e o Não-Repúdio (Howard, 2013).

Estes conceitos podem-se definir segundo FM3-13 (2003) como:

1. Disponibilidade, isto é, oportuna, acesso seguro a dados e serviços por usuários autorizados. Os SI deverão estar disponíveis quando necessário;
2. Confidencialidade significa proteção contra divulgação não autorizada;
3. Integridade significa proteção contra alteração não autorizada, incluindo a destruição. Os SI com integridade devem funcionar corretamente, da melhor forma, e com precisão;
4. Autenticação significa a validação/identificação do usuário, garantindo apenas a informação a que tem autorização de aceder;
5. Não-Repúdio significa a identificação do remetente.

Segundo uma revisão de literatura e um *focus group*, não se identificou a existência ou a aplicação de um modelo ou método de segurança, que apresente uma visão integrada de gestão de segurança da informação e dos SI para as unidades militares (Martins et al. 2012b).

A adoção de um sistema de gestão de segurança da informação deve ser uma decisão estratégica da própria organização. Essa decisão estratégica deve ser influenciada pelas necessidades, objetivos, requisitos de segurança e por último pela dimensão e estrutura da organização. A decisão estratégica da organização deve ser constantemente avaliada, adaptando-a a cada momento. É compreensível que estes fatores mudem ao longo do tempo (ISO/IEC 27001, 2013).

Segundo o artigo "Modelo de Segurança da Informação para Organizações Militares em Ambiente de Guerra da Informação" de Martins et al. (2012a), para a adoção de um sistema de gestão de segurança da informação existem inúmeras normas orientadoras. De acordo com o artigo em causa, a norma internacional de gestão de segurança de informação ISO/IEC 27001 (2013) e a publicação de gestão de segurança de sistemas de informação NIST 800-53 r4 (2013) descrevem um conjunto de boas práticas de segurança da informação, assim como, sugerem um conjunto de controlos de segurança da informação.

A ISO/IEC 27001 (2013), foi estabelecida para sugerir os requisitos a estabelecer, a implementar, a manter e a melhorar de forma contínua num sistema de gestão de segurança da informação dentro do contexto da organização (ISO/IEC 27001, 2013).

Como referido anteriormente, a adoção de um sistema de gestão de segurança da informação (SGSI) é uma decisão estratégica da organização, sendo este influenciado pelos objetivos, pelos requisitos de segurança e pelos processos organizacionais. Posto isto, é importante que esse SGSI faça parte da organização e esteja integrado com os processos da mesma (ISO/IEC 27001, 2013).

Esta norma, a ISO/IEC 27001 (2013), foi criada com o intuito de "(…) ser utilizada pelas partes internas e externas para avaliar a capacidade da organização para cumprir os seus próprios requisitos de segurança da informação" (ISO/IEC 27001, 2013, p. 5).

A norma ISO/IEC 27001 (2013) é complementada com outras normas, nomeadamente a ISO/IEC 27000[3], ISO/IEC 27003[4], ISO/IEC 27004[5] e ISO/IEC 27005[6]. Os vários requisitos que a norma ISO/IEC 27001 (2013) abrange são genéricos e pretende-se que sejam aplicáveis a todas as organizações, independentemente do seu tipo, dimensão ou natureza (ISO/IEC 27001, 2013).

Também, a publicação SANS (2013) é um documento elaborado pela SANS[7], que recomenda um conjunto de controlos focados na cibersegurança. Estes controlos cuja implementação é sugerida tendo por base os ataques mais comuns focados nos relatórios elaborados por algumas agências governamentais[8]. Os mesmos são constantemente atualizados com base em novos ataques que são identificados e analisados por grupos especialistas (SANS I. , 2016).

Os controlos fornecidos pela Publicação SANS, têm como objetivos: "fortalecer a postura defensiva da segurança da informação das organizações, reduzir os esforços de recuperação e custos associados, proteger ativos críticos e infraestruturas (…)" (SANS, 2013, p. 3).

[3] *Information technology – Security techniques – Information security management systems – Overview and vocabulary*. Esta norma compreende as informações básicas sobre as restantes normas da série 27000.
[4] *Information technology – Security techniques – Information security management system implementation guidance*. Esta norma abarca as instruções específicas para implementação de um SGSI.
[5] *Information technology – Security techniques – Information security management – Measurement*. Esta norma contém as diretrizes sobre as métricas e relatórios do SGSI.
[6] *Information technology – Security techniques – Information security risk management*. Esta norma abrange as diretivas para o processo de gestão de risco de segurança da informação.
[7] Centro de segurança norte-americano, estabelecida em 1989.
[8] Como a *National Security Agency Red*, departamento de laboratórios de energia nuclear dos EUA e organizações policiais.

Por outro lado, a publicação NIST 800-53 r4 (2013), divulgada em abril de 2013, pela agência governamental NIST[9], tem o propósito de fornecer um conjunto de controlos de segurança dos SI a implementar nas organizações a fim de proteger as suas operações, os seus ativos[10] e os seus colaboradores. Os controlos referidos abordam um conjunto diversificado de requisitos com vista a adaptar-se ao tipo específico de negócio, tecnologia ou ambiente de operação (NIST 800-53 r4, 2013).

Para além destes controlos descritos, o NIST 800-53 r4 (2013) fornece um conjunto de controlos a implementar num SGSI (ao nível organizacional e não ao nível individual), assim como um conjunto de boas práticas que auxiliam as organizações a cumprir os requisitos de segurança da informação (NIST 800-53 r4, 2013).

Visto isto, é sugerido no Apêndice A deste TIA um conjunto de boas práticas, que as organizações devem ter em consideração para além de implementar controlos de segurança da informação.

A lista de controlos fornecidos pela publicação NIST 800-53 r4 (2013), abordam uma perspetiva funcional[11] e de garantia[12]. Assim sendo, agrupando estas duas perspetivas, os controlos de segurança de informação implementados num SGSI, garantem uma segurança com um nível elevado de confiança (NIST 800-53 r4, 2013).

Segundo o NIST 800-53 r4 (2013) a seleção e implementação de controlos de segurança, para os SI e as organizações, representam uma tarefa importante, uma vez que, mal implementados podem levar a quebras de segurança em operações ou ativos da organização, assim como à falha de bem-estar de indivíduos ou de uma nação. De acordo com a publicação em questão, os controlos de segurança da informação podem ser definidos como contramedidas estabelecidas, para os SI ou organizações, com vista a proteger a confidencialidade, integridade e disponibilidade da informação que é processada, guardada ou transmitida pelos SI, assim como satisfazer um conjunto de requisitos de segurança definidos previamente.

Para integrar o processo de gestão de risco em toda a organização e tratar de forma eficaz as preocupações da segurança da informação, o NIST 800-53 r4 (2013) sugere uma

[9] Agência governamental não regulatória da tecnologia do Departamento de Comércio dos Estados Unidos, fundada em 1901.
[10] Os ativos da organização podem-se caraterizar como todos os sistemas da organização onde as informações são criadas, processadas, armazenadas ou transmitidas.
[11] Perspetiva funcional carateriza-se pela robustez dos mecanismos de segurança apresentados.
[12] Perspetiva de garantia carateriza-se pela confiança nas medidas de segurança implementadas.

visão a três níveis distintos, o nível da organização, o nível do processo das missões/negócios e o nível do sistema de informação (NIST 800-53 r4, 2013).

Este processo de gestão de risco deve ser realizado através dos três níveis anteriormente descritos. Este propósito tem o intuito de criar uma preocupação de tratamento do risco ao nível completo da organização, e de garantir uma comunicação eficaz intra-níveis e inter-níveis, criando-se assim um ciclo de reações/respostas para uma melhoria contínua (NIST 800-53 r4, 2013). Este conceito é descrito de acordo com a Figura 1.

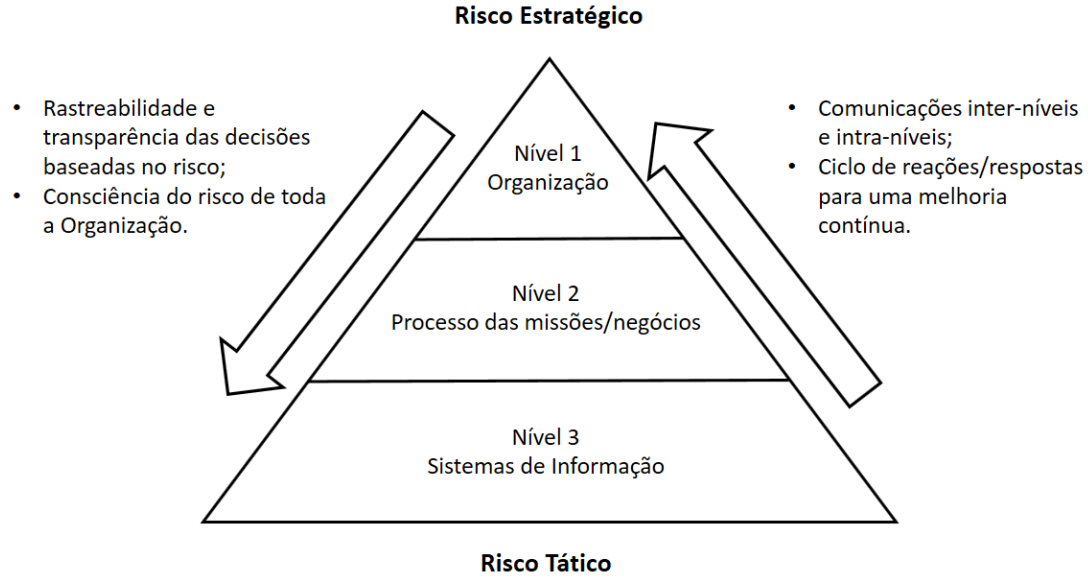


**Figura 1 - Abordagem de Gestão de Risco por Três Níveis.**

**Fonte: Adaptado de NIST 800-53 r4 (2013, p.30).**

De acordo com o NIST 800-53 r4 (2013), o nível 1 (nível da organização), prioriza as funções das missões/negócios da organização que por sua vez impulsiona estratégias de investimento e de financiamento rentáveis, indo de encontro às metas estabelecidas com os objetivos estratégicos[13] da organização.

No que concerne ao nível 2 (nível do processo das missões/negócios) este remete para definir quais os processos de missões/negócios necessários para apoiar as funções das missões/negócios organizacionais, quais as categorias de segurança de SI necessárias para

[13] Estes objetivos remetem ao risco estratégico que é abordado na figura 1.

executar esses processos, assim como quais os respetivos requisitos de segurança de informação. Este nível remete ainda para criar uma arquitetura de segurança da informação a fim de facilitar a partilha dos controlos de segurança da informação para os SI organizacionais (NIST 800-53 r4, 2013).

Por último, o terceiro nível da abordagem de gestão de risco sugerida pela publicação NIST 800-53 r4 (2013), remete para uma *Framework* de análise do risco proposta pela publicação em questão. Esta *Framework* de tratamento de risco é constituída por seis passos, sendo eles: Classificar os Sistemas de Informação; Selecionar os Controlos de Segurança; Implementar os Controlos de Segurança; Avaliar os Controlos de Segurança; Autorizar os Sistemas de Informação; e Monitorizar os Controlos de Segurança (NIST 800-53 r4, 2013).

Esta *Framework*, de tratamento de risco, é sugerida na Figura 2.

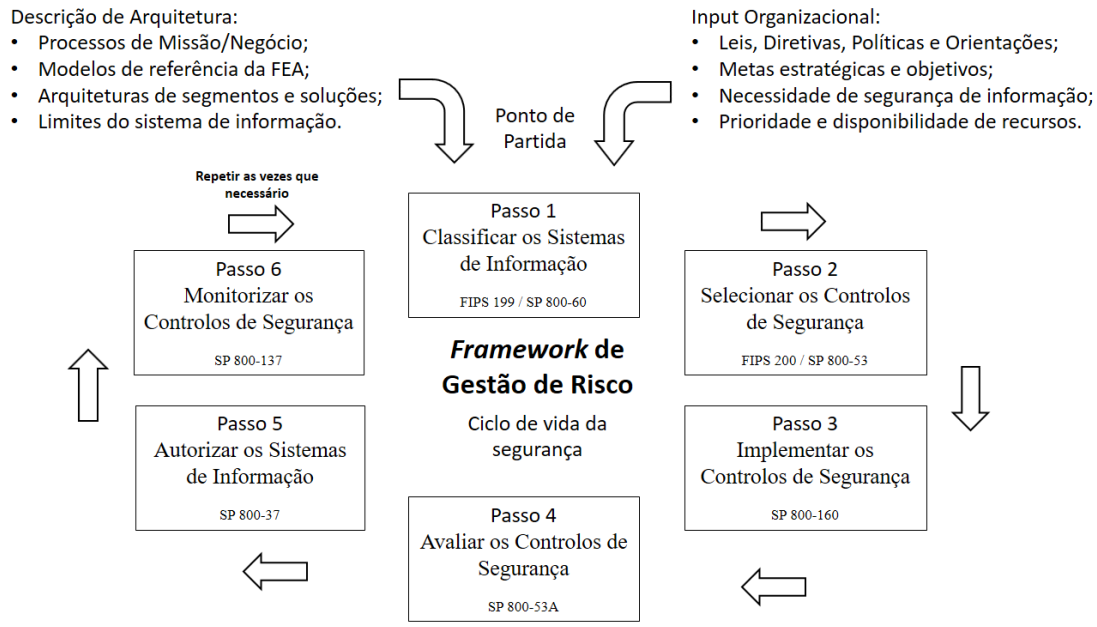


**Figura 2 - *Framework* de tratamento de risco.**

**Fonte: Adaptado de NIST 800-53 r4 (2013, p.30).**

Em suma, o NIST 800-53 r4 (2013) foca-se no segundo passo da *Framework* de tratamento de risco, isto é, no "Selecionar os Controlos de Segurança".

Contudo, para selecionar os controlos de segurança de informação a implementar numa organização é necessário numa primeira fase, de acordo com este estudo em

concreto, identificar quais são as dimensões (no caso NIST 800-53 r4 (2013) as famílias), categorias e só depois os controlos de segurança da informação imprescindíveis a implementar.

## 1.2. Dimensões, Categorias e Controlos de Segurança da Informação

As dimensões de segurança de informação, possibilitam identificar as funções críticas e vitais para a organização na perspetiva da Segurança da Informação tendo como aspeto principal garantir a continuidade do negócio (NIST 800-53 r4, 2013).

De acordo com o Estudo de Caso *Information Security - Military Standards versus ISO 27001* realizado por Martins et al. (2013), as principais dimensões de segurança da informação são:

1. Física: garantir a proteção física das instalações, das infraestruturas de apoio aos SI e de todos os equipamentos;
2. Humana: reduzir os riscos de erros humanos intencionais ou por negligência, evitando principalmente os ataques de Engenharia Social;
3. Organizacional: consiste fundamentalmente na dimensão de planeamento e de comando e controlo da segurança da informação (i.e., a direção, a coordenação, a revisão e a monitorização);
4. Tecnológica: garantir o correto processamento, transmissão e armazenamento dos dados e da informação. Deve ter em consideração os novos projetos de SI desde a análise até à sua implementação e posterior manutenção.

Cada dimensão ao nível da segurança de informação, apresenta um conjunto de categorias. Estas categorias podem ser definidas como "possibilidades lógicas nas quais se pode situar um objeto em relação a uma dada característica" (Freixo, 2010, p.271).

Por outro lado, cada categoria de segurança de informação é constituída por um conjunto de controlos. Os controlos podem ser definidos como uma ação, procedimento ou técnica que remove ou reduz vulnerabilidades (Pfleeger & Pfleeger, 2006).

Em suma, ao nível da segurança da informação, esta apresenta várias dimensões. Cada dimensão é constituída por um conjunto de categorias, e por sua vez, cada categoria é constituída por um conjunto de controlos. Estes conceitos estão explícitos de acordo com a Figura 3.

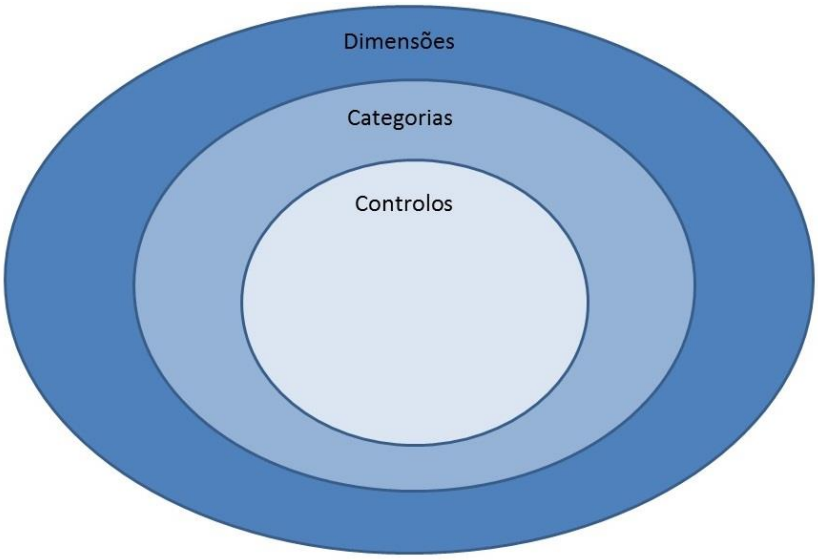


**Figura 3 - Organização das Dimensões, Categorias e Controlos.**

**Fonte: Elaboração Própria.**

A Figura 4 demonstra um exemplo de uma dimensão de segurança, a Tecnológica, constituída por três categorias, uma das quais a "Segurança lógica", que por sua vez é constituída por cinco controlos, como por exemplo "Controlo de Acessos".

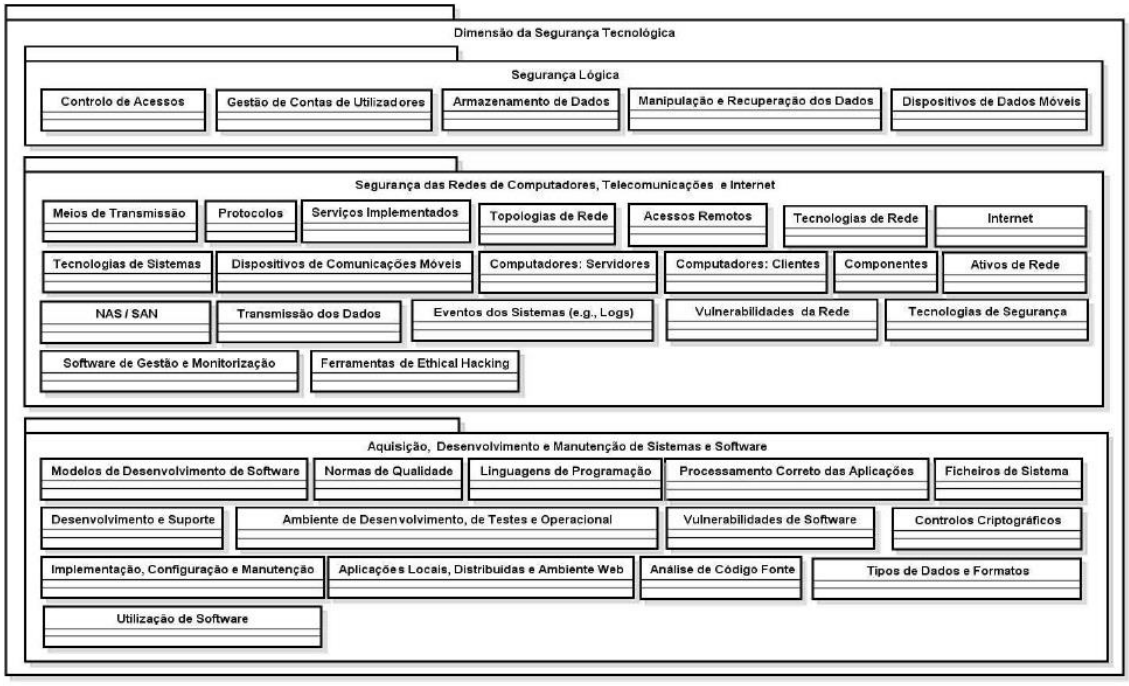


**Figura 4 - Categorias e controlos da dimensão Tecnológica.**

**Fonte: Martins et al. 2012b, p.8.**

## 1.3. Adoção de um Sistema de Segurança da Informação em Organizações Militares

De acordo com o conceito *Information Assurance* explicado anteriormente, para se fazer face a este é necessário criar um modelo de segurança da informação. Para isso, o modelo deverá responder a três questões fundamentais: "O que fazer", "Porquê fazer" e "Como fazer" (Martins et al. 2012a).

