TÉCNICO LISBOA

UMA ARQUITETURA DE INFORMAÇÃO PARA O QUADRO NACIONAL DE REFERÊNCIA PARA A CIBERSEGURANÇA

Edna Stella Batista Quaresma

Dissertação para obtenção do Grau de Mestre em
Engenharia de Telecomunicações e Informática

Orientadores: Prof. André Ferreira Ferrão Couto e Vasconcelos
Prof. José Luís Brinquete Borbinha

Júri

Presidente: Prof. Ricardo Jorge Fernandes Chaves
Vogal: Prof. André Ferreira Ferrão Couto e Vasconcelos
Vogal: Prof. Paulo Jorge Tavares Guedes

Dezembro 2021

Para as minhas filhas Carolina e Mariana

Agradecimentos

Agradeço primeiro e acima de tudo às minhas filhas, por me permitirem hipotecar as suas vidas em troca de uma promessa. São a minha maior inspiração. Agradeço ao meu marido, pela paciência, pelo amor.

Agradeço ao meu co-orientador Professor José Borbinha, por partilhar o conhecimento sem soberba, pela paciência, por ter mantido a razão quando eu a perdi, pela oportunidade que criou para que me apaixonasse pela cibersegurança. Ao meu orientador Professor André Vasconcelos pelo conhecimento, pela partilha, pelo método e principalmente pela tranquilidade que transmite acreditando em mim e nos outros alunos por igual.

Mais me importa que saibam, que agradeço de coração e de cabeça, à minha mãe Oyá, que alimenta a minha coragem, a minha fé e a minha força. Que não me permite desistir e que nunca me abandona. Epahey Oyá!

Resumo

A segurança da informação e cibersegurança, são preocupações transversais a organizações de todos os setores e áreas de negócio. Normas e standards que uniformizam medidas adaptáveis à realidade de cada país crescem globalmente garantindo a cooperação de todos no combate ao cibercrime.

Em Portugal, o Centro Nacional de Cibersegurança traduz a implementação destas informações de referência no Quadro Nacional de Referência para a Cibersegurança (QNRCS). O foco desta dissertação é compreender e simplificar a implementação das medidas descritas neste documento.

Mediante a existência de um conjunto de evidências de implementação previstas pelo documento, e integrando técnicas de arquitetura empresarial, consolidou-se a procura por uma arquitetura de informação que expresse o contexto do QNRCS.

Definir com clareza a lista destas evidências, permitiu o desenvolvimento de uma ferramenta que permite aferir o estado de implementação dos processos de segurança numa organização, facilitando a determinação do estado *AS-IS* ou a construção duma visão *TO-BE* quanto à cibersegurança ou segurança da informação das organizações, de acordo com a regulação europeia, no âmbito das medidas ISO 27001, da Diretiva (UE) n.º 2016/1148, entre outras normas e standards.

Como resultado, contribui-se objetivamente através da identificação unívoca das evidências de implementação e da elaboração uma possível arquitetura da informação, que facilita o mapeamento da informação existente numa organização, com a requerida pelo documento em estudo, e apresenta-se uma demonstração de resultados através de um caso de estudo.

Palavras-chave: Cibersegurança, Segurança da Informação, QNRCS, CNCS, Arquitetura de Informação.

Abstract

Information security and cybersecurity are cross-cutting concerns for organizations from all sectors and business areas. Norms and regulation to standardize measures suitable to the reality of each country, are globally growing, guaranteeing cooperation in the fight against cybercrime.

In Portugal, the National Cybersecurity Center translates the implementation of this reference information into the National Cybersecurity Framework of Reference (QNRCS). The focus of this dissertation is to understand and simplify the implementation of the measures described in this document.

Through the existence of a set of implementation evidences foreseen by the document, and integrating enterprise architecture techniques, the search for an information architecture that expresses the QNRCS context was consolidated.

Clearly defining the list of these evidences, allowed the development of a tool enabling the assessment of the implementation status over the security processes of an organization, thus facilitating the determination of *AS-IS* status or the construction of a *TO- BE* vision, regarding cybersecurity or information security of organizations, in accordance with European regulation, within the scope of ISO 27001 measures, of Directive (EU) No. 2016/1148, among other norms and standards.

As a result, an objective contribution is made, through the unambiguous identification of implementation evidence and the elaboration of a possible information architecture that facilitates the mapping of existing information in an organization with that required by the document under study, providing a demonstration of results through a case study .

Keywords: Cybersecurity, Information Security, QNRCS, CNCS, Information Architecture.

Conteúdo

Lista de Figuras

Lista de Tabelas

1 Introdução

No início de 2013, nos Estados Unidos da América, iniciou-se a criação de um modelo de cibersegurança, com o propósito de aumentar a segurança de infraestruturas críticas. Esta responsabilidade a cargo do *National Institute of Standards and Technology* (NIST), resultou na criação da *Cyber Security Framework* (CSF) em 2014, com as premissas Identificar, Proteger, Detetar, Responder e Recuperar, e foi adotada por organizações de todos as áreas.

Na mesma altura a União Europeia (UE), denota crescentes ameaças de segurança decorrentes de falha técnica, não intencional, erro humano ou ataque malicioso deliberado, podendo afetar serviços essenciais de fornecimento de eletricidade, transportes, água, saúde, e outras infraestruturas digitais cuja disrupção é considerada crítica. Nesse sentido, à semelhança da *CSF Framework*, foi criada em 2016 a *Network and Information Systems (NIS) Directive*, tornando-se parte da lei em 2018. Os estados membros da UE, ficaram assim obrigados a adotar uma estratégia nacional para a segurança das redes e sistemas de informação, orientados por esta diretiva. A referida estratégia, deve incluir a criação de uma Autoridade Nacional Competente, um *Single Point of Contact*(SPOC) para cooperação entre fronteiras e um *Computer Security Incident Response Team* (CSIRT) com a responsabilidade de monitorizar incidentes a nível nacional, integrando a rede de cooperação europeia de equipas de resposta a incidentes.

Em Portugal, foi criado o Centro Nacional de Cibersegurança (CNCS) para o efeito, sendo o órgão responsável pela transposição da *NIS Directive* para o cenário nacional, resultando na criação do Quadro Nacional de Referência para a Cibersegurança (QNRCS). A complexidade do documento, levanta a necessidade de simplificar ou guiar a sua implementação. Este trabalho propõe uma abordagem possível para o efeito, intercalando conceitos de arquitetura empresarial, com particular foco na *Phase C: Information Architecture (Data)* da metodologia TOGAF ADM.

Nesse sentido, esta investigação tem como base uma análise detalhada do QNRCS, sobre o qual propõe a identificação de forma clara e inequívoca, de uma lista de documentos, que materializa o conjunto de evidências de implementação, das medidas de mitigação expressas pelo QNRCS. Após análise das informações de referência que suportam as subcategorias do QNRCS foi possível apresentar uma lista das referidas evidências, tratá-las como Entidades de Informação (EI), e de acordo com o método TOGAF ADM, apresentar num quadro (ou modelo), uma proposta de arquitetura de informação, que está de acordo com o contexto definido no QNRCS, dando também enquadramento aos processos COBIT 5 considerados no documento em estudo.

A investigação realizada, pretende oferecer uma contribuição objetiva, tanto para organizações em fase de projeto, como para organizações que já tenham implementado as medidas referidas no QNRCS. O modelo que resulta deste estudo, deve servir para guiar organizações em fase inicial da implementação das medidas de mitigação de risco, assim como, para validação nos casos em que as organizações já tenham a implementação da estratégia de segurança de acordo com o QNRCS. Como resultado pretende-se um suporte objetivo no desenvolvimento da arquitetura de informação, ou adequação de uma arquitetura existente, sempre com base na documentação que representa prova ou evidência da implementação das medidas já referidas.

1.1 Motivação

A implementação da uma arquitetura empresarial que contempla a cibersegurança em Portugal, tem como referencial a seguir o QNRCS. Este documento, transpõe as diretivas europeias de cibersegurança para o âmbito nacional, incluindo a implementação de medidas mitigação de risco. Estas medidas são

agrupadas pelos objetivos identificar, proteger, detetar, responder e recuperar de ameaças contra a segurança da informação e cibersegurança, de organizações públicas e privadas.

É cada vez mais evidente para as organizações, a necessidade de uma arquitetura empresarial de referência, que favoreça a implementação dos requisitos, de acordo com a regulamentação e legislação. De acordo com o QNRCS, a gestão de risco é fortemente suportada pela gestão de incidentes, que por sua vez depende da existência e análise constante de ocorrências, ou seja, de registos. Estes registos fazem parte do conjunto de documentos que representam entidades de informação, e que em conjunto com outros documentos estruturais como estratégias, planos ou políticas, formam a arquitetura de informação definida pelo QNRCS. Apesar do reconhecimento de que, a gestão de incidentes de segurança de informação é cada vez mais considerada pelas organizações, existem poucas certezas sobre qual o modelo a implementar para garantia de uma gestão eficiente da informação.

A principal motivação desta investigação, é contribuir para que as organizações possam rever a sua arquitetura de informação, oferecendo alguma certeza quanto ao cumprimento dos principais requisitos do QNRCS. Será apresentado um caso de estudo, tendo como alvo a Agência para a Modernização Administrativa (AMA), um instituto público responsável pela promoção e desenvolvimento da modernização administrativa em Portugal, que representa uma boa referência na Administração Pública, quanto ao seu sistema de gestão da segurança da informação. O método proposto será portanto testado com esta organização.

1.2 Contexto e Análise do Problema

O Quadro Nacional de Referência para a Cibersegurança, define medidas de segurança da informação que geram documentos ao ser implementadas. Estes documentos representam as evidências de implementação das medidas expressas no QNRCS.

As referidas evidências, são igualmente referidas no Quadro de Avaliação de Capacidades de Cibersegurança (QACC), um documento complementar ao QNRCS para a cibersegurança, onde se definem três níveis de capacidade para cada medida de cibersegurança definida pelo QNRCS. As evidências de implementação das medidas, encontram-se assim distribuídas pelos três níveis definidos, permitindo assim medir o nível de segurança de uma organização.

Os níveis de capacidade definidos neste documento, encontram-se descritos na tabela da figura 1, e a lógica de posicionamento de uma organização define que, para uma organização se posicionar ao nível 3, deve implementar os níveis 2 e 1, e assim sucessivamente. O documento pode ser consultado na integra [1].

[1] https://www.cncs.gov.pt/docs/cncs-quadrodeavaliacao.pdf

NÍVEIS DE CAPACIDADE	DESCRIÇÃO	EVIDÊNCIAS
1 – Inicial	Medidas de segurança básicas que poderiam ser implementadas para alcançar o objetivo de segurança, nomeadamente em iniciativas *ad-hoc*, por iniciativas isoladas e pouco formais.	Evidência de implementação das medidas de nível Inicial.
2 – Intermédio	Medidas de segurança que atendem à maioria dos casos e necessidades para atingir os objetivos de segurança da informação. As medidas são atingidas formalmente.	Evidência de implementação das medidas de nível Intermédio.
3 – Avançado	Medidas de segurança avançadas que envolvem a monitorização contínua dos controlos, avaliação e revisão recorrentes, levando em consideração alterações, incidentes, testes e exercícios, para melhoria proativa das mesmas.	Evidência de implementação das medidas de nível Avançado.

Figura 1: Níveis de capacidade definidos pelo QACC (imagem retirada QACC)[1]

Ao analisar ambos os documentos (QNRCS e QACC), verifica-se que o nome das evidências de implementação referidas em ambos, está exposto de forma ambígua, e sujeito a interpretações que podem levar a erros de implementação. A tabela 1 compara as evidências de implementação da medida **ID.GA-1** - "Os dispositivos físicos, redes e sistemas de informação existentes na organização devem ser inventariados", referidas em ambos os documentos, de forma a demonstrar a ambiguidade:

QNRCS	QACC
Inventário atualizado dos ativos com: a. Informação de inventário; b. Identificação dos responsáveis pelos ativos; c. Classificação dos ativos em função da sua criticidade.	**Nível 1 - Inicial**: Ficheiros isolados de registo dos ativos com alguma informação sobre os ativos; Alguma identificação de responsáveis por ativos. **Nível 2 - Intermédio**: Ferramentas/aplicações de gestão integrada de ativos; Políticas de inventário de ativos; Registos de endereços IP, número de inventário, dados do equipamento, etc.; Associação de nome e contacto do colaborador responsável pelo ativo; Classificação dos ativos quanto à sua criticidade. **Nível 3 - Avançado**: Indicadores e registos de acompanhamento dos inventários; Sistemas de monitorização dos inventários; Sistema de identificação automatizada de novos ativos ou alterações dos ativos existentes; Avaliações e auditorias dos sistemas e processos de inventário de ativos.

Tabela 1: Ambiguidade do nome das evidências para a medida ID.GA-1.

Ao elaborar a lista de evidências que constam no QNRCS, a partir da relação subcategoria (medida)/evidências de implementação, verifica-se que ao longo do documento existem evidências com o mesmo nome, mas que pelo contexto, não são necessariamente o mesmo documento. Por exemplo, na subcategoria **ID-AR-3 - As ameaças internas e externas devem ser identificadas e documentadas na metodologia de gestão do risco**, requer como evidência de implementação o documento com a descrição "Documento que suporta a metodologia de gestão do risco", exactamente a mesma descrição que a evidência de implementação da medida **ID.GR-2 - A organização deve determinar e identificar a sua tolerância ao risco**. Pela análise das informações de referência indicadas no QNRCS, é possível verificar que não se trata do mesmo documento. O primeiro problema a resolver, é exactamente a apresentação de uma listagem da referida documentação, que permita identificar os documentos designados por evidências, de forma clara e sem ambiguidades.

Ao longo deste estudo será criada uma lista clara das evidências de implementação das medidas de segurança. Se estas evidências forem ser tratadas como entidades de informação, trazendo para o QNRCS um conceito claramente expresso no meta-modelo TOGAF, será possível apresentar uma arquitetura de informação dos processos de segurança da informação referidos pelo QNRCS. Ou seja, demonstrar de forma inequívoca, qual a estrutura de informação a implementar ou estando implementada, esclarecer de que forma se aproxima da arquitetura de informação desenhada pela **Estratégia de segurança da informação** definida no QNRCS. A presente investigação, pretende ser complementar ao QNRCS e apoiar organizações que pretendem iniciar ou aferir o estado atual da implementação das medidas do referido documento. Este apoio ou complementaridade é entregue através da integração do conhecimento expresso no QNRCS com conceitos de arquitetura empresarial, oferecendo como resultado uma lista de entidades de informação que compõem a arquitetura da informação que aqui se propõe, fiel ao contexto do documento em estudo. Pretende utilizar-se esta listagem, como forma de validação da documentação de uma organização, com o propósito de conferir a existência dos documentos exigidos pelo QNRCS, cujos resultados permitem concluir sobre o estado de preparação ou possíveis lacunas, tanto da documentação que compõe a arquitetura de informação, quanto dos processos que com esta se relacionam. Dada a relação expressa no QNRCS, entre estas entidades de informação e os processos COBIT 5, prevê-se a possibilidade de oferecer às organizações, uma visão dos processos implementados mediante a existência dos documentos em estudo.

1.3 Resultados Esperados

Este estudo pretende listar de forma inequívoca, todas as entidades de informação que representam as evidências de implementação das medidas de segurança descritas pelo QNRCS. Neste estudo, pretende-se ainda concluir sobre a relação estrutural entre diferentes entidades de informação, e as relações derivadas com os processos envolvidos. Para esse efeito serão apresentados de quadros/matrizes que demonstrem a relação entre as entidades de informação e os processos COBIT 5.

Será apresentado um quadro/modelo representando uma arquitetura de informação, que reflita o contexto definido pelo QNRCS, com base nas entidades de informação apuradas.

Esta investigação apresenta um caso de estudo, colocando em prática a validação da documentação existente na organização AMA, para demonstração da aplicabilidade deste estudo, como descrito No capítulo 4, onde se encontra também a definição dos parâmetros adotados para análise de resultados.

A partir da validação referida, são apresentadas conclusões sobre o estado de implementação dos processos COBIT 5 sugeridos pelo QNRCS, assim como, o estado de preparação (ou existência) da arquitetura de informação da organização, passível de mapear com a arquitetura de informação apresentada no quadro/modelo já referido.

Sendo que o QNRCS oferece medidas de mitigação de risco, a sua implementação prevê uma análise de risco prévia. Assim, as medidas a implementar variam de organização para organização, não sendo previsível que uma organização implemente a totalidade das medidas sugeridas.

Através da ferramenta desenvolvida facilita-se a possibilidade de mapear uma arquitetura de informação já existente, com a arquitetura definida pelo QNRCS.

Ao longo deste trabalho, procura-se responder às seguintes questões:

1. Considerando que as evidências de implementação exigidas pelo QNRCS são documentos, qual o nome que as identifica univocamente?

2. Se tratarmos estas evidências como entidades de informação, sabemos à partida que existe uma relação

com processos a implementar. Então, quais os processos a implementar, segundo o QNRCS, e qual é a sua relação com as entidades de informação?

3. É possível integrar noções de arquitetura empresarial seguindo o método TOGAF ADM de forma a favorecer a implementação/entendimento do QNRCS?

4. Qual a contribuição do método desenvolvido, na análise do estado de implementação do QNRCS numa organização?

Da ferramenta desenvolvida, espera-se uma contribuição objectiva, que responde a problemas concretos e esclarece os critérios utilizados, tal como exposto na tabela 2.

Problema	Resultado Esperado	Critério utilizado
Lista de evidências complexa, sujeita a interpretações e pouco evidente na documentação do QNRCS.	Elaboração de uma lista de documentos tratados como entidades de informação.	Atribuição de um nome em conformidade com as informações de referência. Tratamento da informação conforme o conceito de entidades de informação, permitindo que conceitos de arquitetura sejam capturados, filtrados, consultados e representados dando suporte á consistência, integridade e rastreabilidade da informação.
Como aferir o estado AS-IS de processos referentes á implementação das medidas de risco?	Criação de matrizes EI-processos e elaboração diagramas de processos.	Utilizar os princípios de construção das matrizes CRUD, para elaboração de grelhas com a relação EI-Processos (COBIT 5). Apresentação de resultados na forma gráfica, pela criação diagramas (ArchiMate) de processos, integrando noções de arquitetura empresarial.
Como definir um ponto de partida, no sentido de implementação de medidas, ou aferir o estado de medidas implementadas?	Construção de uma *framework* com a arquitetura de informação prevista pelo QNRCS.	Entidades de informação destinam-se a capturar o contexto circundante de modelos de arquitetura formal, pelo que modelo que se apresenta irá permitir o mapeamento da documentação existente numa organização, com as entidades de informação alcançadas pela investigação.

Tabela 2: Resultado esperado face aos problemas encontrados.

Ao criar uma solução que engloba tanto o conhecimento expresso no QNRCS como aspetos de arquitetura empresarial, prevê-se alcançar uma ferramenta que se preste a guiar organizações em diferentes fases da implementação das medidas de segurança, oferecendo os resultados de forma simplificada.

1.4 Estrutura do Documento

O capítulo 1 introduz a necessidade de uma estratégia de segurança da informação no panorama nacional, com referência ao objeto de estudo desta investigação, o QNRCS. Descreve a motivação, contexto e análise do problema exposto, assim como uma previsão dos resultados.

No capítulo 2 são exploradas algumas estratégias de segurança adotadas por outros países, de forma a expor o estado de arte da matéria em estudo. De seguida é feita uma revisão das metodologias adotadas neste trabalho no âmbito da arquitetura empresarial, de forma a justificar a metodologia apresentada.

No capítulo 3, é feita a exposição da metodologia usada para explorar a hipótese em estudo. São apresentados os parâmetros utilizados na análise de resultados, e reserva-se a secção 3.3 para a apresentação do quadro que resulta da investigação realizada.

No capítulo 4, apresenta-se o método de avaliação do trabalho desenvolvido que inclui medidas de avaliação, a exposição de um caso de estudo e uma breve entrevista com a opinião de um especialista.

Por fim, No capítulo 5 apresentam-se considerações finais sobre trabalho desenvolvido e resultados conseguidos, assim como alguma reflexão sobre melhorias futuras.

2 Conceitos Base e Trabalho Relacionado

Na defesa da Cibersegurança e preocupação com a proteção de sistemas contra ameaças que podem comprometer a continuidade dos negócios, e no compromisso da partilha de conhecimento, nasceram e cresceram medidas normativas e de regulação, com o propósito de conduzir a implementação de arquiteturas que visem incluir estes objetivos de segurança.

Na Europa, as medidas adotadas são fortemente impulsionadas por standards como ISO/IEC 27001, ISO/IEC 27032 e ISO 22301 que orientam os sistemas a alcançar estas metas de segurança, integrando a gestão de risco e planos para gestão da segurança de informação para dados e para ativos críticos.

Após a publicação da Diretiva (UE) n.º 2016/1148, do Parlamento Europeu e do Conselho, de 6 de Julho, ficou determinado que cada estado membro da UE, tem a responsabilidade de definir uma estratégia nacional de segurança das redes e dos sistemas de informação, bem como a criação de organismos de cooperação estratégica e intercâmbio de informações.

Em Portugal ficou definido que o Gabinete Nacional de Segurança/Centro Nacional de Cibersegurança (GNS/CNCS) passariam a liderar o processo de transposição da Diretiva SRI para o ordenamento jurídico nacional. Na Resolução de Conselho de Ministros 92/2019 (RCM 92/2019) e Resolução de Conselho de Ministros 41/2018 (RCM 41/2018), definem-se diretrizes técnicas para a Administração Pública quanto à arquitetura de segurança de redes e sistemas de informação, e o Quadro Nacional de Referencia para a Cibersegurança apresenta-se como uma transposição da regulamentação europeia, em particular da Diretiva (UE) 2016/1148, e em conformidade com as normas ISO mais especificamente da família 27001. O documento permite às organizações reduzir o risco associado às ciberameaças, disponibilizando as bases implementação dos requisitos mínimos de segurança das redes e sistemas de informação, refletindo a realidade organizacional portuguesa e respondendo à necessidade de implementar medidas de Identificação, Proteção, Deteção, Resposta e Recuperação de ameaças à segurança do ciberespaço.

2.1 Resolução de Conselho de Ministros nº41/2018

O RCM 41/2018, surge no sentido complementar à regulamentação existente, de forma a adicionar novas regras e procedimentos do ponto de vista tecnológico, com base nos pontos que se descreve [2]:

1. "Aprovar os requisitos técnicos mínimos das redes e sistemas de informação que são exigidos ou recomendados a todos os serviços e entidades da Administração direta e indireta do Estado, os quais constam do anexo à presente resolução e que dela faz parte integrante."

2. "Recomendar a aplicação dos requisitos técnicos a que se refere o número anterior também nas redes e sistemas de informação do setor empresarial do Estado."

3. "Determinar que cada serviço e entidade da Administração direta e indireta do Estado deve avaliar a conformidade dos requisitos técnicos das redes e sistemas de informação em uso com as finalidades e princípios de segurança que se pretendem alcançar com os requisitos estabelecidos no anexo à presente resolução."

4. "Determinar que os requisitos referidos no anexo à presente resolução devem ser implementados no prazo máximo de 18 meses após a data de entrada em vigor da presente resolução."

5. "Estabelecer que a presente resolução entra em vigor no dia seguinte ao da sua publicação."

Trata-se da especificação de um conjunto de “Requisitos Gerais”, agrupando cada um deles um conjunto de ”Requisitos Específicos”, que garantem a segurança da informação. Quando aplicável, os ”Requisitos específicos” são diferenciados por Front-end (FE), Camada de aplicativo (App) e DatabaseLayer (BD). Por fim, são classificados como recomendados ou obrigatórios. O RCM 41/2018, é fortemente apoiado pela diretiva europeia sobre segurança de redes e sistemas de informação (Diretiva (UE) 2016/1148), que fornece medidas legais para aumentar o nível geral de cibersegurança na União Europeia. Em suma, o RCM 41/2018 define-se no compromisso de aprofundar a segurança das redes e da informação, para garantir a proteção e defesa do ciberespaço.

2.2 Quadro Nacional de Referência para a Cibersegurança

Cada membro da União europeia tem a liberdade de escolher o modelo que pretende utilizar para transposição da Diretiva (UE) 2016/1148. Em Portugal, a Estratégia Nacional de Segurança do Ciberespaço expressa-se pelo QNRCS, que pretende ser um instrumento de apoio à implementação de sistemas de segurança e resposta sistemática, em conformidade com a Lei n.º 46/2018, como base jurídica para a segurança do ciberespaço.

Esta estratégia baseia-se em três princípios, tratados pelo QNRCS como (1) Subsidiariedade, uma ferramenta para todas as organizações envolvidas no ciberespaço para garantir a soberania e os princípios constitucionais; (2) Complementaridade, que propõe um conjunto de medidas para sensibilizar todos os atores envolvidos no ciberespaço e a posição que nele ocupam; (3) Proporcionalidade, entre objetivos de segurança, propondo a adaptação das medidas à organização, quanto à sua aplicabilidade, porte, setor de atividade e caracterização dos riscos identificados. Seguindo a Diretiva (UE) 2016/1148, a implementação do QNRCS possibilita a obtenção de uma estrutura reutilizável com medidas globalmente direcionadas aos três pontos que se representam no diagrama na Figura 2.

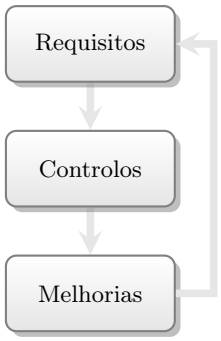


Figura 2: Estrutura das medidas orientadoras do QNRCS

A estratégia define uma infraestrutura de pessoas ou dispositivos dedicados à segurança, começando pela necessidade de implementação de uma figura de "Chief Information Security Officer"(CISO), como responsável máximo pela segurança da informação, em seguida, um "Security Operations Center"(SOC) para fornecer as instalações necessárias e equipas de suporte e, finalmente, uma "Computer Security Incident Response Team"(CSIRT) para operar nas instalações do SOC.

O CISO, representa um grande papel na análise e identificação das medidas necessárias para a segurança da organização. De acordo com o documento em estudo, esta deve ser uma função exercida na organização (não um serviço externo), com o objetivo de garantir a melhoria da continuidade dos processos e atividades

para garantir a resiliência adequada em termos de segurança da informação e cibersegurança. O CISO reporta à gestão de topo de uma organização e, devido ao impacto de sua responsabilidade, deve ter pleno conhecimento dos processos-chave da organização. Em geral, o CISO deve ser capaz de traduzir os objetivos da organização em requisitos de segurança da informação.

O SOC é por definição referente à equipa e instalações organizadas para prevenir, detectar e responder a ameaças/incidentes de cibersegurança, e garantir a aplicação da lei, sendo uma parte essencial do plano de proteção de dados. Tem como principais responsabilidades a identificação, categorização e monitorização de redes e sistemas, dever ser proativo na deteção de atividades maliciosas e corrigir ativamente as vulnerabilidades detetadas. A existência do SOC deve ser ajustada à realidade de cada organização, podendo caracterizar-se por Virtual, Dedicado, Distribuído, de Comando, Multifunções, de Fusão ou Externalizado.

A constituição de um CSIRT deve ser adequada ao porte da organização e sua exposição ao ciberespaço, geralmente seguindo o modelo de "Security Incident Management Maturity" (SIM) que se baseia em quatro vetores: organizacional, humano, ferramentas e processos. De acordo com o QNRCS, um CSIRT fornece três tipos de serviços específicos:

> Serviços Reativos: Alertas e avisos; Resposta a incidentes; Gestão de vulnerabilidades; Gestão de artefatos.
>
> Serviços Proativos: Campanhas de sensibilização; Monitorização de tecnologia; Auditorias e avaliações de segurança; Configuração e manutenção de ferramentas de segurança, aplicações e infraestrutura; Desenvolvimento de ferramentas de segurança; Serviços de detecção de intrusão; Divulgação de informações de segurança.
>
> Serviços de gestão da qualidade de segurança: Análise de risco; Planeamento para continuidade de negócios e recuperação pós-desastre; Consultoria de segurança; Sensibilização de segurança; Treino e formação; Avaliação e certificação de produtos.

Conforme exigido pela regulamentação internacional, a elaboração do QNRCS materializa uma visão homogénea e inclusiva da realidade organizacional portuguesa (pública e privada), no que diz respeito à implementação do regime jurídico da segurança do ciberespaço. O Documento fornece medidas técnicas e procedimentais, e destaca a implementação de medidas para Identificar, Proteger, Detectar, Responder e Recuperar, de forma a responder aos desafios de ciberespaço, e propõe a implementação de procedimentos orientados à gestão de riscos, garantia de confidencialidade, disponibilidade e integridade na prestação de bens ou serviços. Esses processos são realizados para caracterizar a situação atual, para definir objetivos e para determinar a evolução positiva da situação, apoiados por princípios e orientações genéricas fornecidos na ISO/IEC 310001 e apoiados pelos requisitos da ISO/IEC 27001 para um Sistema de Gestão de Segurança da Informação (SGSI). O documento estende-se às especificações dos processos de gestão de riscos para "Sistemas de Informação" definidos pela ISO/IEC 27005 tratados com a perspectiva de Evitar, Aceitar, Mitigar e Transferir. Estes processos estão descritos de forma a contemplar quatro principais aspetos da gestão de risco: Definir o Contexto; Identificar o Risco; Analisar o risco e determinar o Nível de Risco.

O QNRCS é aplicável a todas as organizações públicas e privadas nacionais, nomeadamente: (1) Administração Pública; (2) Operadores de infraestrutura crítica; (3) Operadores de serviços essenciais; (4) Provedores de serviços digitais; (5) Quaisquer outras organizações que usam redes e sistemas de informação. Tem por objetivo ser utilizado por uma organização, como instrumento de apoio ao processo de gestão de riscos de cibersegurança, permitindo a identificação de lacunas na estratégia de cibersegurança e promovendo a definição de um caminho de melhoria futura.

