INSTITUTO SUPERIOR DE TECNOLOGIAS AVANÇADAS

Harmonized privacy and information security framework, including maturity and risk exposure

Carlos Manuel Coelho Lopes

Dissertação para obtenção do Grau de Mestre em

INFORMÁTICA

Júri

Presidente: Professora Doutora Gisela dos Santos Machado Canelhas

Arguente: Professora Doutora Maria Inês Vasconcellos Furtado

Orientador: Professor Doutor Pedro Ramos dos Santos Brandão

Coorientador: Engenheiro Pedro Nunes Oliveira Machado

Agosto de 2025

ISTEC

Instituto Superior de Tecnologias Avançadas

Campus Académico do Lumiar, Lisboa

Dissertação

Mestrado em Informática

Por Carlos Manuel Coelho Lopes

Harmonized privacy and information security framework, including maturity and risk exposure

Dissertação de mestrado apresentada ao Instituto Superior de Tecnologias Avançadas de Lisboa, para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Informática, realizada sob a orientação científica do Professor Doutor Pedro Brandão e coorientação do Engenheiro Pedro Nunes Oliveira Machado.

Agosto de 2025

Agradecimentos

A vida traz-nos surpresas e desafios inesperados, muitos dos quais se revelam transformadores e revitalizadores. Na verdade, nunca esperei estar a reforçar as minhas competências após os 50 anos de idade, com a realização de um Mestrado em Informática, que se tem revelado tão profícuo para a minha carreira. Quando em 2017 abracei um novo desafio profissional que requereu competências multidisciplinares, fui levado a trilhar um caminho que me conduziu a este Mestrado, após a conclusão de duas pós-graduações em áreas análogas à Informática.

Todos seremos, um dia, forçados a tomar decisões que nos tiram do nosso campo de conforto. Foi, precisamente, nessa senda, que constatei que acabam sempre por aparecer pessoas que nos ajudam a trilhar o caminho, dando apoio e orientação.

Em primeiro lugar, uma palavra de agradecimento à minha família, pois é por eles que tento sempre alcançar mais alguma coisa.

Uma palavra muito especial para o Pedro Machado, pelo incentivo, pela paciência e por me manter no caminho certo em mais esta jornada, pois sem ele nada disto teria sido possível. Também à Ana Costa pelas análises conjuntas e pelo pensamento fresco. E a toda a restante equipa com quem trabalho diariamente.

Ao professor Doutor Pedro Brandão, meu orientador e a todos os professores do ISTEC.

A todos estes, o meu sentido e reconhecido agradecimento.

Resumo

Numa sociedade de consumo cada vez mais digital onde as organizações estrategicamente têm de adotar o seu modelo de negócio a essa realidade, mas ao mesmo tempo têm também de garantir a conformidade com recursos limitados, a um número crescente de obrigações legais relacionadas com a Privacidade e Proteção de Dados, Segurança de Informação e Cibersegurança, serão metas difíceis de realizar.

A conformidade legal, por exemplo com o RGPD ou com a NIS na Europa, poderá ser garantida através da utilização de partes de standards ou *frameworks* existentes sobre estes temas, nomeadamente, a utilização das ISO/IEC, das NIST, da ENISA, da Nymity, entre outras. No entanto, a questão dos recursos sejam eles humanos, financeiros ou de outra natureza não são infindáveis, e nem sempre estão disponíveis com a mesma ordem de grandeza nas organizações.

O desenvolvimento de uma *framework* harmonizada, que abranja as temáticas de Privacidade, Segurança de Informação e Cibersegurança, que inclua por cada requisito uma visão de maturidade e exposição ao risco será fundamental e contribuirá para as organizações poderem fazer uma gestão mais eficaz e eficiente dos seus objetivos, recursos, riscos, e ainda garantirem um grau de maturidade mais elevado face aos requisitos legais.

Palavras-chave: Framework harmonizado, Conformidade, Privacidade, Proteção de dados, Segurança de informação, Cibersegurança

Abstract

In an increasingly digital consumer society, organizations must strategically adapt their business models to this reality, while simultaneously also ensuring compliance with limited resources, with a growing number of legal obligations related to Privacy and Data Protection, Information Security, and Cybersecurity. However, achieving these goals with limited resources present significant challenges.

Conformity, for example, with the GDPR or NIS in Europe, can be ensured using parts of existing standards or frameworks on these topics, such as ISO/IEC, NIST, ENISA, Nymity, among others. However, resources, whether human, financial, or otherwise, are not endless and are not always available in the same order of magnitude across organizations.

The development of a harmonized framework covering the topics of Privacy, Information Security, and Cybersecurity, which includes a maturity and risk exposure view for each requirement, will be fundamental and will help organizations to manage their objectives, resources, and risks more effectively and efficiently, while also ensuring a higher degree of maturity concerning legal requirements.

Keywords: Harmonized framework, Compliance, Privacy, Data Protection, Information Security, Cybersecurity

Glossário:

CCPA - *California Consumer Privacy Act*

CIS - *Critical Security Controls*

CMMI - *Capability Maturity Model Integration*

COBIT - *Control Objectives for Information Technologies*

CSF - *Cyber Security Framework for Critical Infrastructure*

CSIRT - *Computer Security Incident Response Team*

DPIA - *Data Protection Impact Assessment*

AIPD – Avaliação de Impacto de Proteção de Dados

DORA - *Digital Operational Resilience Act*

DSRM - *Design Science Research Methodology for Information Systems Research*

ENISA - *European Union Agency for Cybersecurity*

FISMA - *Federal Information Security Management Act*

GDPR – *General Data Protection Regulation*

HIPAA - *Health Insurance Portability and Accountability Act*

IA - Inteligência Artificial (AI – *Artificial Inteligence*)

IAPP - *International Association of Privacy Professionals*

ID - Identificador

IEC - *International Electrotechnical Commission*

ISACA - *Information Systems Audit and Control Association*

ISO - *International Organization for Standardization*

KGI - *Key Goal Indicators*

KPI - *Key Performance Indicators*

KRI - *Key Risk Indicators*

LGPD - Lei Geral de Proteção de Dados (Brasileira)

NIS - *Network and Information Systems*

NIST - *National Institute of Standards and Technology*

PME – Pequena e Média Empresa

RGDP – Regulamento Geral sobre a Proteção de Dados

SEI - *Software Engineering Institute*

SGSI - Sistema de Gestão de Segurança da Informação

UE – União Europeia

Conteúdo

Índice de Tabelas

Índice de Figuras

1 Introdução

As organizações enfrentam atualmente desafios e riscos relacionados com temas de privacidade, segurança da informação e cibersegurança. Estes resultam da densificação da legislação aplicável, da complexidade e interconetividade entre sistemas, da automatização e/ou digitalização de processos, do uso de Inteligência Artificial (IA), do crescente aumento do volume de dados tratados pelas organizações, assim como de ciberameaças *(World Economic Forum, 2023).*

Centrando a análise na densificação da legislação, dependendo da geografia, do sector de atividade, e do modelo de negócio seguido, quando uma organização pretende garantir a conformidade com obrigações legais relativas à privacidade, segurança da informação e cibersegurança depara-se com um vasto número de legislações por geografia (ex. Europa, Estados Unidos da América, Brasil, etc.), por vezes, com definições e princípios antagónicos.

A título de exemplo, a União Europeia (EU), de entre outras legislações, entre 2016 e 2024 publicou Diretivas e Regulamentos de alta complexidade, para identificação e implementação de requisitos de conformidade pelas organizações, designadamente (não exaustivo):

- Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas singulares, no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (RGPD) (Parlamento Europeu e do Conselho, 2016);
- Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022, relativo à resiliência operacional digital do setor financeiro (DORA) (Parlamento Europeu e do Conselho, 2022b);
- Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União (NIS 2) (Parlamento Europeu e do Conselho, 2022a);
- Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho de 13 de junho de 2024, que cria regras harmonizadas em matéria de inteligência artificial (AI act) (Parlamento Europeu e do Conselho, 2024).

Na UE, a regulamentação é percecionada por 60% das organizações como um obstáculo ao investimento, com 55% das Pequenas e Médias Empresas (PME) a assinalarem os obstáculos regulamentares e a carga administrativa como o seu maior desafio. A UE impõe também um ónus proporcionalmente mais elevado às (PME) e às pequenas empresas de média capitalização do que às grandes empresas. Por este motivo, apenas as organizações de maior dimensão, frequentemente sediadas fora da UE, têm capacidade financeira e de mobilização para suportar os custos da conformidade (Mario Draghi, 2024).

Com a densificação de legislação, as organizações deparam-se com dificuldades na gestão dos seus recursos financeiros, humanos ou de outra natureza, a fim de evitarem lacunas e questões de adaptação às mudanças provenientes de obrigações regulamentares. Ambas as situações, contribuem para uma gestão de risco menos eficiente e com menor maturidade por parte das organizações face aos requisitos de conformidade aplicáveis.

Perante este cenário, será indispensável que as organizações adotem metodologias que assegurem a privacidade e a proteção dos dados, especialmente se tratarem dados sensíveis, uma vez que a sua natureza representa maior risco para os direitos, liberdades e garantias fundamentais dos titulares dos dados. A privacidade e a proteção dos dados, nos dias de hoje, assumem um papel preponderante nas organizações, como por exemplo, em temas como ações de marketing a realizar ou em situações de exfiltração de dados, onde podem ser divulgadas informações com risco para a privacidade dos titulares dos dados visados. Razões pelas quais, se torna imperativo que as organizações entendam a privacidade e a proteção dos dados, como um objetivo estratégico, quer no cumprimento das obrigações legais, quer na proteção da privacidade dos titulares dos dados, onde as entidades têm responsabilidades no seu tratamento.

Adicionalmente, a utilização de standards e/ ou *frameworks* poderá constituir uma solução exequível, para ajudar as organizações a garantirem a conformidade com a crescente legislação (Ghorashi et al., 2023).

Face às questões enumeradas, o desidrato principal desta dissertação de mestrado será a conceção de uma *framework* harmonizada de privacidade, segurança de informação e cibersegurança, que inclua por requisito a exposição ao risco e a maturidade inerente, simplificando o ordenamento de requisitos aplicável, contribuindo para a eficácia do cumprimento e eficiência dos custos associados. Pretende-se com este artefacto ajudar as organizações, na gestão eficiente dos seus recursos e riscos, a garantir a conformidade com a regulamentação aplicável, bem como disponibilizar à academia uma ferramenta que possa ser utilizada e melhorada.

2 Motivação do estudo

A necessidade de conceção desta *framework*, decorre de desafios e riscos, que emergem da complexidade do panorama regulamentar com que as organizações se deparam atualmente de modo a assegurar a conformidade, em temas como a privacidade, segurança de informação e cibersegurança.

A título de exemplo, o RGPD, de aplicação obrigatória pelos Estados-Membros da UE, enfatiza a proteção da privacidade dos titulares dos dados, mas carece de orientações técnicas específicas, relativamente à sua aplicação prática. O mesmo acontece com outras disposições, onde a decomposição das obrigações legais em forma de requisitos, que possam ser utilizados pelas

organizações para garantir a conformidade, não será um caminho fácil. Deste modo, a solução poderá passar pela utilização de standards ou *frameworks,* devido às orientações processuais e técnicas abrangentes, visando colmatar as lacunas existentes entre a legislação e a sua aplicação prática (Ghorashi et al., 2023).

Todavia, a escolha destas ferramentas não será uma decisão fácil de tomar pelas organizações, dado que os standards e *frameworks* também têm limitações, nomeadamente, o facto de, por norma, endereçarem temáticas de forma singular, isolada, por silos, tais como a privacidade, a segurança da informação e a cibersegurança.

Ao analisar o *Cyber Security Framework for Critical Infrastructure* (NIST CSF), verificam-se limitações quando se compara a abrangência dos requisitos que o compõe com a de outros *frameworks,* como o *Control Objectives for Information and Related Technologies* (COBIT) ou a ISO/IEC 27001 - *Information Security Management Systems* (Almuhammadi & Alsaleh, 2017). Desta forma, a seleção do standard ou *framework* mais adequado é uma decisão complexa, que deve ser tomada com base nas expetativas e objetivos de cada organização, a fim de se verificar o alinhamento com os mesmos. Ainda assim, em alguns casos, a adoção de um standard ou *framework* não chega a ser suficiente para satisfazer as expectativas de uma organização (Taherdoost, 2022).

Por conseguinte, a existência de uma *framework* de requisitos harmonizados e abrangente, que oriente as organizações na gestão dos temas de privacidade, segurança da informação e cibersegurança, corporiza uma atividade fundamental. As organizações, na ausência de uma *framework* harmonizada, poderão enfrentar dificuldades na adaptação às obrigações legais. Desta forma comprometem os seus objetivos, contribuem para uma gestão de risco menos eficaz e assumem um grau de maturidade mais reduzido, face aos requisitos regulamentares que lhes são aplicáveis.

3 Metodologia

O principal objetivo desta dissertação de mestrado será a definição de uma *framework* harmonizada, baseada em requisitos legais, de standards e boas práticas relacionadas com a privacidade, segurança da informação e cibersegurança, que permita às organizações cumprir com as obrigações decorrentes da legislação sobre estas matérias. Adicionalmente, pretende-se que a utilização desta *framework* permita às organizações evidenciar uma visão da maturidade e de exposição ao risco por cada requisito.

Para se atingir os objetivos mencionados, será fundamental no âmbito da privacidade, segurança de informação e cibersegurança:

I. Identificar artigos de referência para o objeto de estudo, desenvolvendo uma avaliação crítica das diversas fontes, de forma a obter um resultado relevante e profícuo do ponto de vista da *framework* a produzir;
II. Identificar a legislação aplicável e, decompor em requisitos as obrigações decorrentes das mesmas;
III. Identificar standards internacionais e *frameworks* aplicáveis e, analisar a(s) sua(s) abrangência(s) e limitações;
IV. Identificar critérios que suportem a avaliação do risco por requisito;
V. Identificar critérios que suportem a avaliação da maturidade por requisito;
VI. Apresentar uma *framework* harmonizada sobre privacidade, segurança da informação e cibersegurança:
    a. Baseada em requisitos decorrentes de legislação, standards internacionais e *frameworks* existentes;
    b. Que proporcione uma visão por requisito, uma perspetiva de *conformidade,* com avaliação do risco e da maturidade e,
    c. Que assegure a exequibilidade desta proposta, numa proposta de valor para a academia e as organizações.