Segundo os autores Martins et al. (2012a), a segurança da informação pode ser orientada através de métodos e normas baseadas na gestão do risco da segurança da informação (e.g. ISO/IEC 27005, OCTAVE); identificam também normas de certificação e boas práticas de segurança da informação (e.g. ISO/IEC 27001, ISO/IEC 27002); normas e orientações de segurança da informação do foco mais tecnológico (e.g. NIST 800-53, ISO/IEC 13335-4); e normas orientadas à certificação do produto ou do sistema (e.g. ISO/IEC 15408).

Atualmente já existem vários estudos com propostas de *Frameworks* que sugerem a integração de diferentes aproximações com base em normas focadas em tecnologias, tendo em conta o ambiente organizacional e humano das organizações. Também existem orientações para garantir a segurança da informação nas organizações. Existem ainda recomendações de organizações independentes (e.g. Centro de Estudos para Respostas e Tratamento de Incidentes em Computadores, ENISA, *Information Security Forum*) que podem ser consideradas para apoiar o planeamento das medidas de segurança a implementar nas organizações militares. Neste âmbito, a nível militar, existe o modelo de segurança da OTAN, podendo ser levada em consideração na construção do sistema de segurança da informação. Contudo, nas Forças Armadas Portuguesas, principalmente no Exército, a principal doutrina de segurança adotada é a doutrina produzida na OTAN. No entanto existe alguma doutrina desenvolvida pelo Exército Português, apesar de esta ser semelhante à doutrina produzida pela OTAN (Martins et al. 2012a).

Segundo Martins et al. (2012b) atestam no seu artigo que "os resultados obtidos justificam a relevância deste assunto no âmbito da organização militar Exército e a sua preocupação permanente com esta temática" (Martins et al. 2012b, p.2).

Visto isto, pode-se afirmar que a garantia da segurança da informação é realizada através da implementação de um conjunto de controlos de segurança físicos, técnicos,

humanos e administrativos que visam garantir a confidencialidade, a disponibilidade e a integridade da informação. Nas U/E/O militares do Exército Português é necessário planear e implementar uma *baseline*[14] de controlos de segurança, os quais devem ser monitorizados e auditados após a sua implementação de modo a simultaneamente garantir a obtenção e a partilha de lições aprendidas, o que se propõe através da BD desenvolvida.

Consequentemente, esta *baseline* de controlos de segurança materializa-se numa BD que visa gerir toda a informação relacionada com os controlos de segurança da informação implementados nas U/E/O militares do Exército Português.

## 1.4. Fundamentos de um Sistema de Gestão de Base de Dados

### 1.4.1. Ficheiro

Para se compreender o funcionamento de um Sistema de Gestão de Base de Dados (SGBD), é necessário inicialmente compreender alguns conceitos, nomeadamente a definição de ficheiro.

Visto isto, um ficheiro pode ser definido como um bloco básico de informação que o sistema operativo pode identificar, atribuindo-lhe um nome. Os ficheiros podem dividir-se em dois tipos, os ficheiros de códigos[15] e os ficheiros de dados[16]. Contudo, independentemente de qual for o tipo de ficheiro, para o sistema operativo, no que concerne ao armazenamento, esse mesmo ficheiro não é mais do que um conjunto de *bytes*[17]. Embora se constate este facto, nos SI empresarial, a informação armazenada em ficheiros é estruturada sob a forma de registos[18]. Em suma, "Um ficheiro é assim logicamente constituído por um conjunto de registos, sendo um registo, por sua vez, dividido em um ou mais campos" (Carriço & Carriço, 1998, p. 21).

### 1.4.2. Sistema de Gestão de Base de Dados

Com vista a conservar um conjunto de registos, torna-se necessário armazená-los num sistema capaz de registar, atualizar, manter e disponibilizar a informação, ou seja,

[14] É um modelo, um guia do que foi planeado, incluindo atributos já aprovados, ou seja, é um projeto pronto a ser utilizado.
[15] Este tipo de ficheiro pode assumir diversos formatos.
[16] Este tipo de ficheiro pode conter informação de diversos tipos, nomeadamente texto, imagens, sons, vídeos, entre outros.
[17] *Byte* é uma unidade de informação digital que corresponde a oito *bits*. Esta unidade de medida especifica e quantifica a memória.
[18] Estes registos, normalmente são divididos em um ou mais campos.

uma BD. Contudo, esta informação armazenada na BD deve ficar organizada de modo a uma futura compreensão e utilização. Para que tal seja possível, torna-se imprescindível que exista um sistema de *software* capaz de organizar de forma estruturada toda a informação. Basicamente, existem dois sistemas de organização de dados, o sistema de ficheiros (SF) e o sistema de base de dados (SBD) (Carriço & Carriço, 1998).

Quanto ao SF, a informação é criada e mantida pelas aplicações. Por outro lado, o SBD, assegura uma dependência entre as aplicações e os dados, sob a mediação do SGBD. Este, é "um sistema de *software* situado entre as aplicações e os dados" (Carriço & Carriço, 1998, p. 22). Neste ponto de vista, o SGBD organiza de forma estruturada toda a informação que é criada por uma aplicação e posteriormente armazenada numa BD.

Este SGBD "é um componente de *software* que assegura a implementação e a gestão das estruturas de dados responsáveis pelo armazenamento da informação" (Carriço & Carriço, 1998, p. 56).

Um SBD abrange três componentes elementares: a estrutura lógica[19] e física[20] onde a informação é organizada; o SGBD; e os utilizadores[21] (Carriço & Carriço, 1998).

No que concerne à informação da BD, esta pode ser visualizada segundo três níveis, o nível físico, o nível concetual e o nível externo:

1. Quanto ao nível físico, este "respeita a forma como a informação é efetivamente armazenada nos suportes externos de informação" (Carriço & Carriço, 1998, p. 54);
2. No que se refere ao nível conceptual, este "representa a base de dados tal como ela é vista pelo conceptor (…) Esta visão conceptual representa um sistema virtual de armazenamento, proporcionada pelo sistema de gestão de base de dados" (Carriço & Carriço, 1998, pp. 54-55). No caso de uma BD relacional, a BD é construída como um conjunto de tabelas relacionadas;
3. Por último, quanto ao nível externo, o SGBD pode proporcionar diferentes níveis de visualização, isto é, para cada utilizador é fornecida uma visão parcial da BD, contendo a informação que é relevante[22] para esses utilizadores (Carriço & Carriço, 1998).

[19] A informação é percecionada como um conjunto de tabelas.
[20] A estrutura é criada e mantida em suportes externos de informação pelo *software* SGBD.
[21] Podem ser classificados em utilizadores finais, utilizadores especializados, programadores, ou gestores de informação.
[22] Uma visão coerente, mas limitada de acordo com o perfil de cada utilizador.

Resumindo, um sistema de bases de dados permite três níveis de visualização da informação, o nível físico, o nível conceptual e o nível externo:

> "O nível físico corresponde às estruturas de informação criadas nos discos. O nível conceptual correspondente ao desenho lógico da base de dados, como um todo. O nível externo corresponde às diferentes visões que diferentes utilizadores podem ter da base de dados" (Carriço & Carriço, 1998, p. 55).

Em suma, estes níveis de visão da informação dependem do tipo de utilizador, seja ele Utilizador Final, Utilizador Especializado, Programador, ou Gestor de Informação.

### 1.4.3. Modelo Relacional

Atualmente, existem vários modelos concetuais de BD, mas o modelo mais usado pelos programadores é chamado o Modelo Relacional. No modelo de BD relacional, a informação é armazenada em tabelas[23] ou relações, que são estruturadas de forma a englobar os dados referentes a entidades ou relacionamentos que dão origem à informação que a BD deve registar, atualizar ou manter. Posto isto, uma tabela é um conjunto de linhas[24], e uma linha é um conjunto de colunas[25]. Contudo, uma tabela não deve[26] apresentar linhas repetidas (Carriço & Carriço, 1998).

Em suma, uma BD relacional é:

> "um conjunto de relações materializado num sistema concreto de hardware e software através de um sistema de gestão de bases de dados relacionais. Esse sistema (…) cria, nos sistemas de armazenamento permanente, estruturas de dados que são visualizadas pelos utilizadores sob a forma de tabelas" (Carriço & Carriço, 1998, pp. 77-78).

Por outo lado, numa primeira fase, usar-se-á o Modelo Entidade-Relação (Modelo E-R), "é um modelo em rede que descreve a diagramação dos dados armazenados de um sistema de alto nível de abstração" (Yourdon, 1990, pp. 289, 290). Este modelo está demonstrado na Figura 5.

### 1.4.4. Chaves Primárias

De modo a garantir que uma tabela não apresente linhas[27] repetidas[28], isto é, cada entidade do mundo real é única (distinta das restantes), é necessário criar um mecanismo que verifique esta condição. Este mecanismo pode ser validado com a imposição de uma

[23] Uma tabela constitui a materialização do conceito mais geral de relação.
[24] Numa relação, as linhas definem-se por *tuplos*.
[25] Numa relação, as colunas definem-se por atributos.
[26] O sistema de gestão de bases de dados relacional Microsoft Access permite, em certas condições, a ocorrência de linhas repetidas numa tabela.
[27] Cada linha da tabela representa uma entidade do mundo real.
[28] Uma relação não apresenta *tuplos* repetidos.

chave primária (CP) em cada tabela. CP define-se como um conjunto, formado por uma ou mais colunas, que identifica inequivocamente cada linha da tabela. Após ser definida uma CP, o SGBD passa a controlar cada valor inserido nessa chave, recusando valores que originem uma duplicação na mesma (Carriço & Carriço, 1998). O exemplo de CP pode ser demonstrado na Figura 5, por exemplo "ChavePrimaria1" na "Entidade A".

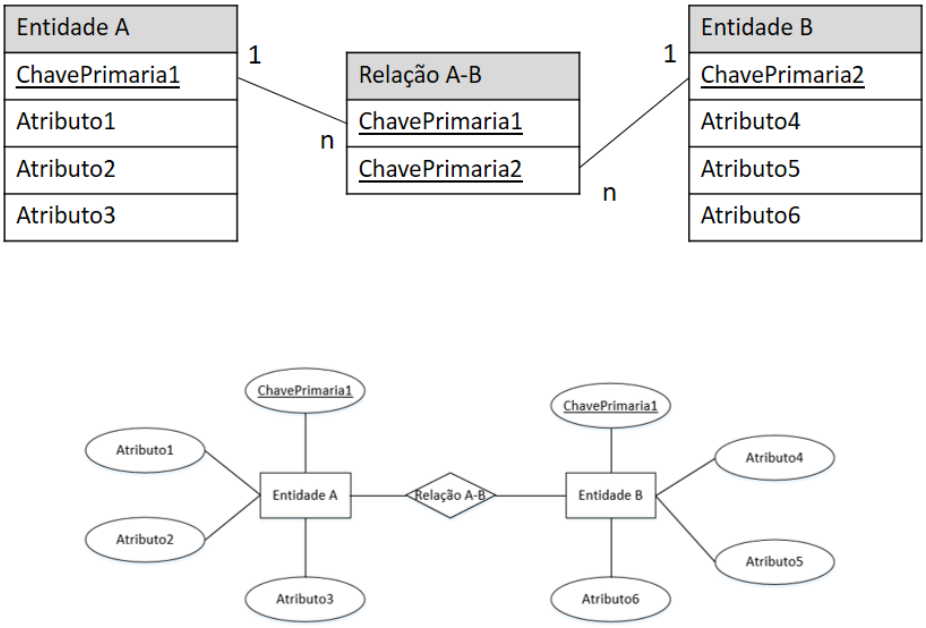


**Figura 5 - Exemplo de Modelo E-R / Modelo Relacional**

**Fonte: Elaboração Própria.**

No Modelo E-R, ou no Modelo Relacional, as CP são graficamente representadas com o nome do respetivo atributo, ou conjunto de atributos, em sublinhado, assim como está plasmado na Figura 5.

Designa-se Chave Estrangeira[29] (CE) a conjuntos de uma ou mais colunas de determinada tabela, que referenciem a CP de outra tabela (exemplo de acordo com a Figura 5, a "ChavePrimaria1" na entidade "Relação A-B"). Este facto torna-se essencial para os sistemas de bases de dados relacionais, uma vez que através deste mecanismo é possível as tabelas relacionarem, e serem relacionadas por outras (Carriço & Carriço, 1998).

[29] Também conhecida como Chave Externa.

### 1.4.5. Restrições de Integridade

De modo a garantir que a informação armazenada na BD seja consistente e compatível com as regras da organização, devem ser implementadas restrições de integridade. O princípio da Integridade de Entidade, determina que: "Nenhum componente da chave primária de uma tabela pode conter nulos" (Carriço & Carriço, 1998, p. 105). O valor nulo significa que esse mesmo valor não existe, ou seja, é desconhecido. Em suma, esta evidência verifica a condição do princípio da Integridade de Entidade. Isto deve-se, ao facto de que a CP identifica cada uma das entidades registadas, e uma violação ao princípio anteriormente referido levaria a que a BD registasse uma entidade não identificável (Carriço & Carriço, 1998).

Por outro lado, também o princípio da Integridade Referencial deve-se verificar. Este princípio atesta que "o valor de uma chave externa tem de existir na tabela referenciada" (Carriço & Carriço, 1998, p. 105). Ou seja, um valor que não exista como CP de uma tabela, não pode ser usado como CE noutra tabela. De acordo com a Figura 5, a "ChavePrimaria1" na entidade "Relação A-B" só poderá existir se existir previamente um valor correspondente ao mesmo atributo na "Entidade A".

Para definir as tabelas a implementar num SGBD, é necessário compreender que uma tabela materializa uma entidade. Cada entidade define uma determinada classe de elementos (objetos), ou seja, uma entidade "designa uma classe de 'objetos' que possuem um conjunto de atributos comuns" (Carriço & Carriço, 1998, p. 287). Concluindo:

> "as entidades representam coisas, seres, conceitos ou acontecimentos do mundo real. Esses elementos são portadores de caraterísticas ou atributos. Esses atributos representam informação sobre os elementos da entidade. Assim, para além da identificação de uma entidade, torna-se necessário definir quais os atributos caracterizadores dessa unidade" (Carriço & Carriço, 1998, p. 289).

Visto isto, uma entidade pode ser representada por uma tabela, onde as colunas da tabela representam os atributos da entidade e, as linhas da tabela representam os elementos da entidade (Carriço & Carriço, 1998).

Cada atributo está ainda associado a um domínio. Este domínio deve representar a mais pequena parcela de informação que possua um sentido próprio. Assim, os atributos que apresentam esta condição designam-se por atributos elementares. Por outro lado, os atributos que ainda podem ser divididos em atributos elementares definem-se por atributos compostos (Carriço & Carriço, 1998). Estes conceitos tornam-se importantes para a modelação da BD. Esta modelação será explanada no subcapítulo 1.4.6. (Formas Normais).

As bases de dados relacionais, assentam no conceito de associações. Estas associações representam os relacionamentos existentes entre os elementos das várias entidades. De acordo com Carriço e Carriço (1998), na maior parte dos casos, as associações são binárias[30]. Contudo, também se pode considerar associações entre mais do que duas entidades[31], ou ainda, a associação entre elementos de uma mesma entidade[32].

Contudo, numa associação, nem todas as entidades necessitam de ser obrigatórias, isto é, uma entidade só se considera obrigatória se todos os elementos da entidade participam obrigatoriamente na associação. Posto isto, podemos perceber que numa associação nem todos os elementos de uma entidade necessitam de participar na associação.

Ainda no que concerne a associações, além de se definir a obrigatoriedade ou não de entidades numa associação, deve-se ainda definir as associações quanto ao número de elementos que participam na mesma. "As três hipóteses a considerar são as seguintes: associações de um-para-um (ou de 1-para-1), associações de um-para-vários (ou 1-para-n) e associações de vários-para-vários (ou de n-para-n)" (Carriço & Carriço, 1998, p. 305).

Uma associação é do tipo (Carriço & Carriço, 1998):

1. 1-para-1, quando cada elemento de uma entidade está associado no máximo com um elemento de outra entidade;
2. 1-para-n (numa associação entre A e B), quando cada elemento da entidade A pode estar associado com vários elementos da entidade B, mas cada elemento da entidade B apenas pode estar associado, no máximo, com um elemento da entidade A;
3. n-para-n (numa associação entre A e B), quando cada elemento da entidade de A pode corresponder a vários elementos da entidade de B, e ainda, cada elemento da entidade de B pode corresponder a vários elementos da entidade de A.

Visto isto, um Modelo E-R deve ser graficamente representado através de diagramas[33]. Para se poder representar um Diagrama Entidade-Associação (DEA) deve-se primeiro definir os diferentes símbolos a representar, nomeadamente os símbolos para as entidades, as associações e os atributos (Carriço & Carriço, 1998). Estes símbolos são representados de acordo com a Figura 6.

[30] Envolvem o relacionamento entre elementos de duas entidades distintas.
[31] Uma associação entre três entidades distintas designa-se de associação ternária.
[32] Uma associação entre elementos da mesma entidade designa-se de associação unária.
[33] Designam-se por Diagramas Entidade-Associação.

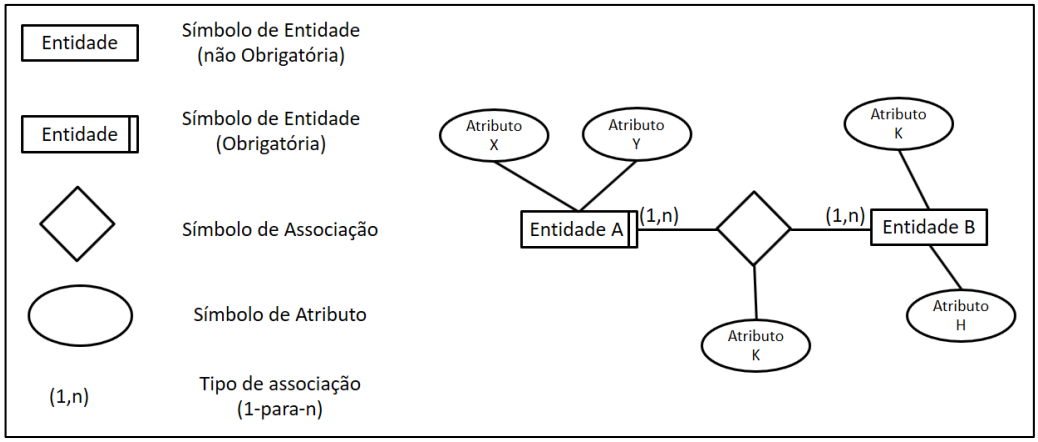


**Figura 6 - Diagrama Entidade-Associação e Simbologia.**

**Fonte: Elaboração Própria (adaptado de Carriço e Carriço, 1998).**

Após o DEA estar concluído, torna-se mais simples a sua implementação em SGBD, uma vez que todas as entidades, atributos, associações e tipo de associação estão definidas.

### 1.4.6. Formas Normais

De forma a evitar redundâncias desnecessárias, e alguns problemas associados à inserção, eliminação e atualização de dados, a BD deve estar normalizada. "A normalização é um processo que consiste em estruturar a informação em tabelas na forma que pode ser considerada mais adequada do ponto de vista das operações a executar sobre a informação armazenada (…)" (Carriço & Carriço, 1998, p. 361).

Inicialmente, o Modelo Relacional sugeria a existência de três formas normais onde, na prática, os procedimentos de normalização se consideravam satisfatórios se as suas tabelas atingissem a Terceira forma normal[34]. Contudo, estudos subsequentes do modelo, chegaram à conclusão que em certas situações a 3FN não constitui o estado final "ideal" a que as relações de uma BD relacional devem obedecer. Perante isto, foram criadas especificações complementares conhecidas como Forma Normal de *Boyce/Codd* (FNBC), Quarta forma normal (4FN) e Quinta forma normal (5FN) (Carriço & Carriço, 1998).

[34] As tabelas que se encontram na terceira forma normal encontram-se igualmente na segunda forma normal e, consequentemente na primeira forma normal.

Assim, foi estabelecida uma hierarquia de formas normais (Carriço & Carriço, 1998): (i) Primeira forma normal (1FN); (ii) Segunda forma normal (2FN); (iii) Terceira forma normal (3FN); (iv) Forma Normal de *Boyce/Codd* (FNBC); (v) Quarta forma normal (4FN); (vi) Quinta forma normal (5FN).

Para que as relações do modelo relacional atinjam a 1FN, todos os seus atributos devem estar definidos em domínios que assumam apenas valores atómicos ou elementares. Também, para se atingir a 2FN, todas as relações já se encontram na 1FN e todos os atributos que não pertencem à chave, dependem da chave através de uma dependência funcional elementar[35]. Caso a chave não seja composta por um conjunto de atributos (chave constituída por um único atributo), os restantes atributos apenas dependem funcionalmente da chave (Carriço & Carriço, 1998).