Além disso, oferece uma linguagem comum de comunicação de requisitos entre os diferentes atores, para apresentação do contexto, procedimentos e mecanismos semânticos. A definição de todas as categorias, subcategorias, controlos e objectivos/medidas de segurança, seguem os princípios abaixo descritos:

1. "Considerar todos os aspetos definidores de um ecossistema de cibersegurança nas organizações nacionais, independente da sua dimensão, natureza (pública ou privada), criticidade ou orientação tecnológica;"
2. "Abranger transversalmente todos os setores de atividade;"
3. "Atender às características específicas e definidoras do tecido social e económico do país;"
4. "Permitir e promover que determinadas organizações (por exemplo: reguladores) possam definir o respetivo contexto de aplicação do QNRCS para o seu sector de atividade/regulação."

A estrutura central do QNRSC, é constituída por objetivos de segurança e medidas de segurança, através dos quais, sistematiza a revisão de práticas de segurança de informação, através de um conjunto de medidas que permitem a comparação das medidas de cibersegurança existentes numa organização e sua conformidade com os standards.

Por cada objetivo de segurança, são apresentadas uma ou mais medidas de segurança, por sua vez, cada medida de segurança, traduz-se em categorias que se dividem em subcategorias associadas a controlos e/ou referências, relacionados com a implementação da medida em questão. Por fim são indicadas genericamente **evidências** que demonstram a implementação/aplicação da correspondente medida. A tabela 3 resume a estrutura do QNRCS.

Objetivo	Medidas de Segurança					
IDENTIFICAR	Categorias	Subcategorias	Implementação Técnica	Implementação Processual	Evidências	Referências Normativas
PROTEGER	Categorias	Subcategorias	Implementação Técnica	Implementação Processual	Evidências	Referências Normativas
DETETAR	Categorias	Subcategorias	Implementação Técnica	Implementação Processual	Evidências	Referências Normativas
RESPONDER	Categorias	Subcategorias	Implementação Técnica	Implementação Processual	Evidências	Referências Normativas
RECUPERAR	Categorias	Subcategorias	Implementação Técnica	Implementação Processual	Evidências	Referências Normativas

Tabela 3: Estrutura base do QNRCS

Portanto, os objetivos e propósitos do QNRCS devem ser usados numa perspectiva de melhoria contínua ao invés do uso estático de práticas, de acordo com a maturidade da organização e seu contexto, focado em fornecer: (1) um conjunto de medidas de segurança (bem descritas), traduzindo objetivos específicos; (2) Referências e orientações que permitem a sistematização de processos, procedimentos e ferramentas; (3) Representação dos principais objetivos reconhecidos pelas várias partes interessadas, como suporte ao processo de gestão de risco de segurança de informação.

Como produto complementar ao QNRCS, o CNCS desenvolveu o QACCS, onde se definem para cada uma das medidas de cibersegurança do QNRCS, três níveis de capacidade (Inicial, Intermédio e Avançado), abrangendo os cinco objetivos de cibersegurança, tendo em consideração o contexto e dimensão variável das organizações. Estes níveis de capacidade aplicáveis a cada organização dependem das suas características

específicas, tendo sido o documento criado de forma suficientemente flexível para aplicação em diferentes contextos.

O CNCS, desenvolveu também a ferramenta **Ciberchecкup**, que permite às organizações, uma auto avaliação quanto em termos de cibersegurança, considerando o QNRCS e o QACCS, validando a existência das evidencias de implementação de medidas e considerando os 3 níveis de capacidade [3].

2.3 ISO 27001

As práticas e controlos recomendados pelo QNRCS, são complementares às recomendações internacionais para segurança da informação e cibersegurança, como CIS CSC 7.0 Center of Segurança da Informação (CIS); COBIT 5; ISO / IEC 27001; NIST SP-800-53 Rev4 NIST93.

O QNRCS respeita a orientação ISO 27001 em relação a promover a melhoria continua, distribuindo as medidas a implementar entre os cinco objetivos:

1. IDENTIFICAR - Um contexto apropriado, incluindo os ativos que suportam os processos críticos e os riscos associados relevantes, permitindo à organização definir e priorizar seus recursos e investimentos de forma consistente.

2. PROTEGER - Medidas para proteger a organização (Pessoas, Processos, Ativos e Tecnologia), independentemente de sua natureza tecnológica. Ferramentas de suporte para limitar ou conter o impacto da eventual ocorrência de um incidente de segurança cibernética, por meio da implementação de verificações de identidade e respectivas autorizações, formação, ações de consciencialização e implementação de procedimentos, processos e tecnologias de proteção da informação.

3. DETETAR - Medidas para identificar incidentes que representem eventos com efeito prejudicial sobre a segurança de redes e sistemas de informação. Desenvolver práticas adequadas para detetar a ocorrência de eventos de cibersegurança, por meio do monitorização contínua de redes e sistemas de informação, e implementação de processos de deteção.

4. RESPONDER - Medidas de ação apropriadas no caso de um incidente ser detectado, para mitigar o impacto do incidente e potenciais efeitos adversos. Planeamento da resposta ao incidente e da comunicação com as partes interessadas relevantes, analisando e mitigando incidentes, e promovendo melhorias por meio das lições aprendidas.

5. RECUPERAR - Gestão dos planos e medidas de recuperação dos processos e serviços afetados por um incidente de segurança digital. Reduzir os impactos de um incidente ocorrido, promover a execução de continuidade de negócio, elaborar planos de recuperação, executar de exercícios de simulação de crises e atualizar planos de ação promovendo melhorias.

"Medidas de segurança", "Categorias"e "Subcategorias"constituem um alto nível de abstração das atividades, de forma a simplificar o processo de organização da informação e tomada de decisão em função dos objetivos. O que implica dizer que essas medidas, estão alinhadas com as metodologias de gestão de incidentes e demonstram o impacto do investimento em cibersegurança, subdividido em categorias que agrupam funções programáticas e objetivas, e atividades específicas.

Com base na anterior experiência ISO, o ISO 27001 influencia a estratégia nacional a implementar um ciclo PDCA (*Plan, Do, Check, Act)* representado na figura 3, estabelecendo um conjunto de requisitos gerais e medidas de controlo e melhorias. No que confere ao QNRCS o standard em questão estabelece esta

relação, sendo que *Plan* refere-se à definição do sistema de gestão de segurança da informação, *Do* refere-se à implementação deste sistema, *Check* representa a necessidade de monitorização e revisão do mesmo (controlos), e *Act* diz respeito à manutenção e acções de melhorias sobre este.

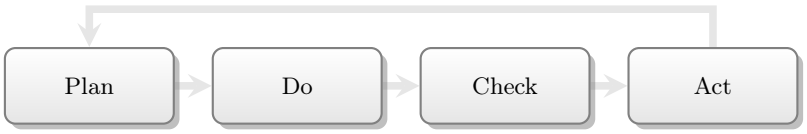


Figura 3: Diagrama PDCA

Para esta investigação, as referências normativas têm particular importância, visto se encontrarem na base da análise das evidências de implementação do QNRCS. Para esse efeito é de relevância a tabela 4, que resume a estrutura global do ISO 27001, onde se enquadram políticas, planos de acção, definições de responsabilidades, práticas, procedimentos, processos e recursos, que orientam as organizações na implementação do seu sistema de gestão da segurança da informação.

Global Structure	Clause 4: Context of the organization Clause 5: Leadership Clause 6: Planning Clause 7: Support Clause 8: Operation Clause 9: Performance evaluation Clause 10: Improvement

Tabela 4: Estrutura Global do ISO 27001

Esta norma, apresenta-se em dois componentes fundamentais, o designado Anexo A que se resume na tabela 5, composto por um conjunto de controlos, que representam as ferramentas para implementar, operar, monitorizar, rever, manter e melhorar o ISMS. O outro componente, é uma ferramenta de suporte para o desenvolvimento do conjunto de medidas, requisitos e métodos de análise a implementar, suportando igualmente a definição do contexto da organização no âmbito da segurança e designa-se por "Rules and Requirements"[4].

ISO 27001 Annex A	A.5 Information security policies A.6 Organisation of information security A.7 Human resource security A.8 Asset management A.9 Access control A.10 Cryptography A.11 Physical and environmental security A.12 Operations security A.13 Communications security A.14 System acquisition, development, maintenance A.15 Supplier relationships A.16 IS incident management A.17 IS business continuity management A.18 Compliance

Tabela 5: Resumo do Anexo A - controlos

2.4 Directive (EU) 2016/1148

A Diretiva (UE) 2016/1148 oferece um quadro jurídico para a segurança de redes e sistemas de informação (*Network and Information Systems* - NIS) para membros da UE. Os principais pontos descritos nesta diretiva definem:

1. Disposições gerais - Âmbito e contexto, processamento de dados pessoais, harmonização mínima, definições, identificação de operadores de serviços essenciais, efeito disruptivo significativo.

2. Estratégias nacionais de segurança para NIS - Obrigação de definir estratégias nacionais de segurança, autoridades nacionais competentes e ponto único de contato, equipas de resposta a incidentes de segurança informática (CSIRTs), cooperação a nível nacional.

3. Cooperação - Grupo de cooperação, rede CSIRTs, cooperação internacional

4. Segurança dos operadores de serviços essenciais - Requisitos de segurança e notificação de incidentes, implementação e aplicação.

5. Segurança dos prestadores de serviços digitais - Requisitos de segurança e notificação de incidentes, implementação e aplicação, jurisdição e territorialidade.

6. Padronização e notificação voluntária - Padronização das comunicações e notificação voluntária de eventos maliciosos.

A diretiva, fornece informações detalhadas sobre serviços essenciais e serviços digitais, e estabelece objetivos gerais para um nível comum de segurança dos sistemas de informação para os Estados-Membros. Declara o dever de desenvolver quadros (ou modelos) nacionais, e disponibiliza documentação para orientar a adoção de uma estratégia nacional para a segurança de informações e sistemas [5]. Define também medidas claras para cooperação e coordenação estratégica de troca de informações.

É fortemente recomendado neste documento, a criação de programas de consciencialização e capacitação de segurança e planos de desenvolvimento relativos à gestão de riscos. A diretiva em foco, estabelece um "Grupo de Cooperação"para apoiar e facilitar a cooperação estratégica e troca de informações através de uma rede sustentada de "Equipas de Resposta a Incidentes de Segurança"(*Computer Securitity Incident Response Teams* - CSIRTs) dos Estados-Membros.

Os Estados-Membros devem assegurar que os operadores de serviços essenciais tomem medidas adequadas para gestão do risco de segurança das redes e dos sistemas de informação, evitando que incidentes de segurança se transformem em catástrofes. Define que as autoridades competentes devem ter os poderes e meios necessários para avaliar a conformidade dos operadores de serviços essenciais e descrever suas obrigações.

Os requisitos e obrigações dos provedores de serviços digitais, encontram-se igualmente esclarecidos na Diretiva (UE) 2016/1148, assim como, os operadores de serviços essenciais.

A diretiva incentiva o uso de padrões europeus (ou internacionalmente aceites), em especificações relevantes para a segurança de redes e sistemas de informação, promovendo a normalização, remetendo para a Agência Europeia para a Segurança das Redes e da Informação (*European Union Agency for Cybersecurity* - ENISA), em colaboração com os Estados-Membros, a responsabilidade pelo aconselhamento e orientação relativamente a questões técnicas.

Por fim, promove a notificação voluntária de ocorrências, em entidades não consideradas como operadoras de serviços essenciais nem provedores de serviços digitais.

2.5 CIS CSC 7.0

O QNRCS refere que "O Catálogo de controlos críticos de segurança (*Critical Security Controls* - CSC) é publicado pelo *Center for Internet Security* (CIS). Este catálogo disponibiliza uma lista de ações, priorizadas, que é regularmente revista pela comunidade académica, de forma a ser utilizável pelas organizações".

O CIS desenvolveu controlos de segurança críticos para a cibersegurança, composto por 20 controlos, com base nas informações mais recentes sobre ataques comuns, e refletem a troca de conhecimento de especialistas. Estes controlos são usados para estabelecer rapidamente as acções de proteção nas organizações que permitem, evitar e eliminar rapidamente o risco de ataques digitais. Estas acções, crescem a nível de complexidade, começando pelo nível **Básico**, que contém os controlos entre 1 e 6, que ajudam uma organização a avaliar sua segurança atual e tomar medidas simples para melhorá-la. Entre o controlo 7 e 16, trata-se do nível **Fundacional** que contém orientações mais avançadas para melhorar a segurança de uma organização. Por fim, controlos 17 a 20, o nível **Organizacional** contém controlos que fazem alterações nas políticas de uma organização para melhorar e manter sua segurança cibernética.

Os controlos CIS, têm como principal função priorizar a cibersegurança com base nos riscos, oferecendo abordagens eficientes na mitigação dos mesmos, portanto complementar a outras *frameworks* como a *NIST Cybersecurity Framework* (CSF), mais focadas na análise do risco [6]. O Anexo 1 - CIS Controlos, lista os 20 controlos referidos.

2.6 COBIT 5

Originalmente o COBIT surgiu como um conjunto de objetivos de controlo para ajudar a comunidade de auditoria financeira a lidar melhor com ambientes relacionados a tecnologias de informação (TI), tendo crescido para uma *framework* de boas práticas de governação TI, que contribui para o equilíbrio fornecend benefícios como a otimização dos níveis do risco e a utilização dos recursos disponíveis, endereçando a definição e implementação de processos, estruturas e mecanismos de segurança de informação aos processos de negócio. O COBIT 5, é responsabilidade do *Information Systems Audit and Control Association* (ISACA), e assente em cinco princípios fundamentais [7]:

1. Satisfazer necessidades das partes interessadas, garantindo um alinhamento estratégico e retorno sobre o investimento;

2. Cobrir a organização de ponta a ponta, responsabilizando a gestão de topo em envolver-se no desenvolvimento e manutenção das estratégias de TI;

3. Aplicar uma *framework* integrada e única, que engloba outros padrões e *frameworks* relevantes como COSO, ITIL e TOGAF;

4. Possibilitar uma visão holística, pela definição de um sistema organizacional que inclui os interesses visando processos, estruturas e pessoas;

5. Separar a governação da gestão, declarando que os processos de gestão e governação dos sistemas de informação, se referem a atividades diferentes. A implementação de processos seguindo o método COBIT,contribui para a otimização dos níveis do risco e dos recursos disponíveis nas organizações. Em 2019, foi lançada a versão mais recente do COBIT, o COBIT 2019, cuja principal actualização, trata de orientações que ajudam as organizações a criar uma solução personalizada de governação de TI.

Os objetivos de governação e gestão desta *framework*, estão agrupados em cinco domínios. No domínio *Evaluate, Direct and Monitor* (EDM), são avaliadas as opções estratégicas e e monitorizado o seu cumprimento englobando todos os *stakeholders* da hierarquia. Os objetivos de gestão agrupam os restantes domínios: *Align, Plan and Organize* (APO); *Build, Acquire and Implement* (BAI); *Deliver, Service and Support* (DSS) e *Monitor, Evaluate and Assess* (MEA). O "Anexo 2 - Processos COBIT 5"detalha o *COBIT Core Model* numa imagem retirada da página isaca.org.

2.7 Estratégias de Cibersegurança

Um pouco por todo o mundo, os governos criaram novos sistemas de segurança ou melhoraram sistemas existentes, regulados por diretrizes internacionais e cooperando internacionalmente para um propósito comum. A tabela 6 reflete o estado da transposição da Diretiva (UE) 2016/1148 para a estratégia nacional adotada por alguns destes países.

	Alemanha	Suécia	Inglaterra	Portugal
Estado da transposição	Transposto	Transposto	Transposto	Transposto
Estratégia Nacional para NIS	Publico	Publico	Publico	Publico
Ponto de contacto (SPOC)	Bundesamt für Sicherheit in der Informationstechnik	Swedish Civil Contingencies Agency MSB	The National Cyber Security Centre	Centro Nacional de Cibersegurança
Autoridade competente (DSPs)	Igual ao SPOC	Post- och telestyrelsen - PTS	ICO: Information Commissioner's Office	Igual ao SPOC
Autoridade competente (OES)	Igual ao SPOC	Difere para Energia, Transportes, Banca e infraestruturas financeiras, Saúde, Distribuição e fornecimento de água, infraestruturas digitais - Igual ao SPOC	Igual ao SPOC	Igual ao SPOC
Resposta a Incidentes (CSIRT)	Igual ao SPOC	MSB/CERT-SE	Igual ao SPOC	CERT.PT
Estado	Completo	Completo	Completo	Completo

Tabela 6: Estrutura base do QNRCS

De acordo com o *British Standards Institution* (BSI), no Reino Unido as organizações podem guiar-se pela *Cyber Assessment Framework* (CAF), desenvolvida pelo *UK National Cyber Security Centre* (NCSC) bem como pela *Cybersecurity Framework* (CSF) desenvolvida pelo *National Institute of Standards and Technology* (NIST) . A CAF foi desenvolvida para órgãos da administração pública, reguladores e indústria, oferecendo um método sistemático de verificação da adequação das medidas de gestão de risco, no que respeita à disponibilidade dos serviços essenciais. Esta *framework* destina-se a fazer cumprir os requisitos da Diretiva NIS, bem como outras necessidades mais específicas da *Critical National Infrastructure* (CNI). A CSF consiste em standards, *guidelines* e boas práticas para gestão do risco relacionado com a cibersegurança, apresentado-se

como flexível e de baixo custo, apoia a proteção e resiliência de infraestruturas críticas e outros sectores importantes da economia nacional.

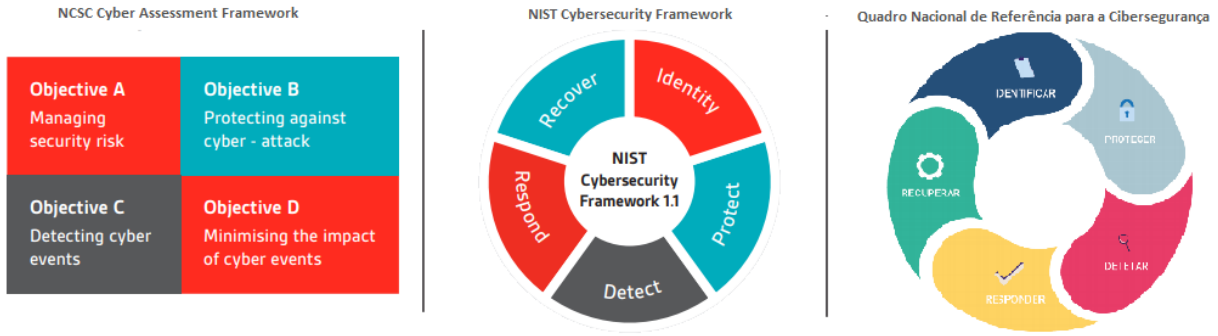


Figura 4: Comparação de *frameworks* usadas em UK (imagem retirada do Web Site da BSI) e do QNRCS.

O BSI apresenta uma justaposição de ambas, concluindo que existe uma clara sobreposição conceptual. Embora a NCSC CAF apresente uma avaliação baseada em objectivos, é muito evidente a sobreposição quando comparamos o "Objective A"(*Managing security risk*) com o "Segment Identify". À semelhança com estas *frameworks* o QNRCS apresenta-se distribuído por cinco objetivos, numa relação muito direta com a NIST CSF conforme ilustrado na figura 4.

Apesar das estratégias referidas ou similares terem sido adotadas por diversos países, alguns estudos dedicam-se à análise de lacunas nestes documentos, como por exemplo o artigo *Cyber security management of critical energy infrastructure in national cybersecurity strategies: cases of USA, UK, France, Estonia and Lithuania* [8], que analisa as soluções adotadas pelos países referidos, defendendo que as estratégias que transpõem a Diretiva NIS, são geralmente pouco eficientes na proteção de infraestruturas críticas.

A estratégia adotada pela França, colocou o país em terceiro lugar no *ranking* da cibersegurança em 2019, com uma estratégia de segurança mais direcionada para o nível internacional que nacional. No caso da Lituânia, fica claro que a cibersegurança não se trata apenas de aspetos técnicos, tendo sido promulgada a *Lithuanian Cybersecurity Law* que define um conjunto de medidas legais, de divulgação de informações, organizacionais e técnicas necessárias para prevenir, detectar, analisar e responder a incidentes.

As estratégias adotadas pelos vários países são muitas vezes acompanhadas por guias, que pretendem apoiar a sua implementação. Validar uma implementação existente, cai muitas vezes no âmbito da certificação, orientado aos standards ou normas existentes como é o caso da Certificação ISO27001.

2.8 Arquitetura Empresarial

O termo "Arquitetura"é tão facilmente compreensível que está quase isento de definição, no entanto, o contexto onde é usado pode obrigar a um refinamento. Neste trabalho "Arquitetura"é o termo para definir a organização fundamental de um sistema, consubstanciado nos seus componentes, relações entre si, o contexto em que se encontram e os princípios que orientam o seu desenho e evolução. Além disso, quando o termo arquitetura é usado para se referir ao modelo de um sistema, a sua estrutura e relação entre componentes, a definição tem uma `perspectiva descritiva`. Por outro lado, se o termo é usado para se referir a um modelo onde são fornecidas diretrizes, regras ou princípios para projetar uma solução, ele define em um `perspectiva prescritiva`.

A "Arquitetura Empresarial (AE)"é o *master plan* da organização, levando em consideração a estratégia de negócios e seus objetivos. Este plano está bem organizado em grupos de interesse ou camadas, de soluções de infraestrutura tecnológica, com o objetivo da segurança da informação. Quando esta arquitetura corporativa é bem conhecida e aplicada a padrões conhecidos, é possível minimizar riscos, ser preventivo e flexível para mudanças, respondendo aos requisitos do negócio. "Arquitetura Empresarial", é a expressão assumida ao trazer o conceito de Arquitetura para o campo das tecnologias de informação, pela dependência que esta arquitetura tem na organização da empresa.

Este conceito é composto por muitas vistas arquiteturais, que devem ser entendidas pelas diferentes partes interessadas, para uma boa percepção do negócio, da tecnologia envolvida e sua evolução. As arquiteturas corporativas descrevem fundamentalmente o cenário atual dos recursos de gestão da organização (*hardware*, *software*, instalações ou pessoas) e interação entre eles nas diferentes camadas da arquitetura. Define igualmente, possíveis soluções para problemas previsíveis e o planeamento estratégico de melhorias [9].

2.8.1 Camadas de Arquiteturais

Frameworks de arquitetura empresarial, sejam conceptuais ou metodológicas, podem resultar em diferentes camadas organizacionais. A complexidade das relações entre as camadas vem da construção de diferentes vistas (*views*) e pondos de vista (*viewpoints*) das partes interessadas (*stakeholders*), geralmente englobado em três áreas principais:

Arquitetura de negócio - Serve de base às restantes arquiteturas pela relação com o negócio da organização, espelhando todas as atividades, modelos de informação e contexto da organização.

Arquitetura aplicacional e de dados - Expressa da gestão ao serviço, a relação entre aplicações e dados (informação).

Arquitetura tecnológica - Define a estrutura, plataformas, interações de serviços e componentes tecnológicos (lógicos e físicos).

2.8.2 Outros conceitos e definições em AE

O proposta desta investigação, foca-se na camada de dados, no entanto, a noção de arquitetura expressa-se por conceitos e termos que se consideram importantes apresentar pelo contexto da investigação realizada.

O conceito de *Design*, no âmbito da arquitetura empresarial tem a função de expor os atores e comportamentos esperados, de preferência na forma de diagrama (*workflow*) demonstrando todas as etapas necessárias para completar um processo. Este diagrama inclui a definição de comunicações/dependências entre processos, e esclarece quem são os responsáveis ou *stakeholders* por cada ação, e quais as alternativas previsíveis (*elseif*) para cada acção[10].

Em AE, a noção de "padrões"oferece ao arquiteto, um recurso importante e uma garantia de rigor nas descrições e referências, apresentando um conceito *standard* para o desenho eficaz de soluções, geralmente fáceis de entender, representando uma ferramenta de decisão importante na composição e modelação das *views* e *viewpoints* que compõem a arquietura. Os padrões expressam a estrutura organizacional e contribuem na definição de subsistemas especificando responsabilidades, regras e relações. Esta definição, acomoda a arquitetura como um *blueprint* (uma estrutura a ser implementada), bem como, a arquitetura como uma decisão (princípios gerais). A finalidade de cada padrão pode ser apresentada como "Visão Holística", numa perspectiva de gestão, usando uma visualização de notação muito simples (diagrama UML ou ArchiMate),

documentar tarefas da camada de negócios (*Business View*), ou destacar a tecnologia expondo serviços, clientes, *hardware*, etc. (*Technological view*). Entre os tipos de padrões conhecidos, consideram-se de particular relevância os que se apresenta na tabela 7, não obstante, aprofundar o tema não adiciona valor a este estudo [11].

Padrão	Descrição
Business	Diretamente rellacionados com processos de negocio, dependentes do setor.
Support	Serviços da organização não sem relação direta com os processos de negócio.
Infrastructure	Serviços de base para todos os padrões, geralmente inacessíveis ao utilizador final.

Tabela 7: Tipos de padrões

A ponte relacional entre as metas de negócios e a estratégia de TI é chamada de "Princípio". Esses princípios são definidos pela lógica da arquitetura corporativa, numa linguagem de alto nível, atuando como diretrizes ou regras gerais na implementação e definição de recursos. Definem um vínculo consensual com entre os elementos duma organização e representam a base para o eventual crescimento do negócio. Os princípios de arquitetura, apoiam o processo de enquadramento de problemas, e formam uma base de decisão. Portanto, o design de princípios deve ser padronizado, claro e objetivo, promovendo o entendimento e aceitação em si mesmos. O design dos princípios seguem modelos previamente convencionados.

Um *stakeholder* (ou parte interessada) é um indivíduo, equipe ou organização com interesses ou preocupações que envolvem o sistema onde está integrado. A principal preocupação de uma parte interessada não é a arquitetura empresarial, no entanto, é essencial para o arquiteto, que irá reunir as preocupações de todas as partes interessadas na solução. O arquiteto deve ser capaz de explicar a solução para as várias partes interessadas (com experiências e expectativas diferentes)[12]. Cada *stakeholder* traz a sua perspectiva para a arquitetura corporativa, que será transformada numa visão abstrata, como modelo reutilizável. *Viewpoints* são ferramentas para conceptualizar e descrever as técnicas para construir essas *views*. O conceito central de *viewpoints* é fazer corresponder as preocupações dos utilizadores, às suas rotinas diárias na arquitetura empresarial. Portanto, o trabalho do Arquiteto deve garantir que a arquitetura `comunica com` e é `compreendida por` todas as partes interessadas em distintos domínios ou áreas da empresa, sendo possível a sua utilização como convenções no desenvolvimento da arquitetura. O arquiteto projeta uma *view* corporativa, como um conjunto de *views* contemplando a estratégia, o negócio,a informação, os sistemas de informação e a infraestrutura (tecnologia).

Ao definir uma arquitetura empresarial, são utilizados padrões que se adequam a diferentes níveis, ao que designamos níveis de abstração. Cada padrão é motivado por um ponto de vista de negócio ou camada, com impacto direto na camada seguinte (visão holística), o que leva a alguma perda de detalhe. *Stakeholders* distintos, têm diferentes níveis de abstração, o que promove dificuldades de comunicação. No decorrer do processo de desenvolvimento duma arquitetura empresarial, é espectável que o conceito de padrões introduza alguma reusabilidade, melhorando a eficácia do trabalho, evitando repetir as mesmas ações e a propagação de erros, e acelerando todo o processo desde o desenho à implementação [9].

2.9 The Open Group Architecture Framework

No sentido de estruturar a arquitetura empresarial podem ser utilizadas *frameworks*, cujo propósito passa pela utilização de técnicas para descrever a estrutura da arquitetura, identificando e relacionando os diferentes *viewpoints* e respetivas técnicas de modelação. Estas *frameworks* não oferecem concretamente técnicas de

modelação, no entanto podem estar intimamente ligadas a alguma linguagem ou conjunto de linguagens de modelação.

Um método de arquitetura empresarial, é uma coleção de técnicas e processos para criar e manter a arquitetura empresarial, especificando as várias fases do ciclo de vida da arquitetura. Estre os métodos mais conhecidos encontram-se o *Rational Unified Process* (RUP), o UN/CEFACT *Modelling Methodology* (UMM) e o TOGAF *Architecture Development Method* (ADM). Enquanto o primeiro e o segundo são iterativo e incremental (respetivamente) TOGAF ADM oferece um conjunto de fases bem descritas para o desenvolvimento de uma arquitetura de TI.

No campo das framworks de arquitetura, destacam-se a *Federal Enterprise Architecture Framework* (FEAF), a Zachman *Framework*, a *Open Group Architecture Framework* (TOGAF) e a OMG's *Model-Driven Architecture*, entre outras.

Para enquadramento do presente estudo exime-se a explicação aprofundada dos métodos e *frameworks* referidas, e segue-se para a descrição da ferramenta que melhor suporta esta investigação [9].

2.9.1 TOGAF ADM

Inicialmente, o *Open Group Architecture Framework* (TOGAF), representava uma metodologia genérica para desenvolvimento de arquiteturas técnicas, tendo evoluído para uma *framework* de arquitetura empresarial. Entre as principais ferramentas disponibilizadas pelo TOGAF ADM encontram-se:

Architecture Development Method (ADM) - Com base em quatro conceitos interrelacionados: Arquitetura de negócio, Arquitetura de Informação, Arquitetura Aplicacional, Arquitetura tecnológica. Sendo considerado o *core* do TOGAF, o ADM introduz uma abordagem cíclica e gradual.

TOGAF *Enterprise Continuum* - Com o propósito de ilustrar um desenvolvimento contínuo de arquiteturas, partindo de sistemas simples e arquiteturas específicas para arquiteturas personalizadas.

TOGAF *Resource Base* - Um conjunto de ferramentas e técnicas disponíveis para implementar TOGAF e TOGAF ADM (*views* e *viewpoints* de arquitetura, cenários de negócios, ADML, casos de estudo, outras estruturas de arquitetura, e um mapeamento do TOGAF para a *framework* Zachman.