3.1 Questões em análise

A dissertação de mestrado denominada "*Harmonized privacy and information security framework, including maturity and risk exposure*" procurará dar resposta às seguintes questões:

i. Qual o impacto de uma simplificação e harmonização de requisitos de privacidade e segurança da informação, na eficácia e eficiência de uma organização?
ii. É possível harmonizar requisitos, por meio de uma *framework* que assegure um eficaz cumprimento de legislação aplicável?
iii. Como desenvolver uma *framework* de conformidade que inclua a avaliação da maturidade e do risco no cumprimento de requisitos harmonizados?

Para responder às questões apresentadas, a metodologia utilizada será o "*Design Science Research Methodology for Information Systems Research*" (DSRM) partilhada na Figura 1 – Metodologia DSRM (Peffers, 2007):

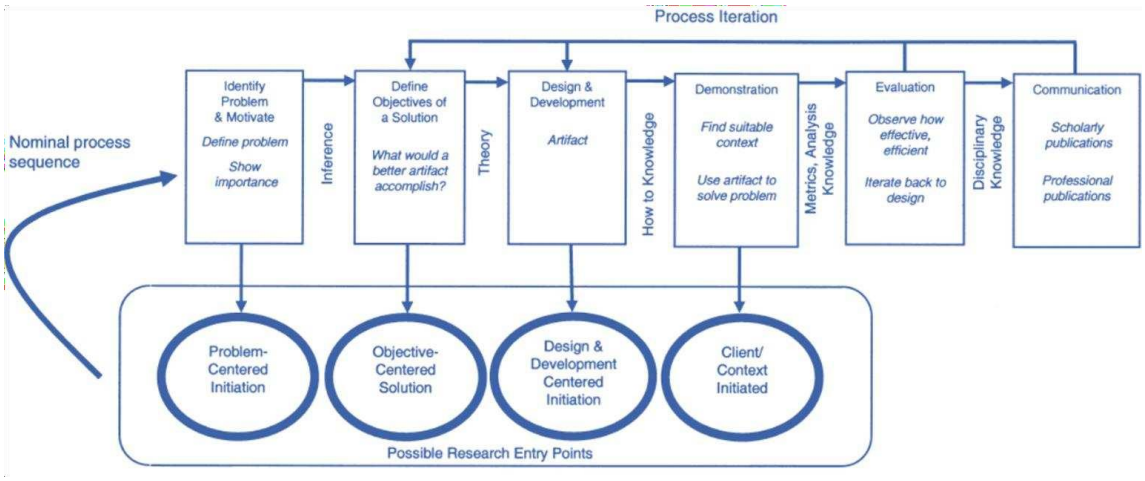

FIGURA 1 – METODOLOGIA DSRM

Esta metodologia tem por objetivo, criar e avaliar artefactos que são concebidos para resolver problemas organizacionais reais, permitindo às organizações a evolução de uma situação atual, para uma situação desejada. Logo, é uma metodologia que se centra na resolução de problemas (Deng & Ji, 2018)

Esta metodologia é composta por 6 fases:

(I). *Indentify Problem & Motivate* - identificação e contextualização do problema, que será suportado por uma revisão de artigos científicos, análise de normas internacionais e *frameworks*, onde serão inferidas as suas aplicações práticas e as suas limitações face a requisitos legais, que servirão para fundamentar a razão do desenvolvimento desta *framework* harmonizada;

(II). *Define Objectives of a Solution* - tendo em consideração as aplicações práticas e as limitações encontradas, serão definidos os requisitos provenientes das várias fontes identificadas (legislação, standards internacionais e *frameworks*), bem como a definição de critérios para a avaliação de risco e maturidade para cada requisito da *framework*;

(III). *Design & Development* - será desenvolvida a *framework* em folha Excel respeitando a inclusão por requisito de uma visão de risco e maturidade;

(IV). *Demonstration* - será efetuada uma simulação da *framework*, para garantir o seu funcionamento e a sua efetividade na resposta às questões propostas;

(V). *Evaluation* - será efetuada a observação se a *framework* criada consegue responder às questões propostas. Para fundamentar os resultados da avaliação, poderá ser feita uma comparação de resultados entre esta *framework* e outras, mas não se exclui a utilização de outras visões qualitativas ou quantitativas para suportar a avaliação. Desta avaliação é expectável que sejam identificadas também as forças e fraquezas da *framework,* assim como potenciais pontos de melhoria;

(VI). *Communication* - pressupõe a apresentação da *framework* à academia e à sociedade em geral.

Tendo em consideração a abordagem centrada na identificação do problema, da solução, o desenvolvimento do artefacto, a contribuição para a teoria e para a prática, e a sua natureza interdisciplinar, fazem com que a metodologia DSRM se alinhe com o objetivo desta dissertação de mestrado.

3.2 Fases da metodologia

No âmbito da presente dissertação de mestrado, e tendo em consideração a metodologia adotada, as seguintes fases identificadas na Tabela 1 – Metodologia DSRM, termos de implementação e desidratos, serão realizadas com o objetivo de responder às questões identificadas. É, assim, pretendido, com cada fase desta metodologia, alcançar os seguintes propósitos:

TABELA 1 – METODOLOGIA DSRM, TERMOS DE IMPLEMENTAÇÃO E DESIDRATOS

Fase	Aplicação	Desidrato
1. Identificação do problema & Motivação (*Problem Identification & Motivation*)	Revisão de literatura, análise de obrigações decorrentes da legislação. Identificação de standards e *frameworks* e análise da abrangência e limitações. Fundamentação para o desenvolvimento de uma *framework* harmonizada, que inclua a avaliação da exposição ao risco e a maturidade por requisito.	Analisar a situação atual e suportar questões identificadas para justificar o motivo da definição da *framework*, realçando as implicações práticas e os potenciais benefícios decorrentes da harmonização proposta.
2. Definição dos Objetivos para uma Solução (*Defining Objectives for a Solution*)	Com base nas questões identificadas, definição de objetivos claros e exequíveis para a *framework*: ➢ Harmonização de requisitos; ➢ Por requisito, disponibilização de visão de risco e maturidade.	Identificação dos requisitos, bem como dos critérios a utilizar para avaliar a exposição ao risco e a maturidade por requisito.
3. Conceção e Desenvolvimento (*Design & Development*)	Criação de uma *framework* que atinja os objetivos e responda às questões identificadas.	Disponibilização da *framework* em suporte de Excel.
4. Demonstração (*Demonstration*)	Demonstração do uso da *framework* recorrendo a dados "*dummy*" para evidenciar a sua forma de funcionamento e efetividade.	Simular o funcionamento da *framework*, demonstrando como atinge os objetivos e responde às questões identificadas.

Fase	Aplicação	Desidrato
5. Avaliação (*Evaluation*)	Avaliação da *framework* em termos dos objetivos propostos, o que poderá ser feito, por exemplo, pela comparação com outras *frameworks* existentes.	Documentar a evidência das suas forças e fraquezas, bem como de potenciais pontos de melhoria.
6. Comunicação (*Communication*)	Sustentação e formalização da *framework.* Pressupõe a entrega do documento de dissertação, bem como a eventual publicação de artigos científicos e apresentação em conferências.	Disponibilização do documento da dissertação, bem como potenciais documentos de suporte a publicações ou conferências da especialidade.

3.3 Identificação da literatura

Para a seleção dos estudos relevantes para o desenvolvimento da dissertação de mestrado, foi utilizada a fonte "*Google Scholar*". Foram efetuadas, nesta plataforma, várias pesquisas em função do tema, utilizando os termos identificados na Tabela 2:

TABELA 2 – IDENTIFICAÇÃO DOS CRITÉRIOS DE PESQUISA DE LITERATURA

Tema	Termo	Idioma
Cibersegurança	"*Cybersecurity "and "Cybersecurity framework" and "NIS directive" and "NIST cybersecurity framework"*	Inglês
DRMS	*"Design Science Research in Information System "*	Inglês
RGPD	*"GDPR" and" GDPR monitoring" and "GDPR article 32, technical and organizational measures"*	Inglês
Maturidade	*"Maturity models" and "Comparison of maturity models" and "CMMI maturity level rating"*	Inglês
Privacidade	*"Privacy" and "Privacy frameworks" and "Privacy definition" and "Privacy meaning" and "Privacy and Brazilian law" and "Five safes"*	Inglês
Risco	"*Risk concept evolution" and "Key Risk Indicator's*"	Inglês
Segurança de Informação	*"Information security" and "Technical and organization measures" and* "Segurança da Informação"	Inglês e Português

Foram analisados vários artigos dentro dos temas referenciados na Tabela 2, de vários autores, com antiguidades de publicação entre 2003 e 2024.

Foram, igualmente, utilizadas publicações no âmbito do desenvolvimento da dissertação de mestrado provenientes de várias organizações privadas ou estatais reconhecidas pelo trabalho desenvolvido nestas temáticas. No âmbito da privacidade, do IAPP - *International Association of Privacy Professionals*, da ISO - *International Organization for Standardization* e da IEC - *International Electrotechnical Commission*. No âmbito da segurança de informação e cibersegurança, da ENISA - *European Union Agency for Cybersecurity*, do ISACA - *Information Systems Audit and Control Association*, da NIST - *National Institute of Standards and Technology*, da ISO - *International Organization for Standardization* e da IEC - *International Electrotechnical Commission*.

Ao nível da legislação identificada na dissertação de mestrado, a mesma é, essencialmente, proveniente do estado português e da EU, embora tenham sido identificadas legislações de outras geografias, como do Brasil e dos Estados Unidos da América

Toda esta informação está descrita no capítulo 9 do presente documento, designado por Bibliografia.

4 Conceitos

4.1 Privacidade

De acordo com o Tribunal Europeu dos Direitos do Homem, definir privacidade é um desafio. A privacidade tem uma relação estreita com a dignidade humana, a liberdade e a independência do indivíduo, sendo atualmente posta em causa, devido ao rápido desenvolvimento tecnológico da sociedade da informação (Lukács, 2016).

Foram várias, as tentativas de definir a privacidade ao longo dos últimos anos, por via de definições como "*the right to be left alone*" (o direito de ser deixado em paz), a autonomia em matéria de assuntos pessoais, ou o controlo pelo indivíduo da sua própria informação (Moore, 2003).

O *National Institute of Standards and Technology* (NIST) define a privacidade como o direito de uma parte, manter o controlo e a confidencialidade das informações que lhe dizem respeito, e a liberdade de não estar sujeito a intromissões na sua vida ou assuntos privados, aquando dessa intromissão resulta da recolha e utilização indevida, ou ilegal de dados pessoais sobre essa mesma pessoa (National Institute of Standards and Technology (NIST), 2024b).

Por sua vez, a *International Association of Privacy Professionals* (IAPP), define privacidade como o direito de ser deixado em paz, ou a liberdade de interferência ou intrusão *(International Association of Privacy Professionals (IAPP), 2024)*.

4.2 Segurança da Informação e Cibersegurança

Quando se analisam os conceitos de segurança da informação e de cibersegurança, verifica-se que existe alguma sobreposição conceptual, todavia são conceitos diferenciados. A segurança da informação ultrapassa os limites da cibersegurança para incluir, não só a proteção dos recursos de informação, mas também a de outros bens, incluindo a proteção das próprias pessoas (Von Solms & Van Niekerk, 2013).

O objetivo da segurança da informação, é o de assegurar a continuidade das atividades e minimizar os prejuízos para as organizações, limitando o impacto dos incidentes de segurança (Von Solms & Van Niekerk, 2013).

Em termos de definição de segurança da informação, o standard internacional ISO/IEC 27001 de 2022, publicado pela *International Organization for Standardization* e pela *International Electrotechnical Commission*, define a segurança da informação, como a preservação da confidencialidade, integridade e disponibilidade da informação, através da aplicação de um processo de gestão de risco, que proporciona confiança às partes interessadas, em como os riscos são geridos adequadamente (ISO/IEC, 2022a). Conforme referenciado na Figura 2 – Representação espectral das propriedades da Segurança da Informação, a integridade, confidencialidade e disponibilidades podem ser definidas como:

- Integridade:
  - Proteção contra perdas, destruição ou danos acidentais (Huth & Matthes, 2019);
- Confidencialidade:
  - Proteção contra o processamento não autorizado ou ilegal;
  - Propriedade de que a informação não seja disponibilizada ou divulgada a indivíduos, entidades ou processos não autorizados (Huth & Matthes, 2019);
- Disponibilidade/Acesso - propriedade de ser acessível e utilizável a pedido de uma entidade autorizada (Huth & Matthes, 2019).

Em outras publicações científicas, a segurança da informação é também definida:

- Como a proteção da informação e dos seus elementos críticos, incluindo os sistemas e o hardware que utilizam, armazenam e transmitem essas informações (Whitman, 2011);
- Como a proteção da informação contra uma ampla gama de ameaças, a fim de se garantir a continuidade das operações, minimizar os riscos de negócio e maximizar o retorno sobre os investimentos e as oportunidades de negócio (Laura et al., 2021).