Podemos definir Dependência Funcional (DF) quando um atributo depende de outro atributo, ou seja, quando a combinação de um ou mais atributos corresponde sempre para o mesmo valor de um outro atributo (Carriço & Carriço, 1998).

Uma tabela considera-se que se encontra na 3FN, quando esta estiver na 2FN, e simultaneamente nenhum dos seus atributos, que não pertençam à chave, for funcionalmente dependente de qualquer combinação dos restantes. Ou seja, além da tabela se encontrar na 2FN, a 3FN determina ainda que cada atributo apenas dependa da chave e não de qualquer outro atributo (ou conjunto de atributos). Para se verificar esta condição, é necessário que todos os atributos que não pertençam à chave, sejam mutuamente independentes, por outras palavras, são atualizados independentemente uns dos outros (Carriço & Carriço, 1998).

Segundo Carriço e Carriço (1998), as especificações da FNBC vêm reforçar as especificações da 3FN, onde verifica a existência de mais do que uma chave candidata e, ainda, que duas chaves candidatas possuam elementos comuns. Ou seja, uma tabela está na FNBC quando os únicos determinantes são as chaves candidatas. Em suma, se uma tabela apresentar três atributos, dos quais apresentam duas possíveis chaves candidatas (conjunto de dois atributos), isto leva a que as duas chaves candidatas tenham atributos comuns. Posto isto, esta tabela apresenta um determinante que não é chave primária, logo não se encontra na FNBC. Este facto leva a problemas na eliminação, uma vez que ao apagar um registo pode levar à perda de informação (Carriço & Carriço, 1998).

[35] Dependem do conjunto (chave) e não dependem de nenhum dos seus elementos ou subconjuntos isoladamente.

Quanto à 4FN, uma tabela encontra-se nessa forma quando as únicas multidependências (dependência de valores múltiplos) elementares são aquelas em que uma chave determina um atributo, ou seja, visa eliminar a possível existência de grupos repetidos independentes. Entende-se por multidependência quando numa tabela A com os atributos x, y, z e w, o atributo x multidetermina y, se a um determinado valor de x está associado um conjunto de valores de y e, ainda, esse conjunto de valores de y é independente dos restantes atributos da tabela (os atributos z e w). Isto é, quando numa tabela existam vários atributos que podem assumir conjuntos de valores (independentes entre eles), esta não se encontra na 4FN (Carriço & Carriço, 1998).

Por último, pode-se afirmar que uma tabela se encontra na 5FN se qualquer dependência de junção é implicada pelas chaves candidatas. Por outras palavras, quando se decompõe uma tabela nas projeções correspondentes aos subconjuntos formados pelos atributos, e de seguida a partir da junção dessas mesmas projeções se obtém novamente a tabela inicial, significa que existe uma dependência de junção dessas projeções. Visto isto, se essa dependência de junção é implicada pelas chaves candidatas, significa que se atingiu a 5FN (Carriço & Carriço, 1998).

O problema central no que concerne à modelação da BD relacional é determinar quais são as relações necessárias que representem o sistema real. Para facilitar esta compreensão utiliza-se o DEA. Contudo, para apresentar este diagrama relativo ao sistema real, torna-se necessário normalizar a BD de modo a evitar redundâncias desnecessárias, e alguns problemas associados à inserção, eliminação e atualização de dados. Posto isto, esta normalização descreve uma técnica formal que analisa os dados e os agrupa da melhor forma possível com vista a facilitar futuras alterações e minimizar o impacto dessas mudanças no sistema. Esta técnica é conseguida através da subdivisão de relações já existentes, noutras de menor grau (dividir para conquistar) (Carriço & Carriço, 1998).

Visto isto, o processo de desenvolvimento de um modelo de BD relacional bem estruturado, inicia-se com o estudo das relações originais com vista a decompô-las através de uma série de etapas sucessivas. Estas decomposições seguem determinadas regras de modo a cumprir as condições impostas pelas formas normais anteriormente descritas. Uma tabela que esteja na 2FN obedece igualmente às condições da 1FN e assim sucessivamente, de acordo com a hierarquização das formas normais.

Em suma, pode-se afirmar que uma BD relacional está normalizada quando todas as suas relações cumprem as condições impostas pela 5FN.

# CAPÍTULO 2. METODOLOGIA CIENTÍFICA

Neste capítulo, pretende-se identificar a metodologia científica usada no decorrer desta investigação. Para tal, identifica-se a natureza da investigação, o objetivo da investigação, a forma de abordagem, os procedimentos técnicos e por último a técnica de recolha de dados.

Finalizando este capítulo, apresenta-se o desenho de estudo, resumindo toda a metodologia científica adotada neste TIA.

## 2.1. Natureza da Investigação

Num Trabalho de Investigação, a natureza do trabalho pode ser Investigação Fundamental ou Investigação Aplicada.

A Investigação Aplicada tem por objetivo encontrar uma aplicação prática para os novos conhecimentos, adquiridos no decurso da realização de trabalhos originais (Carvalho, 2009).

No decurso da realização deste TIA, uma BD relacional de controlos de segurança da informação será criada com vista à sua implementação nas U/E/O militares do Exército Português. O seu desenvolvimento será com base em todo o estudo efetuado, de modo a gerir os controlos de segurança das U/E/O militares.

## 2.2. Objetivo da Investigação

Os objetivos da investigação podem dividir-se em: objetivos exploratórios, objetivos descritivos e objetivos explicativos.

O objetivo deste tema de trabalho será o objetivo descritivo, envolvendo técnicas padronizadas de recolha de dados, como análise de documentos. Também o objetivo explicativo está presente nesta investigação, explicando o porquê das coisas, visando identificar os fatores que determinam ou contribuem para a ocorrência dos fenómenos, assumindo a forma de pesquisa experimental. Por último, também o objetivo exploratório está presente no trabalho. Este objetivo pretende desenvolver, esclarecer ou modificar

conceitos e ideias, tendo em vista a formulação de problemas mais precisos, ou hipóteses pesquisáveis para estudos posteriores (Gil, 2008).

Em suma, no decorrer deste trabalho, pretende-se descrever (objetivo descritivo) quais as principais dimensões, categorias e controlos de segurança da informação a implementar numa U/E/O militar do Exército Português, através da análise de documentos. Também, o objetivo explicativo está presente ao longo do decorrer do trabalho, explicando quais são os requisitos funcionais necessários a implementar numa BD de controlos de segurança da informação, a fim de a implementar nas U/E/O militares do Exército Português. Por último, através do objetivo exploratório pretende-se efetuar um estudo exploratório, com o intuito de comprovar a eficácia da BD desenvolvida ao longo do trabalho, a fim de criar hipóteses pesquisáveis para estudos posteriores (Gil, 2008).

Contudo, embora este estudo exploratório pretenda comprovar a eficácia da BD desenvolvida para as U/E/O militares do Exército Português, esta amostra não é representativa, uma vez que é uma amostra por conveniência. Esta amostra, define-se por amostras selecionadas pelo autor, onde normalmente, são utilizadas para testar ou obter ideias sobre determinado assunto de interesse. Estas amostras são eficazes no que concerne aos objetivos de pesquisa exploratória (Mattar, 2012).

## 2.3. Forma de Abordagem

Quanto à forma de abordagem[36], esta pode ser do tipo quantitativa, qualitativa ou mista. A estratégia de investigação qualitativa assenta numa relação indissociável entre o mundo real e a subjetividade do sujeito, não sendo possível ser expressa em números (Santos, et al., 2014). Neste caso concreto, o estudo assenta na compreensão da realidade social das U/E/O do Exército Português, através da exploração da funcionalidade da BD relacional numa unidade, alcançando assim uma interpretação da realidade social de todas as U/E/O militares do Exército Português.

De acordo com Santos et al (2014), no método qualitativo a recolha de dados é efetuada recorrendo à entrevista, à análise documental e à observação. A entrevista será efetuada com vista a identificar os requisitos necessários a implementar na BD relacional de controlos de segurança de informação. A análise documental será efetuada com o

[36] Também conhecido como Estratégia de Investigação.

intuito de identificar os controlos necessários a implementar na BD, de modo a eliminar as falhas detetadas ao nível da segurança da informação nas U/E/O militares do Exército Português. Por último, a observação será efetuada de modo a comprovar a eficácia da BD relacional, colocando uma determinada amostra a usar a BD.

Segundo Freixo (2011), existem vários tipos de investigação. A investigação científica pode dividir-se em diferentes estratégias. Estas estratégias deram origem a várias variantes, nomeadamente o método indutivo, o método dedutivo e o método hipotético-dedutivo.

"O método indutivo corresponde a uma operação mental que tem como ponto de partida a observação de factos particulares para, através da sua associação, estabelecer generalizações que permitam formular uma lei ou teoria" (Santos, et al., 2014, p. 13).

O método indutivo prevê um uso do maior número possível de observações, não apresentando qualquer tipo de considerações pessoais, com a finalidade de representar a realidade tal como ela é, sem qualquer interferência. Este, parte de questões particulares até chegar a conclusões generalizadas, ou seja, o raciocínio faz-se do particular para o geral. Inicialmente observam-se os fenómenos, depois categorizam-se as observações, de seguida formulam-se as hipóteses, e por último, confirmam-se essas mesmas hipóteses. O método indutivo generaliza então a uma população, o que foi provado em algumas amostras, sendo este erro tanto menor, quanto maior for a amostra (Santos, et al., 2014).

Em suma, na realização do TIA, o método que se irá usar será o método indutivo, identificando numa primeira fase as dimensões, categorias e controlos de segurança da informação ao nível organizacional. Posteriormente, após esta análise, serão conduzidas entrevistas, a três colaboradores ligados à área da segurança da informação, com o objetivo de identificar os requisitos que a BD deve responder, a fim de corresponder às necessidades de U/E/O militares do Exército Português, tornando-se assim nas hipóteses. Por último, após o desenvolvimento da BD, e de ser conduzido um estudo exploratório, essas mesmas hipóteses serão confirmadas. Resumindo, partindo de questões particulares (análise documental e entrevistas) chega-se a conclusões generalizadas, abrangendo as necessidades de todas as U/E/O do Exército Português (Freixo, 2011).

## 2.4. Procedimentos Técnicos

No que concerne aos procedimentos técnicos, este pode ser do tipo experimental, transversal, longitudinal, estudo de caso, comparativo, histórico ou *Grounded Theory*. No respeitante ao método comparativo, este tipo de investigação é usado quando se pretende estudar dois ou mais casos contrastantes. "A lógica da comparação tem subjacente a ideia que os fenómenos sociais são mais facilmente apreendidos se forem comparados com outros casos ou situações, que apresentem diferenças significativas entre si" (Bryman, 2012, p.72, citado em Santos et al., 2014, p.26).

No que diz respeito ao método comparativo, este usar-se-á no decorrer do presente trabalho, a fim de comparar três normas internacionais de controlos de segurança da informação (através de um modelo de análise), identificando assim qual das normas se usará para validar a implementação da BD, através da resposta aos requisitos funcionais obtidos.

## 2.5. Técnica de Recolha de dados

As técnicas de investigação podem classificar-se quanto à recolha de dados, segundo várias modalidades, nomeadamente análise documental, inquérito por questionário, inquérito por entrevista, observação, análise de conteúdo e escalas.

No decorrer da elaboração do TIA, serão usadas as seguintes técnicas:

1. Análise documental;
2. Inquérito por entrevista.

Inquérito por Entrevista define-se como técnica em que o investigador se apresenta em frente ao investigado e lhe formula perguntas, com a finalidade de obter os dados necessários à investigação. Pode caracterizar-se como uma forma de diálogo assimétrico, em que uma das partes busca recolher dados e a outra se apresenta como fonte de informação (Gil, 2008).

A realização deste TIA, terá por base a análise documental, analisando principalmente relatórios científicos internacionais, com vista a identificar as principais dimensões, categorias e controlos de segurança da informação. Também, inquéritos por entrevista serão utilizados como ferramentas de trabalho, para inquirir três colaboradores

(Major Pessoa Dinis, Major Nuno Gois e Major Francisco Salvador), ligados à área da segurança da informação de várias U/E/O militares, a fim de se identificarem os requisitos necessários a implementar na BD relacional. Estas entrevistas serão diretivas[37], apresentando assim um guião de entrevista rígido.

## 2.6. Desenho de Estudo

Em suma, de acordo com a metodologia explicada anteriormente, a Figura 7 (Desenho de Estudo) pretende resumir a metodologia adotada ao longo da elaboração deste trabalho.

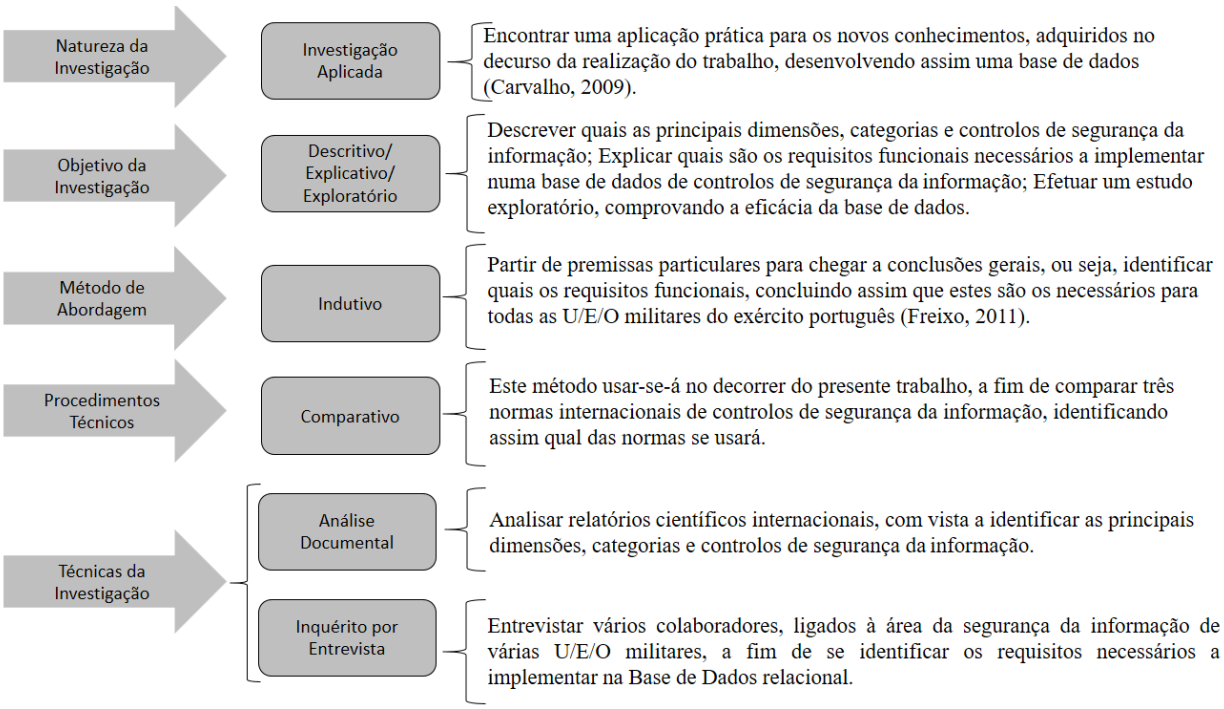


**Figura 7 - Desenho de Estudo**

**Fonte: Elaboração Própria, adaptado da Unidade Curricular Metodologia da Investigação da Academia Militar.**

[37] Também denominadas de Entrevistas Estruturadas.

# CAPÍTULO 3. DESENVOLVIMENTO DE *SOFTWARE*

A Engenharia de *Software* preocupa-se com teorias, métodos e ferramentas necessárias para desenvolver um *software*. A Engenharia de *Software* "é a aplicação de um processo sistemático, disciplinado, e simplificado ao desenvolvimento, operação e manutenção de *software*; ou seja, a Engenharia de Software é a aplicação de técnicas de engenharia ao *software*" (IEEE, 1993 citado em Silva & Videira, 2001).

As ações que a Engenharia de *Software* compreende, podem ser agrupadas em três grandes fases: conceção, implementação e manutenção. Contudo, estas fases ainda podem ser divididas noutras fases mais básicas (Silva & Videira, 2001).

Este capítulo está dividido em dois subcapítulos, onde se descreve os modelos de processos e uma das técnicas e metodologias de modulação (Modelo Relacional), que se usará na fase da análise do sistema.

## 3.1. Modelo de Processo

Os modelos de Processos podem dividir-se, de acordo com Silva e Videira (2001), segundo dois grandes grupos: os que seguem uma aproximação conforme um modelo em cascata e os que têm uma aproximação iterativa.

De acordo com Silva e Videira (2001), os processos mais comuns no que concerne ao desenvolvimento de *software* são caraterizados por adotarem um modelo em cascata. Este modelo remete para a ideia de que as atividades a executar são agrupadas em tarefas, executando-se de forma sequencial, de modo a que uma tarefa só tem início quando a anterior terminar. "O modelo em cascata tem a vantagem que só se avança para a tarefa seguinte quando o cliente aceita e valida os produtos finais da tarefa atual" (Silva & Videira, 2001, p. 60). Em suma, compreende-se que neste processo, o cliente participa ativamente no projeto. Este modelo está representado na Figura 8.

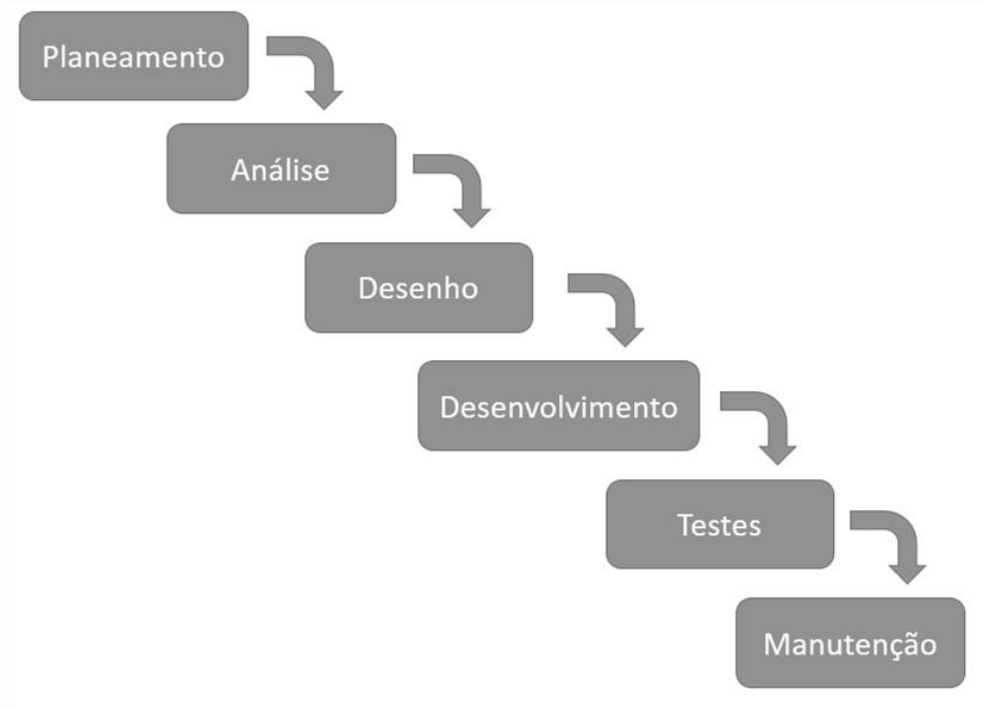


**Figura 8 - Modelo em Cascata.**

**Fonte: Silva & Silveira, 2001, pág.60.**

Contudo, este modelo apresenta algumas limitações, nomeadamente (Silva & Videira, 2001):

1. As atividades a executar são agrupadas em tarefas, provocando um desencorajamento de comunicação e partilha de visões em todos os intervenientes[38] do projeto;
2. Dificulta o impacto da compreensão adquirida no decorrer do projeto, uma vez que o processo não pode voltar atrás, como se constata na Figura 8. Este facto impede que se altere os modelos e as conclusões das tarefas anteriores, tornando-se comum que novas ideias sobre o sistema não sejam tidas em conta.

De acordo com as limitações descritas, e de forma a ultrapassar este problema, este processo (modelo em cascata) foi revisto. Para se eliminar estas limitações, pretende-se que no decorrer do processo, a partir de qualquer tarefa do ciclo seja possível voltar a uma anterior, de modo a contemplar alterações funcionais, assim como técnicas que tenham surgido. Este novo modelo, que contempla estas novas funcionalidades é descrito como Modelo em Cascata Revisto (Figura 9) (Silva & Videira, 2001).

[38] Os analistas, os responsáveis pelo desenho, os programadores e os utilizadores.