O TOGAF ADM prevê um conjunto de *views* e correspondentes *viewpoints* que devem existir numa arquitetura: *Business Architecture Views* que aborda as preocupações dos utilizadores e os fluxos de informação, e contempla vistas de processos, funções, informações de negócio, performance, entre outros. *Engineering Views* com preocupações ao nível da engenharia de sistemas e de *software*, e integração de componentes do sistema. Contempla vistas de segurança, de engenharia de software, de dados, de engenharia de sistemas e de engenharia de comunicações. *Enterprise Manageability Views* que aborda preocupações dos administradores de sistemas operadores e gestores. *Acquirers Views* com preocupações logísticas e de compras, responsáveis pela aquisição de *hardware* e *software*. Contempla vistas de custos e *standards*, incluindo normalmente os edifícios.

Do ponto de vista da arquitetura empresarial, TOGAF oferece uma aproximação para o seu desenho, planeamento, implementação e governação. Em particular o TOGAF ADM descreve o método para desenvolver e gerir a arquitetura empresarial no seu ciclo de vida útil. Este método, é iterativo considera amplamente a empresa em toda a sua cobertura, podendo ser implementado a diferentes tipos de organizações e setores. As fases descritas no método TOGAF ADM, devem ser implementadas considerando outras estruturas operacionais de uma organização, apresentando-se como procedimentos para desenvolvimento de uma solução que

inclui as tecnologias de informação, e engloba vários domínios. O TOGAF ADM apresenta-se distribuído nas fases explicadas na tabela 8

Fase	Descrição	Objetivo
	Preliminar	Determinar a capacidade da arquitetura incluindo o contexto, *scope*, *frameworks*, princípios, métodos e ferramentas.
A	Visão de Arquitetura	Desenvolver uma visão de alto nível das capacidades, que estabelece um projeto de arquitetura, identifica *stakeholder* e suas preocupações, requisitos e objetivos do negócio, avalia as capacidades de negócio e prepara para transformações, define a *scope*, elabora princípios e desenvolve métricas de avaliação de *performance*, acrescentando valor ao negócio.
B	Visão de Negócio	Desenvolver uma arquitetura de negócio, que descreve estratégias para alcançar metas e responder aos pontos definidos na visão da arquitetura, fazendo corresponder o trabalho da arquitetura com as preocupações dos *stakeholders*. Entre os passos sugeridos para esta fase, destaca-se a descrição da arquitetura de negócio (de base e objectivo), o *roadmap* de componentes e análise de lacunas, revisão formal dos *stakeholders* e a criação de um documento da definição da arquitetura.
C	Arquitetura de Sistemas de Informação	Desenvolver uma arquitetura de sistema de informação que descreva a forma de aplicação da arquiteturas de negócio e da visão de arquitetura. Nesta fase o TOGAF junta as arquiteturas de dados e de aplicação. Entre os passos para o desenvolvimento, define-se nesta fase uma descrição e base para a arquitetura de dados e um objetivo para a arquitetura aplicacional, o *roadmap* de componentes e análise de lacunas, revisão formal dos *stakeholders* e a criação de um documento da definição da arquitetura.
D	Arquitetura de Tecnologia	Desenvolver a arquitetura tecnológica, que se pretende alcançar de forma a habilitar aplicações físicas e lógicas e os componentes de dados da visão de arquitetura. Prevê-se nesta fase a resolução de inconformidades.
E	Oportunidades e Soluções	Gerar a versão inicial da Arquitetura com base na análise de lacunas e do *roadmap* de componentes identificados nas fase B,C e D.
F	Planeamento de Migrações	Terminar o *roadmap* de Arquitetura e apoiar o Plano de Implementação e Migração, garantir que a implementação e o Plano de Migração são coordenado com a abordagem da empresa de gestão de mudanças, por fim, garantir os custo do trabalho e arquiteturas de transição são compreendidos pelas principais partes interessadas.
G	Governação da Implementação	Garantir a conformidade da arquitetura alvo implementando projetos previamente definidos. Os passos que definem as execução desta fase incluem definir prioridades, responsabilidades, recursos e revisões de conformidade.
H	Arquitetura de Gestão de Mudanças	Garantir a manutenção do ciclo de vida da arquitetura, e execução da *framework* de governação e que a capacidade da arquitetura empresarial corresponde aos requisitos.

Tabela 8: TOGAF ADM - fases

2.9.2 Phase C - Arquitetura de sistemas de informação

Por fazer sentido para o trabalho desenvolvido, mais se detalha a "Fase C - Arquitetura de sistemas de informação", em particular, arquitetura de informação.

Nesta fase do método TOGAF ADM, existem dois objetivos claros: (1) Definir a Arquitetura do Sistema de Informação de pretendido (Dados e Aplicação), descrevendo de que forma o sistema de informação irá servir a arquitetura de negocio e visão de arquitetura, de forma a relacionar os requisitos às necessidades dos *stakeholders*; (2) Indicar os componente de arquitetura que se propõem a colmatar as lacunas identificadas. Com estes dois objetivos. pretende-se a apresentação de uma arquitetura aplicacional e uma arquitetura de dados (informação).

Pela essência do presente trabalho, considera-se que a arquitetura aplicacional, por implicar uma arquitetura empresarial (ne negócio) existente, se encontra fora do âmbito.

A arquitetura de informação, refere-se à gestão e estrutura da informação de um sistema, pois define a informação utilizada pelos processos de uma organização. Os dados presentes na arquitetura de informação, podem ter a forma de catálogos ou componentes de dados, entidades de informação, matrizes (dados/processos ou funções, dados/aplicações) e diagramas (existem alguns diagramas específicos previstos pelo TOGAF que podem descrever desde conceitos, relações lógicas até ao ciclo de vida dos dados).

Os passos para desenvolver uma arquitetura de informação encontram-se bem definidos no método, sendo que este trabalho se deixa influenciar pelos mesmos, seguindo critérios que promovem o desenvolvimento da descrição de bases e objetivos da arquitetura de dados, pelo propósito de resolver incongruências do cenário global, pela necessidade de garantir a definição de uma arquitetura, e de a documentar formal e apropriadamente.

No decorrer desta investigação, não foram encontrados estudos que relacionassem diretamente estratégias nacionais de segurança da informação com arquitetura empresarial, apesar da evidente relação entre ambas. Em particular, os estudos realizados a respeito destas transposições de normas internacionais para o contexto das nações, têm por objetivo, procurar soluções para lacunas nestes documentos, no âmbito da (in)segurança da informação. No que respeita à implementação e verificação de sistemas implementados, existem soluções comerciais para o efeito, direcionadas para o campo das certificações, em particular em ISO 27001. Por esse motivo, considera-se que o método resultante da presente investigação, será uma mais valia no âmbito da implementação e validação de medidas de segurança da informação no contexto nacional.

Em suma, a Estratégia Nacional de Segurança do Ciberespaço em Portugal expressa-se pelo QNRCS, uma transposição da Diretiva NIS e dos seus princípios, requisitos, controlos e melhorias. As medidas definidas nesta estratégia são transversais aos setores de atividade e áreas de negócio devendo ser utilizadas numa perspectiva de melhoria contínua. As práticas e controlos recomendados pelo documento, são impulsionadas por recomendações internacionais, fundamentais para o desenvolvimento desta investigação, em particular o ISO / IEC 27001, a Diretiva (UE) 2016/1148, os controlos CIS CSC 7.0 e o quadro CCOBIT 5 . Nesta secção comparou-se Portugal a outros países da UE na implementação de estratégias de cibersegurança e apresentou-se uma revisão de conceitos de arquitetura empresarial fundamentais para o enquadramento da investigação.

3 Desenho da Solução e Produção de Resultados

Face à proposta de encontrar uma ferramenta de suporte ou verificação da implementação das medidas de segurança, determinadas pelo QNRCS, realizou-se uma análise prévia e um conjunto de ferramentas e documentos que o suportam. Desta análise, verificou-se a existência de um conjunto de evidências, que servem como prova da implementação da estratégia de segurança de informação e cibersegurança definida para o contexto nacional. No entanto, não foi encontrada nenhuma forma material simplificada ou estruturada, que facilite a identificação destes documentos.

3.1 Método da Solução

O método utilizado para alcançar a uma solução, cresceu iterativamente mediante as oportunidades oferecidas por cada iteração. O diagrama da figura 5 sumaria os passos da abordagem que se descreve de seguida.

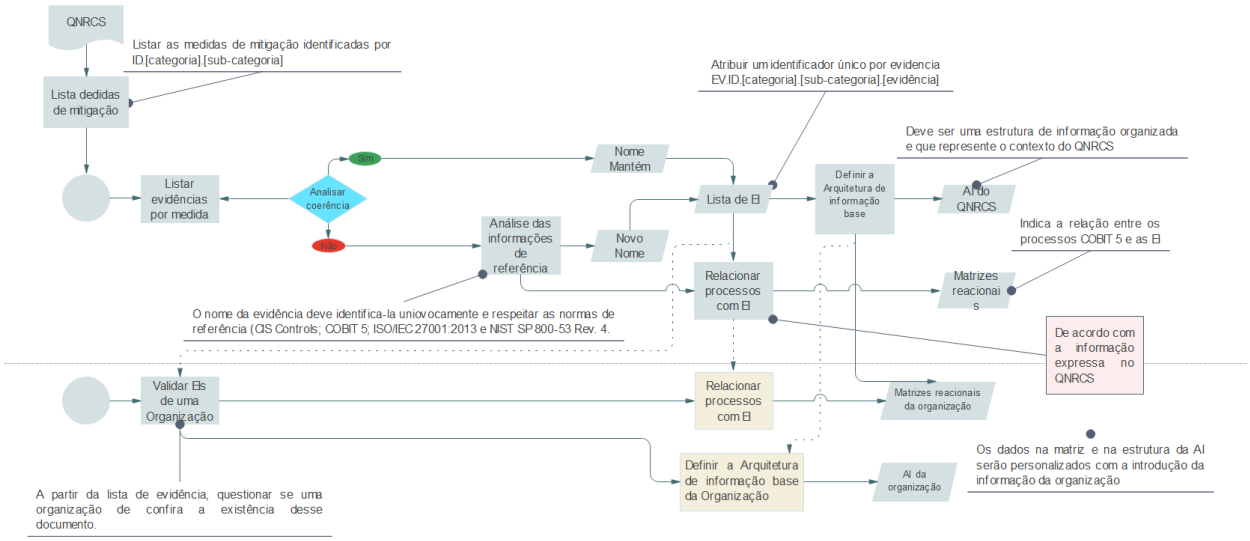


Figura 5: Diagrama do método utilizado

Procedeu-se a uma avaliação mais detalhada da documentação relativa ao QNRCS, levantando-se a hipótese de encontrar uma possível estrutura de informação composta pelos documentos referidos (as evidências), e desta forma enquadra-la no conceito de arquitetura de informação. Por cada categoria definida no QNRCS, sugere-se a implementação de medidas de segurança da informação, estando estas enquadradas em categorias, que se dividem em subcategorias. A implementação das medidas de seguranças referidas em cada uma destas subcategorias, dá origem a uma ou mais evidências de implementação por medida de mitigação. As referidas evidências, são tratadas neste estudo como entidades de informação (EI). Do conceito de arquitetura de informação, pretende-se demonstrar as EI aqui tratadas, formam a arquitetura de informação dos processos de segurança da informação, também referidos pelo QNRCS. Numa primeira abordagem, procurou-se elaborar uma lista de evidências e identificá-las como entidades de informação, que por sua vez formam a arquitetura de informação definida pelo QNRCS.

A partir do "Anexo 1 - Quadro Resumo"[2] do QNRCS, disponível no site do CNCS , foi possível obter uma lista de todas as medidas de segurança em questão. Posteriormente foi criado o ficheiro "**ENTIDADES DE INFORMAÇÃO**"[3], sobre o qual se realizaram as alterações que em seguida se descreve. Adicionou-se uma coluna com o nome "ID", servindo esta para isolar o identificador das subcategorias (já presente no documento), de forma a facilitar a manipulação da informação. Adicionou-se a coluna "Evidências", onde foram inseridas as evidências referentes a cada ID, como mostra a figura 6, que representa um recorte da primeira linha da tabela em questão.

OBJETIVO	CATEGORIA	SUBCATEGORIA	INFORMAÇÕES DE REFERÊNCIA	ID	Evidências
IDENTIFICAR (ID)	**Gestão de ativos (ID.GA)**	ID.GA-1 – Os dispositivos físicos, redes e sistemas de informação existentes na organização devem ser inventariados	CIS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8, PM-5	ID.GA-1	Inventário atualizado dos ativos com informação de inventário; Identificação dos responsáveis pelos ativos; Classificação dos ativos em função da sua criticidade.

Figura 6: Recorte da tabela **ENTIDADES DE INFORMAÇÃO** - Evidências

Com a listagem de evidências completa, identificou-se que, vários documentos são referidos pelo mesmo nome, sendo que, pelo contexto em que se encontram podem não representar o mesmo documento. Na figura 7, pode verificar-se que a evidência "Documento de suporta a metodologia de gestão de risco", comprova a implementação das subcategorias ID.AR-3 e ID.GR-2, não obstante de uma ser referenciada por NIST SP 800-53 Rev. 4 **RA-3, SI-5, PM-12, PM-16** (Avaliação de risco; Alertas de segurança, recomendações e diretivas; Programa de ameaças internas; Programa de Consciencialização de Ameaças) e a outra por NIST SP 800-53 Rev. 4 **PM-9** (Estratégia de Gestão de Risco). Apesar dos aspetos em comum, foi necessária uma análise detalhada da informação disponível no QNRCS, assim como, de toda a informação de referência, de forma a viabilizar uma proposta de nome unívoco para ambas as evidências.

OBJETIVO	CATEGORIA	SUBCATEGORIA	INFORMAÇÕES DE REFERÊNCIA	ID	Evidências
Identificar	**Avaliação de risco (ID.AR)**	ID.AR-3 – As ameaças internas e externas devem ser identificadas e documentadas na metodologia de gestão do risco	CIS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 ISO/IEC 27001:2013 Clause 6.1.2 NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16	ID.AR-3	Documentos que suportem a metodologia de gestão do risco
	Estratégia de Gestão de Risco (ID.GR)	ID.GR-2 – A organização deve determinar e identificar a sua tolerância ao risco	COBIT 5 APO12.06 ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3 NIST SP 800-53 Rev. 4 PM-9	ID.GR-2	Documentos que suportem a metodologia de gestão do risco

Figura 7: Recorte do quadro **ENTIDADES DE INFORMAÇÃO** - Demonstração de ambiguidade

Para efetuar o escrutínio quanto à ambiguidade do nome destes documentos, é imprescindível uma análise cuidada das normas indicadas na coluna "INFORMAÇÕES DE REFERÊNCIA", pelo que, para maior clareza foram adicionadas 4 grupos de informação referente a: CIS Controls; COBIT 5; ISO/IEC 27001:2013 e NIST SP 800-53 Rev. 4. A figura 8 demonstra a alteração.

CIS Controls	CIS Controls Descrição	COBIT	Processos BAI	Processos DSS	Processos APO	Processos EDM	Processos MEA	ISO/IEC 27001:2013	Descrição	NIST SP 800-53 Rev. 4	Descrição
		COBIT 5, APO12.02			Gestão de Risco.			ISO/IEC 27001:2013,	Tratamento de risco de segurança da	NIST SP 800-53 Rev. 4 S	Análise de criticidad
CIS CSC 4	Configuração segura de ativos corporativos e software	COBIT 5 APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02	Gestão de Programas, Gestão de Definição de Requisitos, Gestão de Disponibilidade e capacidade		Gestão de Fornecedores., Gestão de Risco., Gestão de Segurança.			ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2	Política de Segurança da Informação para Relações com Fornecedores, Relacionar os contratos de fornecedores com segurança, Tecnologia de comunicação e informação da Cadeia logística; Monitorização e revisão de serviços de fornecedor, Gestão de alterações nos serviços de fornecedores.	NIST SP 800-53 Rev. 4 SA-9, SA-12, PM-9	Serviços de sistema de informação externos; Proteção da cadeia logística; Estratégia de Gestão de Risco

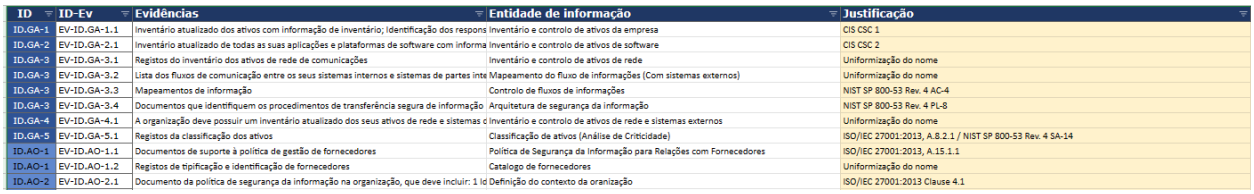
Figura 8: Recorte do quadro **ENTIDADES DE INFORMAÇÃO** - Normas

[2] https://www.cncs.gov.pt/pt/quadro-nacional/quadro-resumo
[3] https://docs.google.com/spreadsheets/d/1E65zYZvAMyj04ctpVyK5p$_k$7 − 5$CB5FqgmLKkXwNEX_s$/$edit?usp = sharing$

O ficheiro **ENTIDADES DE INFORMAÇÃO**, apresenta a informação em estudo, começando pela apresentação em 5 folhas, de cada categoria definida pelo QNRCS. As alterações anteriormente referidas foram realizadas para todos as categorias, estabelecendo-se assim, o conjunto de dados que formam a base deste estudo.

Iniciou-se uma análise detalhada dos requisitos do QNRCS e das informações de referência, a partir da compilação de toda a informação presente no mapa da folha "ANÁLISE"do mesmo ficheiro.

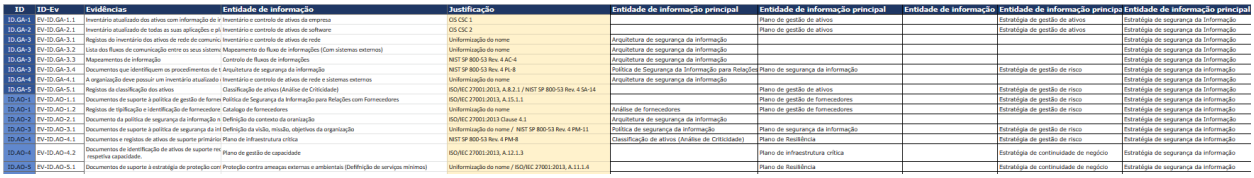
Na folha "Entidades de Informação", expõe-se o resultado desta análise. As colunas "ID"e "Evidências"são copiadas integralmente, e foi adicionada a coluna "ID-Ev"que introduz um identificador único para cada evidência, tal como se exige para uma entidade de informação. Foi adicionada a coluna "Entidade de informação"onde se propõe uma alteração ao nome da evidência, sempre que se justifique. Na coluna "Justificação"encontra-se a informação de referência que influencia a escolha do nome para cada entidade de informação [13][14]. A figura 9 é demonstrativa da folha em questão.



ID	ID-Ev	Evidências	Entidade de informação	Justificação
ID.GA-1	EV-ID.GA-1.1	Inventário atualizado dos ativos com informação de inventário; Identificação dos respons	Inventário e controlo de ativos da empresa	CIS CSC 1
ID.GA-2	EV-ID.GA-2.1	Inventário atualizado de todas as suas aplicações e plataformas de software com informa	Inventário e controlo de ativos de software	CIS CSC 2
ID.GA-3	EV-ID.GA-3.1	Registos do inventário dos ativos de rede de comunic	Inventário e controlo de ativos de rede	Uniformização do nome
ID.GA-3	EV-ID.GA-3.2	Lista dos fluxos de comunicação entre os seus sistemas internos e sistemas de partes inte	Mapeamento do fluxo de informações (Com sistemas externos)	Uniformização do nome
ID.GA-3	EV-ID.GA-3.3	Mapeamentos de informação	Controlo de fluxos de informações	NIST SP 800-53 Rev. 4 AC-4
ID.GA-3	EV-ID.GA-3.4	Documentos que identifiquem os procedimentos de transferência segura de informação	Arquitetura de segurança da informação	NIST SP 800-53 Rev. 4 PL-8
ID.GA-4	EV-ID.GA-4.1	A organização deve possuir um inventário atualizado dos seus ativos de rede e sistemas c	Inventário e controlo de ativos de rede e sistemas externos	Uniformização do nome
ID.GA-5	EV-ID.GA-5.1	Registos da classificação dos ativos	Classificação de ativos (Análise de Criticidade)	ISO/IEC 27001:2013, A.8.2.1 / NIST SP 800-53 Rev. 4 SA-14
ID.AO-1	EV-ID.AO-1.1	Documentos de suporte à política de gestão de fornecedores	Política de Segurança da Informação para Relações com Fornecedores	ISO/IEC 27001:2013, A.15.1.1
ID.AO-1	EV-ID.AO-1.2	Registos de tipificação e identificação de fornecedores	Catalogo de fornecedores	Uniformização do nome
ID.AO-2	EV-ID.AO-2.1	Documento da política de segurança da informação na organização, que deve incluir: 1 Id	Definição do contexto da oranização	ISO/IEC 27001:2013 Clause 4.1

Figura 9: Recorte da folha **Entidades de Informação** - Entidade de informação

Criou-se a folha "Dados para ARQUITETURA DE INFORMAÇÃO"que junta a informação da folha anterion a 4 colunas novas (figura 10), reservadas para as entidades de informação principal, que partilham uma relação hierárquica com cada EI (i.e. políticas, planos ou estratégias referentes à segurança da informação). As EI referidas, constituem uma arquitetura de informação base resultante das medidas que compõem a "Estratégia de Segurança da Informação".



ID	ID-Ev	Evidências	Entidade de informação	Justificação	Entidade de informação principal	Entidade de informação principal	Entidade de informação	Entidade de informação principa	Entidade de informação principal
ID.GA-1	EV-ID.GA-1.1	Inventário atualizado dos ativos com informação de ir	Inventário e controlo de ativos da empresa	CIS CSC 1		Plano de gestão de ativos		Estratégia de gestão de ativos	Estratégia de segurança da Informação
ID.GA-2	EV-ID.GA-2.1	Inventário atualizado de todas as suas aplicações e pl	Inventário e controlo de ativos de software	CIS CSC 2		Plano de gestão de ativos		Estratégia de gestão de ativos	Estratégia de segurança da Informação
ID.GA-3	EV-ID.GA-3.1	Registos do inventário dos ativos de rede de comunic	Inventário e controlo de ativos de rede	Uniformização do nome	Arquitetura de segurança da informação				Estratégia de segurança da Informação
ID.GA-3	EV-ID.GA-3.2	Lista dos fluxos de comunicação entre os seus sistem	Mapeamento do fluxo de informações (Com sistemas externos)	Uniformização do nome	Arquitetura de segurança da informação				Estratégia de segurança da Informação
ID.GA-3	EV-ID.GA-3.3	Mapeamentos de informação	Controlo de fluxos de informações	NIST SP 800-53 Rev. 4 AC-4	Arquitetura de segurança da informação				Estratégia de segurança da Informação
ID.GA-3	EV-ID.GA-3.4	Documentos que identifiquem os procedimentos de t	Arquitetura de segurança da informação	NIST SP 800-53 Rev. 4 PL-8	Política de Segurança da Informação para Relações	Plano de segurança da Informação		Estratégia de gestão de risco	Estratégia de segurança da Informação
ID.GA-4	EV-ID.GA-4.1	A organização deve possuir um inventário atualizado	Inventário e controlo de ativos de rede e sistemas externos	Uniformização do nome	Arquitetura de segurança da informação				Estratégia de segurança da Informação
ID.GA-5	EV-ID.GA-5.1	Registos da classificação dos ativos	Classificação de ativos (Análise de Criticidade)	ISO/IEC 27001:2013, A.8.2.1 / NIST SP 800-53 Rev. 4 SA-14		Plano de gestão de ativos		Estratégia de gestão de risco	Estratégia de segurança da Informação
ID.AO-1	EV-ID.AO-1.1	Documentos de suporte à política de gestão de forne	Política de Segurança da Informação para Relações com Fornecedores	ISO/IEC 27001:2013, A.15.1.1		Plano de gestão de fornecedores		Estratégia de gestão de risco	Estratégia de segurança da Informação
ID.AO-1	EV-ID.AO-1.2	Registos de tipificação e identificação de fornecedore	Catalogo de fornecedores	Uniformização do nome	Análise de fornecedores	Plano de gestão de fornecedores		Estratégia de gestão de risco	Estratégia de segurança da Informação
ID.AO-2	EV-ID.AO-2.1	Documento da política de segurança da informação n	Definição do contexto da oranização	ISO/IEC 27001:2013 Clause 4.1	Arquitetura de segurança da informação				Estratégia de segurança da Informação
ID.AO-3	EV-ID.AO-3.1	Documentos de suporte à política de segurança da inf	Definição da visão, missão, objetivos da organização	Uniformização do nome / NIST SP 800-53 Rev. 4 PM-11	Política de segurança da Informação	Plano de segurança da Informação		Estratégia de gestão de risco	Estratégia de segurança da Informação
ID.AO-4	EV-ID.AO-4.1	Documentos e registos de ativos de suporte primários	Plano de Infraestrutura crítica	NIST SP 800-53 Rev. 4 PM-8	Classificação de ativos (Análise de Criticidade)	Plano de Resiliência		Estratégia de gestão de risco	Estratégia de segurança da Informação
ID.AO-4	EV-ID.AO-4.2	Documentos de identificação de ativos de suporte res respetiva capacidade.	Plano de gestão de capacidade	ISO/IEC 27001:2013, A.12.1.3		Plano de Infraestrutura crítica		Estratégia de continuidade de negócio	Estratégia de segurança da Informação
ID.AO-5	EV-ID.AO-5.1	Documentos de suporte à estratégia de proteção com	Proteção contra ameaças externas e ambientais (Definição de serviços mínimos)	Uniformização do nome / ISO/IEC 27001:2013, A.11.1.4		Plano de Resiliência		Estratégia de continuidade de negócio	Estratégia de segurança da Informação

Figura 10: Recorte da folha **Dados para ARQUITETURA DE INFORMAÇÃO** - Entidades de informação principal

Neste ponto, reúnem-se as condições para evidenciar a relação dos processos COBIT 5 indicados pelo QNRCS com as entidades de informação apuradas. Os dados foram trabalhado num ficheiro distinto, **Matriz_De_Processos-EI**[4], onde se alcançam os resultados da análise de processos/entidades de informação. Neste ficheiro, a folha **MATRIZ** inclui todas as EI e processos COBIT 5 referidos no QNRCS. A folha **MACRO PROCESSOS** reduz os processos específicos a macro processos para melhor legibilidade, ou seja, nesta iteração os processos COBIT 5 referidos para cada medida de mitigação, são agrupados em processos EDM, BAI, DSS, APO e MEA, de forma a reduzir o numero de processos a representar, os quais se passa a referir como "macro processos". A folha **MACRO PROCESSOS'** é outra iteração da folha

[4]https://docs.google.com/spreadsheets/d/13xd8hisWNCapZ1IiFd19h5R-lO8$_U vTwpSeuJxqIuqk/edit?usp = sharing$

anterior adicionando as cores do QNRCS para cada objectivo, para melhor identificação gráfica. A relação Processos-EI é apresentada por categorias, (i.e) a folha **IDENTIFICAR** cruza todos processos com as entidades de informação referidos nas medidas que pertencem à categoria identificar. A folha **IDENTIFICAR'** representa uma iteração da anterior, onde se ordena a informação de forma a excluir processos sem relação com as entidades de informação. Este procedimento repete-se para as cinco categorias. As matrizes têm o propósito de uma matriz CRUD, e servem de apoio à criação de *vistas* ou diagramas, oferecendo um suporte gráfico da implementação (ou validação) do documento em estudo. A figura 11, ilustra o resultado das iterações referidas, quanto à matriz IDENTIFICAR'.