FIGURA 2 – Representação espectral das propriedades da Segurança da Informação

Relativamente à temática da cibersegurança, existem múltiplas definições de várias fontes:

- Capacidade de proteger ou defender a utilização do ciberespaço de ciberataques *(National Institute of Standards and Technology (NIST), 2024a)*;
- Conjunto de ferramentas, políticas, conceitos de segurança, diretrizes, gestão de riscos, abordagens, ações, formação, melhores práticas, garantias e tecnologias que podem ser utilizadas para proteger o ambiente cibernético, os ativos da organização e os utilizadores (Von Solms & Van Niekerk, 2013);
- É o conjunto de recursos, processos e estruturas utilizadas para proteger o ciberespaço e os sistemas conectados ao ciberespaço contra ocorrências que coloquem em causa os direitos de propriedade previstos na lei (Craigen et al., 2014).

4.3 Standards e *Frameworks*

De acordo com a organização *Standards Austrália*, os standards são documentos que definem especificações, procedimentos e diretrizes, com o objetivo de garantir a segurança, consistência e fiabilidade nos produtos, serviços e sistemas. Já as organizações ISO/IEC defendem que os standards são elaborados com base num acordo geral e validados por uma entidade jurídica, que ajudam a atingir resultados, em termos de *guidance*, modelo ou amostra, num determinado contexto. São, pois, documentos estabelecidos por organismos profissionais que podem ser utilizados pelas organizações (ex. programas, standards técnicos), ou standards de práticas técnicas (ex.: standards práticos de cibersegurança) (Taherdoost, 2022).

Relativamente às *frameworks*, estas corporizam diretrizes gerais que abrangem uma vasta gama de domínios e componentes nas organizações. As *frameworks* são flexíveis e podem dar aos utilizadores a liberdade de escolherem algumas partes ou a totalidade do modelo, métodos ou práticas técnicas, oferecendo orientações gerais que podem ser adotadas, bem como sugestões a aplicar na organização (Taherdoost, 2022).

4.4 Risco

Os riscos podem ter origem natural ou humana. Apresentam um carácter multidisciplinar, pois têm uma probabilidade e impacto diferentes, consoante o contexto onde são identificados, como por exemplo, se afetam a sociedade em geral, uma organização ou um indivíduo.

Existem vários standards e *frameworks* de gestão de risco aplicáveis ao sector financeiro e não financeiro, em diferentes áreas de negócio, que incluem definições de risco (Popchev et al., 2021).

A NIST define risco como a medição da exposição de uma entidade a uma ameaça potencial, decorrente de uma circunstância ou evento se materializar, em termos de impactos adversos e probabilidade de ocorrência *(National Institute of Standards and Technology (NIST), 2024b).*

O standard internacional ISO/IEC 31000:2018 define risco como o efeito da incerteza nos objetivos. Sendo que o efeito, é um desvio relativamente ao esperado. Este pode ser positivo, negativo ou ambos, e pode abordar, criar ou resultar em oportunidades ou ameaças. O risco é frequentemente expresso em termos de fontes de risco, eventos potenciais, suas consequências e verossimilhança (ISO/IEC, 2018).

4.5 Maturidade

A maturidade pode ser definida como o estado em que as organizações estão em perfeitas condições para atingir os seus objetivos (Becker et al., 2010) ou a metodologia que uma organização possui para avaliar as capacidades relativamente, a uma determinada disciplina (Khoshgoftar & Osman, 2008).

A Associação de Auditoria e Controlo de Sistemas de Informação (ISACA), define maturidade como uma classificação que descreve o grau em que os processos de uma organização ou de uma área se encontram em conformidade com um conjunto predefinido de boas práticas (ISACA, 2024b).

5 Legislação

Nesta seção será feita uma identificação das legislações que impactam a privacidade, a segurança de informação e a cibersegurança ao nível das obrigações legais decorrentes. O tema da privacidade será analisado em duas perspetivas:

- A licitude do tratamento dos dados pessoais: não limitando aos denominados fundamentos de licitude previstos na lei, porém universalizando a expressão à inclusão dos demais requisitos legais no tratamento de dados pessoais;
- A proteção dos dados pessoais: numa perspetiva mais especificamente relacionada com temas de segurança da informação e cibersegurança.

Será facilitada a compreensão do tema ao longo do documento e testar-se-á se garantir a privacidade implica apenas proteger os dados pessoais.

5.1 Privacidade

Na perspetiva da privacidade existem diferentes legislações por diferentes geografias. Na Europa, foi publicado o RGPD – Regulamento 2016/679 da EU (Parlamento Europeu e do Conselho, 2016b). Em Portugal, as organizações têm de cumprir com o RGPD e com as obrigações previstas na Lei 58/2019, enquanto lei de execução nacional do RGPD (Assembleia da República, 2019). Noutras geografias, como no Brasil, as organizações têm de cumprir com a Lei Geral de Proteção de Dados Brasileira (LGPD) (De Castro et al., 2022), ou nos Estados Unidos da América com o *California Consumer Privacy Act* (CCPA) (Privacy Protection Agency, 2018) ou com a *Health Insurance Portability and Accountability Act* (HIPAA) (US Congress, 1996), que incorpora um conjunto de requisitos específicos sobre a privacidade, detalhados na HIPAA *privacy rule*.

Apesar de terem sido mencionadas várias legislações por geografia, a análise será centrada no Regulamento Europeu (RGDP) e na Lei de Execução Nacional para Portugal, a fim de demonstrar a dificuldade de interpretação das obrigações legais decorrentes, para consubstanciar a importância e benefícios da existência de uma *framework* harmonizada.

5.1.1 RGPD

O RGPD, entrou em vigor em maio de 2018 e constitui uma das mais importantes alterações e reforço da regulamentação, em matéria de privacidade, das últimas décadas (Arfelt et al., 2019). Na verdade, este foi concebido para harmonizar a legislação relativa à proteção de dados em toda a Europa, com o objetivo de providenciar maior proteção e capacidade aos titulares de dados, garantindo que estes tenham controlo das suas informações, face aos novos desenvolvimentos tecnológicos, permitindo desta forma ao cidadão, a salvaguarda destes direitos, liberdades e garantias fundamentais. Em termos de aplicabilidade, visam todas as organizações que tratam dados pessoais dos residentes da União Europeia, independentemente da sua localização física (Ayala-Rivera & Lero@ucd, 2018).

O Regulamento é tão abrangente quanto severo, pelo que o incumprimento dos requisitos técnicos e organizacionais que impõe, pode resultar em multas entre os 10 milhões de euros, 2% do volume de negócios anual da organização, 20 milhões de euros ou 4% do volume de negócios anual da organização a nível mundial (Arfelt et al., 2019).

O RGPD exige, pois, um controlo detalhado das atividades de tratamento de dados pessoais. Requere também, que cada tratamento que envolve dados pessoais, tenha uma base jurídica documentada (fundamento de licitude). Os dados pessoais que, eventualmente, entretanto, não sejam necessários ou que já não estejam em conformidade com a referida base legal, deverão ser

imediatamente apagados. Além disso, os titulares dos dados têm determinados direitos de imposição de restrições às atividades de tratamento dos dados que lhes digam respeito, salvo se esses tratamentos decorrerem de outras obrigações, nos termos da legislação em vigor.

Para estarem em conformidade, as organizações têm não só de cumprir com estas obrigações legais, mas também de as documentar, por forma a facilitar processos de verificação por via de auditorias (Arfelt et al., 2019).

Para uma melhor compreensão do RGPD, importa clarificar alguns conceitos. O RGPD define no seu artigo 4.º:

- Dados pessoais, como a informação relativa a uma pessoa singular identificada ou identificável (titular dos dados);
- Tratamento, como uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

Por sua vez, o artigo 5º prevê que o tratamento dos dados pessoais só é lícito, se for utilizado um fundamento de licitude, como por exemplo:

- O consentimento por parte do titular dos dados;
- No âmbito da execução de um contrato, se o titular fizer parte do mesmo;
- No âmbito do cumprimento de uma obrigação legal.

entre outros fundamentos de licitude que podem ser utilizados como suporte ao tratamento dos dados pessoais pelas organizações.

Todavia, assegurar a Privacidade (P), inclui mais obrigações a cumprir pelas organizações do que a mera questão do fundamento legal para o tratamento dos dados pessoais, conforme as obrigações espelhadas na Tabela 3 do presente ponto.

Já ao nível da Segurança (S) dos dados pessoais, esta deve ser feita em função do plasmado no art.º 32 do RGPD, Segurança no Tratamento. Este artigo determina que as organizações implementem medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco.

Analisando e interpretando os artigos do Regulamento identificam-se na Tabela 3 – Classificação tipológica de artigos do RGDP, as seguintes obrigações legais que as organizações devem endereçar do ponto de vista da Privacidade (P) e Segurança (S), as quais terão uma correspondência com os requisitos da *framework* harmonizada que será apresentado no âmbito desta dissertação.

TABELA 3 – CLASSIFICAÇÃO TIPOLÓGICA DE ARTIGOS DO RGPD

Art.º	Descrição sumária	P/S	Art.º	Descrição sumária	P/S
5º	Princípios relativos ao tratamento de dados pessoais	P	27	Representantes dos responsáveis pelo tratamento ou dos subcontratantes não estabelecidos na União	P
6º	Licitude do tratamento	P	28	Subcontratante	P
7º	Condições aplicáveis ao consentimento	P	29	Tratamento sob a autoridade do responsável pelo tratamento ou do subcontratante	P
8º	Condições aplicáveis ao consentimento de crianças em relação aos serviços da sociedade da informação	p	30	Registos das atividades de tratamento	P
9º	Tratamento de categorias especiais de dados pessoais	P	32	Segurança do tratamento	S
10º	Tratamento de dados pessoais relacionados com condenações penais e infrações	P	33	Notificação de uma violação de dados pessoais à autoridade de controlo	P
12º	Transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados	P	34	Comunicação de uma violação de dados pessoais ao titular dos dados	P
13º	Informações a facultar quando os dados pessoais são recolhidos junto do titular 1.	P	35	Avaliação de impacto sobre a proteção de dados	P
14º	Informações a facultar quando os dados pessoais não são recolhidos junto do titular	P	36	Consulta prévia	p
15º	Direito de acesso do titular dos dados	P	37	Designação do encarregado da proteção de dados	p
16º	Direito de retificação	P	38	Posição do encarregado da proteção de dados	P

Art.º	Descrição sumária	P/S	Art.º	Descrição sumária	P/S
17º	Direito ao apagamento dos dados («direito a ser esquecido»)	P	39	Funções do encarregado da proteção de dados	P
18º	Direito à limitação do tratamento	P	45	Transferências com base numa decisão de adequação	P
19º	Obrigação de notificação da retificação, apagamento dos dados pessoais ou limitação do tratamento	P	46	Transferências sujeitas a garantias adequadas	P
20º	Direito de portabilidade dos dados	P	47	Regras vinculativas aplicáveis às empresas	P
21º	Direito de oposição	P	48	Transferências ou divulgações não autorizadas pelo direito da União	P
22º	Decisões individuais automatizadas, incluindo definição de perfis	P	49	Derrogações para situações específicas	P
24º	Temas legais do responsável pelo tratamento	P	89	Garantias e derrogações relativas ao tratamento para fins de arquivo de interesse público, para fins de investigação científica, histórica ou para fins estatísticos	P
25º	Proteção de dados desde a conceção e por defeito	P/S	91	Normas vigentes em matéria de proteção dos dados das igrejas e associações religiosas	P

Resulta pois claro que, de acordo com os dados da Tabela 3, com exceção dos artigos 25º e 32º, todos os outros estão relacionados com a implementação de medidas que garantem a licitude do tratamento dos dados pessoais. Apenas os artigos 25º e 32º, remetem para aspetos relacionados com a proteção e segurança dos dados pessoais, cuja interpretação pode ser complexa.

Detalhando o artigo 32º relativo à segurança no tratamento, este requere no n.º 1 e no n.º 2, que as organizações apliquem as Medidas Técnicas e Organizativas adequadas ao risco, relativo à garantia dos direitos e liberdades dos titulares dos dados, tendo em consideração o contexto e as finalidades de tratamento dos mesmos. As medidas implementadas devem ser alvo de monitorização regular, com o objetivo de garantir a segurança do tratamento e devem também permitir:

- Assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento,
- A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada, em caso de incidente físico ou técnico.

O artigo refere-se a requisitos, muitas vezes identificados como Medidas Técnicas e Organizativas, tais como a pseudonimização, a cifragem, entre outros. No entanto, é legítimo afirmar que não existe uma Medida Técnica ou Organizacional específica, que possa ser considerada isoladamente para se atingir esses objetivos. Pelo que, terá sempre de se implementar um conjunto de medidas, para se poder alcançar um ou mais objetivos. Como exemplo, para cumprir o objetivo da confidencialidade numa organização, será necessário implementar um conjunto de medidas, que podem ir, desde a encriptação/cifragem do correio eletrónico, controlo do acesso às salas onde os dados pessoais estão a ser tratados, formação sobre privacidade a todos os que exercendo uma função, realizam o tratamento de dados pessoais, de entre outras (Selzer, 2021).

5.1.2 Lei de Execução Nacional 58/2019

Os artigos do RGPD com os números 85, 86, 87, 88 e 90, determinam, que certos aspetos podem ser clarificados e regulamentados, através de leis específicas formalizadas pelos estados-membros, em complemento às próprias obrigações dispostas no Regulamento.