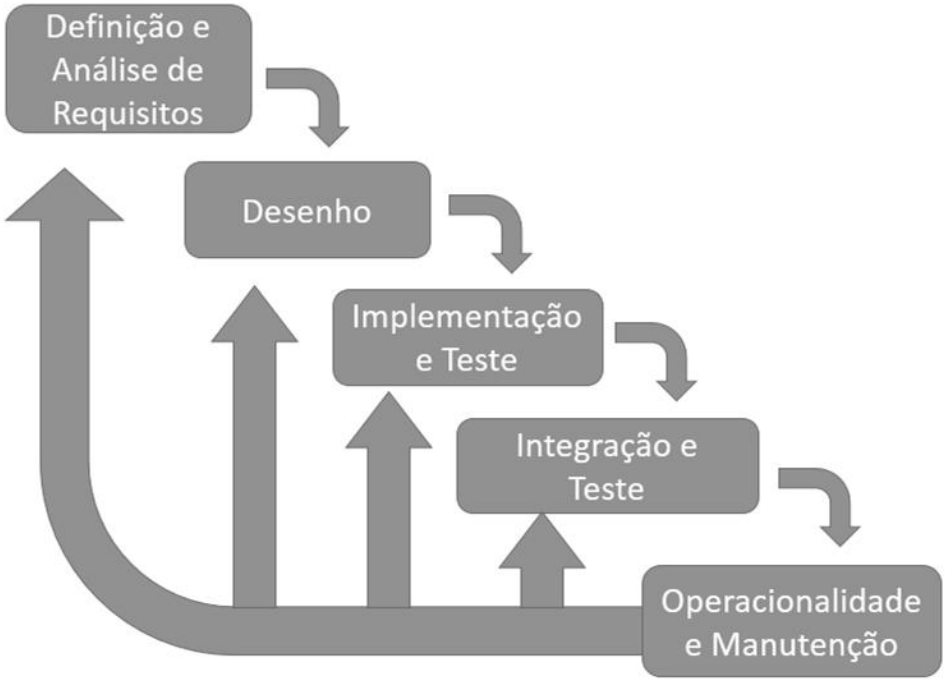


**Figura 9 - Modelo em Cascata Revisto.**

**Fonte: Adaptado de Sommerville, 1995, pág.30.**

Contudo, este modelo apresenta ainda algumas limitações, nomeadamente "na ausência de um processo de gestão de projeto e de controle das alterações bem definido, podemos passar o tempo num ciclo sem fim, sem nunca se atingir o objetivo final que é disponibilizar um sistema a funcionar" (Silva & Videira, 2001, p. 61).

Apesar do risco que esta abordagem acarreta (reduzido nesta investigação), o processo de desenvolvimento de *software* que é utilizado é o Modelo em Cascata Revisto. Neste modelo todas as atividades estão, de um modo geral, bem definidas e satisfazem os objetivos do projeto.

Durante o desenvolvimento do Sistema (BD de controlos de segurança de informação), procura-se garantir os seguintes atributos:

1. Manutenção[39], com vista a adaptar-se às mudanças que se venham a verificar no futuro;

[39] Processo de alterar o sistema após a sua conclusão. Esta alteração pode ser efetuada segundo três tipos: corretivas, adaptativas ou evolutivas.

2. Fiabilidade e Segurança[40], isto é, se o sistema falhar não acarretará prejuízos económicos à organização;
3. Eficiência, não desperdiçar recursos do sistema;
4. Utilização, uma interface com o utilizador adequada;
5. Formação[41] necessária para lidar com o *software* é diminuta.

Por outro lado, no que respeita à complexidade de desenvolvimento de *software*, "a complexidade de *software* é uma propriedade essencial, intrínseca à própria natureza do *software*, e não acidental, que ocorra esporadicamente" (Brooks, 1986 citado em Silva & Videira, 2001, p. 37). Devido a este facto, utiliza-se o princípio da Decomposição Hierárquica, conhecido como *divide and conquer*[42]. Através deste princípio, o problema é dividido em sub-problemas mais elementares e assim sucessivamente, até que a sua resolução seja mais simples (Silva & Videira, 2001). Deste modo, procura-se realizar a modelação da BD, representando em tabelas as entidades que representam a realidade (gestão da segurança da informação) consideradas suficientes para entender e solucionar corretamente o problema em análise.

## 3.2. Técnicas e Metodologias de Modulação

Neste subcapítulo pretende-se identificar a notação gráfica para modelagem de dados que se usará na fase da análise do projeto e na fase de desenho do projeto.

No respeitante à fase de análise do projeto propõe-se o uso do Modelo E-R, contudo na fase subsequente (desenho do projeto) será usado o Modelo Relacional. Estes modelos foram explanados no subcapítulo 1.4. (Fundamentos de um Sistema de Gestão de Base de Dados), sendo demonstrados na Figura 5. Ainda, na Figura 6, pode-se verificar um DEA, usada para apresentar os modelos anteriormente identificados.

Em suma, a modelagem da BD, na fase da análise do sistema, será efetuada usando o Modelo E-R. Contudo, na fase do desenho do projeto será usado o Modelo Relacional, apresentando este uma visão mais intuitiva para a implementação do mesmo.

[40] Será garantido pela autenticação dos utilizadores que pretendam aceder ao Sistema, de acordo com o seu direito de acesso.
[41] A formação necessária pala lidar com o *software* é mínima, uma vez que a interface com o utilizador é intuitiva, e todos os campos estão facilmente identificados e legendados.
[42] Conhecido como dividir para conquistar.

# CAPÍTULO 4. DIMENSÕES, CATEGORIAS E CONTROLOS A IMPLEMENTAR

Neste capítulo pretende-se identificar os diferentes controlos sugeridos pela Norma ISO/IEC 27001, a publicação NIST 800-53 r4 e a publicação SANS. De modo a identificar os controlos necessários a implementar, na BD relacional de controlos de segurança de informação, será analisado numa primeira fase um estudo de caso realizado numa organização militar do Exército Português, elaborado por Martins et al. (2013), onde se identificam os principais controlos de segurança de informação, inoperacionais ou em falta, nas principais dimensões ao nível da segurança de informação.

Posteriormente, numa segunda fase enumerar-se-ão as publicações/normas que fornecem controlos de segurança de informação, comparando-as através de um modelo de análise, com vista a identificar qual destas se usará, para validar a implementação da BD de acordo com os requisitos funcionais.

Na terceira e última fase identificar-se-ão quais são os requisitos necessários a implementar, com base em três entrevistas conduzidas a especialistas da segurança da informação.

## 4.1. Estudo de Caso

Como referido anteriormente, a segurança da informação consiste na proteção da informação armazenada, processada ou transmitida contra a perda de confidencialidade, integridade e disponibilidade, através da implementação de um diverso conjunto de controlos técnicos, físicos e administrativos. Este tipo de segurança é fundamental nas U/E/O militares, uma vez que um dos seus principais objetivos é garantir a superioridade de informação. Atualmente, a importância da segurança da informação nas organizações militares tem crescido devido ao desenvolvimento das doutrinas de ciberguerra em vários países, mais especificamente conhecida como Operações em Rede de Computadores (Martins et al. 2013).

Para fazer face a este conceito é necessário analisar três pontos chave, nomeadamente reconhecer as dimensões e categorias mais relevantes implementadas nas

organizações militares, identificar os principais cenários de incidentes na segurança da informação que se espera que ocorra, e por último qual é o processo de decisão usado para o planeamento e seleção de controlos de segurança da informação. O estudo de caso elaborado por Marins et al. (2013), procura responder a estas questões. Contudo, com vista a responder a estas questões, o estudo referido previamente foi dividido em três fases, na primeira foram reunidos e analisados documentos sobre a organização militar, na segunda foram aplicados questionários na organização a três grupos[43] distintos, na terceira e última fase foram conduzidas entrevistas a especialistas com vista a validar os resultados obtidos nas restantes fases (Martins et al. 2013).

De acordo com o questionário aplicado na organização militar, este foi respondido por cinquenta colaboradores. Este questionário tinha como objetivo identificar a maior preocupação em termos de vetores e métodos de ataque, assim como perceber o processo de decisão usado para o planeamento de segurança de informação. De acordo com os vetores de ataque, os principais vetores identificados foram o físico, o humano e o de infraestrutura tecnológico[44] (Martins et al. 2013).

Colocando em prática o modelo genérico[45] de incidentes de segurança da informação em organizações militares, num ambiente de guerra de informação, é possível identificar as principais preocupações da organização depois de analisar algumas variáveis chave no modelo utilizado através da aplicação do questionário. As variáveis expressas neste modelo identificam os possíveis atacantes, ameaças e métodos de ataque[46] e por último os alvos que podem afetar as propriedades fundamentais de segurança da informação[47]. Ou seja, através do modelo genérico sugerido por Martins et al. (2012a), com a adaptação à análise efetuado dos questionários pelos mesmos autores, as principais preocupações identificadas estão expostas na Tabela 11 do Anexo A.

Na última fase do estudo de caso, foram conduzidas algumas entrevistas, com vista a confirmar os dados obtidos nas restantes fases. Com a análise e interpretação dos resultados obtidos, Martins et al. (2013), identificam que a segurança da informação é baseada em quatro principais dimensões de segurança, a dimensão organizacional, a dimensão física, a dimensão humana e a dimensão tecnológica.

[43] "*Decision-makers, information security specialists, and employees with functions specifically linked to information use*" (Martins, Santos, Rosinha, & Valente, 2013, p. 2).
[44] Vetor de infraestrutura tecnológico suporta a informação processada, transmitida e armazenada.
[45] Modelo desenvolvido por Martins, Santos, Nunes & Silva (2012a).
[46] Ações, ferramentas ou armas.
[47] Confidencialidade, integridade e disponibilidade da informação.

Tendo como base a *Framework* proposta por Martins et al. (2012b), seguidamente identificar-se-ão as principais categorias em falta, apresentadas pelas entrevistas, para cada dimensão de segurança da informação.

No que concerne à dimensão organizacional, de acordo com Martins et al. (2013), as entrevistas permitiram identificar aspetos importantes nas U/E/O militares que não são contemplados na ISO/IEC 27001, como a importância dos valores militares[48]. Outro aspeto relevante a salientar nesta dimensão, é a importância da cadeia de comando nas U/E/O militares, com vista a estabelecer o controlo de acesso à informação organizacional. As principais categorias de segurança de informação da dimensão organizacional em falta nas U/E/O militares estão identificadas na Tabela 12 do Anexo A.

Na dimensão de segurança física, de acordo com a Tabela 13 do Anexo A, é demonstrado que esta dimensão de segurança da informação é a mais coberta, isto é, não apresenta categorias em falta (Martins et al. 2013).

No que se refere à dimensão de segurança humana, as categorias em falta estão identificadas na Tabela 14 do Anexo A. De acordo com a Tabela acabada de referir, a categoria "*Behaviour in Public, Contacts with Public Autorities and Media*" é a que se encontra menos operacionalizada, isto é, pouco hábil (Martins et al. 2013).

Nesta dimensão, as principais especificações incluem: a existência de um processo de acreditação obrigatório para todos os militares que lidam com informação classificada; o fornecimento de um manual aos novos funcionários com vista a esclarecer o processo de funcionamento interno (incluindo a segurança da informação); a existência de um núcleo de apoio ao comando que permite detetar um comportamento impróprio; a preocupação com o alcoolismo e o uso de drogas; a atualização do perfil de competências do empregado; preocupação com a segurança dos funcionários; e ainda a realização de *briefings* diários (Martins et al. 2013).

Por último, na dimensão tecnológica, de acordo com as entrevistas efetuadas, as categorias em falta ou que não estão completamente eficazes, estão demonstradas na Tabela 5 do Anexo A. De acordo com Martins et al. (2013), as categorias que estão menos operacionais são as que dizem respeito ao desenvolvimento interno de *software*. A principal caraterística desta dimensão é a capacidade de transmissão de informações classificadas entre U/E/O militares. Como nos sugere o estudo de caso em causa, esta

[48] Valores como a Lealdade, Responsabilidade e a Confiança, entre outras.

dimensão é a que mais se baseia em normas internacionais de controlos de segurança de informação recomendados pela norma ISO/IEC 27001 e pelo Instituto SANS.

De acordo com o estudo de caso elaborado por Martins et al. (2013), nas organizações militares a implantação de um sistema de gestão de segurança de informação centra-se nomeadamente na missão (necessidades operacionais), estudo do adversário, e estudo do ambiente interno, procurando a melhor combinação de controlos de segurança organizacionais, físicos, humanos e tecnológicos para fazer face a possiveis métodos de ataque.

Resumindo, de acordo com o estudo de caso apresentado, a segurança da informação dentro das U/E/O militares é contruída essencialmente com base nos vetores de ataque físicos, tecnológicos e humanos, direcionados para o sistema de informção. Este estudo de caso remete ainda para os controlos de segurança de informação que estão integrados nas principais categorias de controlos de segurança, dentro da dimensão organizacional, física, humana e tecnológica. Por último, é sugerido a partilha de lições aprendidas, conhecimento obtido, experiência  e formação, com vista a garantir a melhor combinação de controlos de segurança de informação (Martins et al. 2013).

Como referido previamente, apesar de se identificar as principais dimensões e categorias da segurança de informação para U/E/O militares do Exército Português, é necessário ainda identificar os controlos a implementar. Para tal, seguidamente identificar-se-ão as principais normas[49] que fornecem os controlos de segurança da informação.

## 4.2. ISO/IEC 27001

Como referido anteriormente, as U/E/O militares apoiam-se em controlos de segurança de informação sugeridos por inúmeras normas, nomeadamente a norma ISO/IEC 27001 (2013).

A norma ISO/IEC 27001 (2013) apresenta, em anexo (2013, pp.16-29), uma lista abrangente de objetivos de controlo e respetivos controlos, os quais estão alinhados com os controlos referenciados no NIST 800-53 r4 (2013).

[49] As principais normas identificadas anteriormente são: ISO/IEC 27001, NIST 800-53 r4 e a SANS.

## 4.3. *Critical Controls for Effective Cyber Defense* – SANS

Os controlos sugeridos pela publicação em causa, estão classificados por prioridades, podendo dividir-se em: reduzir os ataques conhecidos; abordar uma grande variedade de ataques; identificar e parar os ataques no início de um ciclo (SANS, 2013).

A lista sugerida, apresenta para cada controlo de segurança de informação (SANS, 2013):

1. Um detalhe passo-a-passo de procedimentos e ferramentas para implementar o controlo;
2. Uma explicação de como os atacantes exploram a vulnerabilidade no caso da inexistência do controlo em causa;
3. Diagrama relacional a fim de mostrar como o controlo pode ser implementado;
4. Um conjunto dos subcontrolos mais adequados para implementar, automatizar e medir a sua eficácia;
5. Sínteses de métricas e testes que podem ser usados para avaliar a sua implementação;
6. Lista dos controlos NIST 800-53 r4 (2013) associados ao controlo em causa.

Cada controlo de cibersegurança incluído neste documento apresenta um conjunto de testes que a organização pode realizar de forma periódica, a fim de garantir que a segurança de informação implementada pelo controlo em causa é eficaz. Em suma, a definição dos controlos de segurança de informação é um processo contínuo, ao qual este documento está em constante atualização (SANS, 2013).

## 4.4. NIST 800-53 r4

Na publicação NIST 800-53 r4 (2013), os controlos de segurança apresentados têm uma organização e uma estrutura bem definida. Com o objetivo de facilitar o processo de seleção destes controlos, estes são agrupados em 18 famílias distintas. Cada uma das famílias apresentadas, identificadas por dois carateres, têm um conjunto de controlos adaptados ao tema geral de segurança da família. A lista de famílias de controlos é apresentada na Tabela 1.

**Tabela 1 - Famílias de Controlos de Segurança de Informação.**

| ID | *Family* | ID | *Family* |
|---|---|---|---|
| AC | *Access Control* | MP | *Media Protection* |
| AT | *Awareness and Training* | PE | *Physical and Environmental Protection* |
| AU | *Audit and Accountability* | PL | *Planning* |
| CA | *Security Assessment and Authorization* | PS | *Personnel Security* |
| CM | *Configuration Management* | RA | *Risk Assessment* |
| CP | *Contingency Planning* | SA | *System and Services Acquisition* |
| IA | *Identification and Authentication* | SC | *System and Communications Protection* |
| IR | *Incident Response* | SI | *System and Information Integrity* |
| MA | *Maintenance* | PM | *Program Management* |

**Fonte: NIST 800-53 r4, 2013, p.31**.

A estrutura do controlo é constituída por uma Secção de Controlo, uma Secção de Orientação Suplementar, uma Secção de Controlo de Melhorias, uma Secção de Referências, e uma Secção de Prioridade e Afetação de Referência (NIST 800-53 r4, 2013).

A Secção de Controlo, compreende os controlos. Para alguns controlos de segurança fornecidos pela publicação NIST 800-53 r4 (2013), é garantido um grau de flexibilidade devido ao facto de se permitir que a organização defina valores para alguns parâmetros associados aos controlos. Esta flexibilidade garante às organizações a capacidade de adaptar os controlos de segurança e melhorias de acordo com: requisitos de segurança para apoiar as missões/negócios organizacionais, avaliações de risco e aceitação de risco residual, assim como requisitos de segurança provenientes de leis, ordens executivas, diretrizes, políticas, regulamentos, normas ou orientações (NIST 800-53 r4, 2013).

A Secção de Orientação Suplementar fornece informações adicionais para um controlo de segurança específico. Estas informações adicionais podem fornecer orientações importantes para a implementação dos controlos de segurança, assim como para a avaliação de risco do controlo. Esta secção pode conter ainda uma lista de controlos de segurança relacionados (NIST 800-53 r4, 2013).

A Secção de Controlo de Melhorias fornece as declarações de capacidade de segurança dos controlos, com o propósito de adicionar especificidades/funcionalidades a um controlo, ou aumentar a consistência de um controlo. Normalmente, estas melhorias são usadas nos casos em que se necessita de uma maior proteção, em SI, do que o previsto

pelo controlo. Para cada melhoria do controlo, existe uma legenda para indicar a capacidade de segurança a que se destina (NIST 800-53 r4, 2013).

A Secção de Referências apresenta a lista de leis, ordens executivas, diretrizes, políticas, regulamentos, normas e orientações que são relevantes para um controlo de segurança específico. Esta Secção apresenta ainda *sites* pertinentes a utilizar na obtenção de informações adicionais para a implementação do controlo de segurança e a sua avaliação (NIST 800-53 r4, 2013).

A Secção de Prioridade e Afetação de Referência fornece a recomendação de forma prioritária (sequencial) dos códigos, facilitando assim as decisões de sequência durante a implementação do controlo. Esta recomendação ajuda a garantir que os controlos de segurança fundamentais já estão implementados, quando se implementa novos controlos que dependem destes. Este facto garante que as organizações implementem os controlos de uma forma estruturada e oportuna de acordo com os recursos disponíveis. Esta secção fornece ainda as linhas orientadoras da atribuição inicial de controlos e as suas melhorias (NIST 800-53 r4, 2013).

Os controlos fornecidos por esta publicação, fornecem um conjunto de contramedidas e salvaguardas a implementar em SI. De acordo com estes controlos, estão apresentados no Apêndice B, os que foram registados na BD.

## 4.5. Modelo de Análise

De forma a comparar as normas internacionais anteriormente identificadas, o método comparativo será usado com vista a identificar qual delas se usará, de acordo com a análise anteriormente efetuada. Esta comparação tem em vista selecionar uma norma com o intuito de registar os seus controlos, e posteriormente se poder validar a BD. Contudo, a BD desenvolvida permite o registo dos controlos sugeridos pela publicação NIST 800-53 r4 (2013), pela norma ISO/IEC 27001 (2013) e pela publicação SANS (2013).

Para se poder comparar as normas anteriormente descritas, será criado um modelo de análise. Com vista a criar este modelo, numa primeira fase identificar-se-ão quais os critérios a comparar entre as várias normas. Os critérios a comparar são: Apresentam Métricas, Controlos Agrupados, Orientações para Avaliação do Risco, Direitos de Autor,

Explicação da Implementação, Conjunto de Subcontrolos, Flexibilidade de Adaptação e Conjunto de Melhorias (acrescentar funcionalidades).

A Tabela 2 analisa as normas com base no modelo de análise anteriormente descrito. Representa-se com um sinal "+" um aspeto positivo, e com um sinal "-" um aspeto negativo.