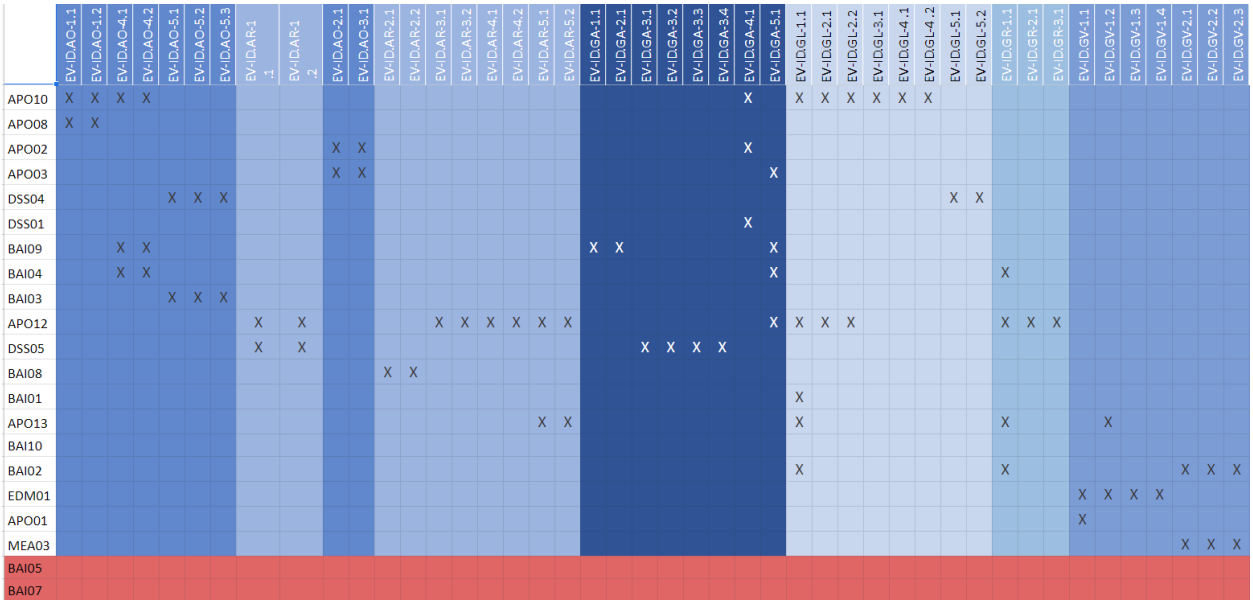


Figura 11: Recorte da **Matriz_De_Processos-EI.xlsx** - IDENTIFICAR'

A partir desta matriz e considerando os macro processos anteriormente referidos, é possível verificar que mediante a existência de todas as entidades de informação ali presentes, a organização deverá ter implementados os processos referidos no diagrama ou *viewpoint* da figura 12

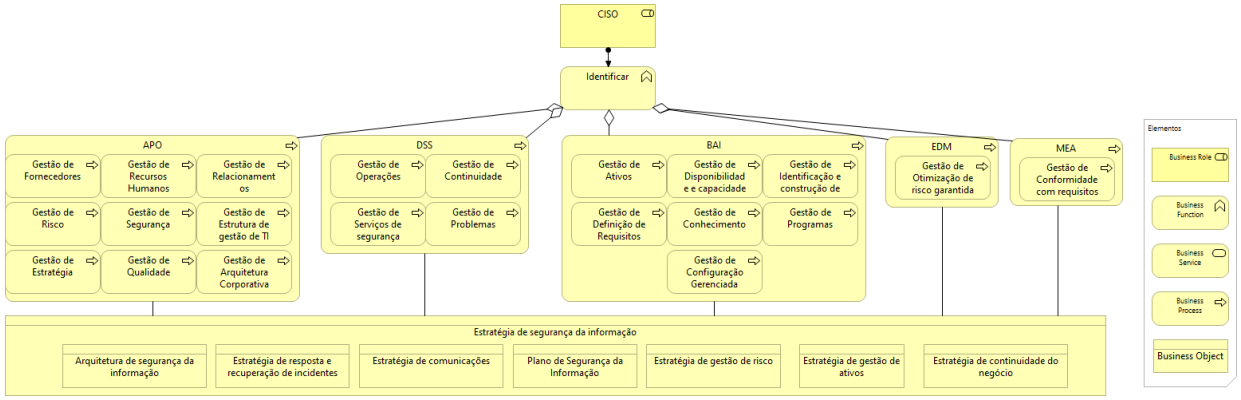


Figura 12: *Viewpoint* dos processos a implementar considerando o objectivo **Identificar**

Este passo na construção da ferramenta, permite aferir quais os processos implementados, com base na documentação existente. Por exemplo, uma organização que identifique a não existência das EI EV-ID.AO-1.1, EV-ID.AO-1.2, EV-ID.AO-4.1, EV-ID.AO-4.2, EV-ID.GA-4.1, EV-ID.GL-1.1, EV-ID.GL-2.1, EV-ID.GL-2.2, EV-ID.GL-3.1, EV-ID.GL-4.1 e EV-ID.GL-4.2, poderá ter em falta a implementação do processo COBIT 5 **APO10 - Gestão de risco**, como esclarece a figura 13

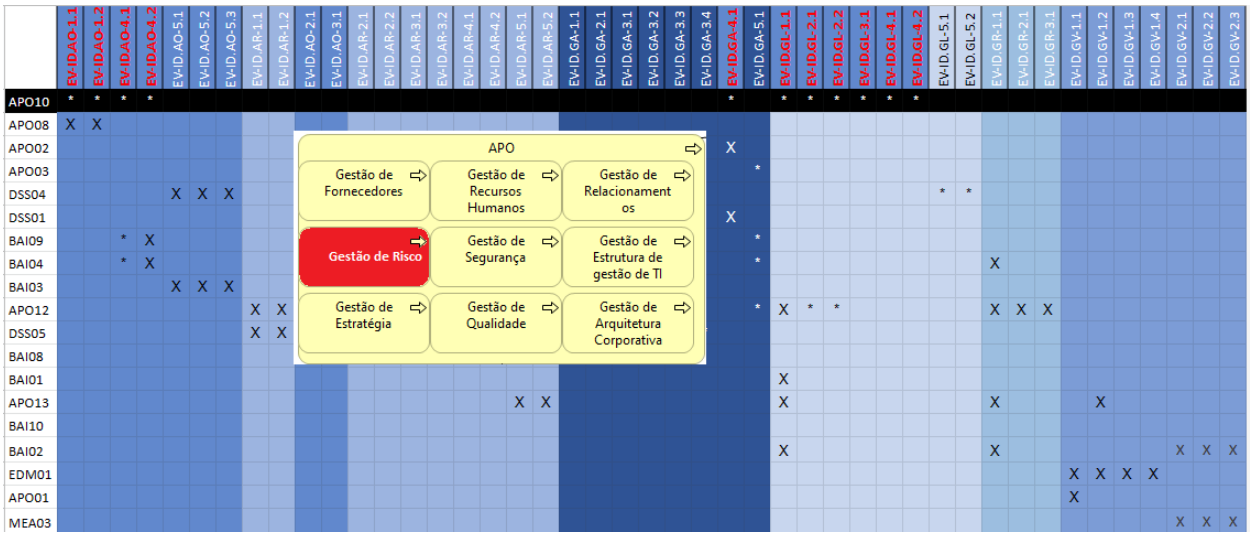
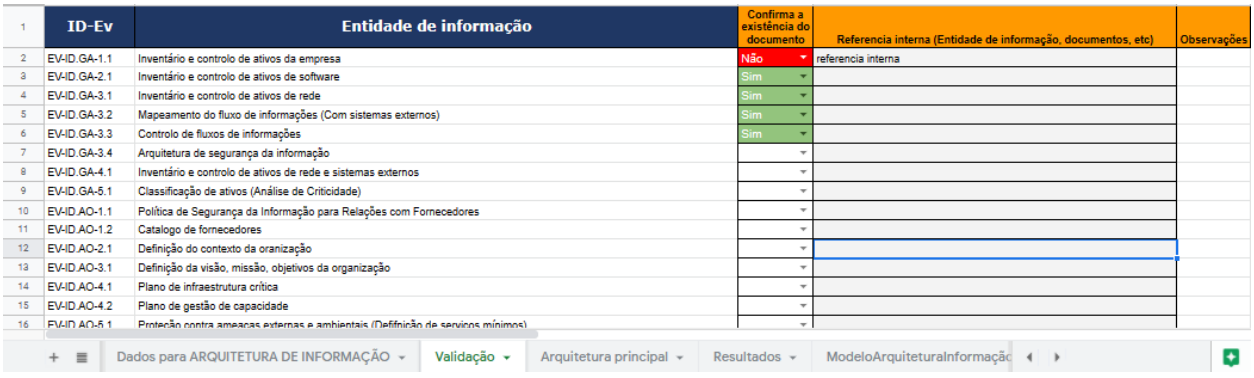


Figura 13: Evidencias afetas ao processo APO10 - gestão de risco

Para determinar quais os processos existentes numa organização, criou-se o mapa **"Check_List"**[5], Composto pelas folhas DADOS e VALIDAÇÃO. A ultima servirá para que uma organização verifique a existência dos documentos listados (EI) indicando **Sim** ou **Não** conforme existam ou não os documentos. Na mesma folha, a organização deve inserir na coluna 'Referencia interna (Entidade de informação, documentos, etc)', para que seja indicado (caso se justifique) o nome da EI usado internamente na organização. Esta coluna, irá permitir que, sem alterações internas, a organização consiga mapear a sua arquitetura de informação, com a definida por este trabalho, enquadrando os documentos existentes no modelo que aqui se apresenta. Os *viewpoints* relativos a cada categoria são disponibilizados no Anexo 1 - Viewpoints.



	ID-Ev	Entidade de informação	Confirma a existência do documento	Referencia interna (Entidade de informação, documentos, etc)	Observações
2	EV-ID.GA-1.1	Inventário e controlo de ativos da empresa	Não	referencia interna	
3	EV-ID.GA-2.1	Inventário e controlo de ativos de software	Sim		
4	EV-ID.GA-3.1	Inventário e controlo de ativos de rede	Sim		
5	EV-ID.GA-3.2	Mapeamento do fluxo de informações (Com sistemas externos)	Sim		
6	EV-ID.GA-3.3	Controlo de fluxos de informações	Sim		
7	EV-ID.GA-3.4	Arquitetura de segurança da informação			
8	EV-ID.GA-4.1	Inventário e controlo de ativos de rede e sistemas externos			
9	EV-ID.GA-5.1	Classificação de ativos (Análise de Criticidade)			
10	EV-ID.AO-1.1	Política de Segurança da Informação para Relações com Fornecedores			
11	EV-ID.AO-1.2	Catalogo de fornecedores			
12	EV-ID.AO-2.1	Definição do contexto da oranização			
13	EV-ID.AO-3.1	Definição da visão, missão, objetivos da organização			
14	EV-ID.AO-4.1	Plano de infraestrutura crítica			
15	EV-ID.AO-4.2	Plano de gestão de capacidade			
16	EV-ID.AO-5.1	Proteção contra ameaças externas e ambientais (Definição de serviços mínimos)			

Figura 14: Recorte da tabela VALIDAÇÂO do documento **Check_List**

[5]https://docs.google.com/spreadsheets/d/1NaMzFVhMWF8q9KfL$_T$7*sbOCljZ*603*CqMcqZSj*5u1$_w$*U/edit?usp = sharing*

Após a recolha dos dados, estes são trazidos para o ficheiro "ENTIDADES DE INFORMAÇÃO", mantendo o nome da folha "VALIDAÇÃO", a partir da qual são alimentadas as folhas "ARQUITETURA PRINCIPAL"e "RESULTADOS". Estas folhas encontram-se ligadas com a folha "VALIDAÇÃO"permitindo visualizar a evolução da arquitetura de informação. Para melhor entendimento, na imagem 15, podemos verificar que a estratégia de segurança da informação é *à priori* composta por 14 documentos. Cada um destes documentos representa uma entidade de informação principal, que pode ser composta por outras entidades do mesmo tipo ou pelas entidades de informação apuradas, aqui referidas pelo seu identificador, e quantificadas por 1 ou 0 conforme exista ou não esse documento na organização.

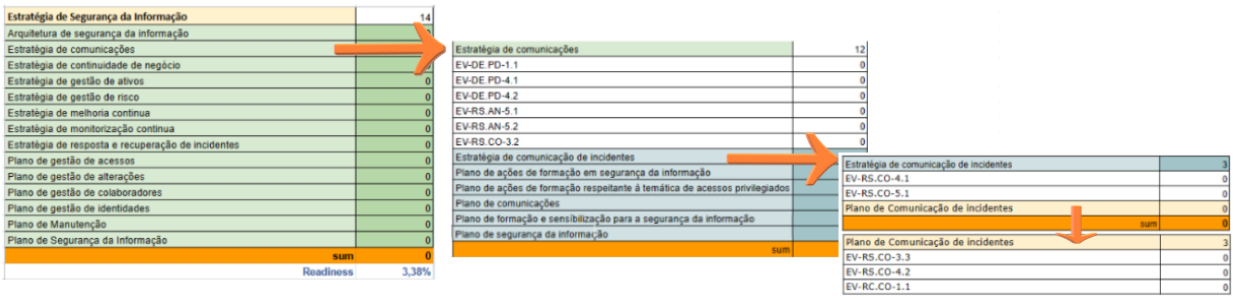


Figura 15: Montagem com tabelas presentes na folha RESULTADOS.

No exemplo da figura, pode ver-se quais as entidades de informação principal que compõem a 'Estratégia de Segurança da Informação'. Pode igualmente observar-se qUe a entidade de informação principal 'Estratégia de comunicações' é definida pelas entidades de informação EV-DE.PD-1.1, EV-DE.PD-4.1, EV-DE.PD-4.2, EV-RS.AN-5.1, EV-RS.AN-5.2 e EV-RS.CO-3.2, e pelas entidades de informação principal 'Estratégia de comunicação de incidentes', 'Plano de ações de formação em segurança da informação', 'Plano de ações de formação respeitante à temática de acessos privilegiados', 'Plano de comunicações', 'Plano de formação e sensibilização para a segurança da informação' e 'Plano de segurança da informação'. Também se detalha a composição da 'Estratégia de comunicação de incidentes' e o 'Plano de comunicação de incidentes'. O preenchimento da folha "VALIDAÇÃO", permite contabilizar as entidades de informação existentes na organização, o que permite calcular a percentagem de EIs existentes por cada entidade de informação principal, e portando, a verificação do estado (de maturidade) em que se encontra a definição da arquitetura de informação.

A folha 'Processos (*readiness*)', permite validar quais os processos que deverão estar implementados, ou em falta, de acordo com os documentos assinalados como existentes. Num procedimento semelhante ao anterior, é medido o estado de prontidão dos macro processos COBIT 5, calculando valores médios ponderado, cujo peso está relacionado com o número de entidades de informação por cada processo. A figura 16 mostra parcialmente a folha em questão, onde se demonstra que (i.e) o processo APO01.02 está relacionado com 8 entidades de informação, enquanto que o processo APO01.03 se relaciona apenas com uma. Esta relação está expressa no QNRCS.

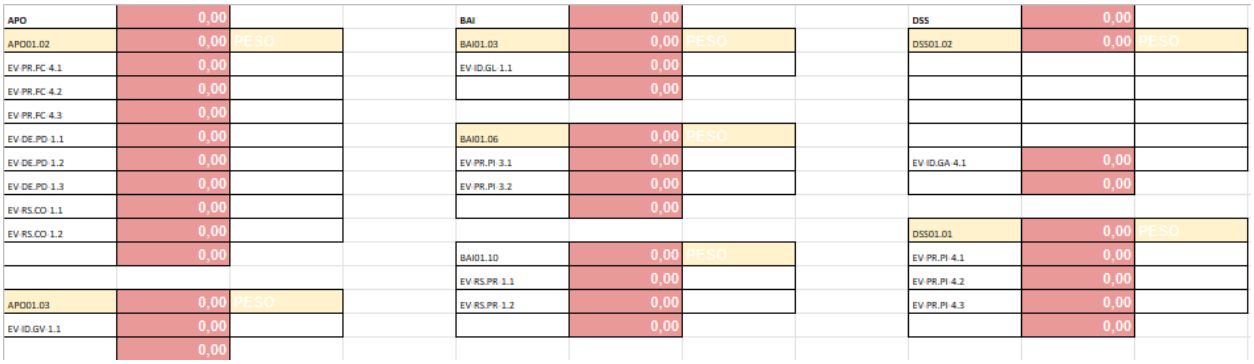


Figura 16: Montagem com tabelas presentes na folha 'Processos (*readiness*)'.

Para resumir a informação referente aos processos, criou-se a folha 'Processos resumo' onde se apresentam os cálculos finais quanto à prontidão dos processos. Os resultados estão dispostos por processos COBIT 5 e por objectivos do QNRCS, como mostra a figura 17

	PROCESSOS	Implementado
COBIT 5	APO	0,00%
	BAI	0,00%
	DSS	0,00%
	EDM	0,00%
	MEA	0,00%

Implementação de processos por objetivo			
OBJETIVOS	Implementado	TOTAL EI	EI EXISTENTES
IDENTIFICAR	0,00%	45	0
PROTEGER	0,00%	112	0
DETETAR	0,00%	51	0
RESPONDER	0,00%	36	0
RECUPERAR	0,00%	8	0

Figura 17: Tabelas presentes na folha 'Processos resumo'.

Este método, prevê a recolha de um tipo de informação, que pode ser trabalhada em níveis de detalhe mais profundos ou personalizados do que aqui se apresenta, de forma a satisfazer necessidades específicas das organizações que o utilizem.

3.2 Quadro-modelo da arquitetura da informação

O QNRCS apresenta um conjunto de recomendações que permitem a definição de uma **Estratégia para a segurança da informação** das organizações, oferecendo uma abordagem homogénea que pretende contribuir para a resposta às ciberameaças, ao nível nacional .

O QNRCS é um documento extenso, e embora o CNCS disponibilize metodologias de suporte à sua implementação, tais como o Quadro de Avaliação de Capacidades de Cibersegurança, o CiberCheckUp e o Roteiro para as Capacidades Mínimas de Cibersegurança, existe a necessidade de visualizar o que pretende ser esta estratégia, tanto para a sua implementação como para a verificação de conformidade em arquiteturas já implementadas.

Além disso, as organizações procuram cada vez mais incluir de forma estrutural nas suas arquiteturas empresariais, metodologias que suportem a segurança das suas redes e sistemas de informação. Os processos de construção definidos em termos de arquitetura empresarial, incluem a conceitos como a definição de princípios e padrões que fortalecem a garantia de segurança, exigida pelas normas da indústria e pela própria lei. A modelação da arquitetura, exige saber de forma clara, quais os processos a implementar e qual a sua

relação com as entidades de informação presentes na arquitetura de informação.

A utilização de técnicas de arquitetura empresarial de acordo com a The Open Group Architecture Framework (TOGAF), vem permitir se enquadrem as propostas do QNRCS endereçando as preocupações, identificando e refinando a motivação e a estratégia expressas, desenvolvendo uma arquitetura de informação com base na informação presente no QNRCS, assim como nos documentos sugeridos como informações de referência.

O método utilizado para definir as entidades de informação, assim como, as relações existentes entre os documentos da estrutura apresentada, encontra-se exposto na secção 3.3.1,

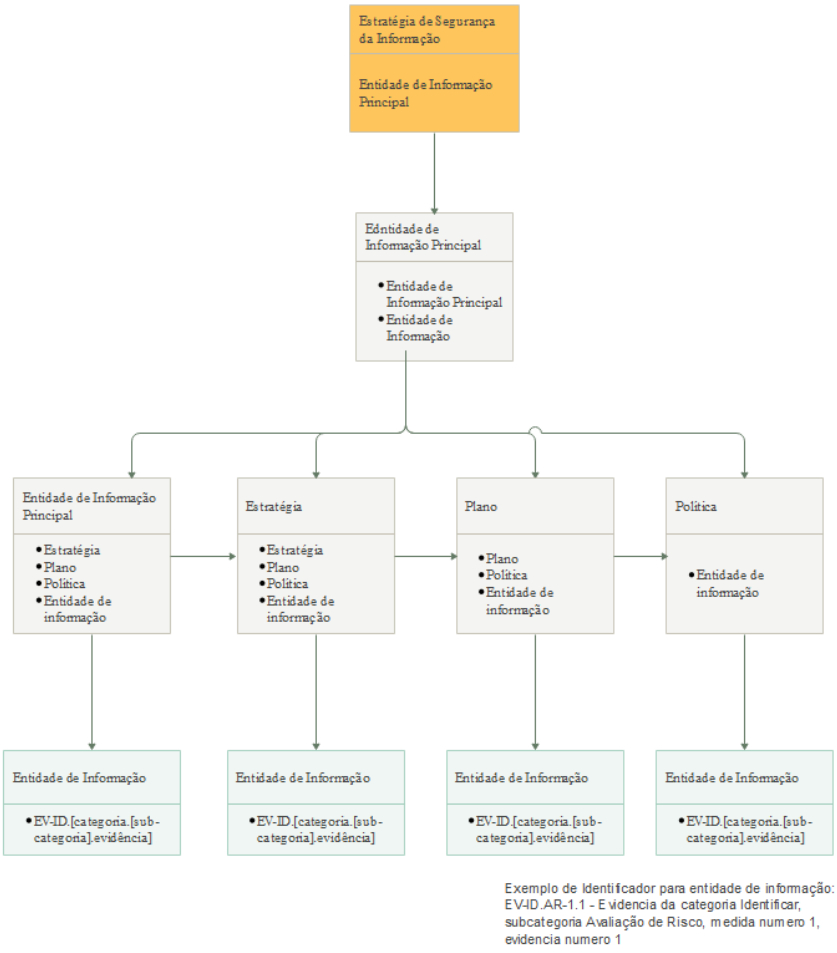


Figura 18: Estrutura da informação

3.3 Arquitetura de Informação

Depois de reunir toda a informação sobre os documentos (evidências) exigidos pelo QNRCS, e analisar as informações de referência para cada documento, é necessário realizar uma análise cuidada das relações existentes entre as entidades de informação.

Por definição, uma arquitetura contempla conceitos fundamentais que definem um ambiente, nos seus princípios e desenho. Como modelo, ou seja, numa perspetiva descritiva, uma arquitetura é o conhecimento sobre a construção de um sistema. Por sua vez, uma arquitetura de informação, define a informação usada por

processos, à qual chamamos 'entidades de informação', e as relações entre si. Estas entidades de informação devem ser identificadas de forma unívoca.

O modelo desenvolvido neste trabalho, representa uma possível arquitetura numa perspetiva prescritiva, no sentido em que concentra a informação descrita no QNRCS num conjunto de entidades de informação principal, reduzindo o grau de liberdade e dispersão da informação gerada. De acordo com os conceitos básicos da *Zachman Framework*, pretende-se enquadrar as relações e características das entidades de informação que compõem a arquitetura de informação aqui desenvolvida, ao nível de abstração das medidas determinadas pelo QNRCS.

O QNRCS apresenta um conjunto de recomendações que permitem a definição de uma estratégia de segurança da informação. Das recomendações indicadas, é possível apurar a existência de um conjunto de documentos, que compõem a estratégia de segurança de informação aos quais designámos por **entidades de informação principais**.

Seguindo o principio base do *TOGAF Content Metamodel*, a arquitetura de informação é aqui apresentada num modelo ou *framework* (quadro) onde se identifica uma possível estrutura para a arquitetura de informação desenvolvida no QNRCS, expondo os seus conteúdos, composição e as relações entre as entidades de informação. Neste modelo, pretende-se evidenciar como se encontra estruturada a arquitetura de informação, e em particular que a estratégia de segurança de informação, de acordo com o descrito ao longo do QNRCS, é composta como se descreve nas subsecções que se seguem.

3.3.1 Entidades de Informação

O desenvolvimento desta arquitetura de informação, nasce da análise cuidada da documentação proposta pelo QNRCS como evidências de implementação. Estas evidências, assim como as informações de referência indicadas para cada uma delas, analisadas com forte escrutínio, permite reunir um conjunto de entidades de informação, identificadas univocamente com um ID, atribuído de forma lógica quanto à sua correspondência com a subcategoria a que se refere.

A análise destas entidades de informação, inclui concluir sobre a relação de cada entidade com documentos estruturais da arquietura de informação, ou seja, permite validar que, a **Estratégia para a segurança da informação** é composta por outras estratégias e por planos de gestão, que por sua vez são compostos por politicas, registos e outros documentos que em conjunto, todas as outras entidades de informação, desenham o âmbito do contexto definido pelo QNRCS.

Ao definir claramente as entidades de informação referidas pelo QNRCS, tornam-se evidentes, quais os processos a implementar e qual a relação entre ambos, o que permite a apresentação de matrizes que expressam esta relação. Estruturar a informação numa fase inicial de projeto, faz parte das boas práticas de *Security by Design*, visando entre outras coisas, a identificação clara das informações que se pretende proteger. Este estudo identificou a partir do QNRCS e das informações de referência, uma possível arquitetura de informação organizada como se resume no diagrama da figura **??**, e se detalha nas secções que se seguem

3.3.2 Arquitetura de segurança da informação

De acordo o QNRCS a Arquitetura de segurança da informação, é um documento que inclui as as entidades de informação identificadas por EV-ID.GA-3.1, EV-ID.GA-3.2, , EV-ID.GA-3.3, EV-ID.GA-4.1, EV-ID.AO-2.1, EV-PR.GA-5.1, EV-PR.GA-5.2, EV-PR.GA-5.4, EV-PR.GA-5.5, EV-PR.TP-4.2 e EV-PR.TP-4.3.

3.3.3 Estratégia de comunicações

De acordo com o QNRCS, a estratégia de comunicação deve ser consolidada pelas entidades de informação EV-DE.PD-1.1, EV-DE.PD-4.1, EV-DE.PD-4.2, EV-RS.AN-5.1, EV-RS.AN-5.2 e EV-RS.CO-3.2, e consolidado com outros planos e estratégias existentes na organização, tais como:

- Estratégia de comunicação de incidentes;
- Plano de ações de formação em segurança da informação;
- Plano de ações de formação respeitante à temática de acessos privilegiados;
- Plano de comunicações;
- Plano de formação e sensibilização para a segurança da informação;
- Plano de segurança da informação.

3.3.4 Estratégia de continuidade de negócio

De acordo com o QNRCS e com o Anexo A.17 do ISO/IEC 27001:2013, a continuidade da segurança da informação deve ser incorporada nos sistemas de gestão da continuidade do negócio da organização, mitigando eventuais adversidades, provocadas por crises ou catástrofe. Apurou-se que no modelo encontrado esta estratégia é composta por:

- Plano de continuidade de negócio;
- Plano de infraestrutura crítica;
- Plano de Resiliência.

3.3.5 Estratégia de gestão de ativos

A gestão de ativos prevista nas normas ISO/IEC 27001:2013 e NIST SP 800-53 Rev. 4, e seguida pelo QNRCS inclui na sua descrição um 'Plano de gestão de ativos' composto pelas EI EV-ID.GA-1.1, EV-ID.GA-2.1, EV-PR.PI-6.2, EV-PR.PI-6.3 e EV-PR.MA-1.3.

3.3.6 Estratégia de gestão de risco

Sendo o QNRCS composto por medidas de mitigação de risco, a estratégia de gestão de risco é um dos documentos mais importantes, composto pelas entidades de informação identificadas por EV-DE.AE-3.3, EV-DE.MC-1.3, EV-ID.GR-1.1, EV-ID.GR-3.1, EV-PR.FC-3.1, EV-PR.MA-2.4, EV-PR.SD-8.1 e EV-PR.SD-8.2. Sendo um dos documentos mais complexos da arquitetura encontrada, é igualmente composto pelas entidades que abaixo se listam:

- Plano de gestão de ativos;
- Plano de gestão de capacidade;
- Plano de gestão de eventos;
- Plano de gestão de fornecedores;
- Plano de gestão de Incidentes;
- Plano de gestão de risco;
- Plano de Manutenção;
- Plano de Resiliência;
- Plano de segurança da informação;

- Estratégia de monitorização continua.

3.3.7 Estratégia de melhoria continua

Segundo o QNRCS, uma organização deve garantir que aprende com os incidentes que ocorrem nas suas redes e sistemas de informação, num processo continuo de melhoria, definido na estratégia de melhoria continua. Esta é composta pelo conjunto de planos que se lista abaixo, e pelas entidades de informação EV-PR.PI-7.2, EV-PR.PI-7.3, EV-PR.PI-8.1, EV-PR.PI-8.2, EV-PR.PI-8.3 e EV-RC.ME-1.1.

- Plano de melhoria (processos de deteção);
- Plano de melhoria continua;
- Plano de resposta a incidentes;
- Plano de testes de deteção.

3.3.8 Estratégia de monitorização continua

A estratégia de monitorização continua inclui as EI EV-DE.MC-6.1 e EV-RS.MI-3.1.

3.3.9 Estratégia de resposta e de recuperação de incidentes

A resposta e recuperação de incidentes é um documento definido pelo QNRCS e fortemente suportado pelas normas de referência, composta pelas entidades de informação identificadas por EV-PR.PI-8.4, EV-PR.PI-9.1, EV-PR.PI-9.2, EV-RC.PR-1.1, EV-RS.AN-1.2 e EV-RS.PR-1.1, e pelos planos abaixo listados:

- Plano de gestão de vulnerabilidades;
- Plano de mitigação;
- Plano de mitigação (incidentes);
- Plano de mitigação (vulnerabilidades);
- Plano de recuperação de Incidentes;
- Plano de recuperação de informação;
- Plano de Resposta a Incidentes.

3.3.10 Plano de gestão de acessos

No modelo de arquitetura de informação encontrado, um plano de gestão de acessos deve incluir as medidas de mitigação que se evidenciam pelas EI EV-PR.GA-1.2, EV-PR.GA-2.1, EV-PR.GA-2.2, EV-PR.GA-3 .1, EV-PR.GA-4.1, EV-PR.GA-4.2, EV-PR.GA-4.3, EV-PR.GA-5.3, EV-PR.GA-6.2, EV-PR.GA-6.3, EV-PR.GA-6.4, EV-PR.GA-7.1, EV-PR.GA-7.2, EV-PR.PI-5.1, EV-PR.TP-2.2, EV-PR.TP-3.1, EV-PR.TP-3.2 e EV-PR.TP-3.3, e pela definição de 'Políticas e procedimentos de gestão do teletrabalho e acessos remotos'.

3.3.11 Plano de gestão de alterações

De acordo com o QNRCS, e com as informações de referência nele indicadas, em particular relativas às categorias proteger e detetar, um plano de gestão de alterações deve incluir as medidas evidenciadas pelas EI EV-PR.PI-1.1, EV-PR.PI-1.2, EV-PR.PI-3.1, EV-PR.PI-3.2, EV-DE.AE-1.1, EV-DE.AE-1.2 e EV-DE.AE-1.3.

3.3.12 Plano de gestão de colaboradores

De acordo com o QNRCS, um plano de gestão de colaboradores deve incluir as medidas que geram as evidências EV-PR.PI-11.1 e EV-PR.PI-11.2.

3.3.13 Plano de gestão de identidades

De acordo com o QNRCS, e com as informações de referência nele indicadas, em particular relativas aos controlos AC-1, AC-2 e IA-4 da norma NIST SP 800-53 Rev. 4, a gestão de identidades deve apresentar-se num plano organizado que preveja as medidas relacionadas com as EI EV-PR.GA-1.1. EV-PR.GA-1.3 e EV-PR.GA-6.1.

3.3.14 Plano de Manutenção

A manutenção e todos os aspetos relacionados com a prestação deste serviço devem ser salvaguardados conforme as medidas expressas pelo QNRCS que resultam nas evidências EV-PR.PI-5.2, EV-PR.MA-1.1, EV-PR.MA-1.2, EV-PR.MA-1.4, EV-PR.MA-2.2 e EV-PR.MA-2.3.