Analisando e interpretando os artigos da Lei de Execução Nacional 58/2019 (Assembleia da República, 2019), relativa à proteção das pessoas singulares no que concerne ao tratamento de dados pessoais e à livre circulação desses dados, identificam-se na Tabela 4 as seguintes obrigações legais que as organizações devem endereçar:

TABELA 4 – MAPEAMENTO DE ARTIGOS DA LEI DE EXECUÇÃO NACIONAL 58/2019

Art.º	Descrição sumária	P/S	Art.º	Descrição sumária	P/S
7	Avaliações prévias de impacto	S	20	Dever de segredo	P
8	Dever de colaboração	P	21	Prazo de conservação de dados pessoais	P
9	Encarregado de proteção de dados (EDP) - Disposição geral	p	22	Transferências de dados	P
11	Funções do encarregado de proteção de dados	P	23	Tratamento de dados pessoais por entidades públicas para finalidades diferentes	P
12	Encarregados de proteção de dados em entidades públicas	P	25	Publicação em jornal oficial	P

Art.º	Descrição sumária	P/S	Art.º	Descrição sumária	P/S
13	Encarregados de proteção de dados em entidades privadas	P	26	Acesso a documentos administrativos	P
15	Códigos de conduta	P	27	Publicação de dados no âmbito da contratação pública	P
16	Consentimento de menores	P	28	Relações laborais	P
17	Proteção de dados pessoais de pessoas falecidas	p	29	Tratamento de dados de saúde e dados genéticos	P
18	Portabilidade e interoperabilidade dos dados	p	30	Bases de dados ou registos centralizados de saúde	P
19	Videovigilância	P	31	Tratamentos para fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos	P

Mais uma vez, resulta claro que nos dados da Tabela 4, existe apenas um único artigo que remete para aspetos relacionados com a Segurança dos dados pessoais.

5.2 Segurança da Informação e Cibersegurança

Na perspetiva da segurança da informação e da cibersegurança existem diferentes legislações por diferentes geografias.

Na Europa, a Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União (NIS 2) (Parlamento Europeu e do Conselho, 2022a), que vem revogar a Diretiva (UE) 2016/1148 (NIS 1) (Parlamento Europeu e do Conselho, 2016a) a partir de 18/10/2024, define um conjunto de obrigações que devem ser cumpridas pelas organizações.

Em Portugal, as obrigações decorrentes da Diretiva NIS foram transpostas para a Lei 46/2108, que estabelece o regime jurídico da segurança do ciberespaço, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (Assembleia da República, 2018).

As obrigações da Lei 46/2018, devem ser analisadas conjuntamente com as obrigações decorrentes do Decreto-Lei 65/2021, da Presidência do Conselho de Ministros, sobre o regime jurídico da segurança do ciberespaço (Presidência do Conselho de Ministros, 2021). Todavia, nos Estados Unidos da América, de entre outras legislações, as organizações têm de cumprir com a *Health Insurance Portability and Accountability* Act (HIPAA) (US Congress, 1996), que incorpora um conjunto de requisitos específicos sobre a segurança da informação e cibersegurança, detalhados no HIPAA *security rule* e com a *Federal Information Security*

Management Act (FISMA) (US Congress, 2014).

Na próxima seção, irá ser abordado de forma sumária, o conteúdo da NIS e da legislação portuguesa, para demonstrar a dificuldade de interpretação das obrigações legais decorrentes, por forma a consubstanciar a importância da existência de uma *framework* harmonizada.

5.2.1 NIS, Lei 46/2018 e Decreto-Lei 65/2021

A Diretiva NIS é a primeira legislação horizontal adotada a nível da União Europeia para a proteção das redes e dos sistemas de informação em toda a União Europeia (Markopoulou et al., 2019). Atribuiu responsabilidades em cibersegurança aos operadores de serviços essenciais de cadeias de abastecimento (Wallis & Johnson, 2020).

Nestes termos, pretende-se que impacte duas categorias de organizações, os (i) operadores de serviços essenciais e os (ii) prestadores de serviços digitais (Tabela 5 – Operadores de serviços essenciais nos termos da Lei 46/2018), sem prejuízo de uma abordagem diferenciada em termos das obrigações impostas (Markopoulou et al., 2019).

TABELA 5 – OPERADORES DE SERVIÇOS ESSENCIAIS NOS TERMOS DA LEI 46/2018

Setores, subsetores e tipos de entidades dos operadores de serviços essenciais		
Setor	**Subsetor**	**Tipo de entidades**
Energia	Eletricidade	Empresa de eletricidade que exerce a atividade de comercialização. Operadores da rede de distribuição. Operadores da rede de transporte.
	Petróleo	Operadores de oleodutos de petróleo. Operadores de instalações de produção, refinamento e tratamento, armazenamento e transporte de petróleo.
	Gás	Empresas de comercialização. Operadores da rede de distribuição. Operadores da rede de transporte. Operadores do sistema de armazenamento. Operadores da rede de gás natural em estado líquido (GNL). Empresas de gás natural. Operadores de instalações de refinamento e tratamento de gás natural.

Setores, subsetores e tipos de entidades dos operadores de serviços essenciais		
Setor	**Subsetor**	**Tipo de entidades**
Transportes	Transporte aéreo	Transportadoras aéreas. Entidades gestoras aeroportuárias, aeroportos e as entidades, que exploram instalações anexas existentes dentro dos aeroportos. Operadores de controlo da gestão do tráfego aéreo, que prestam serviços de controlo de tráfego aéreo.
	Transporte ferroviário	Gestores de infraestruturas. Empresas ferroviárias incluindo os operadores de instalações de serviço.
	Transporte marítimo e por vias navegáveis interiores	Companhias de transporte por vias navegáveis interiores, marítimo e costeiro de passageiros e de mercadorias, não incluindo os navios explorados por essas companhias Entidades gestoras dos portos, incluindo as respetivas instalações portuárias e as entidades que gerem as obras e os equipamentos existentes dentro dos portos. Operadores de serviços de tráfego marítimo.
	Transporte rodoviário	Autoridades rodoviárias. Operadores de sistemas de transporte inteligentes.
Bancário		Instituições de crédito.
Infraestruturas do mercado financeiro		Operadores de plataformas de negociação. Contrapartes centrais.
Saúde	Instalações de prestação de cuidados de saúde	Prestadores de cuidados de saúde.
Fornecimento e distribuição de água potável		Fornecedores e distribuidores de água destinada ao consumo humano, mas excluindo os distribuidores, para os quais a distribuição de água para consumo humano é apenas uma parte da sua atividade geral de distribuição de outros produtos de base e mercadorias não considerados serviços essenciais.

Setores, subsetores e tipos de entidades dos operadores de serviços essenciais		
Setor	**Subsetor**	**Tipo de entidades**
Infraestruturas digitais		Pontos de troca de tráfego. Prestadores de serviços de Sistema de Nomes de Domínio (DNS). Registos de nomes de domínio de topo.

A Diretiva NIS para as organizações no âmbito, define de forma sumária as seguintes obrigações descritas na Tabela 6:

TABELA 6 – MAPEAMENTO E OBRIGAÇÕES DOS OPERADORES DE SERVIÇOS ESSENCIAIS

Art.º	Nome do artigo	Descrição	P/S
20	Governação	Os órgãos de direção das entidades essenciais e importantes, aprovam as medidas de gestão dos riscos de cibersegurança, tomadas por essas entidades.	S
21	Medidas de gestão dos riscos de cibersegurança	Assegurar que as entidades essenciais e importantes tomam medidas técnicas, operacionais e organizativas adequadas e proporcionadas, para gerir os riscos que se colocam à segurança dos sistemas de rede e informação, que utilizam nas suas operações ou na prestação dos seus serviços. E, para impedir ou minimizar, o impacto de incidentes nos destinatários dos seus serviços e noutros serviços. Devem abranger pelo menos os seguintes aspetos: a) Políticas de análise dos riscos e de segurança dos sistemas de informação; b) Tratamento de incidentes; c) Continuidade das atividades, como a gestão de cópias de segurança e a recuperação de desastres, bem como a gestão de crises; d) Segurança da cadeia de abastecimento, incluindo aspetos de segurança respeitantes às relações entre cada entidade e os respetivos fornecedores ou prestadores de serviços diretos; e) Segurança na aquisição, desenvolvimento e manutenção dos sistemas de rede e informação, incluindo o tratamento e a divulgação de vulnerabilidades; f) Políticas e procedimentos para avaliar a eficácia das medidas de gestão dos riscos de cibersegurança;	S

Art.º	Nome do artigo	Descrição	P/S
		g) Práticas básicas de ciber-higiene e formação em cibersegurança; h) Políticas e procedimentos relativos à utilização de criptografia e, se for caso disso, de cifragem; i) Segurança dos recursos humanos, políticas seguidas em matéria de controlo do acesso e gestão de ativos; j) Utilização de soluções de autenticação multifatores ou de autenticação contínua, comunicações seguras.	
23	Obrigações de notificação	As entidades essenciais e importantes notificam as equipas de resposta a incidentes de segurança informática (CSIRT).	S

As obrigações dos operadores de serviços essenciais da NIS foram transpostas para o panorama legal português através da lei 46/2018 (Tabela 7):

TABELA 7 – MAPEAMENTO E OBRIGAÇÕES NO ORDENAMENTO JURÍDICO NACIONAL

Art.º	Nome do artigo	Descrição	P/S
14	Requisitos de segurança para a Administração Pública e operadores de infraestruturas críticas	A Administração Pública e os operadores de infraestruturas críticas devem cumprir as medidas técnicas e organizativas adequadas e proporcionais, para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam.	S
15	Notificação de incidentes para a administração pública e operadores de infraestruturas críticas	Condições para a notificação.	S
16	Requisitos de segurança para os operadores de serviços essenciais	Os operadores de serviços essenciais devem cumprir as medidas técnicas e organizativas adequadas e proporcionais para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam.	S
17	Notificação de incidentes para os operadores de serviços essenciais	Condições para a notificação.	S

Art.º	Nome do artigo	Descrição	P/S
18	Requisitos de segurança para os prestadores de serviços digitais	Os prestadores de serviços digitais identificam e tomam as medidas técnicas e organizativas adequadas e proporcionais para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam, no contexto da oferta dos serviços digitais.	S
19	Notificação de incidentes para os prestadores de serviços digitais	Condições para a notificação.	S
20	Notificação voluntária de incidentes	Sem prejuízo da obrigação de notificação de incidentes prevista na presente lei, quaisquer entidades podem notificar, a título voluntário, os incidentes com impacto importante na continuidade dos serviços por si prestados.	S

A legislação é mais uma vez referente a requisitos de medidas técnicas e organizativas que as organizações têm de implementar. No entanto, é legítimo afirmar que não existe uma medida técnica ou organizacional específica que possa ser considerada, isoladamente, para se atingir esses objetivos. Terá sempre de se implementar um conjunto de medidas, para se poder alcançar um ou mais dos objetivos mencionados, que estarão relacionadas com a segurança da informação e com a cibersegurança. E aí, mais uma vez, os standards e *frameworks* terão uma preponderância na clarificação dos requisitos a implementar para garantir a conformidade e a gestão dos riscos pelas organizações.

A relação entre a NIS e o RGPD também suscita discussão. No entanto, cada quadro jurídico tem os seus próprios objetivos e propósitos e estabelece os seus próprios mecanismos para os alcançar. A sua perspetiva também difere, a cibersegurança, ao contrário da proteção de dados, não concede quaisquer direitos aos titulares dos dados, conforme referenciado na Tabela 3 (subcapítulo 5.1.1), mas ajudará na proteção dos mesmos (Markopoulou et al., 2019).

6 *Frameworks*/ Standards

Nesta seção será feita uma identificação de standards e *frameworks* relacionados com as temáticas da privacidade, segurança da informação e cibersegurança analisando, também, se os mesmos incorporam análises de risco e maturidade por requisito. O objetivo, mais uma vez, será o de estabelecer uma base de fundamentação sobre a necessidade da formalização da *framework* harmonizada.

6.1 Privacidade

Sobre o tema da privacidade existem várias *frameworks* e standards que podem ser utilizados pelas organizações para auxiliar na conformidade legal.

Ao nível das *frameworks*, podem ser utilizados a *Five Safes,* a NIST *privacy framework*, e a *Privacy Management Accountability Framework*.

A *framework Five Safes*, foi desenvolvido pelo *Office For National Statistics* do Reino Unido, para ajudar os investigadores e os académicos. No entanto, também é utilizado por entidades e organizações governamentais. O principal objetivo, é o de criar uma abordagem estruturada, para as organizações no que toca ao acesso e tratamento de dados pessoais, minimizando simultaneamente, os riscos para a privacidade (Ghorashi et al., 2023). Incorpora as cinco dimensões apresentadas na Tabela 8, que pretendem responder às seguintes questões:

TABELA 8 – ÂMBITO PREVISTO NA *FRAMEWORK FIVE SAFES*

Dimensões	Questões	Controlos
Projetos seguros	A utilização dos dados é a adequada?	Controlos de gestão
Pessoas seguras	É possível confiar nos investigadores para utilizarem os dados de forma adequada?	
Contexto seguro	A facilidade de acesso limita a utilização não autorizada aos dados?	
Dados seguros	Existe um risco de divulgação dos dados?	Controlos estatísticos
Outputs confiáveis	Os resultados estatísticos não são reveladores?	