**Tabela 2 - Comparação das Normas Internacionais.**

| | | Normas Internacionais (2013) | | |
|---|---|---|---|---|
| | | NIST 800-53 r4 | SANS | ISO/IEC 27001 |
| Categorias | Apresentam Métricas | - | + | - |
| | Controlos Agrupados | Famílias (+) | Prioridades (+) | Famílias (+) |
| | Orientações para Avaliação do Risco. | + | + | - |
| | Direitos de Autor | + | + | - |
| | Explicação da Implementação | + | + | - |
| | Conjunto de Subcontrolos | + | + | - |
| | Flexibilidade de Adaptação | + | + | - |
| | Conjunto de Melhorias (acrescentar funcionalidades) | + | + | - |
| | Total | 7 | 8 | 1 |

**Fonte: Elaboração Própria.**

Com base na Tabela 2, podemos constatar que, de acordo com o modelo de análise proposto, sugere-se que se use os controlos da norma NIST 800-53 r4 (2013), interligando com as métricas apresentadas pela norma SANS (2013).

## 4.6. Identificação dos Requisitos

Com base nas entrevistas[50] conduzidas a três especialistas ligados à segurança da informação e dos SI das suas unidades, foram identificados diversos requisitos a implementar na BD relacional de controlos de segurança da informação.

A Tabela 3 relaciona as entrevistas conduzidas durante a elaboração deste TIA. O código E1, E2 e E3 corresponde aos identificadores[51] dos entrevistados onde, se apresenta a identificação do requisito pelo respetivo entrevistado, isto é, marcado com "x" quando o referido entrevistado identificou o requisito em causa.

[50] Guião da entrevista no Apêndice C.
[51] Foram usados identificadores com vista a garantir a confidencialidade dos entrevistados.

**Tabela 3 - Identificação dos requisitos**

| Requisitos | Entrevistados | | |
|---|---|---|---|
| | E1 | E2 | E3 |
| Quais os controlos de segurança da informação implementados na organização? | X | X | X |
| Quais os controlos de uma norma implementados na organização? | X | X | X |
| Qual o estado dos controlos implementados na organização? | X | X | X |
| Quais os controlos implementados por dimensão? | X | X | X |
| Quais os responsáveis pelos controlos implementados? | X | X | X |
| Quais as datas de cada controlo implementado? | X | X | X |
| Quais as métricas de cada controlo? | X | X | X |
| Quais as lições aprendidas por controlo? | X | X | X |
| Qual a descrição de cada controlo implementado? | X | X | X |

**Fonte: Elaboração Própria.**

Após a análise das entrevistas, e a elaboração da Tabela anteriormente apresentada, pode-se constatar que a BD deve ser desenvolvida com vista a responder aos requisitos previamente identificados, a fim de a implementar nas U/E/O militares do Exército Português.

## 4.7. Conclusão Capitular

Ao longo deste capítulo, "Dimensões, Categorias e Controlos a Implementar", pode-se extrair diversas conclusões apresentadas durante o desenvolvimento do mesmo.

Numa primeira fase, no subcapítulo 4.2. (ISO/IEC 27001), através da análise de um estudo de caso, pode-se constatar as falhas/inoperacionalidades ao nível da segurança da informação. Aqui, é sugerido que as principais dimensões de segurança ao nível da segurança da informação sejam a Física, a Humana, a Tecnológica e por último a Organizacional. Contudo, a Publicação NIST 800-53 r4 (2013), agrupa os controlos por famílias. Ainda, por outro lado, pode perceber-se quais são as categorias de segurança em falta, ou que não se encontram corretamente operacionais, para cada dimensão de segurança de informação implementadas nas U/E/O militares do Exército Português.

Numa segunda fase, sugere-se as principais normas/publicações, e suas vantagens, que propõem os controlos necessários para uma implementação correta de segurança de informação. A norma ISO/IEC 27001 (2013) sugere, em anexo, um conjunto de controlos de segurança de informação organizado por famílias de controlos. Também, o documento SANS (2013) recomenda um conjunto de controlos de segurança de informação com vista a defender os ataques mais preocupantes atualmente, estando estes classificados por

prioridades, podendo dividir-se em: reduzir os ataques conhecidos; abordar uma grande variedade de ataques; identificar e parar os ataques no início de um ciclo. Por último, a publicação NIST 800-53 r4 (2013), sugere um conjunto de controlos de segurança de informação com uma organização e estrutura bem definida, sendo estes agrupados em dezoito famílias distintas.

Em suma, respondendo à primeira questão derivada, "**Quais as principais dimensões de segurança da informação ao nível organizacional?**", esta pode ser respondida com base no estudo de caso identificado anteriormente, onde se sugere a dimensão Física, dimensão Humana, dimensão Tecnológica e a dimensão Organizacional, embora esta categorização não seja unanimemente sugerida por todas as normas.

No que concerne à segunda questão derivada, "**Quais as principais categorias de segurança da informação ao nível organizacional?**", verifica-se neste estudo, que não existe uma classificação de categorias de segurança de informação unanimemente aceite pela indústria, pelos académicos e pelos militares.

Quanto à terceira questão derivada, "**Quais os principais controlos de segurança da informação a implementar numa organização militar?**", sugere-se a implementação dos controlos propostos pela publicação NIST 800-53 r4 (2013), relacionando com as métricas apresentadas na publicação SANS (2013). Isto torna-se possível, uma vez que estes controlos se relacionam com os controlos apresentados pela publicação NIST 800-53 r4 (2013). Contudo, estes controlos identificados, apenas serão registados na BD com vista à sua validação, uma vez que esta também permite o registo de controlos de outras normas identificadas anteriormente.

Por último, quanto à quarta questão derivada, "**Quais os requisitos funcionais necessários a implementar numa base de dados de controlos de segurança da informação a implementar numa organização militar?**", esta foi respondida com base em três entrevistas conduzidas a especialistas de segurança da informação e SI. Estes requisitos estão identificados na Tabela 3, anteriormente apresentada. Perante estes factos, a BD relacional de controlos de segurança da informação, com futura implementação nas U/E/O militares do Exército Português, será desenvolvida com o objetivo de responder eficazmente aos requisitos funcionais previamente identificados.

Após se identificarem os requisitos e os principais controlos a serem registados na BD, no próximo capítulo proceder-se-á à análise e desenho da mesma.

# CAPÍTULO 5. ANÁLISE, DESENHO E IMPLEMENTAÇÃO DA BASE DE DADOS

No decorrer deste capítulo efetua-se a análise e o desenho da BD, isto é, da estrutura necessária que a BD deve contemplar, a fim de responder aos requisitos anteriormente identificados. Para tal, o desenvolvimento da BD divide-se em quatro fases, a análise do sistema, o desenho do sistema, a implementação da base de dados e por último a validação da base de dados.

Tomando como ponto de partida os requisitos já identificados por especialistas da organização militar, na primeira fase identificar-se-ão as tabelas (entidades) e os campos (atributos) necessários a implementar. Posteriormente, é necessário identificar as relações entre as entidades, assim como a obrigatoriedade das mesmas numa determinada relação, que culminará no Modelo E-R.

Na segunda fase, através do Modelo E-R, transitar-se-á para o Modelo Relacional[52], apresentando este uma visão mais simplificada e estruturada da implementação do sistema da BD no SGBD *Microsoft Access*. Torna-se ainda essencial determinar quais são as tabelas que se relacionam com os requisitos já identificados, para posterior implementação.

Seguidamente, na terceira fase, demonstrar-se-á a implementação da BD, assim como a *interface*[53] que esta apresenta.

Na quarta e última fase, apresentar-se-á a validação do sistema, ou seja, confirmar se a BD responde aos requisitos identificados inicialmente.

## 5.1. Análise do Sistema

### 5.1.1. Modelo Entidade-Relação

Como referido anteriormente, no que concerne à estrutura necessária a desenvolver na BD relacional com vista a gerir os controlos de segurança de informação nas U/E/O

[52] Modelo que apresenta as tabelas e as relações a implementar.
[53] *Interface* é definida como um conjunto de meios dispostos com vista a fazer a adaptação entre dois sistemas, neste caso, a adaptação entre o utilizador e a base de dados.

militares do Exército Português, esta deve responder aos requisitos funcionais já identificados. Posto isto, foi elaborado o seguinte Modelo E-R (Figura 10):

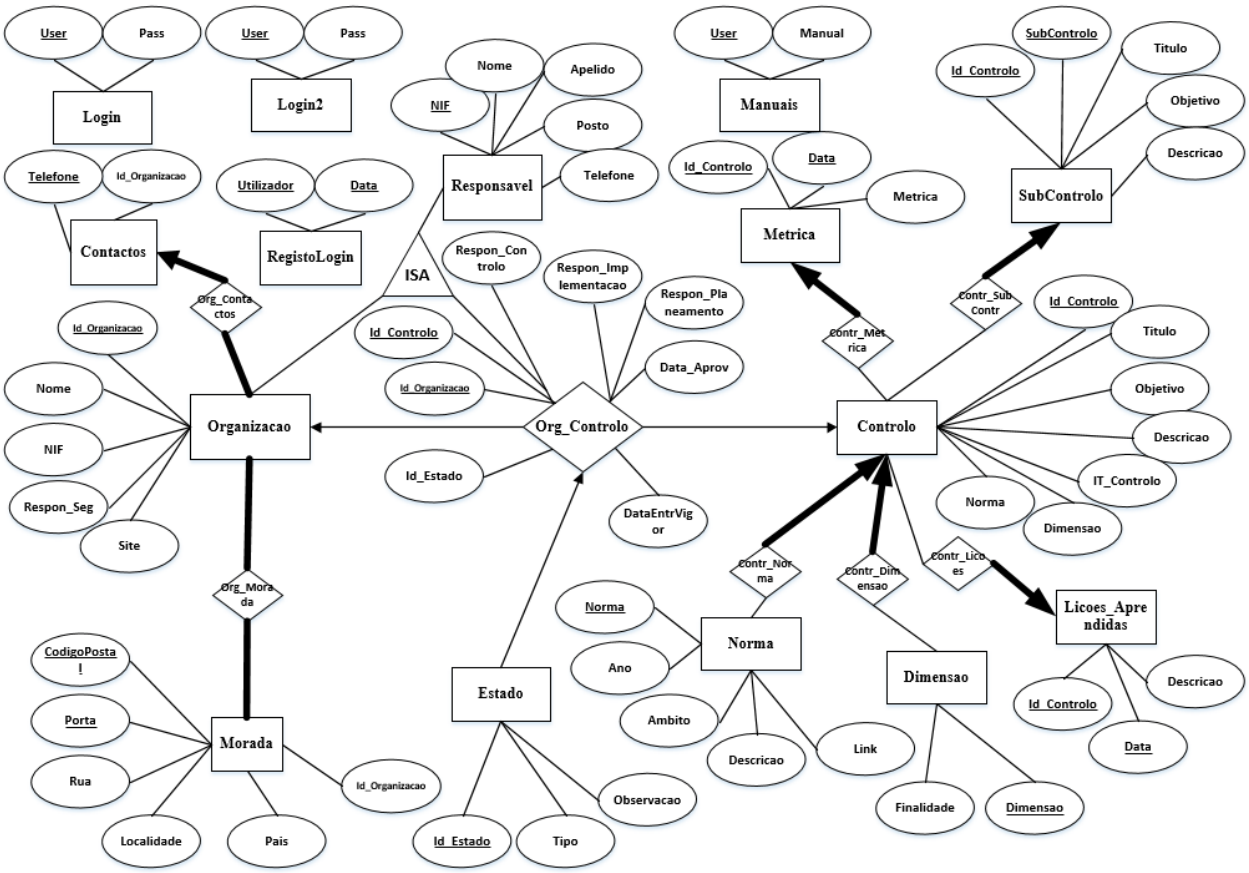


**Figura 10 - Modelo Entidade-Relação.**

**Fonte: Elaboração Própria.**

Este Modelo E-R apresenta as seguintes entidades com os respetivos atributos:

1. Organização (Id_Organização, Nome, NIF, Respon_Seg, *Site*);
2. Morada (Id_Organizacao, CodigoPostal, Porta, Rua, Localidade, País);
3. Contactos (Id_Organizacao, Telefone);
4. Controlo (Id_Controlo, Titulo, Objetivo, Descrição, IT_Controlo, Dimensão, Norma);
5. Metrica (Id_Controlo, Data, Métrica);
6. Estado (Id_Estado, Tipo, Observacao);
7. SubControlo (Id_Controlo, SubControlo, Título, Objetivo, Descrição);
8. Norma (Norma, Ano, Âmbito, Descrição, *Link*, Anexo);

9. Dimensão (Dimensão, Finalidade);
10. Lições_Aprendidas (Id_Controlo, Data, Descrição);
11. Responsável (NIF, Nome, Apelido, Posto, Telefone);
12. Login (*User*, *Pass*);
13. Login2 (*User*, *Pass*);
14. RegistoLogin (Utilizador, Data);
15. Manuais (*User*, Manual).

No ponto de vista do tipo de relações presentes entre as entidades anteriormente identificadas, estas são do tipo:

1. Entre a entidade "Organização" e a entidade "Contactos" (relação Org_Contactos) é do tipo um para muitos (1-para-n), uma vez que uma organização pode ter muitos contactos, mas um contacto apenas pertence a uma organização;
2. Entre a entidade "Organização" e a entidade "Morada*"* (relação Org_Morada) é do tipo um para um (1-para-1), uma vez que uma organização apenas tem uma morada, e uma morada apenas pertence a uma organização;
3. Entre a entidade "Organização" e a entidade "Controlo" (relação Org_Controlo) é do tipo muitos para muitos (n-para-n), uma vez que uma organização pode ter vários controlos implementados, e um controlo pode estar implementado em várias organizações;
4. Entre a entidade "Estado" e a relação "Org_Controlo" é do tipo um para muitos (1-para-n), uma vez que um estado pode pertencer a vários controlos implementados, mas um controlo implementado apenas tem um estado associado;
5. Entre a entidade "Norma" e a entidade "Controlo" (relação Contr_Norma) é do tipo um para muitos (1-para-n), uma vez que uma Norma contém vários controlos, mas um controlo apenas pertence a uma norma;
6. Entre a entidade "Dimensão" e a entidade "Controlo" (relação Contr_Dimensao) é do tipo um para muitos (1-para-n), uma vez que uma dimensão contém vários controlos, mas um controlo apenas pertence a uma dimensão;
7. Entre a entidade "Controlo" e a entidade "Lições_Aprendidas" (relação Contr_Lições) é do tipo um para muitos (1-para-n), uma vez que um controlo pode ter várias lições aprendidas, mas uma Lição aprendida só pertence a um controlo;

8. Entre a entidade “Controlo” e a entidade “SubControlo” (relação Contr_SubContr) é do tipo um para muitos (1-para-n), uma vez que um controlo pode ter vários subcontrolos, mas um subcontrolo apenas pertence a um controlo;
9. Entre a entidade “Controlo” e a entidade “Métricas” (relação Contr_Métrica) é do tipo um para muitos (1-para-n), uma vez que um controlo pode ter várias métricas, mas uma métrica apenas pertence a um controlo.

De acordo com estas relações identificadas previamente, e após a sua análise, pode perceber-se que uma das relações necessita de registar os dados presentes na mesma, contendo assim atributos próprios. A relação existente entre a entidade “Organização” e a entidade “Controlo”, é nomeada de “Org_Controlo” com os seguintes atributos:

1. Org_Controlo (Id_Organização, Id_Controlo, Respon_Controlo, Respon_Implementação, Respon_Planeamento, Data_Aprov, DataEntrVigor, Id_Estado).

No que diz respeito à obrigatoriedade de uma entidade numa determinada relação, está definido da seguinte forma:

1. Na relação “Org_Morada” tanto a entidade “Morada” como a entidade “Organização” são obrigatórias na relação, uma vez que todas as organizações devem ter uma morada associada, e uma morada deve estar associada a uma determinada organização;
2. Na relação “Org_Contactos” tanto a entidade “Organização” como a entidade “Contactos” são obrigatórias na relação, uma vez que todas as organizações devem ter um contacto associado, e um contacto deve estar associado a uma determinada organização;
3. Na relação “Org_Controlos” tanto a entidade “Organização” como a entidade “Controlos” não são obrigatórias na relação, uma vez que podem existir organizações sem controlos implementados, e por outro lado, podem existir controlos que não estejam implementados em nenhuma organização;
4. Na relação “Contr_Norma” a entidade “Controlo” é obrigatória na relação, mas por outro lado, a entidade “Norma” não é obrigatória, uma vez que podem existir normas que não tenham ainda controlos registados, mas todos os controlos têm de estar associados a uma norma;

5. Na relação "Contr_Dimensão" a entidade "Controlo" é obrigatória na relação, mas por outro lado, a entidade "Dimensão" não é obrigatória, uma vez que podem existir dimensões que não tenham ainda controlos associados, mas todos os controlos têm de estar associados a uma dimensão;
6. Na relação "Contr_Lições" a entidade "Controlo" não é obrigatória na relação, mas por outro lado, a entidade "Lições_Aprendidas" é obrigatória, uma vez que podem existir controlos que não tenham ainda lições aprendidas associadas, mas todas as lições aprendidas têm de estar associadas a um controlo;
7. Na relação "Contr_SubContr" a entidade "Controlo" não é obrigatória na relação, mas por outro lado, a entidade "SubControlo" é obrigatória, uma vez que podem existir controlos que não tenham subcontrolos associados, mas todos os subcontrolos têm de estar associados a um controlo;
8. Na relação "Contr_Métrica" a entidade "Controlo" não é obrigatória na relação, mas por outro lado, a entidade "Métrica" é obrigatória, uma vez que podem existir controlos que não tenham ainda métricas associadas, mas todas métricas têm de estar associados a um controlo.

### 5.1.2. Modelação

De acordo com a análise do Modelo E-R anteriormente identificado (Figura 10), podemos atestar que a estrutura de BD apresentada se encontra na 5FN.

Uma vez que todas as tabelas, desta BD, apresentam os seus atributos definidos em domínios que englobem apenas valores atómicos, ou seja, não possuam conjuntos de conjuntos, pode-se assim afirmar que estas se encontram na 1FN (Carriço & Carriço, 1998).

Por outro lado, pode constatar-se ainda que todas as tabelas se encontram na 2FN, uma vez que todos os atributos que não pertencem à chave, dependem da chave através de uma dependência funcional elementar. Isto é, dependem da chave e não dependem de nenhum dos seus elementos ou subconjuntos isoladamente (Carriço & Carriço, 1998).

Quanto à 3FN, esta condição compreende que as tabelas estejam na 2FN, e ainda que nenhum dos atributos que não fazem parte da chave for funcionalmente dependente de qualquer combinação dos restantes, evitando assim a dependência transitiva. Resumindo, todos os atributos de uma tabela que não pertençam à chave devem ser mutuamente independentes, ou seja, devem poder ser atualizados independentemente uns dos outros

(Carriço & Carriço, 1998). Com a análise do Modelo E-R, podemos constatar que todas as tabelas se encontram na 3FN.

No que concerne à FNBC, este estado verifica que os únicos determinantes das tabelas são as chaves candidatas. Observando as tabelas do Modelo E-R, podemos certificar que esta condição é alcançada.

Ainda, no que diz respeito às formas normais, podemos assegurar que as tabelas presentes na BD garantem a condição da 4FN, uma vez que as únicas multidependências elementares são os atributos que são definidos pela chave (Carriço & Carriço, 1998).

Por último, no respeitante á 5FN, podemos observar que a única tabela passível de ainda ser decomposta pelas chaves candidatas é a tabela Org_Controlo. Se observarmos a tabela Org_Controlo, se esta for decomposta em duas projeções (pelas chaves externas), isto é, na projeção (Organização, Controlo) e na projeção (Controlo, Estado), aquando da operação de junção não é possível obter a tabela original. Contudo, se for decomposta em três projeções (Organização, Controlo), (Controlo, Estado) e (Organização, Estado), aquando da operação de junção, já se obtém a tabela original. Posto isto, podemos afirmar que a tabela Org_Controlo apresenta uma dependência de junção das suas projeções (Organização, Controlo), (Controlo, Estado) e (Organização, Estado). Agora, numa visão geral da BD, como não é possível encontrar dependências de junção que não sejam implicadas pelas chaves, então não é possível proceder a uma decomposição das tabelas. Visto isto, podemos então afirmar que as tabelas se encontram na 5FN, uma vez que "(…) qualquer dependência de junção é implicada pelas chaves candidatas" (Carriço & Carriço, 1998, p. 396).

Em suma, com esta estrutura alcançada, na 5FN, podemos afirmar que as tabelas e os atributos se encontram na forma mais adequada e estruturada, com vista a evitar redundâncias desnecessárias, evitando assim problemas com a inserção, eliminação e atualização dos dados (Carriço & Carriço, 1998).

## 5.2. Desenho do Sistema

De acordo com a Análise do Sistema descrita no subcapítulo precedente, e do Modelo E-R apresentado, neste subcapítulo pretende-se desenvolver o desenho do sistema, deduzindo assim o Modelo Relacional (Figura 11).