3.3.15 Plano de segurança da informação

Muitas das medidas de mitigação de risco apresentadas pelo QNRCS fazem parte do planeamento de acções estruturantes de segurança como as que resultam nas entidades de informação EV-ID.GV-1.2, EV-PR.SD-1.1, EV-PR.SD-1.2, EV-PR.SD-1.3, EV-PR.SD-2.1, EV-PR.SD-2.3, EV-PR.SD-3.1, EV-PR.SD-3.2, EV-PR.SD-3.3, EV-PR.SD-5.1, EV-PR.SD-5.2, EV-PR.SD-5.3, EV-PR.SD-6.1, EV-PR.SD-6.2, EV-PR.PI-2.1, EV-PR.TP-2.1, EV-PR.TP-2.3 e EV-DE.MC-5.2. A arquiteura de informação encontrada neste estudo, inclui como parte do plano em questão os seguintes documentos:

- Política de transferência de informação;
- Política de desenvolvimento seguro de software;
- Política de segurança da informação.

O QNRCS define 252 medidas de mitigação de risco, cada uma delas gera como evidência de implementação uma ou mais entidades de informação, que por sua vez se agrupam em entidades de informação principal como planos, políticas ou estratégias. Dado que o resumo apresentado não inclui a totalidade das entidades de informação, disponibiliza-se a informação completa no "Anexo 4 - Arquitetura de informação (estrutura)".

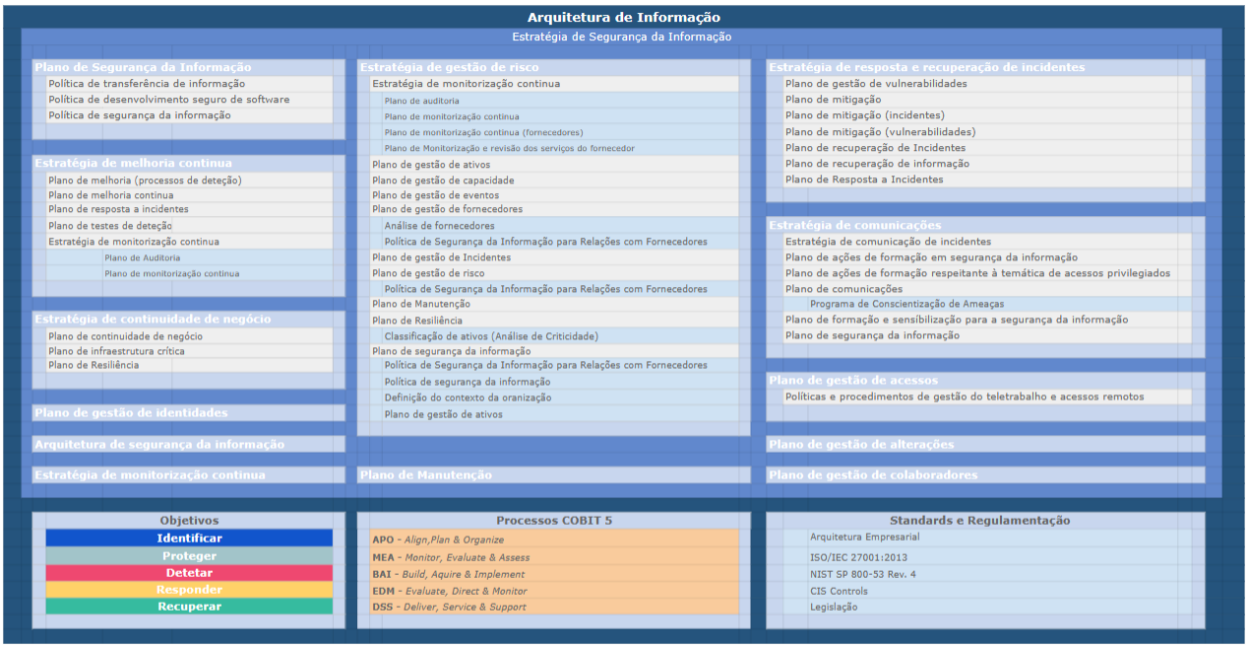


Figura 19: Quadro-Modelo: *Uma* Arquitetura da Informação para o QNRCS

A partir desta análise, é então possível propor uma arquitetura de informação, que estrutura a informação de acordo com o contexto definido pelo QNRCS, reservando um espaço para apresentar os processos COBIT 5 já referidos, as categorias em que se agrupam as medidas de mitigação, as referências normativas em que se baseiam as medidas e as informações de referencia que suportam esta investigação, conforme se demonstra na figura 19, também disponibilizada para maior legibilidade no "Anexo 5 - *Uma* Arquitetura da Informação para o QNRCS".

Em suma, o método para desenhar a solução parte de uma primeira lista das evidências de implementação, da qual se verifica a coerência ou não do nome das evidências.Nomes incoerentes ou duplicados são sujeitos a uma análise criteriosa de todas as informações de referência, de forma a encontrar um nome coerente. Estes Documentos passam a ser tratados como entidades de informação, e são identificadas as relações entre si, que origina a criação de uma estrutura organizada da informação que representa o contexto definido pelo QNRCS. Como resultado é possível uma organização aferir a sua situação atual de implementação de processos e estruturar a sua própria arquitetura de informação.

4 Avaliação e Resultados

De forma a validar a investigação realizada, este capítulo é dedicado à apresentação de alguns aspetos de carácter qualitativo do trabalho desenvolvido. Numa primeira abordagem, trata-se a ferramenta desenvolvida como um artefacto, para uma análise de pontos fortes e pontos fracos, guiada pelos parâmetros da metodologia DSRM (*Science Research Methodology*). Posteriormente são apresentados resultados de um caso de estudo, para validação por observação dos resultados. Além da auto crítica, é apresentada a opinião de um especialista de forma a corroborar a utilidade da ferramenta.

4.1 Medidas de Avaliação

Analisaram-se alguns métodos conhecidos para avaliação de ferramentas na área dos sistemas de informação, tendo sido eleito o método DSRM como o mais adequado tendo em conta a natureza da investigação realizada. A tabela 9 descreve os aspetos do método referido.

Atividade	Preocupações	Aprendizagem
1. Identificação do problema e motivação	Definir o problema e enaltecer a importância da solução	Inferência sobre a situação anual que justifica a investigação.
2. Definição dos objetivos da solução	Descrição teórica da solução, indicação dos critérios que resolvem os aspetos do problema.	Reconhecimento dos métodos, tecnologias e aspetos teóricos da solução.
3. Desenho e desenvolvimento	Desenvolvimento de um artefato que resolve o problema, incluindo métodos, modelos ou *frameworks*	Implementação das tecnologias e conhecimentos no desenvolvimento da solução.
4. Demonstração	Observação de resultados da utilização do artefato	Usabilidade do artefato.
5. Avaliação	Analise qualitativa do artefato quanto é promessa de cumprir os objetivos	Identificação de métricas relevantes.
6. Comunicação	Comunicar o problema, a solução e a utilidade para a área científica da investigação e para outras audiências relevantes	-

Tabela 9: Descrição dos aspetos em avaliação - orientado pelo método DSRM

Seguindo uma lógica DSRM, é necessário realizar algumas considerações, que permitem o enquadramento com as linhas orientadoras do método. Assim, são requisitos do método que a investigação deve conduzir ao desenvolvimento de um artefato, na forma de um método, modelo ou instanciação. Este artefato deve resolver um problema de relevância na área científica da investigação. A utilidade, qualidade e eficácia do artefato, deve ser demonstrada rigorosamente, e apresentados os métodos de avaliação. Devem ser apresentadas as contribuições da investigação, que se pretende rigorosa na metodologia e avaliação. Durante o desenvolvimento devem utilizar-se as ferramentas e tecnologias disponíveis, dentro da lei. A investigação deve ser apresentada para audiências de interesse tecnológico e ou de gestão (que podem beneficiar com o uso). Tendo sido esclarecido o método, procede-se a avaliação do trabalho realizado [15].

1. Identificação do problema e motivação - No capítulo 1, o problema é exposto de forma clara tanto no que confere ao panorama atual da cibersegurança em termos do mundo global, como transpondo para a realidade nacional. É dado um contexto ao problema que emerge da análise prévia do QNRCS

em relação á nomenclatura da documentação requerida pelo mesmo documento. As motivações são expostas num capítulo inteiramente dedicada ao assunto. Os aspetos relevantes para o enquadramento do problema e da solução, são descritos no capítulo 2.

2. Definição dos objetivos da solução - No capítulo 1.3, esclarecem-se os resultados esperados no âmbito da investigação, descrevendo o que se pretende alcançar durante o desenvolvimento. Encontra-se no mesmo capítulo a descrição dos problemas que a ferramenta desenvolvida pretende resolver, bem como os critérios para que seja eficiente no seu propósito.

3. Desenho e desenvolvimento - No capítulo 3, descreve-se detalhadamente a construção da solução. Ao longo da investigação são frequentes as referencias a métodos, *frameworks* e conceitos que suportam o desenvolvimento. Demonstram-se funcionalidades da ferramenta com apresentação cenários para possíveis resultados.

4. Demonstração - No capítulo 4.2, é realizado um *Case Study* para demonstração da ferramenta, e das suas funcionalidades.

5. Avaliação - Na demonstração, são apresentados resultados que validam a qualidade e importância do trabalho realizado. Além disso, para validação do trabalho como um todo é apresentada no capítulo 4.3, uma entrevista ao diretor do CNSC, entidade responsável pelo QNRCS, transcrita na integra.

6. Comunicação - São expostas questões que se consideram importantes para o entendimento histórico, contextual, teórico e prático tanto no âmbito do problema como da solução.

De seguida resume-se na tabela 10 uma análise de pontos fracos e pontos fortes da investigação e do artefato desenvolvido.

Ponto	Avaliação	Output	[○●]
1.	O texto é concreto e claro quanto aos factos, por vezes pouco sucinto.	São apresentados exemplos concretos para facilitar o entendimento.	[● ● ● ● ○○]
2.	A solução é explicada em varias secções, aumentando o detalhe de aspetos conforme se justifique mediante o contexto do capítulo. Os métodos que impulsionam a implementação, são referidos e explicados conforme necessário.	A implementação do método TOGAF ADM não é rigorosa, justamente devido á dificuldade de implementar medidas de arquitetura empresarial face a abstracção de uma arquitetura de negócio sub adjacente.	[● ● ● ○ ○○]
3.	São apresentadas todas funcionalidades propostas, pelo que se considera um bom trabalho em termos de desenvolvimento e com grande potencial de crescimento quanto à sua aplicabilidade. A análise de resultados é apresentada de forma clara, com a apresentação de tabelas e diagramas.	Existem ferramentas mais adequadas para o desenvolvimento realizado, como PowerBi ou mesmo o desenvolvimento de software para o efeito. Nota-se claramente a falta de conhecimento técnico na modelação ArchiMate. Considera-se que a qualidade em termos de design é apenas satisfatória.	[● ● ● ○ ○○]
4.	Os resultados são apresentados considerando um método observacional, apresentado em forma de caso de estudo, o que se considera ter sido uma boa decisão. Os resultados do caso de estudo, são explorados de forma a demonstrar o máximo de aspetos possíveis.	A ferramenta é pouco intuitiva (*user frendly*).	[● ● ● ○ ○○]
5.	É realizada com sucesso uma validação qualitativa do trabalho.	Devido á falta de ferramentas para comparação, não são apresentada métricas de avaliação comparativa.	[● ● ● ○ ○○]
6.	A investigação persegue uma resposta ao problema de forma eficiente e é apresentada a audiências de interesse.	A inexperiência do autor em trabalhos de investigação pode induzir a uma ideia de relevância questionável da ferramenta desenvolvida.	[● ● ○ ○ ○○]

Tabela 10: Tabela de auto-avaliação $\bullet - aspetopositivo$ $\circ - aspetonegativo$

Em 24 pontos (negativos + positivos), a auto avaliação do trabalho indica um total de 18 pontos positivos, o que sugere satisfação do autor com os resultados conseguidos. Os pontos negativos são claros quanto é necessidade de continuidade do trabalho.

4.2 Case Study

O objetivo deste capítulo é apresentar resultados práticos que possam representar numa *proof of concept*, a usabilidade da ferramenta desenvolvida, aplicada ao caso prático da organização AMA. Pretende-se considerar todos os objetivos do QNRCS, independente de uma análise de risco prévia, de forma a explorar os resultados no máximo de perspectivas possíveis.

4.2.1 Definição

A partir do preenchimento da folha 'Validação' (ficheiro Check_List), reúnem-se os dados inerentes à organização AMA. Realiza-se o mapeamento da informação recolhida com a existente na arquitectura de informação desenvolvida, de forma a demonstrar em que fase de implementação se encontra a organização. Com os dados recolhidos serão apresentados resultados nas três perspectivas da ferramenta, ou seja, resul-

tados quanto ao estado da arquitetura de informação, estado da implementação dos processos COBIT 5, apresentação das mesmas informações na perspectiva dos objetivos do QNRCS.

4.2.2 Uso da Ferramenta

Com todos os componentes da ferramenta descritos nos capítulo 3, este capítulo reserva-se à apresentação dos resultados do caso de estudo.

Após introdução dos dados recolhidos na folha VALIDAÇÃO, procedeu-se à análise de resultados, tendo como ponto de partida a estrutura de informação do diagrama da figura 20.A recolha de dados pode ser consultada no "Anexo 7 - Recolha de dados".

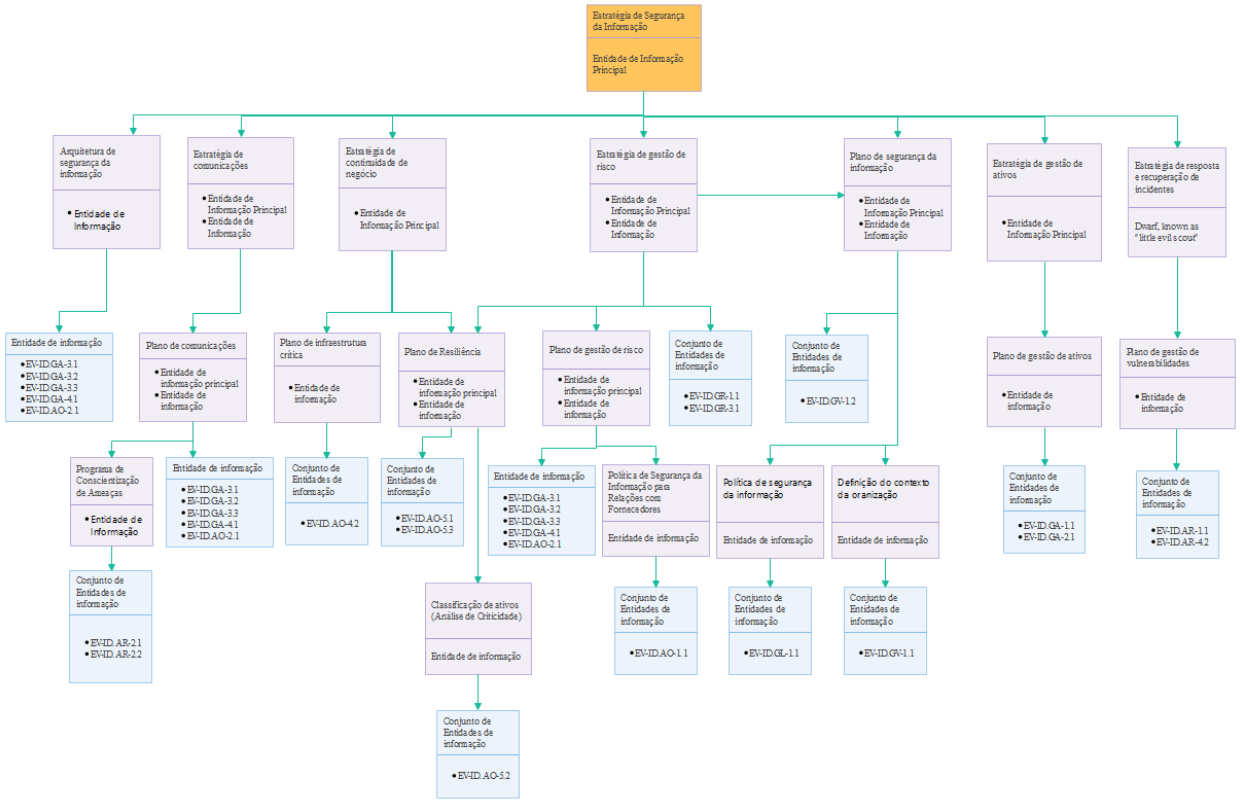


Figura 20: Estrutura da Informação da organização AMA mediante os dados fornecidos.

Na folha "Arquitetura principal", podemos observar que a entidade de informação principal **Estratégia de continuidade de negócio** se encontra assinalada com o número '1', o que significa que todas as EI na sua composição, foram confirmadas. Embora não seja evidente à partida, pode verificar-se na figura 21 que aumentando o numero de casas decimais da coluna de quantidades, verifica-se que foram confirmados outros documentos, apenas não representam a totalidade dos documentos que se agrupam para cada uma das restantes entidades de informação principal.

Estratégia de Segurança da Informação	14
Arquitetura de segurança da informação	0
Estratégia de comunicações	0
Estratégia de continuidade de negócio	1
Estratégia de gestão de ativos	0
Estratégia de gestão de risco	0
Estratégia de melhoria continua	0
Estratégia de monitorização continua	0
Estratégia de resposta e recuperação de incidentes	0
Plano de gestão de acessos	0
Plano de gestão de alterações	0
Plano de gestão de colaboradores	0
Plano de gestão de identidades	0
Plano de Manutenção	0
Plano de Segurança da Informação	0
sum	2
Readiness	13,27%

Estratégia de Segurança da Informação	14
Arquitetura de segurança da informação	0,45
Estratégia de comunicações	0,03
Estratégia de continuidade de negócio	0,67
Estratégia de gestão de ativos	0,40
Estratégia de gestão de risco	0,24
Estratégia de melhoria continua	0,00
Estratégia de monitorização continua	0,00
Estratégia de resposta e recuperação de incidentes	0,02
Plano de gestão de acessos	0,00
Plano de gestão de alterações	0,00
Plano de gestão de colaboradores	0,00
Plano de gestão de identidades	0,00
Plano de Manutenção	0,00
Plano de Segurança da Informação	0,05
sum	2
Readiness	13,27%

Figura 21: Estratégia de segurança da informação mediante os dados fornecidos pela organização AMA.

Seguindo para a folha RESULTADOS, é possível observar com maior detalhe, que a arquitetura de informação da AMA, se encontra 13.27% completa relativamente às evidencias de implementação em análise. Segue-se a análise das entidades de informação principal, cuja existência das EI que a compõem é superior a '0'.

4.2.3 Arquitetura de segurança da informação

De acordo com os dados recolhidos, a organização AMA confirma a existência das EI EV-ID.GA-3.1, EV-ID.GA-3.2, EV-ID.GA-3.3, EV-ID.GA-4.1 e EV-ID.AO-2.1 como se pode verificar na figura 22.

Arquitetura de segurança da informação	11
EV-ID.GA-3.1	1
EV-ID.GA-3.2	1
EV-ID.GA-3.3	1
EV-ID.GA-4.1	1
EV-ID.AO-2.1	1
EV-PR.GA-5.1	0
EV-PR.GA-5.2	0
EV-PR.GA-5.4	0
EV-PR.GA-5.5	0
EV-PR.TP-4.2	0
EV-PR.TP-4.3	0
sum	5

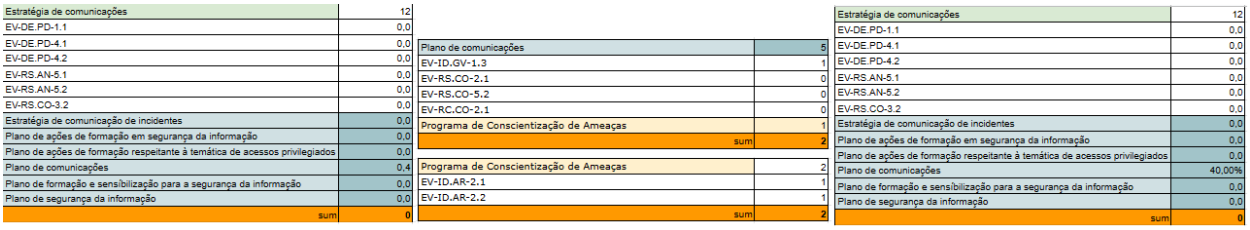
Figura 22: Estado da Arquitetura de segurança da informação da AMA.

Podendo assim concluir-se que se confirma a existência de 5 das 11 EI que compõem a 'Arquitetura de segurança da informação', ou seja, encontra-se 45,45% completa.

4.2.4 Estratégia de comunicações

Seguindo o mesmo raciocínio, verifica-se que foi confirmada a existência das EI EV-ID.GV-1.3 EV-ID.AR-2.1 e EV-ID.AR-2.2, que compõem o 'Programa de Conscientização de Ameaças'. Foi igualmente confirmada

a existência da EI EV-ID.GV-1.3. Desta forma, conclui-se que o 'Plano de comunicações' tem 2 de 5 das EI que o compõem, ou seja, está 40% completo, conforme se pode conferir na figura 23



Estratégia de comunicações	12
EV-DE.PD-1.1	0,0
EV-DE.PD-4.1	0,0
EV-DE.PD-4.2	0,0
EV-RS.AN-5.1	0,0
EV-RS.AN-5.2	0,0
EV-RS.CO-3.2	0,0
Estratégia de comunicação de incidentes	0,0
Plano de ações de formação em segurança da informação	0,0
Plano de ações de formação respeitante à temática de acessos privilegiados	0,0
Plano de comunicações	0,4
Plano de formação e sensibilização para a segurança da informação	0,0
Plano de segurança da informação	0,0
sum	0

Plano de comunicações	5
EV-ID.GV-1.3	1
EV-RS.CO-2.1	0
EV-RS.CO-5.2	0
EV-RC.CO-2.1	0
Programa de Conscientização de Ameaças	1
sum	2

Programa de Conscientização de Ameaças	2
EV-ID.AR-2.1	1
EV-ID.AR-2.2	1
sum	2

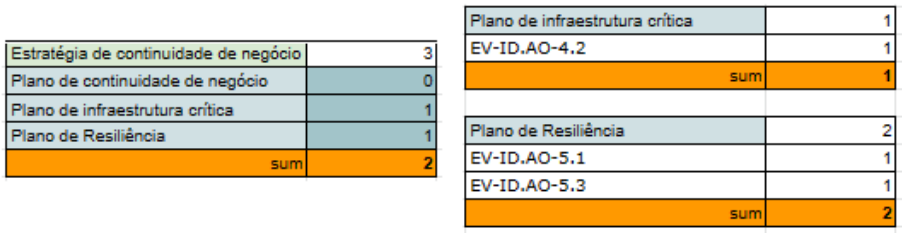
Estratégia de comunicações	12
EV-DE.PD-1.1	0,0
EV-DE.PD-4.1	0,0
EV-DE.PD-4.2	0,0
EV-RS.AN-5.1	0,0
EV-RS.AN-5.2	0,0
EV-RS.CO-3.2	0,0
Estratégia de comunicação de incidentes	0,0
Plano de ações de formação em segurança da informação	0,0
Plano de ações de formação respeitante à temática de acessos privilegiados	0,0
Plano de comunicações	40,00%
Plano de formação e sensibilização para a segurança da informação	0,0
Plano de segurança da informação	0,0
sum	0

Figura 23: Estado da Estratégia de comunicações da AMA.

Desta forma, sendo o Plano de comunicações, a única (de 12) EI confirmada na 'Estratégia de comunicações' pode dizer-se que a mesma se encontra 3,33% completa.

4.2.5 Estratégia de continuidade de negócio

De acordo com os dados recolhidos a 'Estratégia de continuidade de negócio' encontra-se 66,67% completa.



Estratégia de continuidade de negócio	3
Plano de continuidade de negócio	0
Plano de infraestrutura crítica	1
Plano de Resiliência	1
sum	2

Plano de infraestrutura crítica	1
EV-ID.AO-4.2	1
sum	1

Plano de Resiliência	2
EV-ID.AO-5.1	1
EV-ID.AO-5.3	1
sum	2

Figura 24: Estado da Estratégia de continuidade de negócio da AMA.

Conforme se pode verificar na figura 24, a 'Estratégia de continuidade de negócio' é composta pelo 'Plano de continuidade de negócio', do qual não foi confirmada a existência de nenhuma EI, pelo 'Plano de infraestrutura crítica' que contempla a EI EV-ID.AO-4.2, e pelo 'Plano de Resiliência', composto pelas EI EV-ID.AO-5.1 e EV-ID.AO-5.3 ambas validadas pela AMA.

4.2.6 Estratégia de gestão de ativos

Seguindo o método de validação usado até aqui, observa-se que, sendo a 'Estratégia de gestão de ativos' composta unicamente pelo 'Plano de gestão de ativos', e sendo que se confirmou a existência de 2 das 5 EI que o compõem, ou seja 40%, então pode dizer-se que a eEstratégia em epígrafe se encontra também 40% completa, conforme reflete a figura 25.

Estratégia de gestão de ativos	1
Plano de gestão de ativos	0,40
sum	0

Plano de gestão de ativos	5
EV-ID.GA-1.1	1
EV-ID.GA-2.1	1
EV-PR.PI-6.2	0
EV-PR.PI-6.3	0
EV-PR.MA-1.3	0
sum	2

Figura 25: Estado da Estratégia de gestão de ativos da AMA.

4.2.7 Estratégia de gestão de risco

Da análise dos dados, pode concluir-se que a 'Estratégia de gestão de risco' encontra-se 23.6% completa, como se pretende mostrar na figura 26.

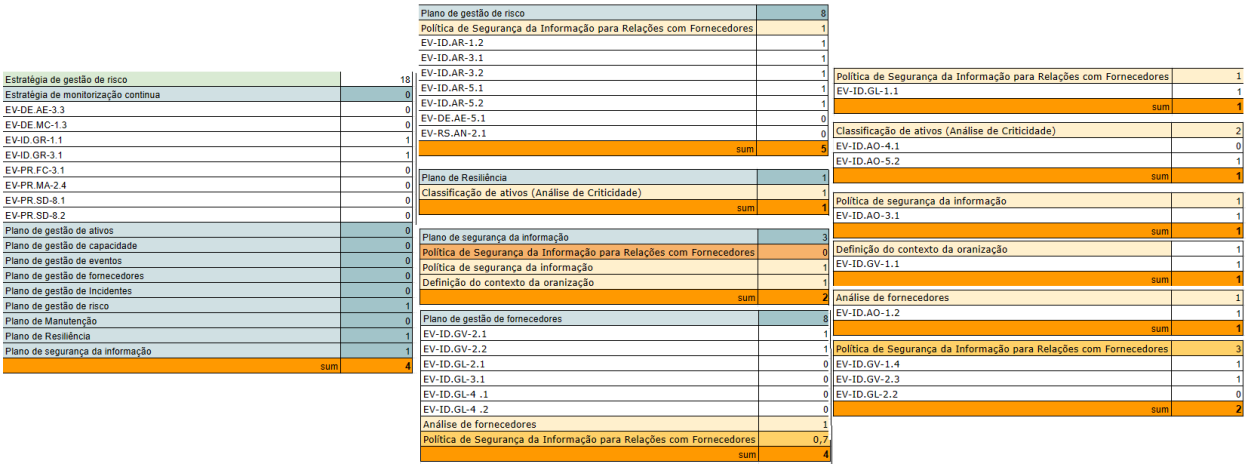


Figura 26: Estado da Estratégia de gestão de risco da AMA.

Analisando objetivamente os resultados, verifica-se a existência das EI EV-ID.GR-1.1 e EV-ID.GR-3.1, assim como do 'Plano de gestão de risco' composto pelo conjunto das EI EV-ID.AR-1.2, EV-ID.AR-3.1, EV-ID.AR-3.2, EV-ID.AR-5.1, EV-ID.AR-5.2, EV-DE.AE-5.1 e EV-RS.AN-2.1, e pela 'Política de Segurança da Informação para Relações com Fornecedores' que contempla a EI EV-ID.GL-1.1. Foi igualmente validada a existência de um 'Plano de Resiliência', contendo o documento 'Classificação de ativos (Análise de Criticidade)' composto por EV-ID.AO-4.1 e EV-ID.AO-5.2. Por fim, validou-se a existência de um 'Plano de segurança da informação', composto pela 'Política de Segurança da Informação para Relações com Fornecedores', pela 'Política de segurança da informação', e pela 'Definição do contexto da organização'. Estas três entidades de informação principal são compostas pelas EI EV-ID.GA-3.4, EV-ID.AO-3.1 e EV-ID.GV-1.1.

4.2.8 Estratégia de resposta e recuperação de incidentes

Apurou-se que 25% dos documentos que compõem o 'Plano de gestão de vulnerabilidades' existem na organização, e que este representa o único documento validado como existente.

Estratégia de resposta e recuperação de incidentes	13
EV-PR.PI-8.4	0,00
EV-PR.PI-9.1	0,00
EV-PR.PI-9.2	0,00
EV-RC.PR-1.1	0,00
EV-RS.AN-1.2	0,00
EV-RS.PR-1.1	0,00
Plano de gestão de vulnerabilidades	0,25
Plano de mitigação	0,00
Plano de mitigação (incidentes)	0,00
Plano de mitigação (vulnerabilidades)	0,00
Plano de recuperação de Incidentes	0,00
Plano de recuperação de informação	0,00
Plano de Resposta a Incidentes	0,00
sum	0

Plano de gestão de vulnerabilidades	8
EV-ID.AR-1.1	1
EV-ID.AR-4.2	1
EV-PR.PI-12.1	0
EV-PR.PI-12.2	0
EV-PR.PI-12.3	0
EV-DE.MC-8.1	0
EV-DE.MC-8.2	0
EV-RS.AN-5.3	0
sum	2

Figura 27: Estado da Estratégia de resposta e recuperação de incidentes da AMA.

A figura 33 mostra que o plano referido é composto pelas EI EV-ID.AR-1.1 e EV-ID.AR-4.2, representando 2 dos 8 documentos que o compõem, de acordo com a investigação realizada. Sendo que o 'Plano de gestão de vulnerabilidades', é o único de documento sinalizado de um conjunto de 13 que compõem a 'Estratégia de resposta e recuperação de incidentes', conclui-se que esta se encontra 1,92% completa.