Estas questões independentes, são utilizadas para se efetuar uma avaliação dos riscos no que se refere ao acesso aos dados e tratamento dos mesmos (Population Data BC, 2024) (ISACA, 2024c)

A NIST *Privacy Framework* (National Institute of Standards and Technology, 2020) foi desenvolvida pelo NIST, que é uma agência federal não reguladora estabelecida no Departamento de Comércio dos Estados Unidos da América. Tem por objetivos, trabalhar com a indústria e o meio académico para reforçar a segurança económica (Taherdoost, 2022). Esta *framework* é composta por três componentes, o *Core* (Núcleo), *Profile* (Perfis) e *Tiers* (Níveis de implementação) conforme apresentado na Figura 3 – Estrutura da Gestão de Risco da Privacidade:

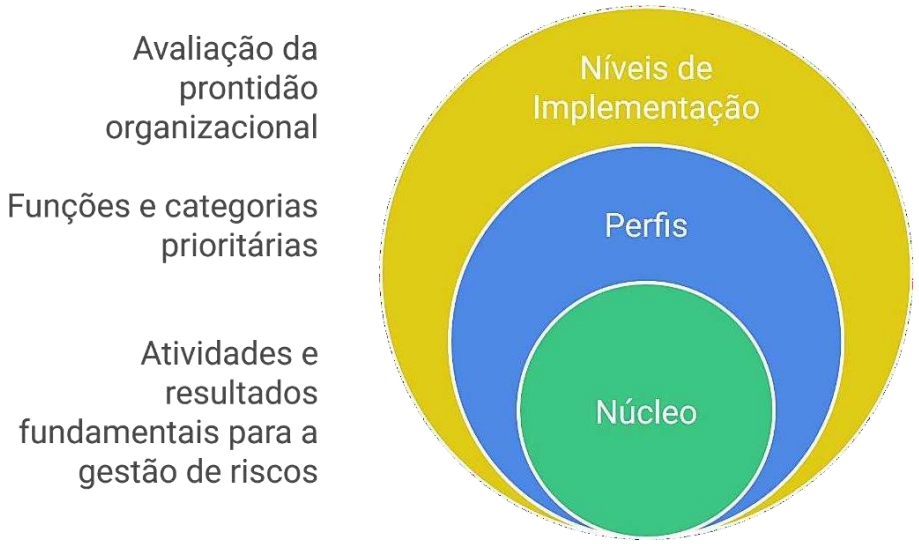

FIGURA 3 – ESTRUTURA DA GESTÃO DE RISCO DE PRIVACIDADE

Cada componente reforça a forma como as organizações podem gerir o risco de privacidade, através da ligação entre o negócio, a missão, as funções e responsabilidades organizacionais e as atividades desenvolvidas pelas organizações nesta matéria (National Institute of Standards and Technology, 2020).

O âmbito desta *framework* abrange um conjunto de preocupações de privacidade, incluindo a identificação, a governação e o controlo de riscos sobre a privacidade. Incorpora, cinco funções principais, Identificar, Governar, Controlar, Comunicar e Proteger, as quais se desagregam em categorias e subcategorias de requisitos (Ghorashi et al., 2023).

A *Privacy Management Accountability Framework* desenvolvida por via da investigação da Nymity's sobre privacidade (TrustArc, 2023), é composto por uma lista de mais de 130 atividades enquadradas em 13 categorias, e ajuda as organizações na gestão da privacidade.

Em termos de standards, a série das ISO 27000, publicadas pela *International Organization for Standardization* e pelo *International Electrotechnical Commission*, contempla as normas que se referem ao Sistema de Gestão de Segurança da Informação (SGSI). Para o tema da privacidade, existe a ISO/IEC 27701 de 2019, denominada por extensão da ISO/IEC 27001 e ISO/IEC 27002 para gestão da informação sobre privacidade (ISO/IEC, 2019). É uma extensão da norma ISO/IEC 27001 (Sistema de Gestão de Segurança da Informação) e ISO/IEC 27002 (Código de prática para controlos da segurança da informação), e tem como objetivo adicionar novos controlos ao sistema de gestão da informação, para auxiliar as organizações na gestão de riscos de privacidade. Incorpora um conjunto de requisitos específicos para organizações que tratam dados pessoais, na qualidade de Responsáveis pelo Tratamento e Subcontratantes (entidades que tratam dados pessoais em nome do Responsável do Tratamento). A sua implementação deve ser feita conjuntamente com a ISO/IEC 27001 (Laura et al., 2021) (Lachaud, 2020).

6.2 Segurança da Informação e Cibersegurança

Sobre os temas da segurança de informação e cibersegurança existem várias *frameworks* e standards, que podem ser utilizados pelas organizações, para auxiliar na conformidade (Taherdoost, 2022).

Ao nível das *frameworks* destacamos a *Control Objectives for Information Technologies* (COBIT) que foi desenvolvida pela ISACA. É uma estrutura para governança e gestão de tecnologias da informação (Taherdoost, 2022). A versão de 2019, inclui 2 áreas de atuação, 40 objetivos e 231 práticas (ISACA, 2024c).

Já o NIST desenvolveu a série SP800. Publicou, de entre outras, as seguintes *frameworks*:

- NIST *Cybersecurity Framework* (CSF), que contém 6 funções, 22 categorias e 107 subcategorias de procedimentos;
- NIST SP800-12, aborda os princípios fundamentais de cibersegurança;
- NIST SP 800-53, que se centra na privacidade e nos controlos dos sistemas de informação com o objetivo de proteger os ativos, as pessoas e as operações das organizações contra diferentes ciberameaças (Taherdoost, 2022).

Outras *frameworks* relevantes identificadas:

- *Security of personal data processing tool,* da *European Union Agency for Cybersecurity* (ENISA), que define controlos enquadrados em 20 tipologias (European Union Agency for Cybersecurity, 2020) para proteger a informação;
- CIS *Critical Security Controls* (V8 & V8.1) publicado pelo *Center for Internet Security*. Incorpora 153 controlos enquadrados em várias tipologias, de acordo com as especificidades dos mesmos (Center for Internet Security, 2024).

Ao nível de standards, existe a série das ISO 27000 (Taherdoost, 2022). São da responsabilidade do *International Organization for Standardization* e pela *International Electrotechnical Commission*, e estão relacionados com a manutenção de um Sistema de Gestão de Segurança da Informação (SGSI):

- ISO/IEC 27001, é uma norma reconhecida internacionalmente que determina os requisitos para implementar um Sistema de Gestão da Segurança da Informação certificado, cuja última versão é de 2022 (ISO/IEC, 2022a);
- A ISO/IEC 27002, determina um conjunto de controlos de segurança de informação que permitem a conformidade com os requisitos da ISO/IEC 27001, cuja última versão é de 2022 (ISO/IEC, 2022b);
- ISO/IEC 27005, determina orientações para a implementação baseada na gestão do risco de cibersegurança, cuja última versão é de 2022 (ISO/IEC, 2022c).

6.3 *Frameworks*/ standards – risco e maturidade por requisito

As *frameworks* e standards mencionadas em 6.1 e 6.2, por requisito, apresentam as seguintes caraterísticas ao nível da avaliação de maturidade e risco:

- A *framework Five Safes*, não incorpora por requisito, qualquer visão de risco ou maturidade;
- As normas ISO, não incorporam por requisito, qualquer visão de risco ou maturidade;
- O COBIT apresenta uma visão de maturidade por requisito;
- As NIST, incorporam por requisito uma visão de risco, mas não incluem o grau de maturidade (Almuhammadi & Alsaleh, 2017);
- A *Privacy Management Accountability Framework* não incorpora por requisito qualquer visão de risco ou maturidade;
- A *framework* da Enisa, não incorpora por requisito qualquer visão de risco ou maturidade;
- O CIS *controls*, incorpora por requisito, uma visão de risco, mas não inclui o grau de maturidade.

7 Desenho da *Framework*

Neste capítulo detalha-se a forma como a *framework* "*Harmonized privacy and information security framework, including maturity and risk exposure*" foi desenvolvida. A *framework* é constituída por 67 requisitos enquadrados em 8 Domínios e 20 Subdomínios.

A explicação acerca do desenvolvimento será feita em função dos elementos recursivos mencionados na Figura 4 – Sistematização do ciclo recursivo de gestão de requisitos, os quais serão detalhados nos próximos subcapítulos:

- Identificação de requisitos;
- Domínios e subdomínios;
- Requisitos – mapeamento com outras *frameworks* e standards;
- Avaliação de requisitos (detalha-se a forma como é feita a avaliação do risco, da conformidade e da maturidade por cada requisito).

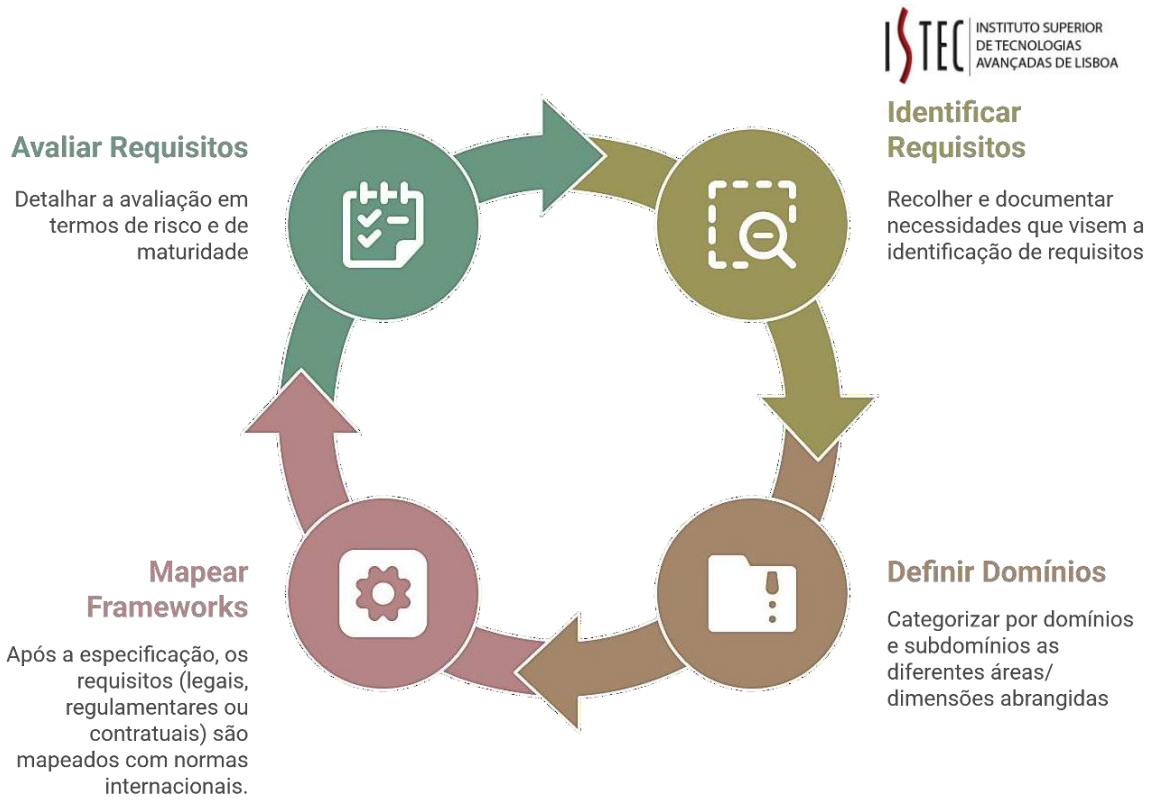

FIGURA 4 – SISTEMATIZAÇÃO DO CICLO RECURSIVO DE GESTÃO DE REQUISITOS

7.1 Identificação de Requisitos

Dos 67 requisitos que compõem a *framework*, 66 foram identificados através das seguintes fontes:

- Desmaterialização em requisitos dos artigos do RGPD;
- Desmaterialização em requisitos dos artigos da lei de Execução Nacional 58/2019, relativa à proteção das pessoas singulares, no que respeita ao tratamento de dados pessoais e à livre circulação desses dados;
- Desmaterialização em requisitos da *Nymity - Privacy Management Accountability Framework.*

Os requisitos com o ID (Identificador), T.IS.2 a T.IS.15 foram identificados através das fontes acima mencionadas, no entanto, a granularidade dos mesmos foi complementada com informação resultante da *framework* da ENISA, *Security of personal data processing tool.*

A identificação do requisito com o ID C.HR.1 não teve por base nenhuma das fontes acima mencionadas. Este, resulta da experiência profissional do autor da presente dissertação de mestrado na condução de avaliações de conformidade com o RGPD, em organizações diversas, desde o ano de 2018.

Os 67 requisitos que compõem a *framework* serão partilhados nas Tabelas seguintes, as quais também incluem uma visão das fontes de identificação, por cada requisito.

Na Tabela 9, requisitos entre o ID G.A.PS.1 a G.A.PS.7:

TABELA 9 – ÂMBITO DE REQUISITOS ENTRE O ID G.A.PS.1 AO G.A.PS.7

Req#ID	***Requirements***	**GDPR** ***article***	**PT** ***Law article***	**Nimyty** ***sections***	**Enisa** ***controls***
G.A.PS.1	*The organization should have a privacy strategy that addresses data value and related risks, combined with a thoughtful governance holistic approach that helps management to create a competitive advantage and build greater trust with stakeholders.*			1	
G.A.PS.2	*Roles and responsibilities related to the processing of personal data should be clearly defined and allocated in accordance with the security policy, namely DPO, Security Officer, and others.* *Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of personal data. For example, the roles of security officer, security auditor, and Data Protection Officer (DPO) should be kept separate to ensure proper oversight and accountability.*	27 38 39	8	1	B1 B5
G.A.PS.3	*The Data Protection Officer (DPO) is appointed and is independent, expert in data protection and related topics, adequately resourced, and reporting to the highest management level.*	37 38 39	9 11 12 13	1	
G.A.PS.4	*Clear appointment of persons in charge of specific security tasks should be performed, including the appointment of a security officer. The tasks and responsibilities of the security officer should also be set and documented.*	27 38	8	1	B3 B4
G.A.PS.5	*The governance bodies of the organization are involved in privacy & data protection issues (Board of Directors (BoD), Audit Committee (AC), Executive Committee (Exco), and Risk Committee).*	33 34		1	
G.A.PS.6	*The areas of the organization are involved in privacy & data protection issues (i.e. Information Security, Technology of Information (IT), Marketing, Human Resources (HR), Procurement, Complaints Management, Contacts Center (CC), Legal, Compliance, Risk Management, Operations, Sales, etc.)*	39		1	
G.A.PS.7	*The organization carries out periodic or regular reporting to the BoD, AC, Exco,*			1	

Req#ID	*Requirements*	GDPR *article*	PT *Law article*	Nimyty *sections*	Enisa *controls*
	Risk Management, and to regulators or other entities (if applicable) in privacy & data protection issues.				