Também, ainda neste subcapítulo, explicar-se-á como os requisitos identificados anteriormente serão implementados na BD. Para tal, recorrer-se-á ao Modelo Relacional do sistema, que seguidamente se apresentará (Figura 11).

### 5.2.1. Modelo Relacional

No que diz respeito às entidades com os respetivos atributos, estas materializar-se-ão em tabelas, onde os seus atributos são os campos. Visto isto, transitando do Modelo E-R para o Modelo Relacional, as entidades representam as tabelas mantendo assim os seus atributos.

Como referido no subcapítulo prévio, no que concerne às relações presentes entre as entidades apresentadas, apenas uma necessita de registar a relação. Ou seja, a associação "Org_Controlo" é a única associação que se materializará numa tabela, registando assim os dados relativos a essa mesma associação.

Após uma análise do Modelo E-R, podemos então transitar para o Modelo Relacional. Este modelo é apresentado na Figura 11.

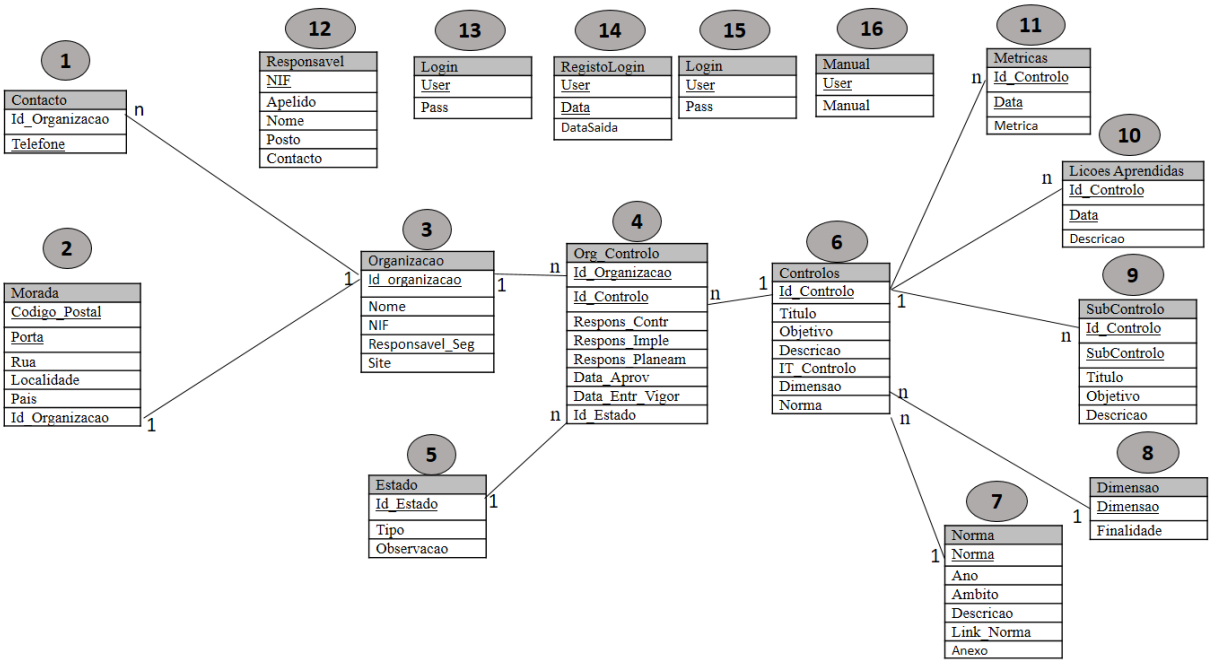


**Figura 11 - Modelo Relacional.**

**Fonte: Elaboração própria.**

Neste modelo, todas as tabelas estão numeradas com vista a possibilitar uma explicação simples no que concerne à forma como a BD responde aos requisitos identificados previamente.

### 5.2.2. Requisitos

No que concerne aos requisitos identificados anteriormente, estes serão respondidos, isto é, validados, recorrendo a consultas (*Queries*), onde a Tabela 4 identifica quais as entidades (tabelas referenciadas na Figura 11) necessárias para que se responda aos mesmos.

**Tabela 4 - Requisitos a implementar.**

| Requisitos | Tabelas utilizadas |
|---|---|
| Quais os controlos de segurança da informação implementados na organização? | 4 |
| Quais os controlos de uma norma implementados na organização? | 4 e 6 |
| Qual o estado dos controlos implementados na organização? | 4 |
| Quais os controlos implementados por dimensão? | 6 |
| Quais os responsáveis pelos controlos implementados? | 4 |
| Quais as datas de cada controlo implementado? | 4 |
| Quais as métricas de cada controlo? | 11 |
| Quais as lições aprendidas por controlo? | 10 |
| Qual a descrição de cada controlo implementado? | 6 |

**Fonte: Elaboração própria.**

Após a implementação da BD, estes requisitos serão materializados em relatórios, onde o utilizador da BD a qualquer momento poderá consultar determinado requisito, estando sempre atualizado.

## 5.3. Implementação da Base de Dados

Após a análise do Modelo Relacional apresentado no subcapítulo anterior, pode perceber-se qual é a estrutura da BD após a sua implementação. O desenho do sistema, de acordo com o Modelo Relacional já referido, é apresentado na Figura 12.

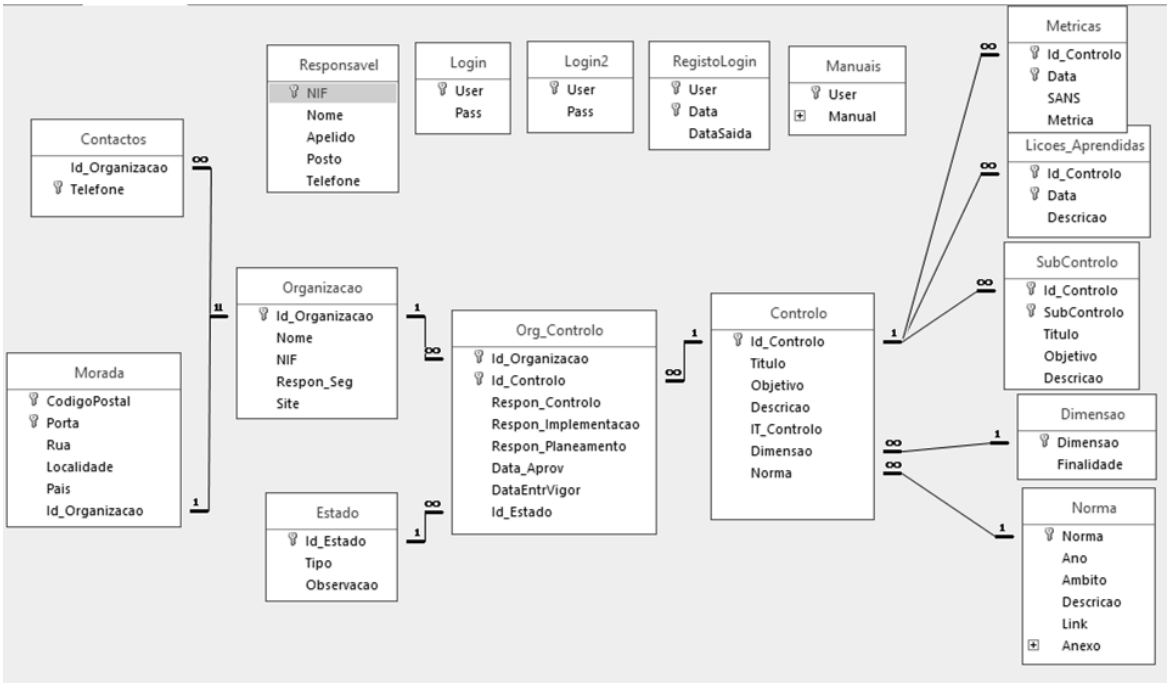


**Figura 12 – Desenho do Sistema.**

**Fonte: Elaboração própria.**

Pode-se constatar no desenho do sistema (Figura 12), que serão implementados no SGBD *Microsoft Access* 16 tabelas. Das tabelas que apresentam relações entre elas, são do tipo 1 para muitos (1 – ∞) assim como do tipo 1 para 1 (1 – 1).

A estrutura da BD apresentada no desenho do sistema ostenta as tabelas e respetivas relações de acordo com o Modelo Relacional referido anteriormente. No entanto, só a implementação das entidades com as respetivas relações não é suficiente para uma fácil utilização da BD.

Posto isto, uma BD além da estrutura relacional, deve apresentar ainda uma interface compreensível que facilite a interação dos utilizadores com a BD. Posto isto, a BD em anexo apresenta um manual de utilizador e de administrador, onde se explica a interface desenvolvida.

Esta BD ostenta uma série de menus dinâmicos, interligados entre si, que estão representados na Figura 13, fornecendo uma vista integrada e completa das suas ligações.

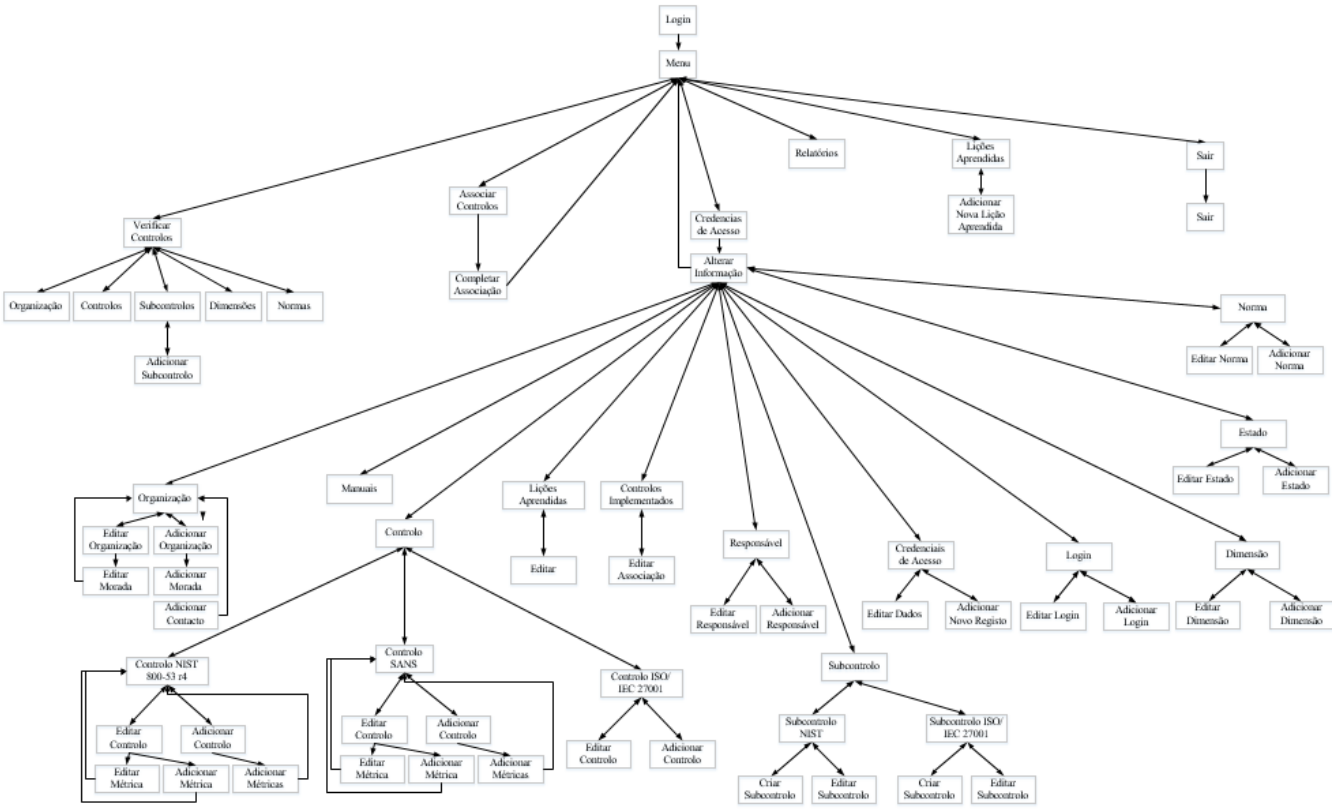


**Figura 13 – Esquematização dos Menus.**

**Fonte: Elaboração Própria.**

A Figura 13, apresenta uma visão geral da ligação entre os menus, podendo-se observar vários percursos que o utilizador/administrador pode efetuar dentro das opções disponíveis. Nesta figura, as setas apresentadas diferenciam os possíveis sentidos a serem percorridos, isto é, uma seta bidirecional remete para um percurso em que é possível voltar atrás. Por outro lado, as setas unidirecionais apenas permitem percorrer o percurso respetivo no sentido por estas indicado.

No que concerne aos requisitos funcionais identificados, na Tabela 6 do Apêndice B pode verificar-se que a BD foi desenvolvida com vista a responder a esses requisitos funcionais, respondendo deste modo à quarta questão derivada de investigação.

Apresenta-se de seguida na Figura 14, alguns menus da *interface* da BD para o utilizador. Estes pretendem somente transmitir uma visão geral da sua implementação. Contudo, pode-se analisar com mais detalhe todos os menus no Manual de Administrador e no Manual de Utilizador em Anexo à BD.


**Figura 14 - Figura Representativa da Base de Dados**

**Fonte: Elaboração Própria.**

Na implementação da BD, foram registados um conjunto de dados. Estes estão identificados no Apêndice B (DADOS INTRODUZIDOS NA BASE DE DADOS).

## 5.4. Validação da Bases de Dados

Procurou-se ao longo da implementação da BD, testar a correta inserção, alteração e remoção de dados das tabelas (testes parcelares). Em aditamento a este facto, esta foi submetida a testes finais (estudo exploratório), nomeadamente no que concerne ao registo de dados, consulta de dados, alteração/eliminação de dados, resposta dos requisitos implementados e facilidade de utilização da interface.

Embora os testes não tenham sido exaustivos e não tenham seguido nenhuma metodologia especial, pode-se afirmar que:

1. No que diz respeito ao teste do registo de dados, foram introduzidos dados em todas as entidades presentes na BD, verificando assim que todas as entidades têm os seus atributos definidos em domínios coerentes com o tipo de dados. Também se confirmou que todas as CP e CE foram bem definidas, podendo-se garantir que não é possível adicionar um registo relativo a um atributo que não existe;

2. No respeitante ao teste da consulta de dados, a *interface* desenvolvida permite consultar todos os dados registados na BD, assim como, através dos relatórios implementados é possível consultar estes mesmos dados;
3. Também no teste de alteração/eliminação de dados, através da *interface* desenvolvida é possível editar ou eliminar qualquer registo presente na BD. Ainda, no que diz respeito a este teste, aquando da eliminação de dados, podemos perceber que todas as imposições de integridade referencial foram bem definidas, uma vez que ao eliminar um determinado registo, a BD elimina todos os dados que dizem respeito a esse mesmo registo, garantindo-se assim que não existem dados sem correspondência lógica;
4. Por outro lado, no que toca ao teste dos requisitos implementados, como referido anteriormente, estes foram materializados em relatórios. Testando os relatórios identificados na Tabela 11 do Apêndice B, pôde-se então verificar que cada uma retoma os dados respeitantes ao requisito em causa. Posto isto, podemos então perceber que os relatórios em causa foram desenvolvidos de acordo com a necessidade de cada requisito;
5. Por último, no teste de desempenho da interface apresentada, foram verificados os seguintes aspetos: (i) ao testar a alteração, inserção ou remoção dos dados, utilizando a interface apresentada, constatou-se que esta satisfaz plenamente a sua função; (ii) ao submeter a aplicação, para utilização, a cinco aspirantes do 5º ano da AM, validou-se a sua simplicidade de acordo com os seus *feedbacks*; (iii) por fim, ao submeter a aplicação a testes por um utilizador especializado, Tenente-Coronel Silva (docente da Unidade Curricular Base de Dados ministrada na AM), esta foi validada pelo seu *feedback* de "funcional". Visto isto, podemos então confirmar que a interface apresentada permite gerir corretamente todos os dados registados na BD em causa.

Em suma, de acordo com os resultados obtidos nos testes, podemos então afirmar que esta BD está desenvolvida de acordo com as necessidades identificadas anteriormente, garantindo assim a sua eficácia. Contudo, uma vez que estes testes (estudo exploratório) foram limitados a uma amostra por conveniência[54], apesar desta demonstrar ser eficaz no que concerne aos requisitos funcionais identificados previamente, não podemos assim generalizar esta eficácia a todas as U/E/O militares do Exército Português.

[54] Desenvolvedor da BD, cinco aspirantes da AM e docente da Unidade Curricular Base de Dados.

# CONCLUSÕES E RECOMENDAÇÕES

Com este estudo, pretende-se identificar os requisitos necessários e suficientes para implementar numa BD relacional de controlos de segurança da informação para U/E/O militares do Exército Português, que permita auditar um sistema de gestão de segurança da informação implementado. Esta investigação aplicada tem ainda a finalidade de criar essa mesma base de dados relacional, em *Microsoft Access*, a fim de possibilitar a sua implementação nas U/E/O militares do Exército Português.

Na revisão de literatura realizada verificou-se que não existe um modelo ou método de gestão de segurança da informação, que apresente uma visão integrada das diversas dimensões de segurança do Exército Português. Este facto remete para a elevada necessidade de uma gestão de segurança da informação nas U/E/O militares eficiente e eficaz, uma vez que um dos seus objetivos principais é garantir a superioridade de informação. Atualmente, a importância da segurança da informação nas organizações militares tem crescido devido ao desenvolvimento das doutrinas de Ciberdefesa (por exemplo na OTAN e EUA), conhecidas também como Operações Centradas em Rede de Computadores. Devido a este facto, torna-se indispensável planear e implementar uma *baseline* de controlos de segurança da informação e de SI.

Para a adoção de um SGSI adequado, as organizações, especialmente a militar, devem ter em consideração um conjunto de normas internacionais e de boas práticas de segurança da informação e de SI, nomeadamente a norma internacional ISO/IEC 27001 de gestão de segurança da informação (2013), a norma nacional dos EUA com a designação de NIST 800-53 r4 (2013) e a *framework* de controlos críticos de Ciberdefesa proposta pela SANS (2013).

Em suma, a garantia da segurança da informação é realizada através da implementação de um conjunto de controlos de segurança físicos, técnicos, humanos e administrativo que visam garantir a confidencialidade, a disponibilidade e a integridade da informação. Nas U/E/O militares do Exército Português é necessário planear e implementar uma *baseline* de controlos de segurança, os quais devem ser monitorizados e auditados após a sua implementação de modo a simultaneamente garantir a obtenção e a partilha de lições aprendidas. Esta *baseline* de controlos de segurança da informação

pretende-se materializar numa BD relacional de controlos de segurança da informação com vista a gerir os controlos implementados nas U/E/O militares do Exército Português.

Por forma a alcançar a temática desta investigação, anteriormente identificada, o estudo procura responder às quatro questões derivadas de investigação propostas. De acordo com a primeira questão derivada: "**Quais as principais dimensões de segurança da informação ao nível organizacional?**", constata-se da revisão de literatura que as principais dimensões são: a Física, a Humana, a Tecnológica e a Organizacional, embora esta categorização não seja unanimemente sugerida por todas as normas internacionais e nacionais.

No que concerne à segunda questão derivada: "**Quais as principais categorias de segurança da informação ao nível organizacional?**", verifica-se neste estudo através da revisão de literatura realizada, que não existe uma classificação de categorias de segurança de informação unanimemente aceite pela indústria, pelos académicos e pelos militares. Deste modo e tendo em consideração que o fundamental para a monitorização e auditoria são os controlos de segurança, considera-se que este assunto embora relevante, não é fundamental para alcançar o objetivo central do estudo, isto é, para identificar os requisitos e posterior a análise, desenho e implementação de uma BD que permita gerir todos os controlos de segurança de informação, implementados e planeados para uma U/E/O militar do Exército Português.

Quanto à terceira questão derivada: "**Quais os principais controlos de segurança da informação a implementar numa organização militar?**", sugere-se a implementação dos controlos propostos na publicação NIST 800-53 r4 (2013), relacionando estes com os controlos referenciados na *framework* de controlos críticos propostos pela SANS (2013).

Por fim, no respeitante à quarta e última questão derivada: "**Quais os requisitos funcionais necessários a implementar numa base de dados de controlos de segurança da informação a implementar numa organização militar?**", esta foi respondida com base em três entrevistas conduzidas a especialistas de segurança da informação. Os requisitos necessários a implementar numa BD relacional de controlos de segurança da informação para U/E/O militares do Exército Português estão identificados na Tabela 3 do capítulo 4.