4.2.9 Plano de Segurança da Informação

Apurou-se que apenas 1, de um conjunto de 21 documentos que fazem parte do 'Plano de Segurança da Informação', existe na organização. Esta informação permite afirmar que o plano em questão se encontra 4,76% completo.

No "Anexo 8 - Afetação de processos no caso de estudo"pode observar-se a relação entre as entidades de informação e cada um dos processos referenciados pelo QNRCS.

4.2.10 Processos COBIT 5

Avançando para a folha "PROCESSOS RESUMO", podemos concluir que, de acordo com a validação realizada, os processos COBIT 5 previstos pelo QNRCS, agrupados nos macro processos APO, BAI, DSS, EDM e MEA, pode dizer-se que se encontram desenvolvidos na percentagem apresentada na tabela da figura 28. Se considerarmos que cada macro processo referido representa 1/5 do total de processos previstos, então podemos dizer que 22,41% dos processos devem estar implementados nesta organização.

PROCESSOS		Implementado
COBUT 5	APO	14,87%
	BAI	13,67%
	DSS	6,83%
	EDM	46,67%
	MEA	30,00%

Figura 28: Percentagem de preparação dos macro processo da AMA.

Das 252 entidades de informação que se pretendia validar, foram validadas apenas as primeiras 38. Sendo que, não se pode concluir a não existência das restante, considerações sobre resultados estão limitadas à categoria identificar como se verifica na figura 29, visto que as primeiras 45 EI se referem a esta categoria apenas.

OBJETIVOS	Implementado	TOTAL EI	EI EXISTENTES
IDENTIFICAR	77,78%	45	35
PROTEGER	0,00%	112	0
DETETAR	0,00%	51	0
RESPONDER	0,00%	36	0
RECUPERAR	0,00%	8	0

Figura 29: Relação de EI existentes/previstas da AMA por objetivos.

De todo o modo, pode dizer-se que cerca de 78% das entidades de informação que comprovam a implementação das medidas de mitigação de risco, relativas à categoria Identificar, foram validadas como existentes. O que significa que das 45 EI que compõem esta categoria, a organização AMA confirma a existência de 35.

A matriz que resulta na folha IDENTIFICAR, relaciona os processos COBIT 5 com as EI para cada medida implementada, de acordo com o QNRCS. A figura 30 mostra essa relação para a organização AMA, sendo que, se a implementação de um processo está prevista, este encontra-se assinalado com **X** quando a coluna se cruza com uma EI validada como existente pela organização. Caso a organização não valide ou valide como inexistente uma determinada EI então o quadro assinala um * na relação EI/ processo prevista pelo QNRCS.

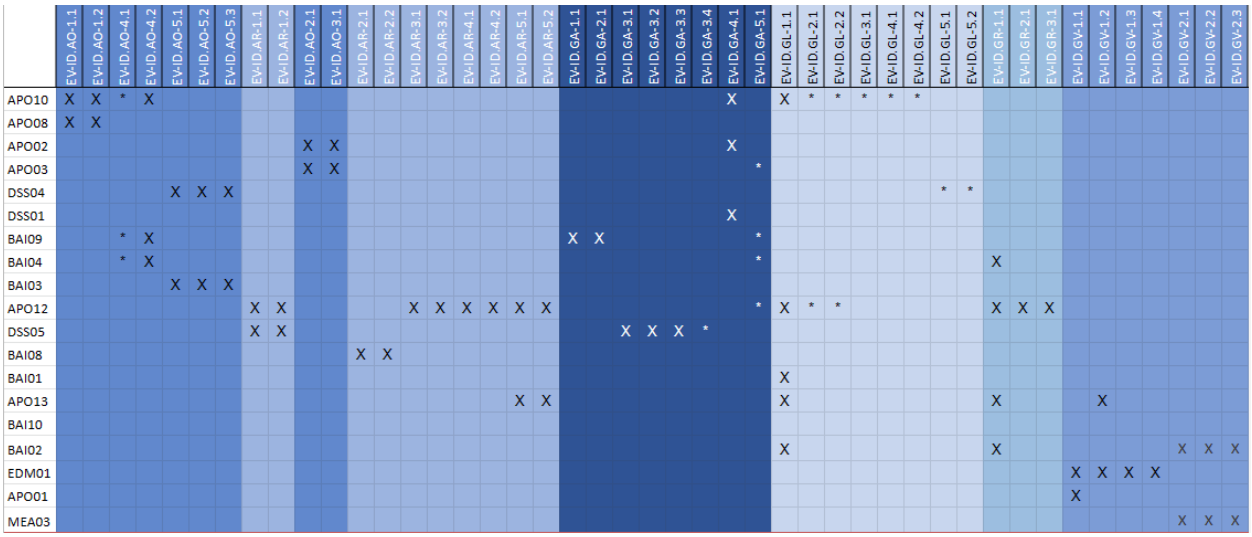


Figura 30: Matriz de processos/EI da categoria Identificar para a AMA.

A partir da matriz apresentada, podemos elaborar o diagrama da figura 31 que realça sobre os processos, a lacuna que se associa à falta das EI. Desta forma, a AMA pode avançar para uma melhoria, que pode ocorrer a nível da documentação ou dos processos (requer avaliação).

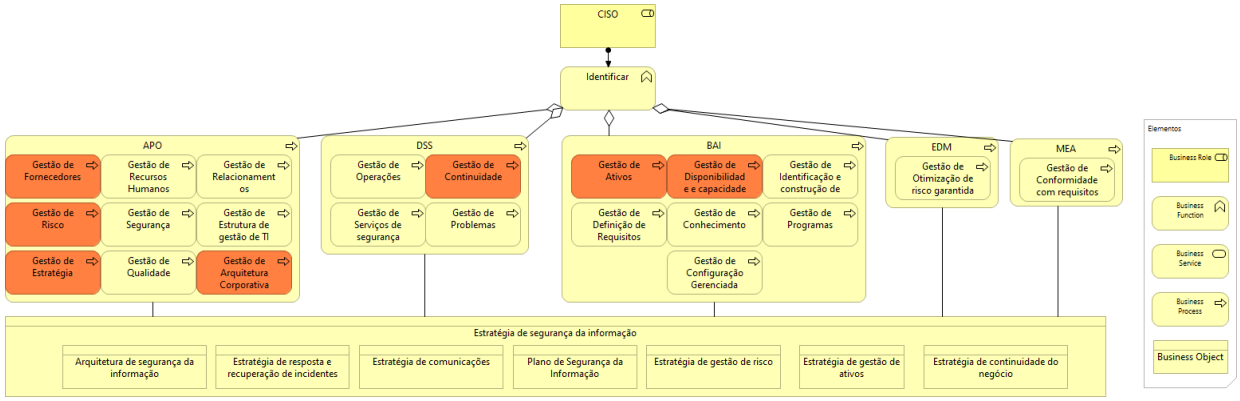


Figura 31: Diagrama da categoria identificar mediante a validação de EI da AMA.

A falta de mais informação impede a demonstração de resultados matriciais para as restantes categorias do QNRCS, sendo que se dá por concluído o caso de estudo.

4.3 Entrevista com Especialista

A conversa com um especialista, tem como propósito validar a utilidade da ferramenta desenvolvida por este estudo, garantindo que não se sobrepõe a nenhuma outra já existente. Lino Santos, coordenador do CNCS, e anteriormente do CERT.pt, licenciado em Engenharia de Sistemas e Informática e mestrado em Direito e Segurança, acedeu ao convite para comentar o trabalho realizado. Numa primeira conversa, refere a existência da plataforma **CyberCheckup** como um método de auto diagnostico para as organizações, esclarecendo que devido ao algoritmo utilizado nesta investigação, as duas ferramentas podem ser complementares. Posteriormente, aceitou responder a algumas questões específicas.

Entidades de informação

Q1 - Como avalia a necessidade de documentar as evidências de implementação das medidas de mitigação propostas no QNRCS, de forma a identifica-las univocamente?
"A recolha e armazenamento de evidências da conformidade com cada um dos controlos previstos no QNRCS é essencial para nós. Estas evidências são a base para um processo de certificação de conformidade que estamos a desenhar."

Q2 - O nome seleccionado para cada entidade de informação, foi considerado através de um processo de análise cuidada das informações de referência indicadas para cada medida (ou subcategoria) do QNRCS. Como avalia esta decisão no sentido de trazer ainda mais conformidade para com as normas e referenciais europeus para o âmbito nacional?
"O trabalho realizado nesta fase introduz um maior rigor na definição das entidades de informação e a sua relação com as principais normas internacionais de referencia."

Arquitetura empresarial

Q3 - Como parte do trabalho realizado, foram utilizados conceitos de arquitetura empresarial, em particular na organização da informação. Desta forma, foi construída uma possível arquitetura de informação,

composta pelas evidencias de informação apuradas. Este conceito já existia na criação do QNRCS? Como avalia esta integração de conceitos?

"Não. O Quadro foi desenhado como um compêndio de controlos a ser usado num processo de gestão de risco (para mitigação dos mesmos). A integração destes dois conceitos parece-me muito útil para a operacionalização de processos que têm como resultado a produção de evidências da conformidade com cada um dos controlos."

Q4 - Como avalia a possibilidade de evidenciar a relação destes documentos (entidades de informação) com os processos **COBIT 5** referidos pelo QNRCS? **"Extremamente útil, no sentido que em que um processo de certificação cruzado possa vir a existir."**

Alternativas

Q5 - Uma organização pode usar o trabalho aqui desenvolvido para validar o estado da sua implementação atual, no entanto, visto que a aplicação das medidas do QNRCS vem como resposta a um levantamento de risco prévio, a ferramenta desenvolvida pode ser utilizada em *backwards*. Ou seja, imagine-se o caso de uma organização que precisa rever o seu plano de segurança da informação, de trás para a frente, é possível verificar quais as EI envolvidas, por conseguinte, saber quais os processos afetados. No que respeita á ferramenta existente, o Cybercheckup, existe uma possibilidade semelhante? Como compara ambas as ferramentas?

"O Cybercheckup não tem este grau de detalhe. É uma ferramenta que proporciona aos seus utilizadores realizar de uma forma intuitiva um *gap analysis* relativamente à totalidade dos controlos do Quadro e nem sequer tem em conta que o mesmo pressupõe uma análise de risco prévia."

Q6 - Considerando os critérios do quadro de avaliação, seria possível integrar o conceito desenvolvido por este trabalho. Qual a sua opinião sobre esta integração? Consegue apontar alguma melhoria imediata para a ferramenta desenvolvida?

"Não consigo identificar uma melhoria na atual proposta. Também precisava de ver na prática esta"

De acordo com a opinião de Lino Santos, teria sido uma mais valia a observação prática dos resultados, no entanto em termos gerais, considera a ferramenta útil, integrável com o conceito existente e compatível com os desenvolvimentos atuais a decorrer no CNSC, e que esta adiciona detalhe na informação que oferece podendo representar a contribuição objetiva que se pretende.

4.4 Cybercheckup

O CNCS disponibiliza *online* uma ferramenta de auto diagnóstico, com o propósito de uma organização aferir o estado da sua cibersegurança. Esta ferramenta é complementar ao Quadro Nacional de Referência para a Cibersegurança e considera os níveis definidos pelo Quadro de Avaliação de Capacidades Minímas em Cibersegurança. Quando comparada com a ferramenta desenvolvida por esta investigação nota-se a enorme diferença no detalhe da informação resultante [16].

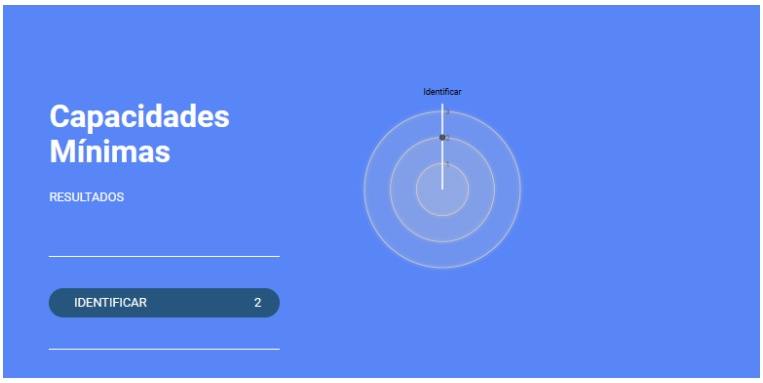


Figura 32: Imagem do resultado da ferramenta Cybercheckup.

A figura 32 é o resultado da introdução dos dados validados no caso de estudo, para a categoria identificar. A imagem indica que a organização se encontra no nível 2 sem mais explicações, e permite imprimir os restantes resultados (Anexo 9 - Resultados do Cybercheckup) onde se listam as perguntas e respostas seleccionadas. Pode assim verificar-se que, além de uma interface web, apelativa e simples de usar, os resultados são apresentados com menos detalhe que a ferramenta e a desenvolvida pela investigação, que acrescenta real valor e cujos resultados são bastante objetivos quanto ao caminho de melhorias a percorrer.

Em suma, a utilização dos dados fornecidos pela AMA, permitiu comprovar a possibilidade de mapeamento da informação da organização com a aqruitetura proposta, desenhar um ponto de partida para a implementação de melhorias, mostrando os resultados em tabelas, diagramas e matrizes que expõem claramente a usabilidade da ferramenta desenvolvida. Nesta secção realizou-se uma auto-avaliação do trabalho e apresentou-se a opinião de um especialista.

5 Conclusão e Trabalho Futuro

Este capítulo encerra o estudo realizado, através da revisão dos aspetos teóricos e práticos obtidos nas secções anteriores. Não serão apresentados novos conceitos, no entanto descrevem-se as contribuições que a investigação oferece, as limitações da investigação e da ferramenta desenvolvida e identifica-se o trabalho futuro a realizar no âmbito desta investigação.

5.1 Contribuições

O estudo realizado, oferece uma contribuição objectiva no que respeita à documentação requerida pelo QNRCS. A implementação das medidas de mitigação de risco geram documentos, para os quais, é sugerida uma alteração ao nome. O nome que se sugere é único e claro quanto ao seu propósito.

A integração de noções de arquitetura empresarial, usando estratégias presentes no método TOGAF ADM, permite tratar estes documentos como entidades de informação, e consequentemente, trazer para o âmbito do QNRCS, uma visão de arquitetura de informação. Esta visão, permite estruturar a documentação e evidenciar a sua relação com os processos COBIT 5, previstos na estratégia nacional para proteção da informação.

A ferramenta desenvolvida com base nestas entidades de informação, permite a uma organização aferir o estado de implementação dos processos de segurança previstos pelo QNRCS, ou seja, a determinação do estado *AS-IS* da organização no que se refere à cibersegurança ou segurança da informação. A partir dos resultados obtidos pelo uso da ferramenta desenvolvida, são dadas indicações do estado de implementação de processos COBIT 5 sugeridos pelo QNRCS, permitindo que se considerem melhorias, indicando quais os processos que contemplam lacunas na sua implementação. Pela forma como são apresentados os resultados, fica claro que as lacunas podem existir a nível da documentação que serve de evidência da implementação dos referidos processos, permitindo que as melhorias ocorram de forma assertiva e eficiente.

No caso de organizações que pretendam iniciar a implementação das medidas, a ferramenta contribui na construção duma visão *TO-BE*, mostrando as falhas ou faltas na implementação dos processos que são sugeridos pelo QNRCS e que seguem a regulação europeia, no âmbito das medidas ISO 27001, da Diretiva (UE) n.º 2016/1148, entre outras normas e standards. Assim, como resultado da investigação apresentada, a ferramenta desenvolvida pode guiar uma organização no sentido da segurança da informação e em conformidade com o QNRCS e com as normas que o impulsionam.

Sendo o Ciberchecкup uma ferramenta de auto avaliação de cibersegurança, e sabendo que esta trata o tema de forma superficial, não aprofundando detalhes que permitam ações de melhoria de facto, existe uma clara possibilidade de integração de ambas as ferramentas, para melhores resultados no âmbito da segurança da informação em Portugal.

5.2 Limitações

Das investigações consideradas no âmbito deste estudo, verificou-se que o foco da análise se centra maioritariamente na procura de lacunas ou áreas não cobertas pelas estratégias nacionais adotadas na Europa, (i.e) falha na determinação de medidas de proteção de infraestruturas críticas. Não foram encontrados estudos relevantes com base na documentação gerada pela implementação das medidas das estratégias, em particular do QNRCS, o que dificultou a investigação no sentido da precisão das considerações sobre resultados, deixando muito espaço para trabalho futuro. Sendo o QNRCS uma ferramenta que deve responder a necessidades específicas, uma organização está isenta da sua implementação como um todo, ou seja a arquitetura

de informação desenvolvida, pode nunca ser alcançada na totalidade. Portanto, ter sido realizado apenas um caso de estudo limita a análise de resultados a um único cenário.

5.3 Trabalho Futuro

Prevendo a continuidade do estudo realizado assim como melhorias na ferramenta desenvolvida, deve ser considerada como prioritária, uma revisão ativa da folha 'Entidades de informação' presente no mapa com o mesmo nome. A atribuição de nomes das evidências, deverá perseguir uma aprovação por parte do CNCS. Ademais, o desenvolvimento de uma interface ou aplicação, que integre as funcionalidades da ferramenta desenvolvida, automatizando o cruzamento da informação assim como o *output*, poderá oferecer maior usabilidade e tornar a ferramenta mais apelativa. A integração da noção de níveis, definida pelo Quadro de Avaliação de Capacidades, pode conduzir a uma integração da ferramenta desenvolvida neste estudo com a **Cybercheckup** do CNSC.

Referências

[1] CNCS Centro Nacional de Cibersegurança. Quadro de avaliaÇÃo de capacidades de ciberseguranÇa. https://www.cncs.gov.pt/docs/cncs-quadrodeavaliacao.pdf. Accessed: 2021-10-28.

[2] Presidência Do Conselho De Ministros. Resolução do conselho de ministros 49/23018. *Diário da República*, 2018.

[3] Coordenador do Centro Nacional de Cibersegurança. Quadro nacional de referência para a cibersegurança. Standard, Centro Nacional de Cibersegurança, Portugal, PT, 2016.

[4] ISO Central Secretary. Information security management. Standard ISO/IEC TR 27001:2013, International Organization for Standardization, Geneva, CH, 2013.

[5] Council of European Union. Council regulation (EU) no 1148/2016. http://data.europa.eu/eli/dir/2016/1148/oj. Accessed: 2021-10-28.

[6] Cybersecurity.org. Election security spotlight – cis controls. https://www.cisecurity.org/spotlight/cybersecurity-spotlight-cis-controls. Accessed: 2021-10-28.

[7] Renê Chiari. O que é cobit? https://www.itsmnapratica.com.br/conceitos-cobit-5/. Accessed: 2021-10-28.

[8] Manuela Tvaronavičienė, Tomas Plėta, Silvia Casa, and Juozas Latvys. Cyber security management of critical energy infrastructure in national cybersecurity strategies: Cases of usa, uk, france, estonia and lithuania. *Insights into Regional Development*, 2(4):802–813, 2020.

[9] Marc Lankhorst et al. *Enterprise architecture at work*, volume 352. Springer, 2009.

[10] Erich Gamma, Richard Helm, Ralph Johnson, John Vlissides, and Design Patterns. Elements of reusable object-oriented software. *Reading: Addison-Wesley*, 1995.

[11] Pedro Sousa and Andre Vasconcelos. *Enterprise Architecture and Cartography*. Number 1. 2018.

[12] Maria Eugenia Iacob, Henk Jonkers, Marc Lankhorst, Erik Proper, and DAC Quartel. Archimate 2.0 specification. 2012.

[13] ISMS.Online. Iso 27001 annex a controls. https://www.isms.online/search/ISO+27001+Annex+A+Controls/. Accessed: 2021-10-28.

[14] CSRC Computer Security Resource Center. Nist risk management framework. https://csrc.nist.gov/projects/risk-management/sp800-53-controls/release-search#!/control?version=4.0&number=SC-17. Accessed: 2021-10-28.

[15] John R Venable, Jan Pries-Heje, and Richard L Baskerville. Choosing a design science research methodology. 2017.

[16] CNCS Centro Nacional de Cibersegurança. Cybercheckup. https://cibercheckup.cncs.gov.pt/. Accessed: 2021-10-28.

Anexos

Anexo 1 - CIS Controlos

Os CIS controlos considerados neste documento foram retirados da ágina web oficial do "*Center for Information Security*"já referenciada, e encontram-se abaixo listados:

CIS Control 1: Inventory and Control of Enterprise Assets

CIS Control 2: Inventory and Control of Software Assets

CIS Control 3: Data Protection

CIS Control 4: Secure Configuration of Enterprise Assets and Software

CIS Control 5: Account Management

CIS Control 6: Access Control Management

CIS Control 7: Continuous Vulnerability Management

CIS Control 8: Audit Log Management

CIS Control 9: Email Web Browser and Protections

CIS Control 10: Malware Defenses

CIS Control 11: Data Recovery

CIS Control 12: Network Infrastructure Management

CIS Control 13: Network Monitoring and Defense

CIS Control 14: Security Awareness and Skills Training

CIS Control 15: Service Provider Management

CIS Control 16: Application Software Security

CIS Control 17: Incident Response Management

CIS Control 18: Penetration Testing

CIS Control 19: Incident Response and Management

CIS Control 20: Penetration Test and Red Team Excercises

Anexo 2 - Processos COBIT 5

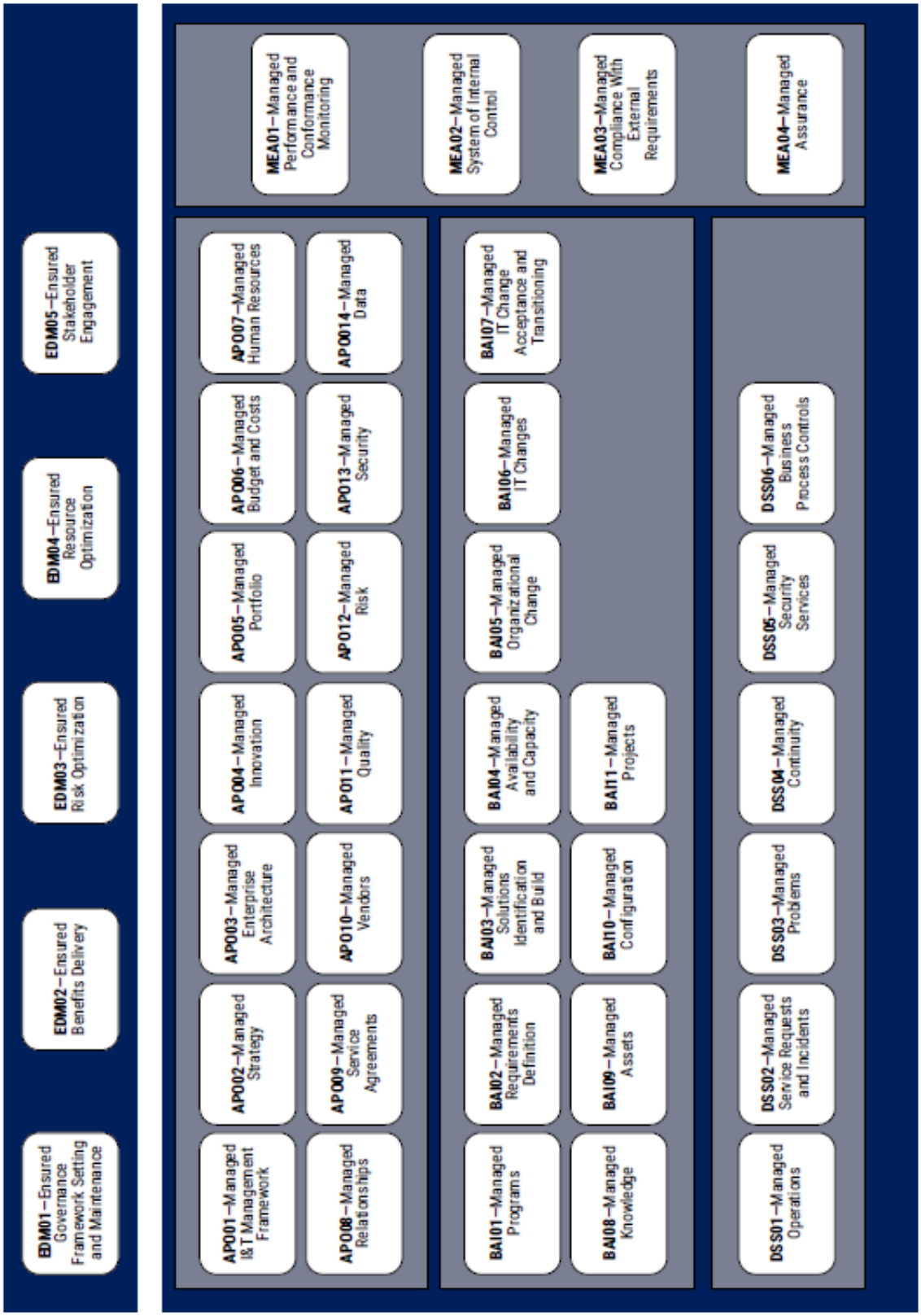


Figura 33: COBIT Core Model in www.isaca.org.

Anexo 3 - Viewpoints

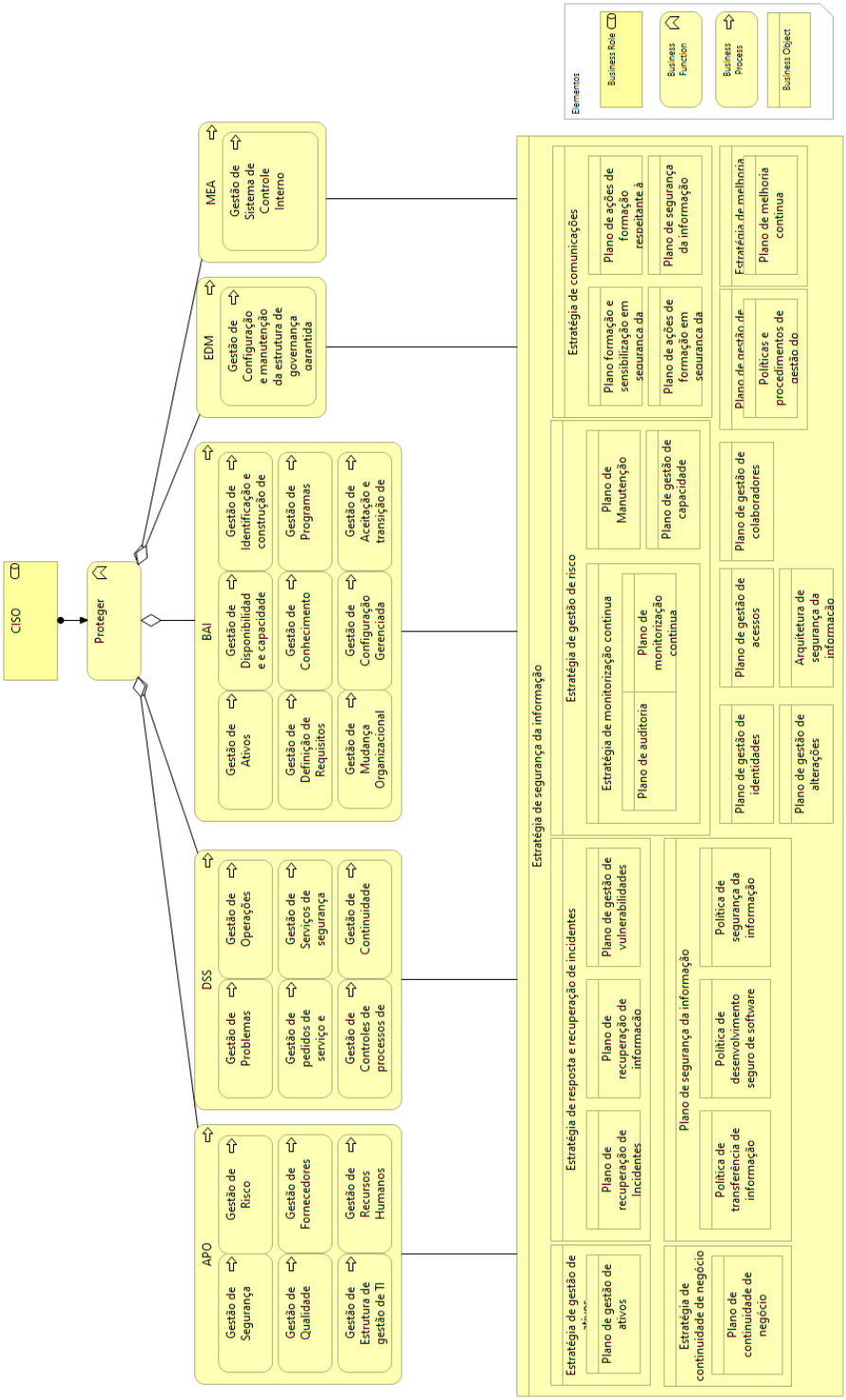


Figura 34: Diagrama Archimate com os processos representados na MATRIZ_PROTEGER.