Na Tabela 10 requisitos do ID G.B.PP.1 ao G.B.PP.2:

TABELA 10 – ÂMBITO DE REQUISITOS ENTRE O ID G.B.PP.1 AO G.B.PP.2

Req#ID	*Requirements*	GDPR *article*	PT *Law article*	Nimyty *sections*	Enisa *controls*
G.B.PP.1	*The organization should document separate and dedicated security and personal data policies, that should be reviewed and revised on an annual basis. Both policies should be approved by management and communicated to all employees and relevant external parties. The security policy should at least refer to the roles and responsibilities of personnel, the baseline technical and organization measures adopted for the security of personal data, and the data processors or other third parties involved in the processing of personal data. Subsequently, to support both policies across the organization, the following policies should also be formalized/covered:* *- Business Continuity Management and related regulations (i.e., Crisis Management, Disaster Recovery, Backups);* *- Acceptable Use of Assets;* *- Access Control Policy;* *- Change Management;* *- Cloud Computing (providers);* *- Other relevant topics for information security;* *- Code of Conduct/Ethics;* *- Vendor Selection/Procurement;* *- Incident Management;* *- Data Retention;* *- Complaints management;* *- Compliance (not mandatory for certain entities);* *- Material contacts with supervisory and control authorities (not mandatory for certain entities).*	5 24 28 32 91	15	3 4 6 7 9 11	A.1 A.2 A.3 A.4 A.6 C.2 E.3 H2
G.B.PP.2	*An inventory of specific policies/procedures related to the security of personal data should be*	5 24 28	15	4	A.5

Req#ID	*Requirements*	GDPR *article*	PT *Law article*	Nimyty *sections*	Enisa *controls*
	created and maintained, based on the general security policy.	32 91			

Quanto ao âmbito de requisitos previstos entre o ID C.HR.1 ao C.HR.10 (Tabela 11), conclui-se como aplicável o seguinte:

TABELA 11 – ÂMBITO DE REQUISITOS ENTRE O ID C.HR.1 AO C.HR.10

Req#ID	*Requirements*	GDPR *article*	PT *Law article*	Nimyty *sections*	Enisa *controls*
C.HR.1	*The organization should have a list/file that refers to all the staff working with the entity, FTEs, external (third parties), temporary, and trainees.*				
C.HR.2	*The organization in what concerns the recruitment process has:* *- A list/signed contracts with all recruitment agencies/entities that include an annex regulating the processing of personal data (Data Processing Agreement (DPA));* *- Information notices available in the channels for the submission of applications or spontaneous applications;* *- Activities of pre-screening of the candidates, before recruitment;* *- Legal deadlines defined for data retention from applications.*	13 14 28		4 6 7 8	
C.HR.3	*Related to employment contracts:* *- The organization should use templates of employment contracts (fixed term, uncertain, intern, temporary) that include information notices and consents for instance for benefits (i.e. for employee meal card or others, or related with the family like health insurance, kindergarten, and school supports, etc.) or other situations related with the use of personal data;* *- Employees involved in high-risk processing of personal data should be bound to specific confidentiality clauses (under their employment contract or other legal act).*	13 14	28 29	1 4 8	I3
C.HR.4	*The organization provides information notices in the process of collection data*	13 14		8	

Req#ID	***Requirements***	**GDPR** ***article***	**PT** ***Law article***	**Nimyty** ***sections***	**Enisa** ***controls***
	of employees and family for tax purposes.				
C.HR.5	*The organization should ensure that all employees understand their responsibilities and obligations related to the processing of personal data. Roles and responsibilities should be communicated during the pre-employment and/or induction process. Also, before starting their duties employees should be asked to review and agree on the organization security policy and sign respective confidentiality and non-disclosure agreements.*			1	I1 I2
C.HR.6	*Regarding the activities of HR that are externalized, the organization has a list/signed contract with all parties that include an annex regulating the processing of personal data (DPA). In particular for:* *- Payroll, training, control attendance, etc.;* *- Occupational Medicine;* *- Benefits provided (to staff: company car, meal card; to family: school support, kindergarten, health insurance, etc.).*	28		7	
C.HR.7	*During internal re-organizations or terminations and changes of employment, revocation of rights and responsibilities with respective handover procedures should be clearly defined.*			4	B2
C.HR.8	*The organization should have a process implemented to manage Data Subject Access Rights (DSAR) from employees.*	7 15 16 17 18 19 20 21 22	18 20	9	
C.HR.9	*The organization accommodates privacy & data protection thematics into health & safety practices.*			4	
C.HR.10	*The organization accommodates privacy & data protection thematics in the interactions with works councils and trade unions.*			4	

Na Tabela 12, requisitos compreendidos entre o ID D.TA.1 ao D.TA.4:

TABELA 12 – ÂMBITO DE REQUISITOS ENTRE O ID D.TA.1 AO D.TA.4

Req#ID	***Requirements***	**GDPR *article***	**PT *Law article***	**Nimyty *sections***	**Enisa *controls***
D.TA.1	*The organization should have a training plan on privacy & data protection revised on an annual basis and applied to all staff (FTEs, trainees, temporary, third parties, others).*	39		5	J3
D.TA.2	*The organization should have structured and regular training programs for staff, including specific programmers for the induction (to data protection matters) of newcomers.*	39		5	J2
D.TA.3	*The organization should ensure that all employees are adequately informed about the security controls of the IT system that relate to their everyday work. Employees involved in the processing of personal data should also be informed about relevant data protection requirements and legal obligations through regular awareness campaigns.*	39		5	J1
D.TA.4	*The organization has a privacy newsletter or incorporates privacy into existing corporate communications, and those communications are available in a repository (e.g. an internal data privacy intranet, yammer community, and others).*			5	

Quanto ao requisito com o ID F.PP.1 (Tabela 13):

TABELA 13 – ÂMBITO DO REQUISITO COM O ID F.PP.1

Req#ID	***Requirements***	**GDPR *article***	**PT *Law article***	**Nimyty *sections***	**Enisa *controls***
F.PP.1	*The organization should have a process implemented for "Crisis management" scenarios related to privacy & data protection defined and embedded in the organization through periodic simulacres exercises.*			11	

Nos termos do âmbito dos requisitos entre o ID G.PD.1 ao G.PD.2 (Tabela 14) é possível concluir:

TABELA 14 – ÂMBITO DE REQUISITOS ENTRE O ID G.PD.1 AO G.PD.2

Req#ID	***Requirements***	**GDPR *article***	**PT *Law article***	**Nimyty *sections***	**Enisa *controls***
G.PD.1	*The organization should have a process implemented for the management of the DPIAs (Data Protection Impact Assessment) related to:* *- New or changes in programs, systems, and processes;* *- Product development activities;* *- And, orientations issued from local*	5 6 25 35 36 39	7	2 10	

Req#ID	*Requirements*	GDPR *article*	PT *Law article*	Nimyty *sections*	Enisa *controls*
	authorities on the need for DPIA. The issues raised in the DPIA are further tested to guarantee the correct implementation.				
G.PD.2	*The organization has a process implemented for counseling activities on privacy & data protection issues.*	5 6 25 39			

Quanto aos requisitos entre o ID R.PA.1 ao R.PA.2 (Tabela 15):

TABELA 15 – ÂMBITO DE REQUISITOS ENTRE O ID R.PA.1 AO R.PA.2

Req#ID	*Requirements*	GDPR *article*	PT *Law article*	Nimyty *sections*	Enisa *controls*
R.PA.1	*The organization should regularly audit the internal compliance with the legal GDPR requirements and obligations.*	24 32 39		12	
R.PA.2	*The data controller's organization should regularly audit the compliance of the data processor to the agreed level of requirements and obligations.*	24 28 32 39		12	F4

Relativamente aos requisitos entre o ID H.RM.1 ao H.RM.3 (Tabela 16):

TABELA 16 – ÂMBITO DE REQUISITOS ENTRE O ID H.RM.1 AO H.RM.3

Req#ID	*Requirements*	GDPR *article*	PT *Law article*	Nimyty *sections*	Enisa *controls*
H.RM.1	*The organization should consider risks of privacy & data protection in the risk assessment process implemented. Should also report those risks in the risk reporting/dashboards of the organization.*	24 39		1 6 12	
H.RM.2	*The organization should have a practice of monitoring external situations (i.e. PESTLE approach - monitor the evolution of legislation, market practices, events occurred such as data breaches, cyber-attacks, other events, etc.) or internal situations (i.e. POTI approach - monitor situations related with the risk arising from DPIAs, health data processing or weaknesses in the Contact Center authentication process, other events) that leads to adjustments of the risk assessments/reports, especially in what concerns privacy & data protection risks.*	24 32 39		6 7 9 10 11 12 13	
H.RM.3	*The organization should have a process implemented to define and monitor the risk tolerance and risk appetite of privacy & data protection risks.*			1 6 12	

Especificamente quanto ao requisito com o ID E.RR.1 (Tabela 17):

TABELA 17 – ÂMBITO DO REQUISITO COM O ID E.RR.1

Req#ID	***Requirements***	**GDPR *article***	**PT *Law article***	**Nimyty *sections***	**Enisa *controls***
E.RR.1	*The organization should have a process implemented for the management of notifications from supervisory authorities, regulators, and other entities (i.e. European Centre for Digital Rights - NOIB) in matters of privacy & data protection.*			1 10 11	

Quanto ao âmbito de requisitos entre o ID J.DD.1 ao J.DD.3 (Tabela 18):

TABELA 18 – ÂMBITO DE REQUISITOS ENTRE O ID J.DD.1 AO J.DD.3

Req#ID	***Requirements***	**GDPR *article***	**PT *Law article***	**Nimyty *sections***	**Enisa *controls***
J.DD.1	*Formal guidelines and procedures covering the processing of personal data by data processors (contractors/outsourcing) should be defined, documented, and agreed upon between the data controller and the data processor (contract with DPA) before the commencement of the processing activities. These guidelines and procedures should mandatorily establish the same level of personal data security as mandated in the organization's security policy. The agreement should also set that:* *- The data processor should provide sufficient documented evidence of compliance;* *- The employees of the data processor who are processing personal data should be subject to specific documented confidentiality/ non-disclosure agreements;* *- Upon a personal data breach, the data processor shall notify the controller without undue delay.*	28 29 32		7	F1 F2 F3 F5
J.DD.2	*The organization should have a process implemented that imposes previous to the contracting of a third party, the realization of an evaluation which guarantees the accommodation by the third party (subcontractor) of the operational and technical measures required by art. º 32 of the GDPR.*	28		7	
J.DD.3	*The organization should have a database/list with all third parties that includes a reference when the third party*	28			

Req#ID	*Requirements*	GDPR *article*	PT *Law article*	Nimyty *sections*	Enisa *controls*
	is a subcontractor (an external entity that has access to personal data on behalf of the Controller).				

Quanto ao requisito com o ID M.CB.1 (Tabela 19):

TABELA 19 – ÂMBITO DO REQUISITO COM O ID M.CB.1

Req#ID	*Requirements*	GDPR *article*	PT *Law article*	Nimyty *sections*	Enisa *controls*
M.CB.1	*The organization should have adequate measures (i.e. standard contractual clauses, binding corporate rules, approvals from regulators, and derogations) to support all transfers of personal data outside the jurisdiction.*	45 46 47 48 49	22	2	

Já relativamente ao âmbito previsto nos requisitos compreendidos entre o ID K.CR.1 ao K.CR.2 (Tabela 20):

TABELA 20 – ÂMBITO DE REQUISITOS ENTRE O ID K.CR.1 AO K.CR.2

Req#ID	*Requirements*	GDPR *article*	PT *Law article*	Nimyty *sections*	Enisa *controls*
K.CR.1	*The organization should have a process implemented to manage DSARs from clients, third parties, and others.*	7 15 16 17 18 19 20 21 22	18 20	9	
K.CR.2	*The organization should have a process implemented to manage Complaints on privacy & data protection. The process should also accommodate:* *- A post-mortem analysis of the root causes of the complaints;* *- A periodic internal reporting on complaints to top management (i.e. Risk Management, Exco, AC, and B&D meetings).*			9	

Quanto aos requisitos entre o ID N.DC.1 ao N.DC.2 (Tabela 21):

TABELA 21 – ÂMBITO DE REQUISITOS ENTRE O ID N.DC.1 AO N.DC.2

Req#ID	*Requirements*	GDPR *article*	PT *Law article*	Nimyty *sections*	Enisa *controls*
N.DC.1	*The organization should have in all channels where personal data is collected, the information notices and consents on physical/digital documentation that supports the*	8 13 14 21		8	

Req#ID	*Requirements*	GDPR *article*	PT *Law article*	Nimyty *sections*	Enisa *controls*
	commercialization of the products, in the processes of creating users in websites/apps or in another type of forms or points of contacts available on websites/apps.				
N.DC.2	*The organization provides information notices in the:* *- IVR's (Interactive Voice Response) scripts of the Contacts Centers;* *- CCTV (Closed Circuit Television)/Video vigilance systems.*	13 14		8	

Os requisitos previstos entre o ID O.UD.1 ao O.UD.3 (Tabela 22) concluem-se como:

TABELA 22 – ÂMBITO DE REQUISITOS ENTRE O ID O.UD.1 AO O.UD.3

Req#ID	*Requirements*	GDPR *article*	PT *Law article*	Nimyty *sections*	Enisa *controls*
O.UD.1	*The organization should have identified the lawful basis used to support all the processes of personal data of the entity (basis: contractual relationship, consent, legitimate interest, legal obligation, vital interest, and public interest). In particular, the existence of a lawful basis for:* *- Marketing actions;* *- Use of cookies and tracking mechanisms;* *- Website/app contact forms;* *- Organization use of social media practices;* *- Use CCTV/Video vigilance;* *- Geo-location practices;* *- Employee monitoring / BYOD (Bring Your Own Device);* *- Automated decisions;* *- AI - Artificial Intelligence;* *- E-discovery practices;* *- Use of personal data in internal investigations;* *- Use of personal data in research practices;* *- Disclose to and for law enforcement;* *- Data used for website authentication;* *- Use of personal data from deceased natural persons;* *- Obtention of feedback (surveys or focus groups, etc.,)* *- others.*	6 7 8 9 10 12 17 19 21 22 25 26 27 31		4	