Resumindo, no que concerne à resposta da questão central, "**Quais os requisitos necessários a implementar numa base de dados relacional de controlos de segurança**

**da informação para U/E/O militares do Exército Português?**", a sua resposta foi obtida a partir das respostas às quatro questões derivadas de investigação anteriormente referidas. Tendo este estudo como *outputs* principais de investigação: (i) o Modelo E-R; (ii) o Modelo Relacional; (iii) e a BD *Microsoft Access* implementada.

Após, a implementação da BD de controlos de segurança da informação de acordo o com o Modelo em Cascata Revisto o *software* foi testado com vista a validar a sua funcionalidade de acordo com os requisitos funcionais obtidos.

A BD responde às necessidades identificadas, no entanto não se pode generalizar a sua eficiência a todas as U/E/O militares do Exército Português, uma vez que este estudo foi conduzido tendo por base uma amostra de conveniência, isto é, os requisitos funcionais foram identificados com base em três especialistas do Exército Português.

Este estudo, embora responda às questões de investigação inicialmente definidas e apresente *outputs* de investigação bem definidos e suportados em disciplinas académicas de referência (e.g. Base de Dados, Segurança de Informação e de Sistemas de Informação) apresenta algumas limitações, face ao tempo disponível para a sua execução, nomeadamente: (i) No que concerne à interface desenvolvida para acesso à BD pelos utilizadores, não foram explorados os critérios que esta deveria contemplar na sua implementação com vista a caracterizar-se melhor a sua simplicidade e tornar-se mais intuitiva para os seus utilizadores; (ii) Os requisitos não funcionais, não foram contemplados na realização deste estudo e na implementação da BD (e.g. segurança, desempenho); (iii) Com a BD implementada não se garante resposta a todos os requisitos funcionais das U/E/O militares do Exército Português, no entanto em virtude da existência do Modelo Relacional seguir as formas normais não se prevê dificuldades na sua ampliação, ou seja, no aumento do número de tabelas/campos atuais.

Deste modo e tendo em consideração as limitações apresentadas, os trabalhos a realizar futuramente no âmbito deste estudo, passam por resolver as limitações identificadas. Dado o repentino desenvolvimento na área dos sistemas de informação, verificado nas últimas décadas, e o consequente despontar de uma panóplia de novas ameaças que lhe são inerentes, urge cada vez mais a necessidade de explorar a área da ciberdefesa, para isso, deixa-se assim um estímulo com vista ao desenvolvimento desta temática.

# BIBLIOGRAFIA


AAP-6. (2008). *NATO Gossary of Terms and Definitions.*

Carriço, R. F., & Carriço, J. A. (1998). *Desenho de bases de Dados e linguagem SQL em Access.* Lisboa: CTI Edições.

Carvalho, J. E. (2009). *Metodologia do Trabalho Científico. "Saber Fazer" da investigação para dissertações e teses.* Lisboa: Escolar Editora.

FM3-13. (2003). *Information Operations: Doctrine, Tactics, Techniques, and Procedures.* Washington: Headquarters, Departament of the Army.

Freixo, M. J. (2011). *Metodologia Científica: Fundamentos, Métodos e Técnicas.* Lisboa: Instituto Piaget.

Gil, A. C. (2008). *Métodos e Técnicas de pesquisa social.* editora atlas.

Howard, N. (2013). Intention Awareness Theory in Information Risk Engineering: Contrived Balance in Integrating Information Assurance and Situation Awareness. *Journal of Information Assurance and Security*, 9-16.

ISO/IEC 27001. (2013). *Tecnologia de informação - Tecnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos.*

Martins, J., Santos, H. d., Nunes, P., & Silva, R. (2012a). Modelo de Segurança da Informação para Organizações Militares em Ambiente de Guerra da Informação. *11th European Conference on Information Warfare and Security*, (pp. 172-179). Laval, França.

Martins, J., Santos, H. d., Nunes, P., & Silva, R. (2012b). Framework de Gestão de Segurança da Informação para Organizações Militares Orientada pelos Principais Vetores de Ataque. *Conferência Anual da Associação Portuguesa de Sistemas de Informação* (pp. 239-265). Lisboa: Academia Militar.

Martins, J., Santos, H. d., Rosinha, A., & Valente, A. (Janeiro de 2013). Information Security - Military Standards versus ISO 27001. Em R. Kuusisto, & E. Kurkinen, *Proceedings of the 12th European Conference on Information Warfare and Security* (pp. 191-200). Filandia.

Mattar, F. N. (2012). *Pesquisa de Markting.* Rio de Janeiro: Elsevier Editora Ltda.

NIST 800-53 r4. (2013). *Security and Privacy Controls for Federal Information Systems and Organizations, NIST 800-53 r4.*

Pfleeger, C. P., & Pfleeger, S. L. (2006). *Security in Computing.* Estados Unidos da América: Prentice Hall.

SANS. (2013). *Critical Controls for Effective Cyber Defense.*

SANS, I. (26 de Abril de 2016). *CIS Critical Security Controls*. Obtido de SANS: *https://www.sans.org/critical-security-controls*

Santos, L., Monteiro, F., Lima, J., Silva, N., Silva, J., & Afonso, C. (2014). *Orientações metodológicas para a elaboração de trabalhos de investigação.* Lisboa.

Silva, A., & Videira, C. (2001). *UML, Metodologias e Ferramentas CASE*. Porto: Centro Atlântico.

Sommerville, I. (1995). *Software Engineering, Nine Edition.* Estados Unidos da América: Person.

Yourdon, E. (1990). *Análise Estruturada Moderna - Tradução da Terceira Edição Americana.* Rio de Janeiro: Campus.

# APÊNDICES

# APÊNDICE A – LINHAS ORIENTADORAS PARA ESTABELECER UM SGSI

Como referido no capítulo 1.1, para o estabelecimento de um SGSI adequado, este deve passar por uma rigorosa fase de planeamento, implementação, manutenção e melhoramento do mesmo. Para tal, de acordo com a norma ISO/IEC 27001 (2013) e a publicação NIST 800-53 r4 (2013), algumas boas práticas, serão sugeridas e deverão ser tidas em consideração pelas organizações.

De acordo com a norma ISO/IEC 27001 (2013), para alcançar os resultados pretendidos ao nível do SGSI, é necessário determinar as questões internas e externas à organização que afetam esta finalidade. Para que tal aconteça, deve-se (ISO/IEC 27001, 2013):

1. Compreender a organização e o seu contexto;
2. Compreender as necessidades e expetativas das partes interessadas (perceber quais são as partes interessadas relevantes para o SGSI, e quais são os seus requisitos);
3. Determinar o âmbito do sistema de gestão de segurança da informação.

No âmbito da implementação de um SGSI apropriado, torna-se necessário que a organização cumpra algumas boas práticas, sendo que parte delas estão explanadas na norma ISO/IEC 27001 (2013), nomeadamente:

1. "A gestão de topo deve demonstrar liderança e comprometimento para com o sistema de gestão de segurança da informação" (ISO/IEC 27001, 2013, p. 7), onde a política e os objetivos da segurança da informação e os requisitos do SGSI são compatíveis com a orientação estratégica da organização; a organização, deve promover a melhoria contínua, assegurar que o SGSI atinge os resultados pretendidos, e orientar os colaboradores para contribuir para a eficácia do SGSI; e comunicar a importância de uma Gestão de Segurança da Informação eficaz e em conformidade com os requisitos do SGSI;
2. A gestão de topo deve estabelecer uma política de segurança da informação que vai de encontro à intenção da organização, inclui os objetivos de segurança da informação e abarca um compromisso para satisfazer os requisitos aplicáveis que são relacionados com a segurança da informação;

3. "A gestão de topo deve assegurar que são atribuídas e comunicadas as responsabilidades e autoridades para funções que são relevantes para a segurança da informação" (ISO/IEC 27001, 2013, p. 8).

Também ao nível do planeamento do SGSI, torna-se necessário efetuar um rigoroso estudo. Para isso, a organização deve determinar os requisitos a implementar, assim como determinar os riscos e as oportunidades, de forma a assegurar que o SGSI possa atingir os resultados pretendidos, evitar ou reduzir os efeitos indesejáveis, e de forma a atingir uma melhoria contínua (ISO/IEC 27001, 2013).

No que concerne ao risco, a organização deve estabelecer e manter os critérios de aceitação do risco, e os critérios para realizar avaliações do risco de segurança da informação. Para isso, é necessário garantir que as constantes avaliações do risco de segurança da informação produzem resultados consistentes, válidos e comparáveis (ISO/IEC 27001, 2013). Em suma, a norma ISO/IEC 27001 (2013) sugere que se faça uma identificação, análise e avaliação dos riscos de segurança da informação.

Segundo a norma ISO/IEC 27001 (2013), quando se trata do tratamento do risco de segurança da informação, a organização deve definir e aplicar um processo de tratamento do risco de segurança da informação, com o propósito de:

1. Selecionar as opções apropriadas de tratamento do risco de segurança da informação (de acordo com os resultados da avaliação do risco);
2. Determinar quais os controlos necessários a implementar, de modo a tratar o risco de segurança da informação apurado;
3. Produzir um plano de tratamento do risco de segurança da informação.

De acordo com a publicação NIST 800-53 r4 (2013), as organizações estão cada vez mais dependentes de serviços de SI externos[55] à organização. Estes serviços externos podem ser providenciados por: entidades dentro da organização, mas fora dos limites de autorização de segurança organizacional; entidades fora da organização[56]; ou combinação entre opções públicas e privadas. O grau de confiança das organizações em usar serviços externos à mesma, pode ser aceitável ou não, dependendo da confiança que as organizações colocam nessas entidades externas. Normalmente, o nível de confiança é

[55] Estes serviços de sistemas de informação externos são serviços de tecnologia de informação implementados, fora dos limites de autorização de segurança das organizações, para os seus sistemas de informação. Estes serviços externos incluem, por exemplo, o uso de arquitetura orientada a serviços, serviços orientados em nuvem (*cloud*) ou operações de *data center*.
[56] Estas entidades podem pertencer ao sector público ou ao sector privado.

baseado na quantidade de organizações que a entidade externa presta serviço, no que diz respeito ao emprego de controlos de segurança e à sua eficácia. Este facto leva a que a organização faça uma análise do nível de aceitação de risco, avaliando se este se encontra dentro da tolerância organizacional. Se o nível de aceitação do risco não se encontra dentro da tolerância organizacional, a publicação sugere algumas ações, das quais se destacam (NIST 800-53 r4, 2013):

1. Mitigar o risco, empregando controlos de compensação[57];
2. Transferir o risco através de um seguro, cobrindo eventuais perdas;
3. Evitar o risco, optando por não obter o serviço de determinadas entidades.

Como sugere a publicação, o termo confiança[58] ao nível dos SI não é alcançado como resultado da interação de um conjunto de sistemas confiáveis, mas sim de uma interação complexa entre entidades. Os SI de confiança são sistemas em que se acredita serem capazes de operar dentro de uma tolerância de risco definida, apesar de erros humanos, falhas estruturais ou ataques intencionais.

De modo a aumentar a força da funcionalidade de segurança, a publicação NIST 800-53 r4 (2013) sugere que os desenvolvedores dos sistemas de segurança, empreguem essa funcionalidade como parte do desenvolvimento do *software*, *hardware* ou *firmware*, criando: políticas de segurança bem definidas, técnicas estruturadas de *design* e desenvolvimento, princípios de segurança de engenharia sólidos. Também, é sugerido ainda, que se executem testes periódicos de segurança por organizações independentes, documentando[59] todo o conteúdo do teste, contribuindo para determinar a eficácia dos controlos de segurança implementados.

De acordo com os vários níveis e funções relevantes dentro da organização, devem ser estabelecidos objetivos de segurança da informação para cada um deles. Os objetivos de segurança da informação devem: ser sólidos com a política de segurança da informação, ser mensuráveis, ser comunicados[60], ter em atenção os requisitos de segurança da informação aplicáveis (assim como os resultados da avaliação do risco) e ser atualizados. Em suma, para ser possível atingir os objetivos definidos anteriormente, a organização

[57] Controlo de compensação pode ser o exemplo de encriptar as informações armazenadas em *clouds*, aumentando a segurança da informação.
[58] O termo confiança, define-se pela crença de que uma entidade irá comportar-se de uma forma previsível durante a execução de funções específicas.
[59] Esta documentação pode incluir relatórios de falhas, registo de ações de correção, os resultados dos relatórios de incidentes de segurança, e os resultados das atividades de monitorização das organizações.
[60] Devem ser comunicados a quem de direito.

deve para cada objetivo determinar o que será feito, que recursos serão necessários, quem será o responsável, quando estará concluído, e como os resultados serão avaliados (ISO/IEC 27001, 2013).

Em relação à seleção dos recursos necessários para o estabelecimento, implementação, manutenção e melhoria contínua do SGSI, a organização deve (ISO/IEC 27001, 2013):

1. Determinar quais as competências necessárias dos seus colaboradores, que influenciam o seu desempenho de segurança da informação;
2. Garantir que os seus colaboradores são competentes (de acordo com uma educação apropriada, formação ou experiência);
3. Sempre que necessário, realizar ações[61] a fim de obter as competências necessárias;
4. Documentar toda a informação que seja apropriada como prova de competência.

Para além da competência dos colaboradores da organização, seja ela através da educação, formação ou experiencia, a organização deve ter um papel importante na consciencialização dos mesmos. De acordo com a norma ISO/IEC 27001 (2013) os colaboradores devem estar cientes:

1. Da política de segurança da informação;
2. Do que podem contribuir para a eficácia[62] do SGSI;
3. Do que compromete a não correspondência com o SGSI.

Como referido anteriormente, toda a informação do âmbito da segurança da informação deve estar documentada a fim de se garantir como prova de competência. Esta documentação deve incluir, entre outras, a informação determinada pela organização[63] como sendo imprescindível para a eficácia do SGSI, como por exemplo os resultados das avaliações do risco de segurança de informação. Para criar e atualizar a informação documentada, a organização deve assegurar de forma apropriada uma identificação e descrição[64], um formato[65] e suporte de dados[66], e uma revisão e aprovação da sua aplicabilidade e adequação. Resumindo, "a organização deve manter a informação

[61] Estas ações podem ser, entre outras, formação ou orientação. Contudo, sempre que se torne necessário, deve-se reafectar colaboradores já existentes ou contratar novas pessoas com as competências necessárias.
[62] Inclui os benefícios que podem promover à organização (ao SGSI).
[63] Esta informação, determinada pela própria organização, pode ter extensões distintas de acordo com as suas particularidades, uma vez que depende da dimensão da mesma, do seu tipo de atividades, processos, produtos e serviços. Depende ainda da competência dos seus colaboradores.
[64] Por exemplo título, data, autor ou número de referência.
[65] Por exemplo idioma, versão do *software*, gráficos, entre outros.
[66] Por exemplo papel ou informático.

documentada, na extensão necessária para poder ter confiança que os processos foram executados conforme planeado" (ISO/IEC 27001, 2013, p. 12).

Relativamente à avaliação de desempenho de segurança da informação e à eficácia do SGSI, a organização deve, entre outros pontos, determinar (ISO/IEC 27001, 2013):

1. O que necessita de ser monitorizado e medido (incluindo os processos e controlos de segurança da informação);
2. Os métodos[67] para monitorizar, medir, analisar e avaliar;
3. Quando e quem deve efetuar a monotorização e medição;
4. Quando e quem deve analisar e avaliar os resultados da monotorização e medição.

Além da monitorização, medição, análise e avaliação, a organização deve ainda orientar auditorias internas, previamente planeadas, com o intuito de verificar se o SGSI está em conformidade com os requisitos da própria organização, e se o SGSI está implementado e mantido com eficácia. Resumindo, a organização deve rever o SGSI em intervalos planeados para assegurar a sua contínua aplicabilidade, adequabilidade e eficácia (ISO/IEC 27001, 2013).

Quando alguma alteração é detetada na avaliação/revisão do SGSI, que comprometa o mesmo, a organização deve de imediato reagir à inconformidade, sendo que, para isso, deve empreender ações[68] para controlar e corrigir a alteração, assim como lidar com as suas consequências. Após ser implementada a ação corretiva, deve-se determinar as causas da inconformidade; se pode ocorrer novamente inconformidades análogas; rever a eficácia das ações corretivas empregues; e proceder (caso se determine a sua necessidade) a alterações ao SGSI (ISO/IEC 27001, 2013).

Também, para fazer face a alguma alteração que possa colocar em causa o SGSI, a publicação NIST 800-53 r4 (2013), recomenda a cooperação dos proprietários, deste sistema, com vista a entender as mudanças das missões/negócios organizacionais, do ambiente operacional e como os sistemas são utilizados, de forma a adaptar rapidamente os controlos implementados no SGSI (NIST 800-53 r4, 2013).

Em suma, "a organização deve melhorar de forma contínua a aplicabilidade, adequabilidade e eficácia do sistema de gestão de segurança da informação" (ISO/IEC 27001, 2013, p. 15).

[67] Os métodos selecionados, para serem válidos, devem gerar resultados comparáveis e reproduzíveis.
[68] As ações corretivas devem ser apropriadas aos efeitos das inconformidades detetadas.

No que diz respeito à implementação de um SGSI, determinar o conjunto apropriado de controlos de segurança eficaz de modo a garantir uma adequada segurança de informação é um desafio significativo para as organizações. Para cada situação, existe um determinado controlo a implementar, ou seja, não existe, portanto, um conjunto de controlos capaz de abordar todas as preocupações de segurança da informação em todas as situações. A organização tem a importante tarefa de selecionar o conjunto mais adequado de controlos de segurança de informação para uma situação específica de forma a mitigar adequadamente o risco. Esta tarefa requer uma compreensão aprofundada das prioridades da organização, de modo a que a segurança da informação garanta mais eficazmente a confidencialidade, a integridade e a disponibilidade de SI (NIST 800-53 r4, 2013).

Contudo, antes de se selecionar os controlos necessários para garantir a segurança de SI organizacional, a Publicação NIST 800-53 r4 (2013), sugere-nos que as organizações determinem o grau de criticidade e sensibilidade da informação organizacional (categorização de segurança) que é processada, armazenada ou transmitida. O resultado desta categorização servirá de apoio para a seleção dos controlos adequados de segurança de informação (NIST 800-53 r4, 2013).

Resumindo, para se estabelecer um SGSI, a organização deve colocar em execução um conjunto de boas práticas ao nível da segurança da informação. Estas linhas orientadoras explanadas anteriormente devem ser analisadas pelos gestores de topo das organizações, adaptando-as sempre que necessário.

# APÊNDICE B – DADOS INTRODUZIDOS NA BASE DE DADOS

Como referido no capítulo 5, no que concerne aos requisitos identificados anteriormente, estes foram implementados no menu "Relatórios" da BD. A Tabela 6 relaciona os requisitos com os relatórios que respondem aos mesmos.

**Tabela 5 - Implementação dos requisitos.**

| Requisitos | Nome do Relatório |
|---|---|
| Quais os controlos de segurança da informação implementados na organização? | Controlos implementados numa Organização. |
| Quais os controlos de uma norma implementados na organização? | Controlos da organização por norma. |
| Qual o estado dos controlos implementados na organização? | Estado dos controlos implementados. |
| Quais os controlos implementados por dimensão? | Controlos por dimensão da Organização. |
| Quais os responsáveis pelos controlos implementados? | Responsáveis de controlo por Organização. |
| Quais as datas de cada controlo implementado? | Datas de controlo por Organização. |
| Quais as métricas de cada controlo? | Métricas dos controlos. |
| Quais as lições aprendidas por controlo? | Lições aprendidas por controlo. |
| Qual a descrição de cada controlo implementado? | Descrição dos controlos. |

**Fonte: Elaboração Própria.**

Contudo, além dos relatórios, apresentados na tabela precedente, que respondem aos requisitos identificados, ainda outros relatórios foram implementados na BD que poderão ser usados pelo utilizador.

Agora, no que diz respeito aos dados introduzidos na BD, esta já apresenta alguns dados relativamente à entidade Estado, Norma, Dimensão, Controlos, Subcontrolos e Métricas.

No que concerne aos dados relativos ao estado de um controlo, estes foram introduzidos previamente uma vez que são atributos pré-definidos, ou seja, são comuns a todos os controlos, abrangendo assim todos os dados necessários à entidade. Estes dados estão representados na Tabela 7.

**Tabela 6 - Dados introduzidos na entidade Estado.**

| Estado | | |
|---|---|---|
| Id_Estado | Tipo | Observação |
| 1 | Planeado | O controlo encontra-se planeado na Organização. |
| 2 | Implementado | O controlo encontra-se implementado na Organização. |
| 3 | Aprovado | O controlo encontra-se aprovado na Organização. |
| 4 | Em Vigor | O controlo encontra-se em vigor na Organização. |
| 5 | Não Previsto | O controlo não está previsto para a Organização. |

**Fonte: Elaboração Própria.**

No que diz respeito aos dados relativos à entidade Norma, estes foram introduzidos previamente uma vez que, esta BD, foi projetada para agrupar controlos relativos à norma ISO/IEC 27001 (2013), à norma NIST 800-53 r4 (2013), e por último à norma SANS (2013). Posto isto, já estão assim introduzidos todos os dados possíveis desta entidade. Estes dados estão apresentados na Tabela 8.