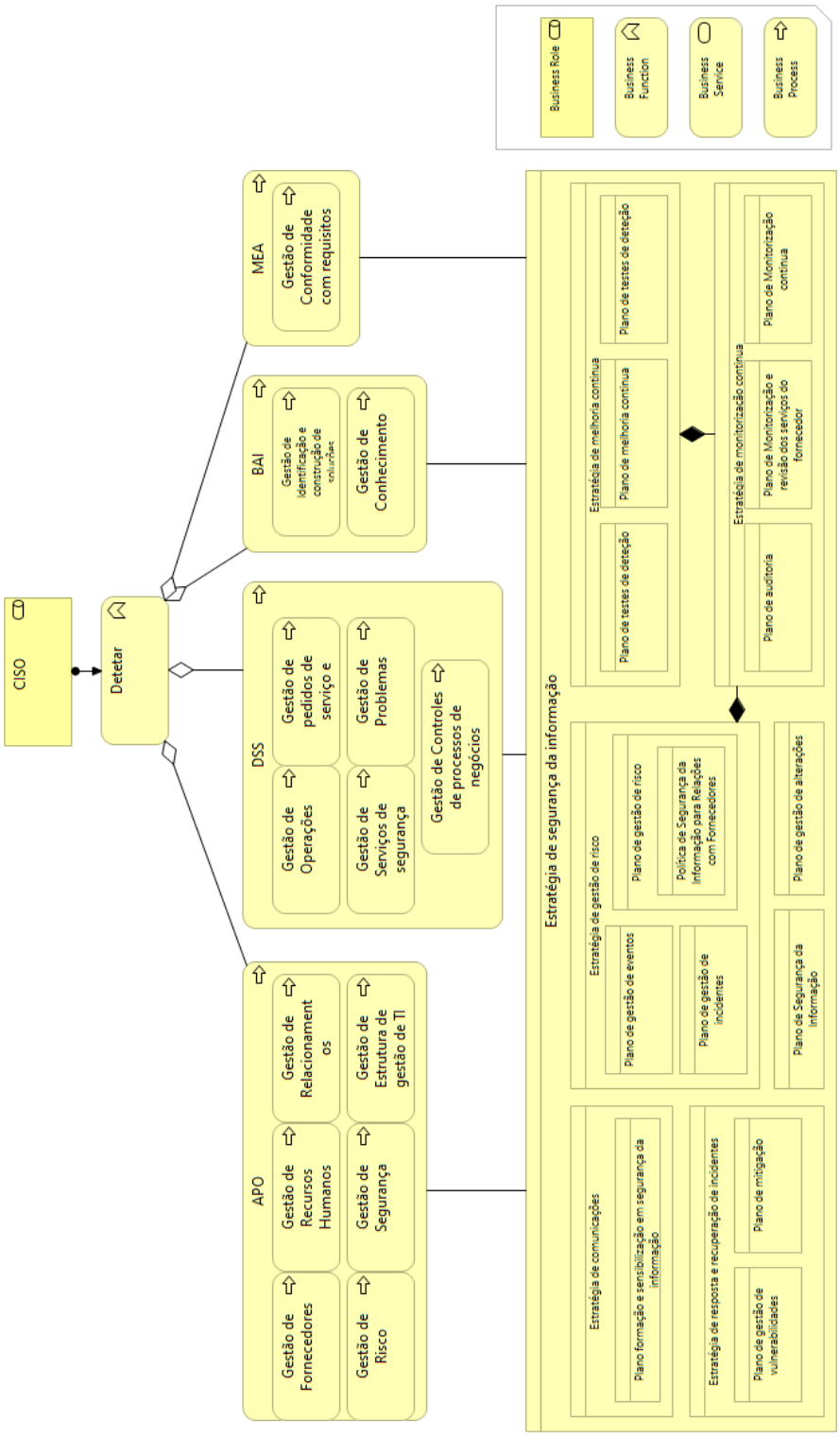


Figura 35: Diagrama Archimate com os processos representados na MATRIZ_DETETAR.

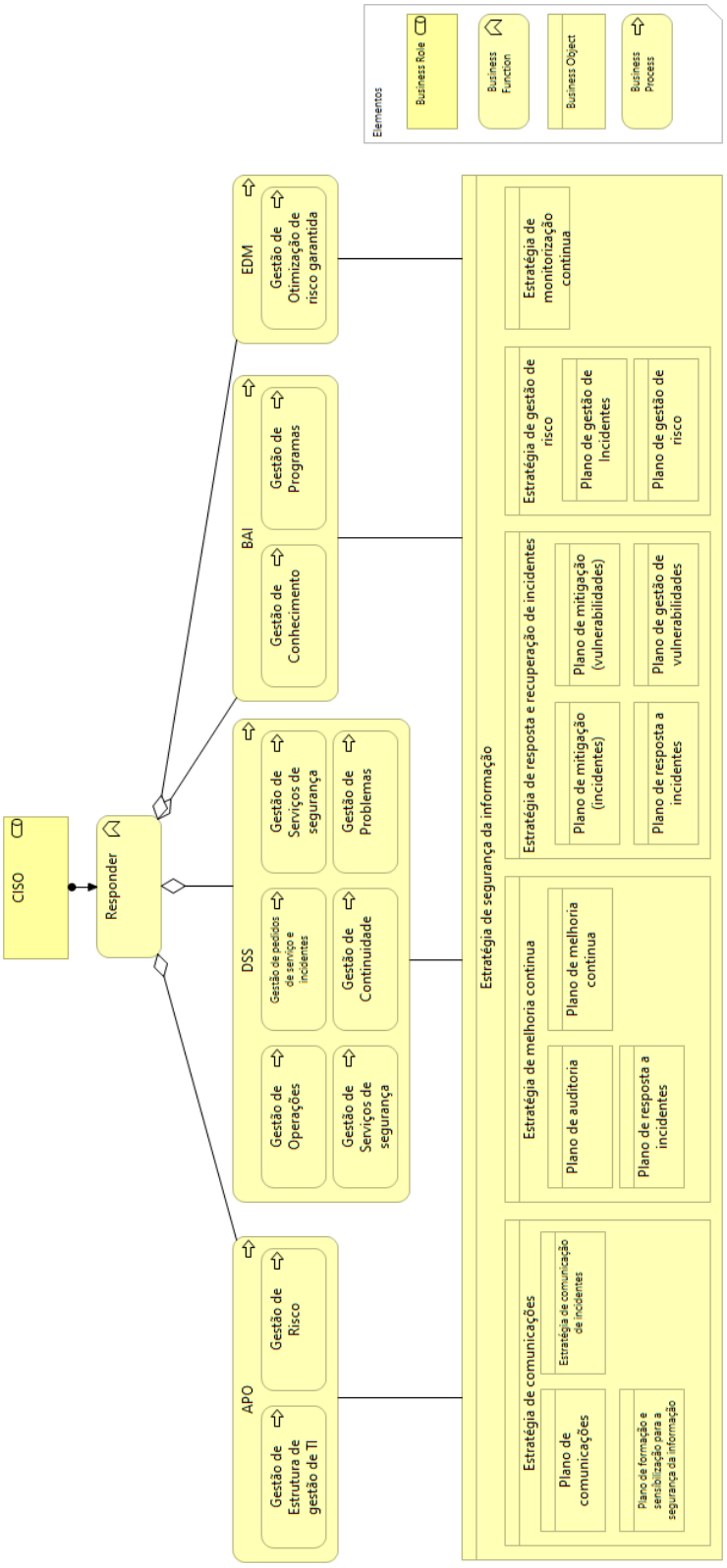


Figura 36: Diagrama Archimate com os processos representados na MATRIZ_RESPONDER.

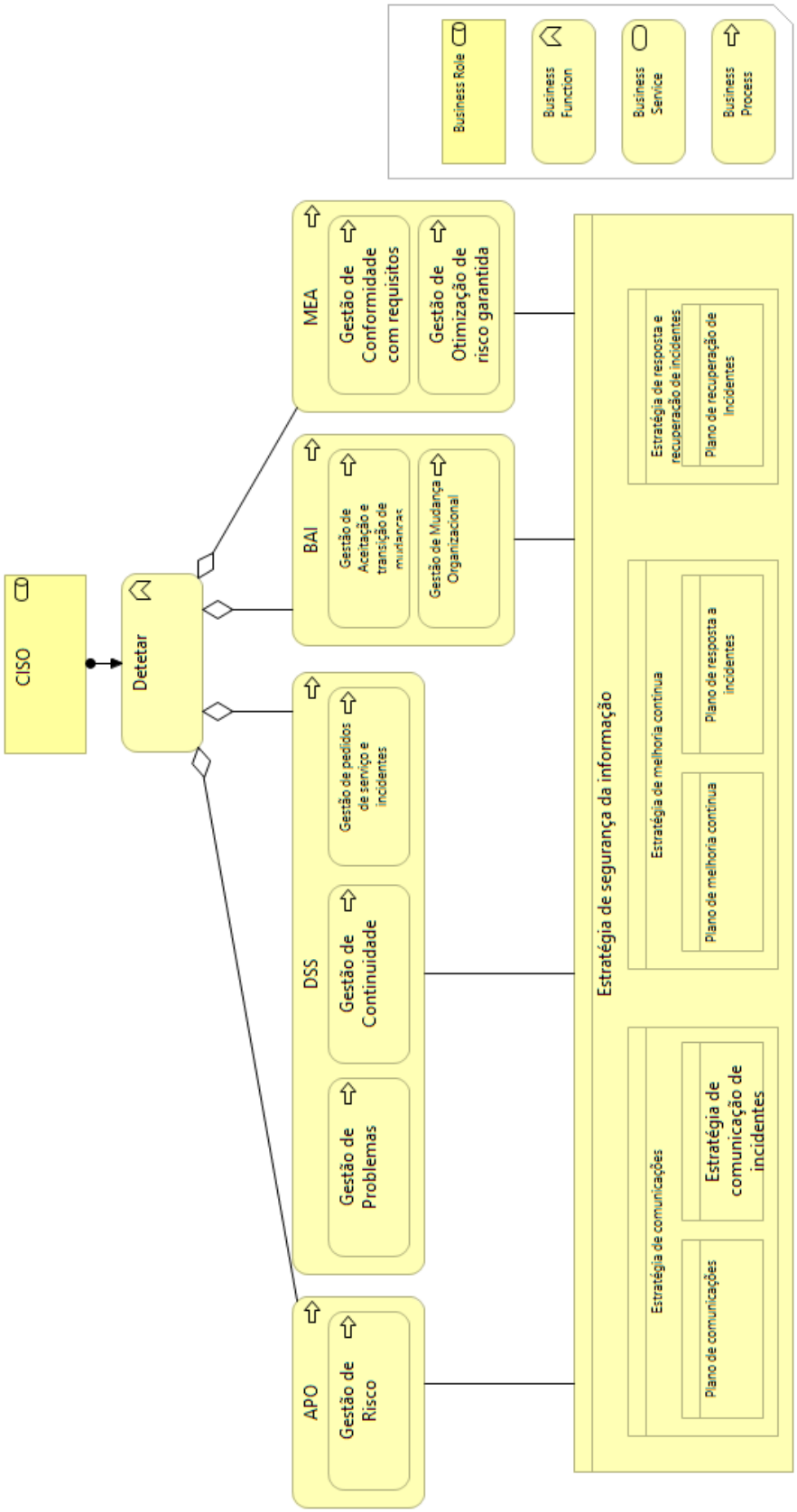
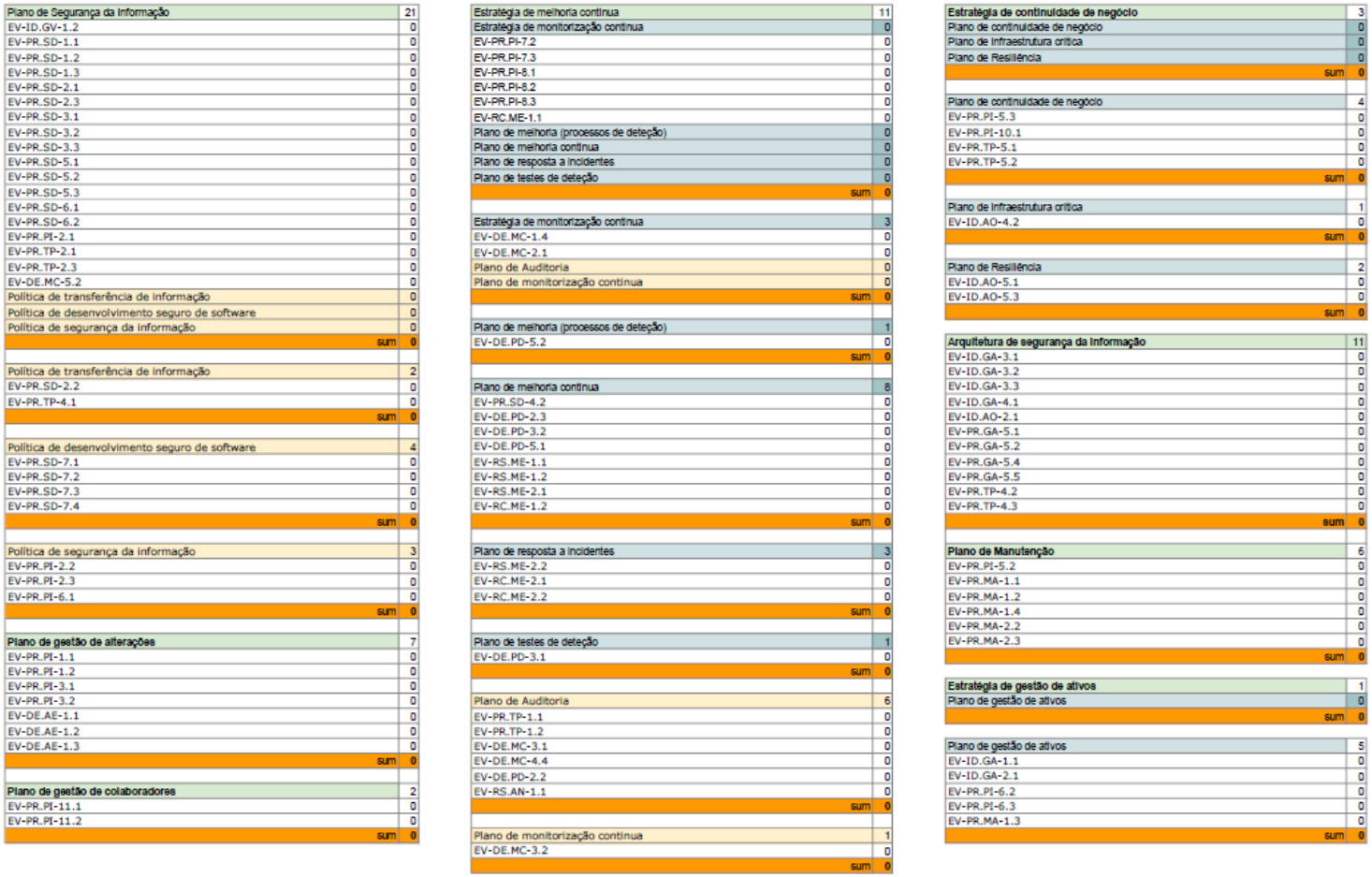


Figura 37: Diagrama Archimate com os processos representados na MATRIZ_RECUPERAR.

Anexo 4 - Arquitetura de informação (estrutura)



Plano de Segurança da Informação	21
EV-ID.GV-1.2	0
EV-PR.SD-1.1	0
EV-PR.SD-1.2	0
EV-PR.SD-1.3	0
EV-PR.SD-2.1	0
EV-PR.SD-2.3	0
EV-PR.SD-3.1	0
EV-PR.SD-3.2	0
EV-PR.SD-3.3	0
EV-PR.SD-5.1	0
EV-PR.SD-5.2	0
EV-PR.SD-5.3	0
EV-PR.SD-6.1	0
EV-PR.SD-6.2	0
EV-PR.PI-2.1	0
EV-PR.TP-2.1	0
EV-PR.TP-2.3	0
EV-DE.MC-5.2	0
Política de transferência de informação	0
Política de desenvolvimento seguro de software	0
Política de segurança da informação	0
sum	0

Política de transferência de informação	2
EV-PR.SD-2.2	0
EV-PR.TP-4.1	0
sum	0

Política de desenvolvimento seguro de software	4
EV-PR.SD-7.1	0
EV-PR.SD-7.2	0
EV-PR.SD-7.3	0
EV-PR.SD-7.4	0
sum	0

Política de segurança da informação	3
EV-PR.PI-2.2	0
EV-PR.PI-2.3	0
EV-PR.PI-6.1	0
sum	0

Plano de gestão de alterações	7
EV-PR.PI-1.1	0
EV-PR.PI-1.2	0
EV-PR.PI-3.1	0
EV-PR.PI-3.2	0
EV-DE.AE-1.1	0
EV-DE.AE-1.2	0
EV-DE.AE-1.3	0
sum	0

Plano de gestão de colaboradores	2
EV-PR.PI-11.1	0
EV-PR.PI-11.2	0
sum	0

Estratégia de melhoria continua	11
Estratégia de monitorização continua	0
EV-PR.PI-7.2	0
EV-PR.PI-7.3	0
EV-PR.PI-8.1	0
EV-PR.PI-8.2	0
EV-PR.PI-8.3	0
EV-RC.ME-1.1	0
Plano de melhoria (processos de deteção)	0
Plano de melhoria continua	0
Plano de resposta a incidentes	0
Plano de testes de deteção	0
sum	0

Estratégia de monitorização continua	3
EV-DE.MC-1.4	0
EV-DE.MC-2.1	0
Plano de Auditoria	0
Plano de monitorização continua	0
sum	0

Plano de melhoria (processos de deteção)	1
EV-DE.PD-5.2	0
sum	0

Plano de melhoria continua	8
EV-PR.SD-4.2	0
EV-DE.PD-2.3	0
EV-DE.PD-3.2	0
EV-DE.PD-5.1	0
EV-RS.ME-1.1	0
EV-RS.ME-1.2	0
EV-RS.ME-2.1	0
EV-RC.ME-1.2	0
sum	0

Plano de resposta a incidentes	3
EV-RS.ME-2.2	0
EV-RC.ME-2.1	0
EV-RC.ME-2.2	0
sum	0

Plano de testes de deteção	1
EV-DE.PD-3.1	0
sum	0

Plano de Auditoria	6
EV-PR.TP-1.1	0
EV-PR.TP-1.2	0
EV-DE.MC-3.1	0
EV-DE.MC-4.4	0
EV-DE.PD-2.2	0
EV-RS.AN-1.1	0
sum	0

Plano de monitorização continua	1
EV-DE.MC-3.2	0
sum	0

Estratégia de continuidade de negócio	3
Plano de continuidade de negócio	0
Plano de Infraestrutura crítica	0
Plano de Resiliência	0
sum	0

Plano de continuidade de negócio	4
EV-PR.PI-5.3	0
EV-PR.PI-10.1	0
EV-PR.TP-5.1	0
EV-PR.TP-5.2	0
sum	0

Plano de Infraestrutura crítica	1
EV-ID.AO-4.2	0
sum	0

Plano de Resiliência	2
EV-ID.AO-5.1	0
EV-ID.AO-5.3	0
sum	0

Arquitetura de segurança da informação	11
EV-ID.GA-3.1	0
EV-ID.GA-3.2	0
EV-ID.GA-3.3	0
EV-ID.GA-4.1	0
EV-ID.AO-2.1	0
EV-PR.GA-5.1	0
EV-PR.GA-5.2	0
EV-PR.GA-5.4	0
EV-PR.GA-5.5	0
EV-PR.TP-4.2	0
EV-PR.TP-4.3	0
sum	0

Plano de Manutenção	6
EV-PR.PI-5.2	0
EV-PR.MA-1.1	0
EV-PR.MA-1.2	0
EV-PR.MA-1.4	0
EV-PR.MA-2.2	0
EV-PR.MA-2.3	0
sum	0

Estratégia de gestão de ativos	1
Plano de gestão de ativos	0
sum	0

Plano de gestão de ativos	5
EV-ID.GA-1.1	0
EV-ID.GA-2.1	0
EV-PR.PI-6.2	0
EV-PR.PI-6.3	0
EV-PR.MA-1.3	0
sum	0

Figura 38: Estrutura da arquitetura de informação (Entidades de informação principal: Plano de Segurança da Informação, Plano de gestão de alterações, Plano de gestão de colaboradores, Estratégia de melhoria continua, Estratégia de continuidade de negócio, Arquitetura de segurança da informação, Plano de Manutenção e Estratégia de gestão de ativos).

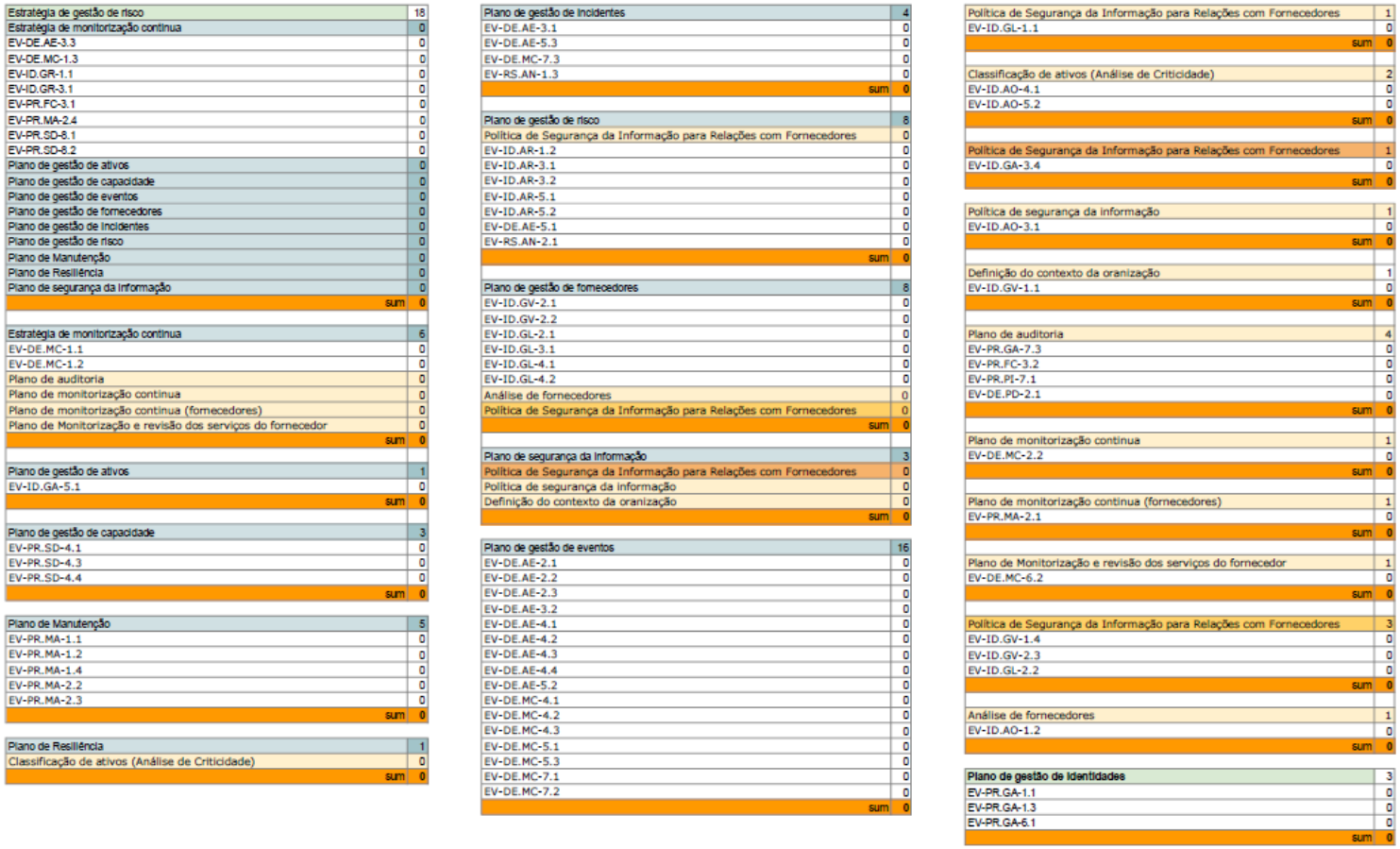


Figura 39: Estrutura da arquitetura de informação (Entidades de informação principal: Estratégia de gestão de risco e Plano de gestão de identidades).

Estratégia de comunicações	12
EV-DE.PD-1.1	0
EV-DE.PD-4.1	0
EV-DE.PD-4.2	0
EV-RS.AN-5.1	0
EV-RS.AN-5.2	0
EV-RS.CO-3.2	0
Estratégia de comunicação de incidentes	0
Plano de ações de formação em segurança da informação	0
Plano de ações de formação respeitante à temática de acessos privilegiados	0
Plano de comunicações	0
Plano de formação e sensibilização para a segurança da informação	0
Plano de segurança da informação	0
sum	0

Estratégia de comunicação de incidentes	3
EV-RS.CO-4.1	0
EV-RS.CO-5.1	0
Plano de Comunicação de incidentes	0
sum	0

Plano de ações de formação em segurança da informação	2
EV-PR.FC-1.2	0
EV-PR.FC-1.3	0
sum	0

Plano de ações de formação respeitante à temática de acessos privilegiados	2
EV-PR.FC-2.2	0
EV-PR.FC-2.3	0
sum	0

Plano de comunicações	5
EV-ID.GV-1.3	0
EV-RS.CO-2.1	0
EV-RS.CO-5.2	0
EV-RC.CO-2.1	0
Programa de Conscientização de Ameaças	0
sum	0

Plano de formação e sensibilização para a segurança da informação	9
EV-PR.FC-1.1	0
EV-PR.FC-1.4	0
EV-PR.FC-2.1	0
EV-PR.FC-3.3	0
EV-PR.FC-4.1	0
EV-PR.FC-4.3	0
EV-DE.PD-1.2	0
EV-DE.PD-1.3	0
EV-RS.CO-1.2	0
sum	0

Plano de segurança da informação	1
EV-PR.FC-4.2	0
sum	0

Plano de Comunicação de incidentes	3
EV-RS.CO-3.3	0
EV-RS.CO-4.2	0
EV-RC.CO-1.1	0

Programa de Conscientização de Ameaças	2
EV-ID.AR-2.1	0
EV-ID.AR-2.2	0
sum	0

Plano de Resposta a Incidentes	14
EV-ID.GL-5.1	0
EV-ID.GL-5.2	0
EV-PR.PI-9.3	0
EV-RS.PR-1.2	0
EV-RS.CO-1.1	0
EV-RS.CO-2.2	0
EV-RS.CO-3.1	0
EV-RS.AN-2.2	0
EV-RS.AN-3.1	0
EV-RS.AN-3.2	0
EV-RS.AN-4.1	0
EV-RS.AN-4.2	0
EV-RS.MI-1.1	0
EV-RS.MI-1.2	0
sum	0

Plano de gestão de acessos	19
EV-PR.GA-1.2	0
EV-PR.GA-2.1	0
EV-PR.GA-2.2	0
EV-PR.GA-3.1	0
EV-PR.GA-4.1	0
EV-PR.GA-4.2	0
EV-PR.GA-4.3	0
EV-PR.GA-5.3	0
EV-PR.GA-6.2	0
EV-PR.GA-6.3	0
EV-PR.GA-6.4	0
EV-PR.GA-7.1	0
EV-PR.GA-7.2	0
EV-PR.PI-5.1	0
EV-PR.TP-2.2	0
EV-PR.TP-3.1	0
EV-PR.TP-3.2	0
EV-PR.TP-3.3	0
Politicas e procedimentos de gestão do teletrabalho e acessos remotos	0
sum	0

Politicas e procedimentos de gestão do teletrabalho e acessos remotos	1
EV-PR.GA-3.2	0
sum	0

Estratégia de resposta e recuperação de incidentes	13
EV-PR.PI-8.4	0
EV-PR.PI-9.1	0
EV-PR.PI-9.2	0
EV-RC.PR-1.1	0
EV-RS.AN-1.2	0
EV-RS.PR-1.1	0
Plano de gestão de vulnerabilidades	0
Plano de mitigação	0
Plano de mitigação (incidentes)	0
Plano de mitigação (vulnerabilidades)	0
Plano de recuperação de incidentes	0
Plano de recuperação de informação	0
Plano de Resposta a Incidentes	0
sum	0

Plano de gestão de vulnerabilidades	8
EV-ID.AR-1.1	0
EV-ID.AR-4.2	0
EV-PR.PI-12.1	0
EV-PR.PI-12.2	0
EV-PR.PI-12.3	0
EV-DE.MC-8.1	0
EV-DE.MC-8.2	0
EV-RS.AN-5.3	0
sum	0

Plano de mitigação	1
EV-DE.MC-8.3	0
sum	0

Plano de mitigação (incidentes)	2
EV-RS.MI-2.1	0
EV-RS.MI-2.2	0
sum	0

Plano de mitigação (vulnerabilidades)	2
EV-RS.MI-3.2	0
EV-RS.MI-3.3	0
sum	0

Plano de recuperação de incidentes	1
EV-RC.PR-1.2	0
sum	0

Plano de recuperação de informação	3
EV-PR.PI-4.1	0
EV-PR.PI-4.2	0
EV-PR.PI-4.3	0
sum	0

Estratégia de monitorização continua	2
EV-DE.MC-6.1	0
EV-RS.MI-3.1	0
sum	0

Figura 40: Estrutura da arquitetura de informação (Entidades de informação principal:Estratégia de comunicações, Plano de gestão de acessos, Estratégia de resposta e recuperação de incidentes e Estratégia de monitorização continua).