Req#ID	*Requirements*	GDPR *article*	PT *Law article*	Nimyty *sections*	Enisa *controls*
O.UD.2	*The organization should have identified the lawful basis used to support all the processes of personal data related to special categories (data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation).*	6 7 8 9 10 12 21	29	4	
O.UD.3	*The organization should analyze based on the legal environment, whether necessary prior to the processing of personal data related to minors, the collection of parental authorization, or others.*	6 7 8 12 21	16	4	

Quanto ao requisito com o ID P.MD.1 (Tabela 23):

TABELA 23 – ÂMBITO DO REQUISITO COM O P.MD.1

Req#ID	*Requirements*	GDPR *article*	PT *Law article*	Nimyty *sections*	Enisa *controls*
P.MD.1	*The organization has implemented means to detect and manage the secondary use of data (processed for a different purpose from the initial).*	6 13 14	23	4	

Especificamente, o requisito com o ID Q.RD.1 (Tabela 24):

TABELA 24 – ÂMBITO DO REQUISITO COM O Q.RD.1

Req#ID	*Requirements*	GDPR *article*	PT *Law article*	Nimyty *sections*	Enisa *controls*
Q.RD.1	*The organization should have implemented data retention procedures (including secure destruction of data) in logical (structured and unstructured) and physical data.*	5	21	4	

Quanto aos requisitos entre o ID S.DF.1 a S.DF.2 (Tabela 25):

TABELA 25 – ÂMBITO DE REQUISITOS ENTRE O ID S.DF.1 AO S.DF.2

Req#ID	*Requirements*	GDPR *article*	PT *Law article*	Nimyty *sections*	Enisa *controls*
S.DF.1	*The organization has records of processing activities according to art. º 30 of GDPR.*	30		2	
S.DF.2	*The organization should have available documents describing the flows of personal data between systems, processes (logical/physical), and countries.*	30 32		2	

Quanto ao requisito com o ID L.DC.1 (Tabela 26):

TABELA 26 – ÂMBITO DO REQUISITO COM O L.DC.1

Req#ID	***Requirements***	**GDPR *article***	**PT *Law article***	**Nimyty *sections***	**Enisa *controls***
L.DC.1	*The organization should have protection measures to classify the structured or unstructured personal data processed (i.e. personal, public, confidential, secret).*	32		2	

Considera-se relativamente aos requisitos previstos entre o ID I.BM.1 ao I.BM.4 (Tabela 27):

TABELA 27 – ÂMBITO DE REQUISITOS ENTRE O ID I.BM.1 AO I.BM.4

Req#ID	***Requirements***	**GDPR *article***	**PT *Law article***	**Nimyty *sections***	**Enisa *controls***
I.BM.1	*An incident response plan with detailed procedures should be defined to ensure effective and orderly response to incidents about personal data. The incident response plan should be documented, including a list of possible mitigation actions and a clear assignment of roles.*			11	G1 G3
I.BM.2	*Personal data breaches should be immediately reported to the management. Notification procedures for reporting breaches to competent authorities and data subjects should be in place, according to art. ºs 33 and 34 of the General Data Protection Regulation (GDPR).*	33 34		11	G2
I.BM.3	*Incidents and personal data breaches should be recorded along with details regarding the event and subsequent mitigation actions performed.*			11	G4
I.BM.4	*The organization, related to incident and breach management should promote:* *- A post-mortem analysis of the root causes of the incidents/breaches;* *- A periodic testing of the incident/breach plan;* *- A periodic internal reporting on incidents/breaches to top management (i.e. Risk Management, Exco, AC, and BoD meetings).*			11	

Quanto aos requisitos entre o ID T.IS.1 ao T.IS.15 (Tabela 28):

TABELA 28 – ÂMBITO DE REQUISITOS ENTRE O ID T.IS.1 AO T.IS.15

Req#ID	*Requirements*	GDPR *article*	PT *Law article*	Nimyty *sections*	Enisa *controls*
T.IS.1	*The organization should consider privacy risks in the security risk assessments.*	32		6	
T.IS.2	*The organization should have implemented the following measures related to resources and asset management:* *- The organization should have a register of the IT resources used to processing personal data (software and network). The register could include at least the following information:* *(i) IT resource;* *(ii) Type (e.g. server, workstation);* *(iii) Location (physical or electronic);* *(iv) Roles related, i.e. business data owner, system data owner, business manager, IT manager, data stewarts.* *- A specific person should be assigned with the task of maintaining and updating the register (e.g. IT officer), and the IT resources should be reviewed and updated at least on an annual basis.*	32	30	6	D1 D2 D3 D4
T.IS.3	*The organization should have implemented the following measures related to change management:* *- Software development should be performed in a special environment that is not connected to the IT system used to processing personal data. When testing is needed, dummy data should be used (not real data). In cases where this is not possible, specific procedures should be in place for the protection of personal data used in testing;* *- All the changes to the IT system are registered and monitored by a specific person (e.g. IT or security officer). Regular monitoring of this process should take place.*	32		4 6	E1 E2
T.IS.4	*The organization should have implemented the following measures related to access policy procedures:* *-Segregation of access control roles (e.g. access request, access authorization, access administration) should be clearly defined and documented;* *- Specific access control rights should be allocated to each role (involved in the processing of personal data) following the need-to-know principle;* *- Roles with excessive access rights*	32		6	C1 C3 C4

Req#ID	***Requirements***	**GDPR** ***article***	**PT** ***Law article***	**Nimyty** ***sections***	**Enisa** ***controls***
	should be clearly defined and assigned to limited specific members of staff.				
T.IS.5	*The organization should have implemented the following measures related to Business Continuity:* *- The organization should establish the main procedures and controls to be followed to ensure the required level of continuity and availability of the IT system processing personal data (in the event of an incident/personal data breach);* *- A BCP should be detailed and documented (following the general security policy). It should include clear actions and assignment of roles;* *- A level of guaranteed service quality should be defined in the BCP for the core business processes that provide for personal data security;* *- Specific personnel with the necessary responsibility, authority, and competence to manage business continuity in the event of an incident/personal data breach should be nominated;* *- An alternative facility should be considered, depending on the organization and the acceptable downtime of the IT system.*	32		6	H1 H2 H3 H4 H5
T.IS.6	*The organization should have implemented the following measures related to logging and monitoring:* *- Log files should be activated for each system/application used for the processing of personal data. They should include all types of access to data (view, modification, deletion);* *- Log files should be timestamped and adequately protected against tampering and unauthorized access. Clocks should be synchronized to a single reference time source;* *- Actions of the system administrators and system operators, including addition/deletion/change of user rights should be logged;*	32		6	L1 L2 L3 L4 L5

Req#ID	***Requirements***	**GDPR** ***article***	**PT** ***Law article***	**Nimyty** ***sections***	**Enisa** ***controls***
	- There should be no possibility of deletion or modification of log files content. Access to the log files should also be logged in addition to monitoring for detecting unusual activity; *- A monitoring system should process the log files and allow reports about the status of the system and notify for potential alerts.*				
T.IS.7	*The organization should have implemented the following measures related to access control and authentication:* *- An access control system applicable to all users accessing the IT system should be implemented. The system should allow creating, approving, reviewing, and deleting user accounts;* *- The use of common user accounts should be avoided. In cases where this is necessary, it should be ensured that all users of the common account have the same roles and responsibilities;* *- An authentication mechanism should be in place, allowing access to the IT system (based on the access control policy and system). As a minimum, a username/password combination should be used. Passwords should respect a certain (configurable) level of complexity;* *- The access control system should have the ability to detect and not allow the usage of passwords that don't respect a certain (configurable) level of complexity;* *- A specific password policy should be defined and documented. The policy should include at least password length, complexity, validity period, as well as number of acceptable unsuccessful login attempts.* *- User passwords must be stored in a "hashed" form;* *- Two-factor authentication should preferably be used for accessing systems that process personal data. The authentication factors could be passwords, security tokens, USB sticks with a secret token, biometrics etc.;* *- Device authentication should be used to guarantee that the processing of personal*	32		6	K1 K2 K3 K4 K5 K6 K7 K8

Req#ID	***Requirements***	**GDPR** ***article***	**PT** ***Law article***	**Nimyty** ***sections***	**Enisa** ***controls***
	data is performed only through specific resources in the network.				
T.IS.8	*The organization should have implemented the following measures related to server/database security:* *- Database and applications servers should be configured to run using a separate account, with minimum Operating System (OS) privileges to function correctly;* *- Database and applications servers should only process the personal data that are needed to achieve their processing purposes;* *- Encryption solutions should be considered on specific files or records through software or hardware implementation;* *- Encrypting storage drives should be considered;* *- Pseudonymization techniques should be applied through the separation of data from direct identifiers to avoid linking to the data subject without additional information;* *- Techniques supporting privacy at the database level, such as authorized queries, privacy preserving data base querying, searchable encryption, etc., should be considered.*	32 89	30	6	M1 M2 M3 M4 M5 M6
T.IS.9	*The organization should have implemented the following measures related to workstation security:* *- Users should not be able to deactivate or bypass security settings;*	32		6	N1 N2 N3 N4 N5

Req#ID	***Requirements***	**GDPR** ***article***	**PT** ***Law article***	**Nimyty** ***sections***	**Enisa** ***controls***
	- Anti-virus applications and detection signatures should be configured on a daily or at least weekly; *- Users should not have privileges to install or deactivate unauthorized software applications;* *- The system should have session time-outs when the user has not been active for a certain time;* *- Critical security updates released by the operating system developer should be installed regularly;* *- It should not be allowed to transfer personal data from workstations to external storage devices (e.g. USB, DVD, external hard drives);* *- Workstations used for the processing of personal data should preferably not be connected to the Internet unless security measures are in place to prevent unauthorized processing, copying and transfer of personal data on store;* *- Full disk encryption should be enabled on the workstation operating system drives.*				N6 N7 N8 N9
T.IS.10	*The organization should have implemented the following measures related to network/communication security:* *- Whenever access is performed through the Internet, communication should be encrypted through cryptographic protocols (TLS/SSL);* *- Wireless access to the IT system should be allowed only for specific users and processes. It should be protected by encryption mechanisms;* *- Remote access to the IT system should in general be avoided. In cases where this is necessary, it should be performed only under the control and monitoring of a specific person from the organization (e.g. IT administrator/security officer) through pre-defined devices;* *- Traffic to and from the IT system should be monitored and controlled through Firewalls and Intrusion Detection Systems;* *- Connection to the internet should not be allowed to servers and workstations used for the processing of personal data;* *- The network of the information system*	32		6	O1 O2 O3 O4 O5 O6 O7

Req#ID	***Requirements***	**GDPR** ***article***	**PT** ***Law article***	**Nimyty** ***sections***	**Enisa** ***controls***
	should be segregated from the other networks of the data controller; *- Access to the IT system should be performed only by pre-authorized devices and terminal using techniques such as MAC filtering or Network Access Control (NAC).*				
T.IS.11	*The organization should have implemented the following measures related to backups:* *- Backup and data restore procedures should be defined, documented, and linked to roles and responsibilities;* *- Backups should be given an appropriate level of physical and environmental protection consistent with the standards applied to the originating data;* *- Execution of backups should be monitored to ensure completeness;* *- Full backups should be carried out regularly;* *- Backup media should be regularly tested to ensure that they can be relied upon for emergency use;* *- Scheduled incremental backups should be carried out at least daily;* *- Copies of the backup should be securely stored in different locations;* *- In case a third party service for backup storage is used, the copy must be encrypted before being transmitted from the data controller;* *- Copies of backups should be encrypted and securely stored offline as well.*	32		6	P1 P2 P3 P4 P5 P6 P7 P8 P9

Req#ID	***Requirements***	**GDPR** ***article***	**PT** ***Law article***	**Nimyty** ***sections***	**Enisa** ***controls***
T.IS.12	*The organization should have implemented the following measures related to mobile/portable devices:* *- Mobile and portable device management procedures should be defined and documented establishing clear rules for their proper use;* *- Mobile devices that are allowed to access the information system should be pre-registered and preauthorized;* *- Mobile devices should be subject to the same levels of access control procedures (to the data processing system) as other terminal equipment;* *- Specific roles and responsibilities regarding mobile and portable device management should be clearly defined;* *- The organization should be able to remotely erase personal data (related to its processing operation) on a mobile device that has been compromised;* *- Mobile devices should support separation of private and business use of the device through secure software containers;* *- Mobile devices should be physically protected against theft when not in use;* *- Two factor authentication should be considered for accessing mobile devices;* *- Personal data stored at the mobile device (as part of the organization's data processing operation) should be encrypted.*	32		4 6	Q1 Q2 Q3 Q4 Q5 Q6 Q7 Q8 Q9
T.IS.13	*The organization should have implemented the following measures related to application lifecycle security:* *- During the development lifecycle best practices, state-of-the-art and well-acknowledged secure development practices, frameworks, or standards should be followed;* *- Specific security requirements should be defined during the early stages of the development lifecycle:* *- Specific technologies and techniques designed for supporting privacy and data protection (also referred to as PETs - Privacy Enhancing Technologies) should be adopted in analogy to the security requirements;* *- Secure coding standards and practices should be followed;*	32		4 6	R1 R2 R3 R4 R5 R6 R7 R8 R9