**Tabela 7 - Dados introduzidos na entidade Norma.**

| Norma | | | | | |
|---|---|---|---|---|---|
| Norma | Ano | Âmbito | Descrição | Link Norma | Anexo |
| ISO/IEC 27001 | 2013 | Controlos de segurança da informação. | Sistemas de gestão de segurança da informação - Requisitos. | (Link) | (Documento em anexo). |
| NIST 800-53 r4 | 2013 | Controlos de segurança da informação. | *Security and Privacy Controls for Federal Information Systems and Organizations.* | (Link) | (Documento em anexo). |
| SANS | 2013 | Controlos de segurança da informação. | *Critical Controls for Effective Cyber Defence.* | (Link) | (Documento em anexo). |

**Fonte: Elaboração Própria.**

Relativamente aos dados referentes à entidade Dimensão, estes foram introduzidos previamente uma vez que, no decorrer deste trabalho, as principais dimensões ao nível da segurança da informação já foram identificadas, contemplando assim a maior parte dos controlos de segurança da informação. Os dados relativos a esta entidade estão demostrados na Tabela 9.

**Tabela 8 - Dados introduzidos na entidade Dimensão.**

| Dimensão | |
|---|---|
| Dimensão | Finalidade |
| Humana | Conjunto de controlos humanos. |
| Física | Conjunto de controlos físicos. |
| Tecnológica | Conjunto de controlos tecnológicos. |
| Organizacional | Conjunto de controlos organizacionais. |

**Fonte: Elaboração Própria.**

No que concerne à entidade Controlos, Subcontrolos e Métricas, uma lista com alguns controlos, respetivos subcontrolos e respetivas métricas foram registadas na BD. A lista desses controlos e subcontrolos encontra-se na Tabela 10.

**Tabela 9 - Lista de Controlos e Subcontrolos registados na Base de Dados**

| Controlo | Subcontrolo | Título do Subcontrolo |
|---|---|---|
| AC-17 | AC-17(01) | *Automated Monitoring/Control* |
| | AC-17(02) | *Protection of Confidentiality/Integrity Using Encription* |
| | AC-17(03) | *Managed Access Control Points* |
| | AC-17(04) | *Privileged Commands/Access* |
| | AC-17(05) | *Monitoring for Unauthorized Connections* |
| | AC-17(06) | *Protection of Information* |
| | AC-17(07) | *Additional Protection for Security Function Access* |
| | AC-17(08) | *Disable Nonsecure Network Protocols* |
| | AC-17(09) | *Disconnect/Disable Access* |
| AC-18 | AC-18(01) | *Authentication and Encryption* |
| | AC-18(02) | *Monitoring Unauthorized Connections* |
| | AC-18(03) | *Disable Wireless Networking* |
| | AC-18(04) | *Restrict Configurations by Users* |
| | AC-18(05) | *Antennas/Transmission Power Levels* |
| CM-01 | N/D | N/D |
| CM-02 | CM-02(01) | *Reviews and Updates* |
| | CM-02(02) | *Automation Support for Accuracy/Currency* |
| | CM-02(03) | *Retention of Previous Configuration* |
| | CM-02(04) | *Unauthorized Software* |
| | CM-02(05) | *Authorized Software* |
| | CM-02(06) | *Development and Tests Environments* |
| | CM-02(07) | *Configure Systems, Components, or Devices for High-Risk Areas* |
| CM-03 | CM-03(01) | *Automated Document/Notification/Prohibition of Changes* |
| | CM-03(02) | *Test/Validate/Document Changes* |
| | CM-03(03) | *Automated Change Implementation* |
| | CM-03(04) | *Security Representative* |
| | CM-03(05) | *Automated Security Response* |
| | CM-03(06) | *Cryptography Management* |
| CM-05 | CM-05(01) | *Automated Access Enforcement/Auditing* |
| | CM-05(02) | *Review System Changes* |
| | CM-05(03) | *Signed Components* |
| | CM-05(04) | *Dual Autorization* |
| | CM-05(05) | *Limit Production/Operational Privileges* |
| | CM-05(06) | *Limit Library Privileges* |

| | | |
|---|---|---|
| | CM-05(07) | *Automatic Implementation of Security Safeguards* |
| CM-06 | CM-06(01) | *Automated Central Management/Application/Verification* |
| | CM-06(02) | *Respond to Unauthorized Changes* |
| | CM-06(03) | *Unauthorized Change Detection* |
| | CM-06(04) | *Conformance Demonstration* |
| CM-07 | CM-07(01) | *Periodic Review* |
| | CM-07(02) | *Prevent Program Execution* |
| | CM-07(03) | *Registration Compliance* |
| | CM-07(04) | *Unauthorized Software/Blacklisting* |
| | CM-07(05) | *Authorized Software/Whitelisting* |
| CM-08 | CM-08(01) | *Updates During Installations/Removals* |
| | CM-08(02) | *Automated Maintenance* |
| | CM-08(03) | *Automated Unauthorized Component Detection* |
| | CM-08(04) | *Accountability Information* |
| | CM-08(05) | *No Duplicate Accounting of Components* |
| | CM-08(06) | *Assessed Configurations/Approved Deviations* |
| | CM-08(07) | *Centralized Repository* |
| | CM-08(08) | *Automated Location Tracking* |
| | CM-08(09) | *Assignment of Components to System* |
| CM-09 | CM-09(01) | *Assignment of Responsability* |
| PM-05 | N/D | N/D |
| PM-06 | N/D | N/D |
| RA-03 | N/D | N/D |
| RA-05 | RA-05(01) | *Update Tool Capability* |
| | RA-05(02) | *Update by Frequency/Prior to New Scan/When Identified* |
| | RA-05(03) | *Breadth/Depth of Coverage* |
| | RA-05(04) | *Discoverable Information* |
| | RA-05(05) | *Privileged Access* |
| | RA-05(06) | *Automated Trend Analyses* |
| | RA-05(07) | *Automated Detection and Notification of Unauthorized Components* |
| | RA-05(08) | *Review Historic Audit Logs* |
| | RA-05(09) | *Penetration Testing and Analyses* |
| SA-01 | N/D | N/D |
| SA-03 | N/D | N/D |
| SA-04 | SA-04(01) | *Functional Properties of Security Controls* |
| | SA-04(02) | *Design/Implementation Information for Security Controls* |
| | SA-04(03) | *Development Methods/Techniques/Practices* |
| | SA-04(04) | *Assignment of Components to Systems* |
| | SA-04(05) | *System/Component/Service Configurations* |
| | SA-04(06) | *Use of Information Assurance Products* |
| | SA-04(07) | *NIAP-Approved Protection Profiles* |
| | SA-04(08) | *Continuous Monitoring Plan* |
| | SA-04(09) | *Functions/Ports/Protocols/Services in Use* |
| | SA-04(10) | *Use of Approved Piv Products* |
| SA-08 | N/D | N/D |
| SC-09 | N/D | N/D |
| SC-18 | SC-18(01) | *Identify Unacceptable Code/Take Corrective Actions* |
| | SC-18(02) | *Acquisition/Development/Use* |
| | SC-18(03) | *Prevent Downloading/Execution* |
| | SC-18(04) | *Prevent Automatic Execution* |
| | SC-18(05) | *Allow Execution Only in Confined Environments* |
| SC-24 | N/D | N/D |
| SC-26 | SC-26(01) | *Detection of Malicious Code* |
| SI-03 | SI-03(01) | *Central Management* |
| | SI-03(02) | *Automatic Updates* |
| | SI-03(03) | *Non-Privileged Users* |
| | SI-03(04) | *Updates Only by Privileged Users* |

| | | |
|---|---|---|
| | SI-03(05) | *Portable Storage Devices* |
| | SI-03(06) | *Testing/Verification* |
| | SI-03(07) | *Nonsignature-Based Detection* |
| | SI-03(08) | *Detect Unauthorized Commands* |
| | SI-03(09) | *Authenticate Remote Commands* |
| | SI-03(10) | *Malicious Code Analysis* |
| SI-04 | SI-04(01) | *System-Wide Intrusion Detection System* |
| | SI-04(02) | *Automated Tools For Real-Time Analysis* |
| | SI-04(03) | *Automated Tool Integration* |
| | SI-04(04) | *Inbound and Outbound Communications Traffic* |
| | SI-04(05) | *System-Generated Alerts* |
| | SI-04(06) | *Restrict Non-Privileged Users* |
| | SI-04(07) | *Automated Response to Suspicious Events* |
| | SI-04(08) | *Protection of Monitoring Information* |
| | SI-04(09) | *Testing of Monitoring Tools* |
| | SI-04(10) | *Visibility of Encrypted Communications* |
| | SI-04(11) | *Analyze Communications Traffic Anomalies* |
| | SI-04(12) | *Automated Alerts* |
| | SI-04(13) | *Analyze Traffic/Event Patterns* |
| | SI-04(14) | *Wireless Intrusion Detection* |
| | SI-04(15) | *Wireless to Wireline Communications* |
| | SI-04(16) | *Correlate Monitoring Information* |
| | SI-04(17) | *Integrated Situational Awareness* |
| | SI-04(18) | *Analyze Traffic/Covert Exfiltration* |
| | SI-04(19) | *Individuals Posing Greater Risk* |
| | SI-04(20) | *Privileged User* |
| | SI-04(21) | *Probationary Periods* |
| | SI-04(22) | *Unauthorized Network Services* |
| | SI-04(23) | *Host-Based Devices* |
| | SI-04(24) | *Indicators of Compromise* |
| SI-07 | SI-07(01) | *Integrity Checks* |
| | SI-07(02) | *Automated Notifications of Integrity Violations* |
| | SI-07(03) | *Centrally-Managed Integrity Tools* |
| | SI-07(04) | *Tamper-Evident Packing* |
| | SI-07(05) | *Automated Response to Integrity Violations* |
| | SI-07(06) | *Cryptographic Protection* |
| | SI-07(07) | *Integration of Detection and Response* |
| | SI-07(08) | *Auditing Capability for Significant Events* |
| | SI-07(09) | *Verify Boot Process* |
| | SI-07(10) | *Protection of Boot Firmware* |
| | SI-07(11) | *Confined Environments With Limited Privileges* |
| | SI-07(12) | *Integrity Verification* |
| | SI-07(13) | *Code Execution in Protected Environments* |
| | SI-07(14) | *Binary or Machine Executable Code* |
| | SI-07(15) | *Code Authentication* |
| | SI-07(16) | *Time Limit on Process Execution W/O Supervision* |
| SI-10 | SI-10(01) | *Manual Override Capability* |
| | SI-10(02) | *Review/Resolution of Errors* |
| | SI-10(03) | *Predictable Behavior* |
| | SI-10(04) | *Review/Timing Interactions* |
| | SI-10(05) | *Restrict Inputs to Trusted Sources and Approved Formats* |

**Fonte: Elaboração Própria**

Contudo, mesmo com a introdução prévia destes dados, a BD desenvolvida ao longo deste trabalho, permite alterar qualquer informação relativa a estas entidades, fazendo face a qualquer alteração de determinada doutrina/norma.

## APÊNDICE C – GUIÃO DE ENTREVISTA

**ACADEMIA MILITAR**

**TRABALHO DE INVESTIGAÇÃO APLICADA**

"Base de dados relacional de controlos de segurança da informação"

**GUIÃO DE ENTREVISTA**

A presente entrevista é um instrumento válido de apoio à análise científica que se enquadra no Trabalho de Investigação Aplicada (TIA), que é parte integrante do mestrado em Ciências Militares do curso de Infantaria, da Academia Militar. Tem como tema "Base de dados relacional de controlos de segurança da informação", e tem como objetivo geral de estudo, **identificar as principais dimensões, categorias e controlos de segurança da informação ao nível organizacional. Neste trabalho pretende-se ainda identificar os requisitos funcionais necessários a implementar numa base de dados relacional de controlos de segurança da informação para U/E/O militares do Exército Português.**
Dada a sua experiencia sobre a temática, a sua participação voluntária nesta entrevista, representará uma ajuda fundamental e uma mais-valia para a elaboração deste trabalho.

**Muito obrigado pela sua colaboração**

**Tiago Gaspar**
**Aspirante de Infantaria**
**Lisboa, maio de 2016**

Antes de começar a entrevista gostaria de saber se tem alguma dúvida acerca do trabalho e sobre a entrevista?

**Nome:_____**

**Cargo / Posto:_____ Função:_____**

**Unidade/local: _____ Distrito:_____**

**Data:_____**

No desenvolvimento deste Trabalho de Investigação Aplicada (TIA), pretende-se identificar quais as dimensões, categorias e controlos de segurança de informação necessários a implementar numa U/E/O militar do Exército Português. A finalidade deste TIA é construir uma base de dados relacional de controlos de segurança de informação que visa gerir todos os controlos de segurança de informação implementados numa U/E/O militar do Exército Português.

Com o objetivo de identificar os requisitos[69] necessários a implementar, na base de dados anteriormente descrita, esta entrevista está divida em duas fases.

Inicialmente, na primeira fase, pretende-se comprovar a necessidade dos requisitos já identificados. Para tal, pedimos que dê a sua opinião se cada um dos requisitos é indispensável ou não à base de dados.

Por último, numa segunda fase, pretende-se que sugira novos requisitos que, no seu ponto de vista, sejam oportunos implementar.

[69] Questões a que a base de dados deverá responder.

**Fase 1 – Comprovação da necessidade dos requisitos a seguir sugeridos**

Para responder a esta necessidade, pretende-se que coloque uma cruz (X) no quadrado correspondente à necessidade, ou não, do requisito.

**Tabela 10 - Identificação dos Requisitos a Implementar**

| Requisitos a implementar | Oportuno | |
|---|---|---|
| | Sim | Não |
| Quais os controlos de segurança da informação implementados na organização? | | |
| Quais os controlos de uma norma implementados na organização? | | |
| Qual o estado dos controlos implementados na organização? | | |
| Quais os controlos implementados por dimensão? | | |
| Quais os responsáveis pelos controlos implementados? | | |
| Quais as datas de cada controlo implementado? | | |
| Quais as métricas de cada controlo? | | |
| Quais as lições aprendidas por controlo? | | |
| Qual a descrição de cada controlo implementado? | | |

**Fonte: Elaboração Própria.**

**Fase 2 – Sugestão de novos requisitos**

No seu ponto de vista é necessário implementar outros requisitos? Quais?

**Muito obrigado pela sua colaboração.**

**Tiago Gaspar**

**Aspirante de Infantaria**

# ANEXOS

# ANEXO A – ESTUDO DE CASO

**Tabela 11 - Principais cenários de métodos de ataque.**

| *Attacker* | *Threat* | *Action* | *Tools* | *Targets* | *Vulnerabilities* | *Properties of Information* | *Operational Effect* |
|---|---|---|---|---|---|---|---|
| *Amateur* | *Interception* | *Physical* | *Physical Means* | *Facilities and Equipment* | *Physical* | *Confidentiality* | *Information Collection* |
| *Professional* | *Interruption* | *Electronic Deception* | *Means of Psychological Operations* | *People* | *Human* | *Integrity* | *Protection* |
| *Organization* | *Modification* | *Electronic Attack* | *Electromagnetic Means* | *Physical Documents* | *Processes* | *Availability* | *Intrusion* |
| *State* | *Fabrication* | *HUMINT* | *Means of Capture Sounds* | *Electromagnetic Spectrum* | *Design* | | *Destruction* |
| *Internal* | *Destruction* | *IMINT* | *Means of Intelligence* | *Sound Waves* | *Implementation* | | *Simulation* |
| *Natural Disasters* | *Disclosure* | *SIGINT* | *Information Exchange* | *Communication Devices* | *Configuration* | | *Financial* |
| | | *MASINT* | *User Command* | *Storage Devices* | | | |
| | | *OSINT* | *Script or Program* | *Account* | | | |
| | | *TECHINT* | *Autonomous Agent* | *Process* | | | |
| | | *Counter Intelligence* | *Toolkit* | *Information* | | | |
| | | *Observe* | *Distributed Tool* | *Component* | | | |
| | | *Perception Managing* | *Data Tap* | *Computer* | | | |
| | | *Probe* | | *Network* | | | |
| | | *Scan* | | *Internetwork* | | | |
| | | *Flood* | | | | | |
| | | *Authenticate* | | | | | |
| | | *Bypass* | | | | | |
| | | *Spoof* | | | | | |
| | | *Read* | | | | | |
| | | *Copy* | | | | | |
| | | *Steal* | | | | | |
| | | *Modify* | | | | | |
| | | *Delete* | | | | | |

**Fonte: Martins, Santos, Rosinha & Valente, 2013, p.5 adaptado de Martins, Santos, Nunes & Silva (2012a).**

**Tabela 12 - Categorias de Segurança de informação da Dimensão Organizacional.**

| *Organizational Dimension* | | | |
|---|---|---|---|
| *Code of Ethics* | *Principles, Requirements and Expectations* | *Information Security Plan* | *Information Security Policy* |
| *Classification of Information and Assets* | *Risk Acceptance Criteria* | *Incident Scenarios Model* | *Disciplinary Sanctions* |
| *Communication Channels* | *Intelligence Reports* | *Certified Companies* | *Project Management* |
| *Information Security Policies* | *Identification of Critical Assets* | *Information Security Process* | *Information Security Responsibilities* |
| *Identification and Risk Assessment* | *Baselines of Information Security* | *Coordination Between Levels of Organization* | *Registration of Event and Reports* |
| *Monitoring of Information Security* | *Incident Response Procedures* | *Information Security Audits* | *Planning and Acceptance of New System* |
| *Operational Procedures* | *Forensic Analysis* | *Business Continuity Management* | *Outdoor Activities* |

**Fonte: Martins, Santos, Rosinha & Valente, 2013, p.8 adaptado de Martins et al (2012a).**

**Tabela 13 - Categorias de Segurança de informação da Dimensão Física.**

| *Physical and Environmental Dimension* | | | |
|---|---|---|---|
| *Facilities Security* | *Barriers to Physical Security* | *Physical Access Control* | *Security Areas* |
| *Personal of Service* | *Data center Security* | *Critical Infrastructure Security* | *Security of Meeting Rooms and Offices* |
| *Strong-Houses, Furniture, Containers and Locks* | *Inspections of Electrical & Electronic Materials* | *Security of Supplies and Equipment* | *Emergency Plan* |
| *Protection of Eavesdropping, Observations and Radiation* | *Maintenance of physical Facilities* | | |
| *Handling of Material and Classified Equipment of Physical Support* | | | |
| *Classification* | *Preparation* | *Reproduction* | *Guard* |
| *Distribution and Transfer* | *Maintenance* | *Reclassification and Declassification* | *Destruction* |

**Fonte: Martins, Santos, Rosinha & Valente, 2013, p.8 adaptado de Martins et al (2012a).**

**Tabela 14 - Categorias de Segurança de informação da Dimensão Humana.**

| *Human Dimension* | | | |
|---|---|---|---|
| *Prior to Employment* | *During Employment* | *Termination or Change of Employment* | *Military Accreditation* |
| *Skills, Training and Awareness* | *Personal of Security* | *Behavior in Public, Contacts with Public Authorities and Media* | |

**Fonte: Martins, Santos, Rosinha & Valente, 2013, p.9 adaptado de Martins et al (2012a).**

**Tabela 15 - Categorias de Segurança de informação da Dimensão Tecnológica.**

| *Dimension Technology* | | | |
|---|---|---|---|
| *Logical Access Control* | *Storage, Handling and Information Retrieval* | *Mobiles of Data Storage* | *Transmission Means* |
| *Data Communication Protocols* | *Systems and Services* | *Network Topologies* | *Internet and Remote Access* |
| *Networking Technologies* | *Mobiles Communications* | *Computers, Components and Peripherals* | *Network Active* |
| *Network Attached and Storage Area Network* | *Exchange of Information* | *Systems Event Management* | *Security Technologies* |
| *Management and Monitoring of Network* | *Active Security* | *Models of Software Development* | *Standards for Software Development* |
| *Programing Languages* | *Correct Processing in Applications* | *Application Development* | *Application Support* |
| *Cryptographic Controls* | *Implementation, Configuration and Maintenance Application* | *Source Code Analysis* | *Types and Data Formats* |
| *Software Use by Employees* | *Maintenance of IS and Communications* | *Licensing and Classification Software* | |

**Fonte: Martins, Santos, Rosinha & Valente, 2013, p.10 adaptado de Martins et al (2012a).**