Anexo 5 - *Uma* Arquitetura da Informação para o QNRCS

Figura 41: Proposta de arquitetura de informação

Anexo 7 - Recolha de dados

ID-Ev	Entidade de informação	Confirma a existência do documento	Referencia Interna (Entidade de Informação, documentos, etc)	Observações
EV-ID.GA-1.1	Inventário e controlo de ativos da empresa	Sim	Encontra-se no sistema de gestão de pedidos do service desk (Easy Vista)	Encontra-se no sistema de gestão de pedidos do service desk (Easy Vista)
EV-ID.GA-2.1	Inventário e controlo de ativos de software	Sim	MD 008 - Inventário de ativos	
EV-ID.GA-3.1	Inventário e controlo de ativos de rede	Sim	MD 008 - Inventário de ativos	
EV-ID.GA-3.2	Mapeamento do fluxo de informações (Com sistemas externos)	Sim	Equipamentos de comunicações	
EV-ID.GA-3.3	Controlo de fluxos de informações	Sim	Equipamentos de comunicações	
EV-ID.GA-3.4	Arquitetura de segurança da informação			
EV-ID.GA-4.1	Inventário e controlo de ativos de rede e sistemas externos	Sim	Equipamentos de comunicações	
EV-ID.GA-5.1	Classificação de ativos (Análise de Criticidade)	Não		
EV-ID.AO-1.1	Política de Segurança da Informação para Relações com Fornecedores	Sim	PO - 005 Politica de Relacao com Fornecedores	
EV-ID.AO-1.2	Catalogo de fornecedores	Sim	MD-002 Requisitos Legais, regulatórios e contratuais.xlsx e MD 008 - Inventário de ativos	
EV-ID.AO-2.1	Definição do contexto da oranização	Sim	PO - 001 Ambito do SGSI	
EV-ID.AO-3.1	Definição da visão, missão, objetivos da organização	Sim	PO - 001 Ambito do SGSI	
EV-ID.AO-4.1	Plano de infraestrutura crítica	Não		
EV-ID.AO-4.2	Plano de gestão de capacidade	Sim	MD 008 - Inventário de ativos	
EV-ID.AO-5.1	Proteção contra ameaças externas e ambientais (Definição de serviços mínimos)	Sim	PR - 013 Processo de Continuidade de Segurança de Informacao e PL-004 Plano de testes de Continuidade da Segurança da Informação	
EV-ID.AO-5.2	Plano da continuidade da segurança da informação	Sim	PR - 013 Processo de Continuidade de Segurança de Informacao	
EV-ID.AO-5.3	Disponibilidade de recursos de processamento da informação	Sim	RL-009 Relatórios atividade DSI e MD - 004 Relatorio previsão capacidades	
EV-ID.GV-1.1	Política de segurança da informação	Sim	PO - 002 Politica de seguranca de informacao	
EV-ID.GV-1.2	Aprovação da Política de segurança da informação	Sim	Acta de aprovação pelo Conselho Diretivo	
EV-ID.GV-1.3	Publicação da Política de segurança da informação em formato digital	Sim	Na intranet	Publicação apenas interna
EV-ID.GV-1.4	Entrevista ou registo da tomada de conhecimento das políticas de segurança	Sim	e-mail para todos os dirigentes e formação online e presencial	
EV-ID.GV-2.1	Identificação de legislação aplicável e requisitos contratuais (com fornecedores)	Sim	MD-002 Requisitos Legais, regulatórios e contratuais.xlsx	
EV-ID.GV-2.2	Relatórios de auditoria de conformidade (Legalidade)	Sim	Temos os relatórios de auditorias externas do SGSI e da certificação EIDAS	
EV-ID.GV-2.3	Política de privacidade	Sim	https://www.ama.gov.pt/web/agencia-para-a-modernizacao-administrativa/politica-de-privacidade.	
EV-ID.AR-1.1	Gestão de vulnerabilidades técnicas (identificação e classificação)	Sim	Plataforma KITS24	
EV-ID.AR-1.2	Revisão de conformidade técnica (registos)	Sim	Plataforma de conformidade e relatórios de incidentes	
EV-ID.AR-2.1	Contato com grupos de interesse especial (registo)	Sim	e-mails trocados com CNCS e newsleters de grupos de interesse	
EV-ID.AR-2.2	Registo de integrações com fontes de conhecimento externas.	Sim	CNCS	
EV-ID.AR-3.1	Avaliação de risco de segurança da informação	Sim	Plataforma de conformidade	
EV-ID.AR-3.2	Catálogo de ameaças	Sim	POL#12.AnaliseRisco	
EV-ID.AR-4.1	Plano de gestão de risco	Sim	Plataforma de conformidade	
EV-ID.AR-4.2	Gestão de Vulnerabilidades Técnicas	Sim	Plataforma de conformidade e KITS24	
EV-ID.AR-5.1	Plano de tratamento de risco	Sim	Plataforma de conformidade	
EV-ID.AR-5.2	Classificação do risco	Sim	Plataforma de conformidade	
EV-ID.GR-1.1	Sistema de gestão de risco (ISMS)	Sim	PR - 003 Procedimento de Gestao de Risco	
EV-ID.GR-2.1	Estratégia de gestão de risco	Sim	PR - 003 Procedimento de Gestao de Risco	
EV-ID.GR-3.1	Plano de resposta ao risco (ativos críticos)	Sim	Plataforma de conformidade	
EV-ID.GL-1.1	Plano de Proteção da cadeia logística	Sim	PO - 005 Politica de Relacao com Fornecedores	
EV-ID.GL-2.1	Política de gestão de fornecedores (categorização de segurança)			
EV-ID.GL-2.2	Categorização de Fornecedores			
EV-ID.GL-3.1	Política de gestão de fornecedores (regras contratuais)			
EV-ID.GL-4.1	Plano de auditorias a fornecedores			
EV-ID.GL-4.2	Lista dos fornecedores			

Figura 42: Dados validados pela AMA

Anexo 8 - Afetação de processos no caso de estudo

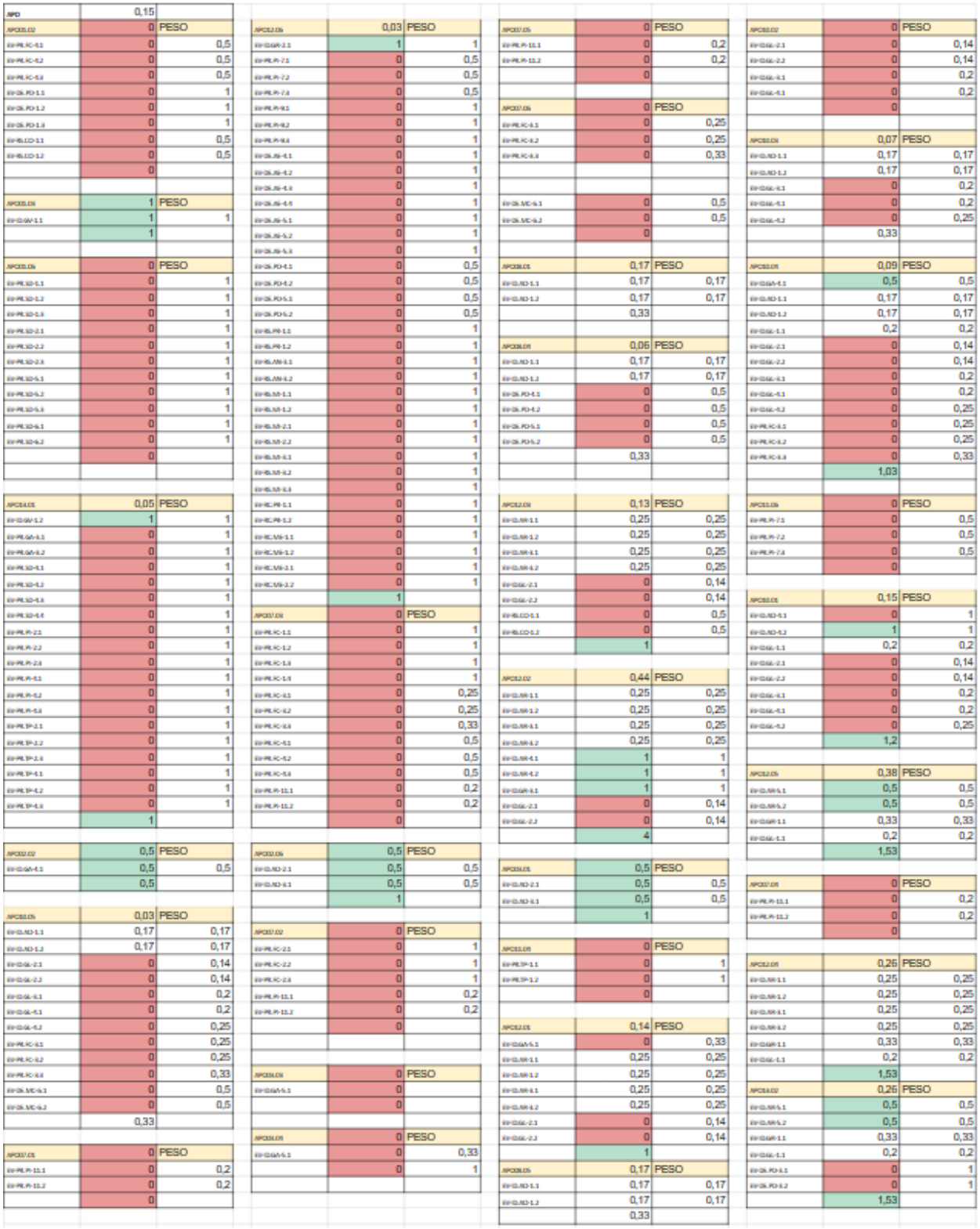


Figura 43: Processos afetos a entidades de informação validadas (APO).

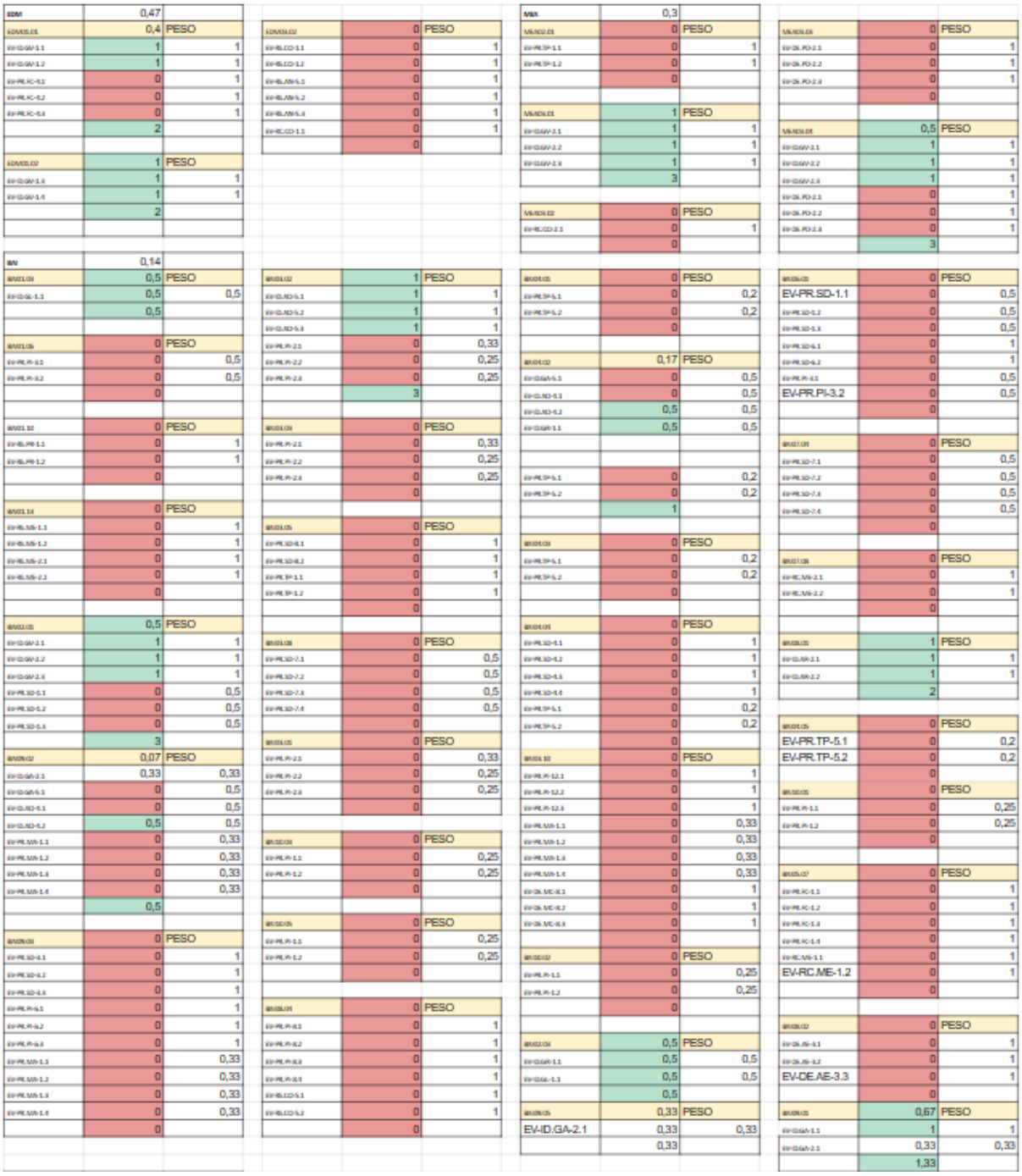


Figura 44: Processos afetos a entidades de informação validadas (EDM, MEA, BAI).

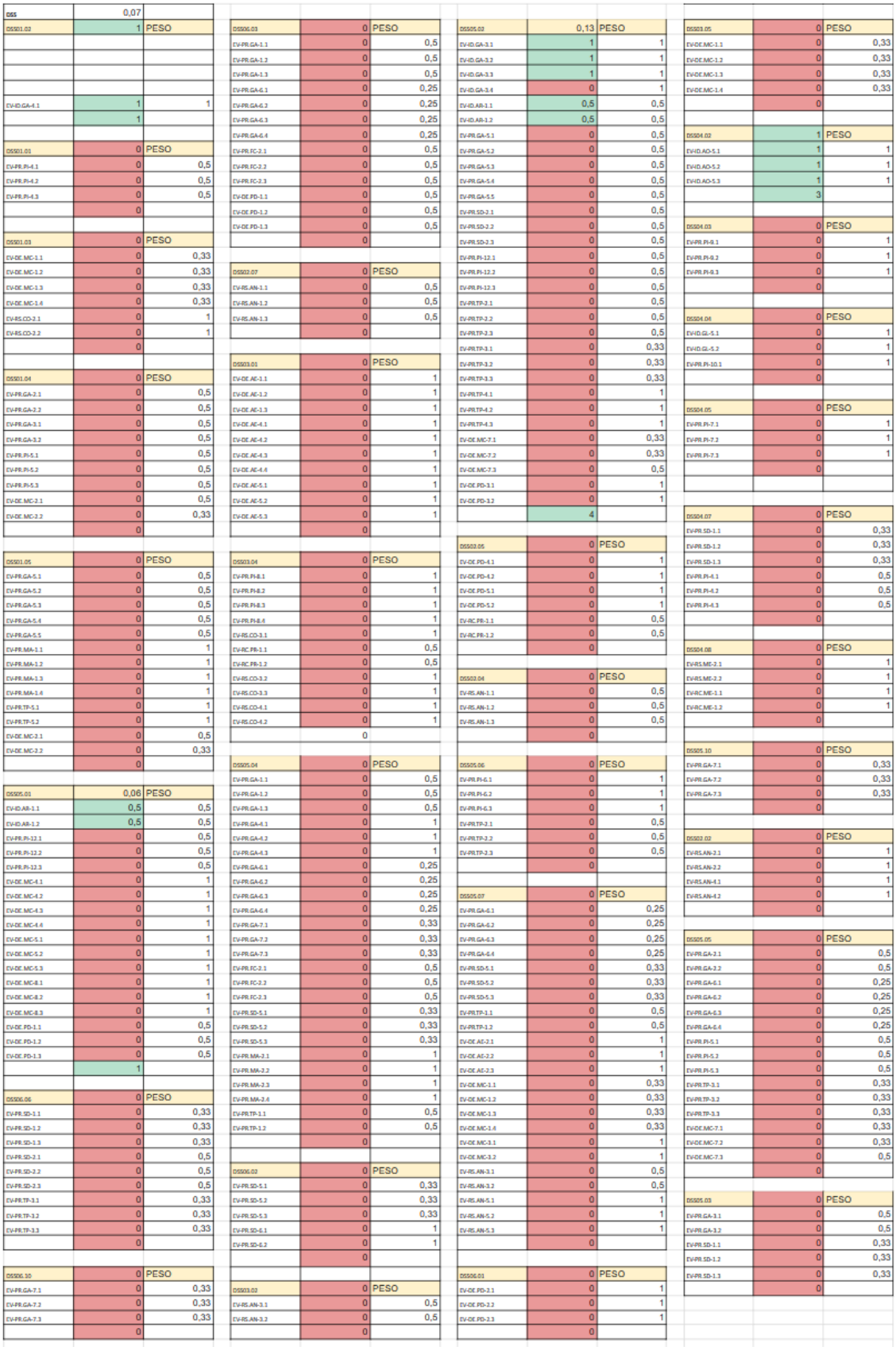


Figura 45: Processos afetos a entidades de informação validadas (DSS).

Anexo 9 - Resultados do Cybercheckup

Capacidades Mínimas

IDENTIFICAR	2

1/1 **Os dispositivos físicos, redes e sistemas de informação da sua organização encontram-se inventariados?**

Encontram-se registados em ferramenta de gestão de ativos físicos

1/2 **As aplicações e plataformas de software são inventariadas?**

Existem registos em ficheiros isolados com informações sobre sistemas

1/3 **As redes e fluxos de dados são mapeados?**

Existem processos e ferramentas para o mapeamento automático de ativos de rede

1/4 **As redes e sistemas de informação externos encontram-se identificados e catalogados?**

Existem processos e ferramentas para mapeamento automático de ativos localizados externamente

1/5 **Os ativos necessários para a prestação de bens e serviços encontram-se classificados?**

Os ativos encontram-se classificados de forma ad hoc

1/6 **A cadeia de logística encontra-se identificada?**

Existem políticas e procedimentos para a relação com fornecedores

1/7 **A missão, visão, valores, estratégias e objetivos encontram-se definidos e comunicados?**

A política de segurança da informação faz referência à missão, visão, objetivos e valores

1/8 **Os requisitos de resiliência para a prestação de serviços críticos estão definidos?**

Existe documentação dos requisitos mínimos de infraestrutura, de forma ad hoc

1/9 **Os requisitos legais e regulamentares para a cibersegurança são cumpridos?**

É efetuada uma revisão regular das leis e regulamentações aplicáveis

1/10 **As vulnerabilidades dos ativos encontram-se identificadas?**

As vulnerabailidades dos ativos são detetadas de forma ad hoc e sem processo de tratamento formal

1/11 **A organização partilha informações sobre ameaças em grupos de interesse?**

Existe um responsável identificado para comunicar sobre ameaças e temas de segurança da informação com grupos de interesse, seguindo um processo formal

1/12 **As ameaças internas e externas são identificadas e classificadas?**

Existe um mapa de ameaças conhecidas associadas a cada tipo de ativo

1/13 **A gestão do risco é efetuada com base na análise de ameaças, vulnerabilidades, probabilidades e impactos?**

Existe um documento com a metodologia de gestão do risco estabelecida

1/14 **O processo de gestão de risco encontra-se definido?**

As estratégias para a gestão de riscos não estão definidas ou não são consistentes em toda a organização

1/15 **A estratégia de tratamento do risco encontra-se definida?**

A estratégia de tratamento de riscos é decidida caso a caso de forma ad hoc

1/16 **O risco da cadeia de logística é gerido?**

A organização aplica a gestão de riscos na sua cadeia logística

1/17 **Os contratos com fornecedores respeitam o plano de gestão do risco para a cadeia logística?**

Existe um processo formal para contratação de fornecedores

1/18 **O plano de resposta e recuperação de desastre é exercitado com os fornecedores?**

Os fornecedores que suportam os processos críticos da organização estão identificados

Anexo 10 - Diagramas

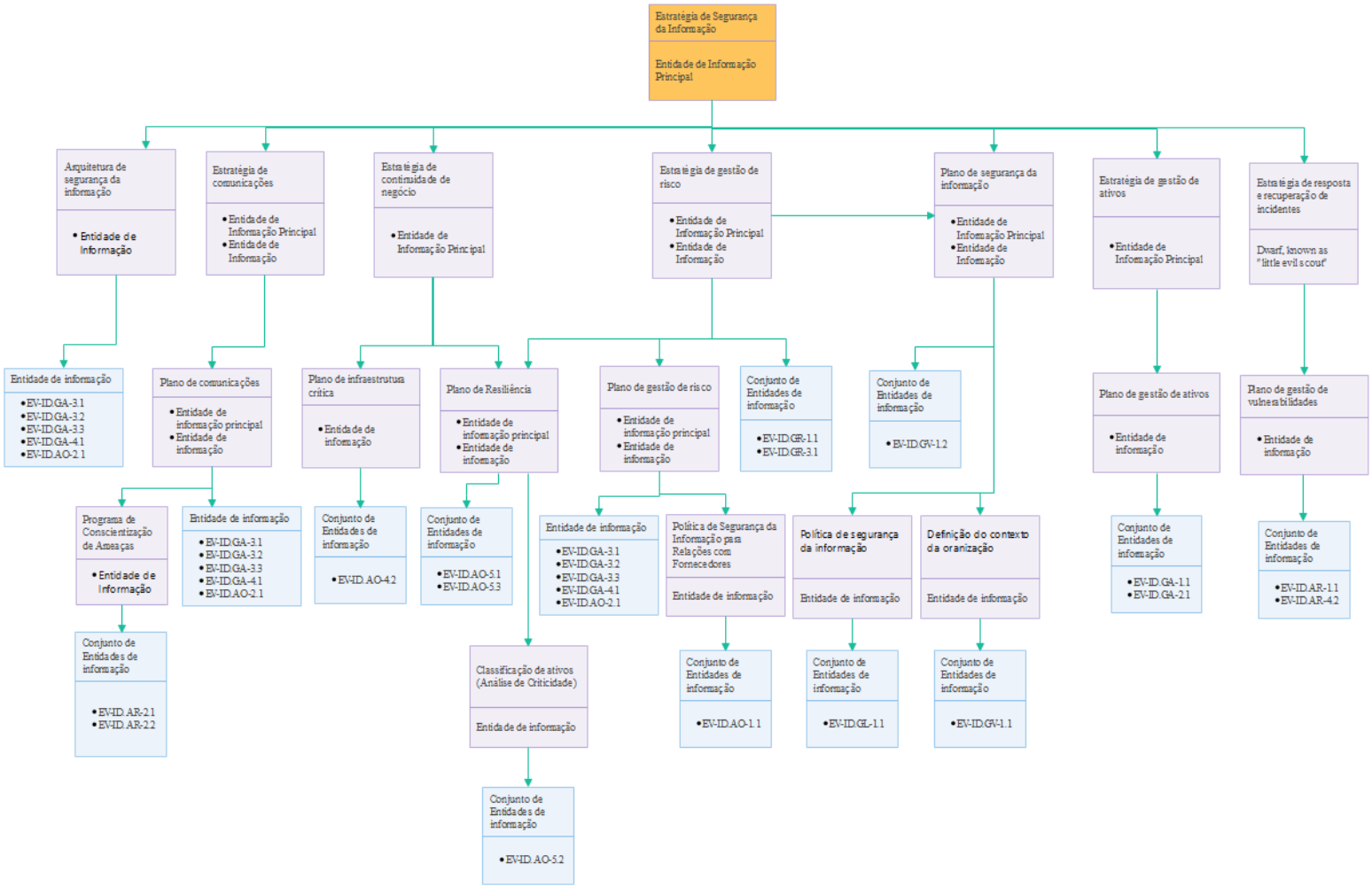


Figura 46: Estrutura da Informação da organização AMA mediante os dados fornecidos.

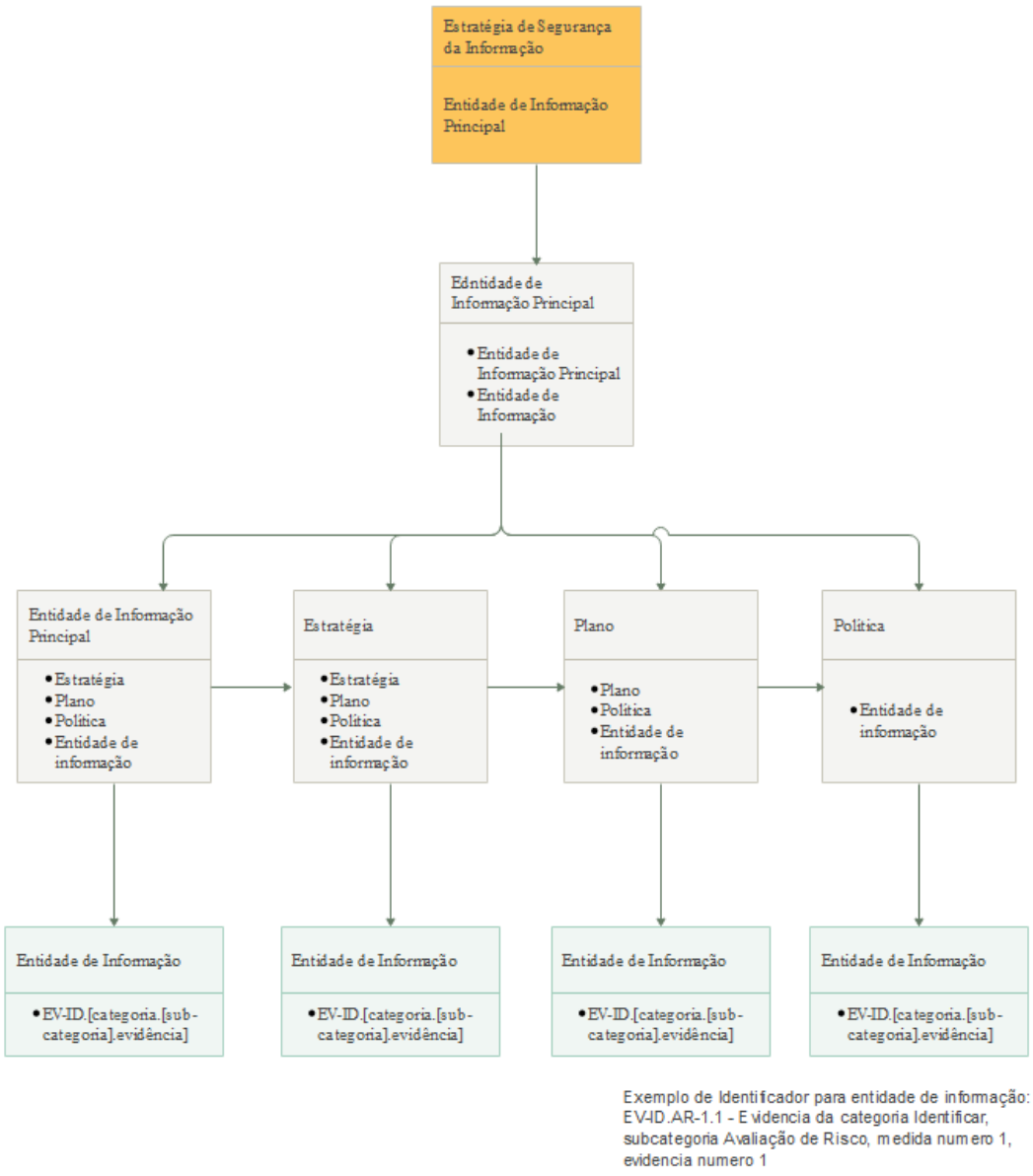


Figura 47: Estrutura da informação que origina a arquitetura de informação

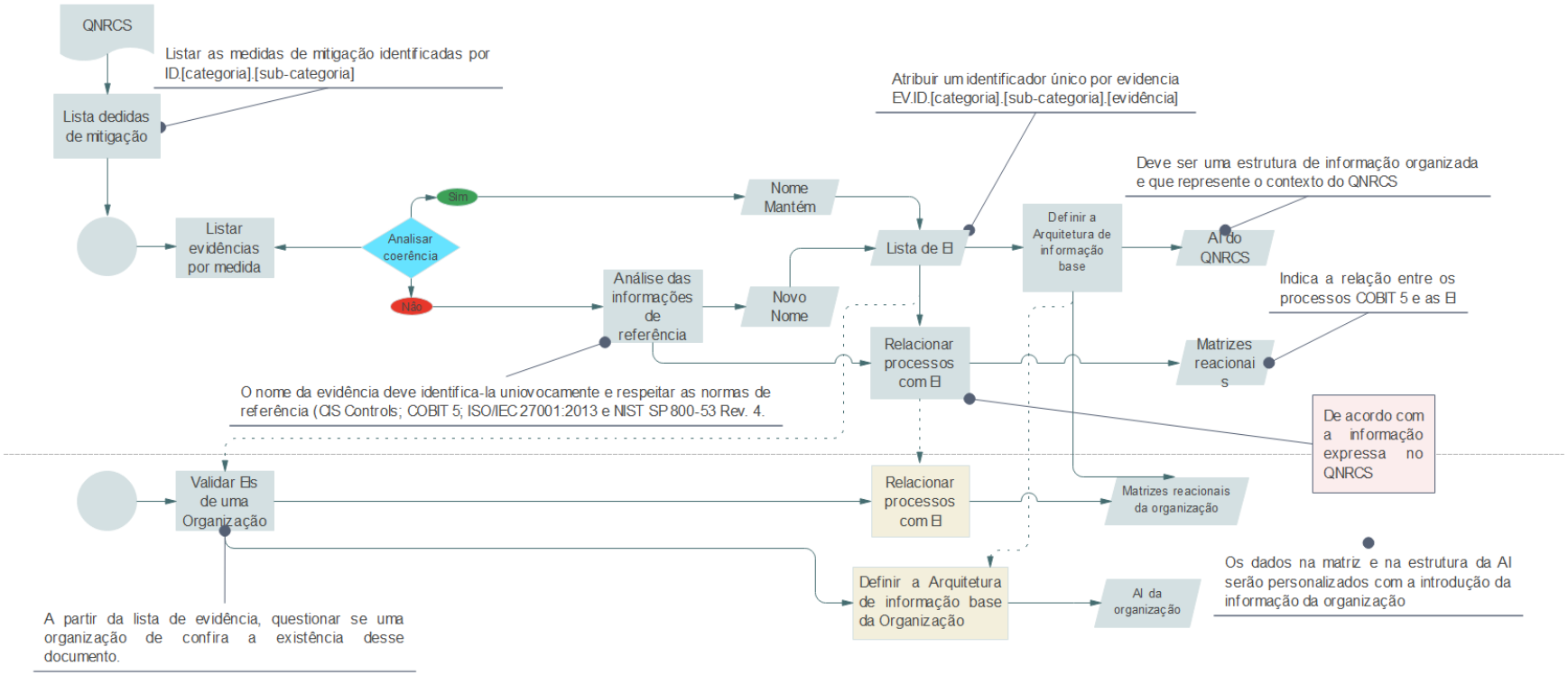


Figura 48: Diagrama do método utilizado para a investigação.