Req#ID	***Requirements***	**GDPR** ***article***	**PT** ***Law article***	**Nimyty** ***sections***	**Enisa** ***controls***
	- During the development, testing and validation against the implementation of the initial security requirements should be performed; *- Vulnerability assessment, application, and infrastructure penetration testing should be performed by a trusted third party before the operational adoption. The application shall not be adopted unless the required level of security is achieved;* *- Periodic penetration testing should be carried out;* *- Information about technical vulnerabilities of information systems being used should be obtained;* *- Software patches should be tested and evaluated before they are installed in an operational environment.*				
T.IS.14	*The organization should have implemented the following measures related to data deletion/disposal:* *- Software-based overwriting should be performed several times on all media before their disposal. In cases where this is not possible (CD's, DVD's, etc.) physical destruction should be performed:* *- Shredding of paper and portable media used to store personal data shall be carried out;* *- If a third party's services are used to securely dispose of media or paper-based records, a service agreement should be in place and a record of destruction of records should be produced as appropriate;* *- Following the software erasure, additional hardware based measures such as degaussing should be performed. Depending on the case, physical destruction should also be considered;* *- If a third party, therefore data processor, is being used for destruction of media or paper based files, it should be considered that the process takes place at the premises of the data controller (and avoid off-site transfer of personal data.*	32		6	S1 S2 S3 S4 S5 S6

Req#ID	***Requirements***	**GDPR** ***article***	**PT** ***Law article***	**Nimyty** ***sections***	**Enisa** ***controls***
T.IS.15	*The organization should have implemented the following measures related to physical security:* *- The physical perimeter of the IT system infrastructure should not be accessible by non-authorized personnel;* *- Clear identification, through appropriate means e.g. ID Badges, for all personnel and visitors accessing the premises of the organization should be established, as appropriate;* *- Secure zones should be defined and protected by appropriate entry controls. A physical log book or electronic audit trail of all access should be securely maintained and monitored;* *- Intruder detection systems should be installed in all security zones;* *- Physical barriers should, where applicable, be built to prevent unauthorized physical access;* *- Vacant secure areas should be physically locked and periodically reviewed;* *- An automatic fire suppression system, closed control dedicated air conditioning system, and uninterruptible power supply (UPS) should be implemented in the server room;* *- External party support service personnel should be granted restricted access to secure areas.*	32		6	T1 T2 T3 T4 T5 T6 T7 T8

7.2 Domínios e subdomínios

A definição, a descrição e o enquadramento dos Domínios e Subdomínios provém das especificidades dos requisitos identificados no capítulo anterior. Todos os requisitos identificados no subcapítulo 7.1 foram acomodados pelos seguintes Domínios e Subdomínios detalhados na Figura 5 – Domínios e Subdomínios da *Framework*:

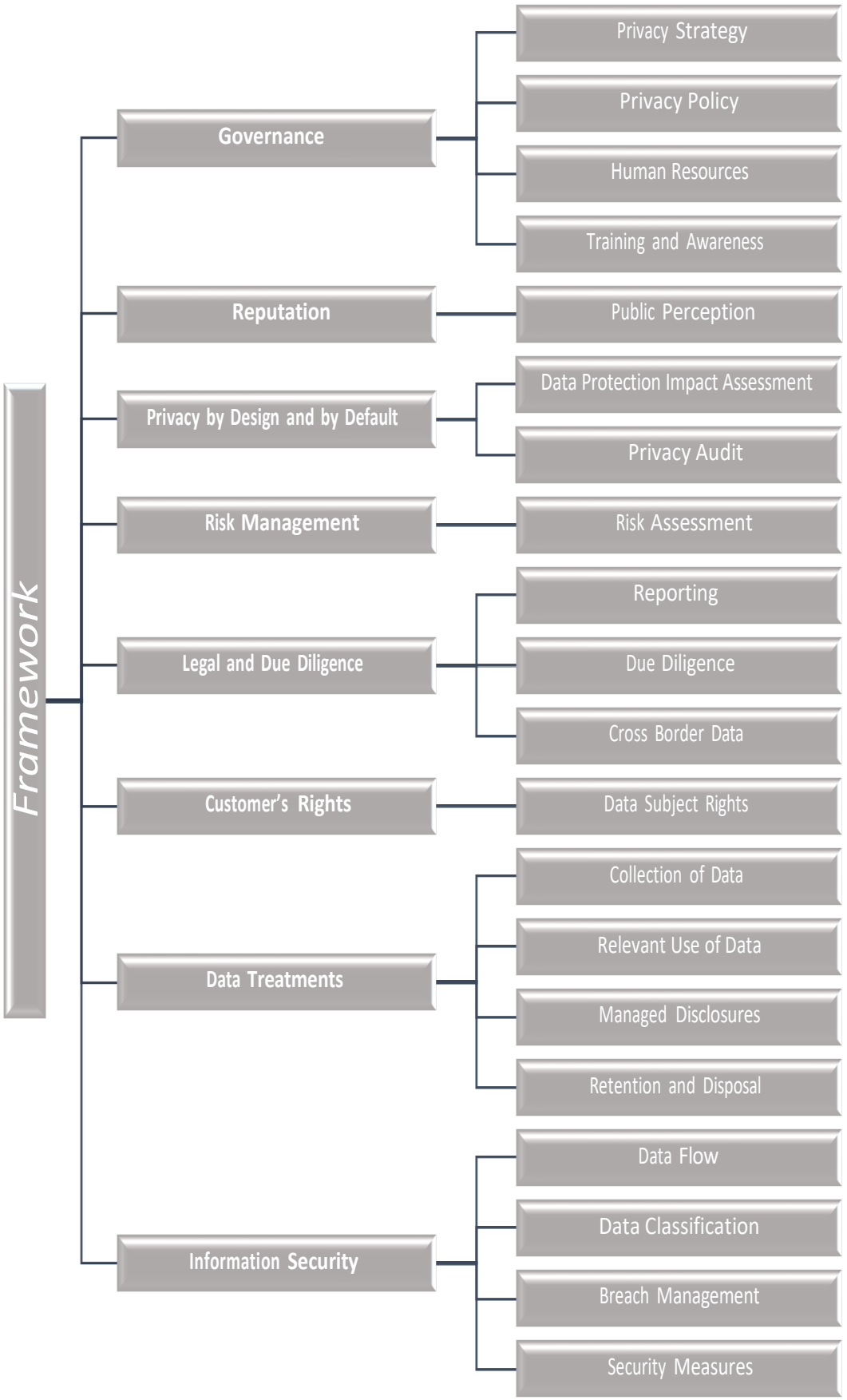

FIGURA 5 – DOMÍNIOS E SUBDOMÍNIOS DA *FRAMEWORK*

O Domínio *Governance* constituído por 4 Subdomínios endereça os seguintes temas e acomoda 23 Requisitos (Tabela 29):

TABELA 29 – DESCRIÇÃO DOMÍNIO *GOVERNANCE*

Subdomain	***Subdomain Description***	***Req#ID***
Privacy Strategy	*Focuses on the organization's privacy & data protection related goals and how they align with the organizational objectives to achieve strategic priorities.*	G.A.PS.1 G.A.PS.2 G.A.PS.3 G.A.PS.4 G.A.PS.5 G.A.PS.6 G.A.PS.7
Privacy Policy	*Focuses on control procedures and mechanisms to be implemented, to protect personal data within the scope of the company. This involves formal development, documentation, review, and approval of data protection standards and guidelines.*	*G.B.PP.1* *G.B.PP.2*
Human Resources	*Focuses on control mechanisms to be implemented to protect the employees' personal data. This involves formal development, documentation, review, and approval of data protection standards and guidelines.*	C.HR.1 C.HR.2 C.HR.3 C.HR.4 C.HR.5 C.HR.6 C.HR.7 C.HR.8 C.HR.9 C.HR.10
Training and Awareness	*Focuses on regular awareness programs that include privacy & data protection related themes defined aiming to up-skill all staff within an organization.*	D.TA.1 D.TA.2 D.TA.3 D.TA.4

O Domínio *Reputation* constituído por 1 Subdomínio endereça 1 Requisito (Tabela 30):

TABELA 30 – DESCRIÇÃO DOMÍNIO *REPUTATION*

Subdomain	***Subdomain Description***	***Req#ID***
Public Perception	*Explores how the organization handles issues in the event of a privacy incident/issue receiving media coverage.*	F.PP.1

O Domínio *Privacy by design and by default* constituído por 2 Subdomínios endereça os seguintes temas e acomoda 4 Requisitos (Tabela 31):

TABELA 31 – DESCRIÇÃO DOMÍNIO *PRIVACY BY DESIGN AND BY DEFAULT*

Subdomain	***Subdomain Description***	***Req#ID***
Data Protection Impact Assessment	*Explores whether the organization has required initiatives in place to complete a Data Protection Impact Assessment (DPIA) at the beginning of new or ongoing initiatives. Privacy by default ensures that only personal data that are necessary for each specific purpose of the processing are processed.*	G.PD.1 G.PD.2
Privacy Audit	*Explores whether the organization has a privacy audit in place. It is good practice for organizations to carry out regular monitoring and audits to identify areas of risk or potential non-compliance so that they can be managed and remediated appropriately.*	R.PA.2 R.PA.2

O Domínio *Risk Management* constituído por 1 Subdomínio, acomoda 3 Requisitos (Tabela 32):

TABELA 32 – DESCRIÇÃO DOMÍNIO *RISK MANAGEMENT*

Subdomain	***Subdomain Description***	***Req#ID***
Risk Assessment	*Assesses the organization's capability to mitigate and evaluate risks related to privacy & data protection. This includes assessing key controls in place to mitigate privacy risks within the organization.*	H.RM.1 H.RM.2 H.RM.3

O Domínio *Legal and Due Diligence* constituído por 3 Subdomínios endereça os seguintes temas e acomoda 5 Requisitos (Tabela 33):

TABELA 33 – DESCRIÇÃO DOMÍNIO *LEGAL AND DUE DILIGENCE*

Subdomain	***Subdomain Description***	***Req#ID***
Reporting	*Guarantees that reporting mechanisms must clearly define reporting channels and procedures that address data protection throughout the information lifecycle; from initial declaration, breach reporting, and remediation.*	E.RR.1
Due Diligence	*"Guarantees that data protection requirements are considered for contracts and obligations with third-party suppliers to safeguard personal data. Appropriate third-party reviews are required to monitor processes in place to ensure that each party's obligations are being duly carried out.*	J.DD.1 J.DD.2 J.DD.3
Cross Border Data	*Guarantees that appropriate transfer mechanisms are in place for personal data to be transferred outside the European Economic*	M.CB.1

Subdomain	*Subdomain Description*	*Req#ID*
	Area (EEA). This includes both intra-group and third-party transfers.	

O Domínio *Customer's Rights* constituído por 1 Subdomínio endereça 2 Requisito (Tabela 34):

TABELA 34 – DESCRIÇÃO DOMÍNIO *CUSTOMER'S RIGHTS*

Subdomain	*Subdomain Description*	*Req#ID*
Data Subject Rights	*Defines and implements procedures through which the organization can respect and comply with all data subject's rights. Analyzes the extent to which data protection complaints are effectively handled within the company.*	K.CR.1 K.CR.2

O Domínio *Data Treatments* constituído por 4 Subdomínios e acomoda 7 Requisitos (Tabela 35):

TABELA 35 – DESCRIÇÃO DOMÍNIO *DATA TREATMENTS*

Subdomain	*Subdomain Description*	*Req#ID*
Collection of Data	*Guarantees that at the point at which personal data is collected, the organization must provide the data subject with a purpose for collecting the data, how it will be used, and whether it will be shared with third parties or transferred outside the EEA.*	N.DC.1 N.DC.2
Relevant Use of Data	*Guarantees that the organization ensures that they use the data for the specified purposes and if they want to use it for other purposes, it must assess the compliance issues.*	*O.UD.1* *O.UD.2* *O.UD.3*
Managed Disclosures	*Guarantees that exists adequate procedures and mechanisms for the disclosure of personal data, ensuring its lawfulness and compliance with the GDPR.*	P.MD.1
Retention and Disposal	*Guarantees that personal data must not be retained longer than strictly necessary to fulfill its purposes. Adopt appropriate records management/data retention policies to ensure over-retention does not occur. When personal data is disposed of or deleted it must be done securely.*	*Q.RD.1*

O Domínio *Information Security* constituído por 4 Subdomínios endereça 22 Requisitos (Tabela 36):

TABELA 36 – DESCRIÇÃO DOMÍNIO *INFORMATION SECURITY*

Subdomain	***Subdomain Description***	***Req#ID***
Data Flow	*Focuses on processes associated with managing the entire lifecycle of personal information. This involves managing identity data and credentials, creating workflow processes for approval of account creation and modification, and the ability to audit and report user identity information.*	S.DF.1 S.DF.2
Data Classification	*Data classification is based on the level of sensitivity of personal information to set appropriate controls to safeguard personal data. This will be determined by the impact on the data of natural persons if their data would be lost, stolen, inappropriately disclosed, altered, or destroyed.*	*L.DC.1*
Breach Management	*Focuses on breach management process, in how the organization deals with a data breach using a clearly defined process to monitor, manage, remediate, and where appropriate report data breaches.*	I.BM.1 I.BM.2 I.BM.3 I.BM.4
Security Measures	*Focuses on controls applied to personal data flows across the organization and mechanisms to prevent the information from being accessed by others than the people who need to use the information for their daily activities.*	*T.IS.1* *T.IS.2* *T.IS.3* *T.IS.4* *T.IS.5* *T.IS.6* *T.IS.7* *T.IS.8* *T.IS.9* *T.IS.10* *T.IS.11* *T.IS.12* *T.IS.13* *T.IS.14* *T.IS.15*

7.3 Requisitos – mapeamento com outras *frameworks* e standards

Concluída a identificação e acomodação dos 67 requisitos que compõem a *framework*, procedeu-se ao mapeamento dos mesmos com requisitos de outras *frameworks* e standards sobre

privacidade, segurança de informação e cibersegurança. O processo de mapeamento teve os seguintes passos também descritos na Figura 6 – Processo de mapeamento e harmonização de requisitos (2º passo):

- 1º passo: mapeamento dos 67 requisitos da *framework* desenvolvida com os requisitos da NIST *Privacy framework* (2020) e da ISO/IEC 27001 e 27002 de 2022 (cláusulas 4 a 10 e controlos do anexo A);
- 2º passo: mapeamento entre a ISO/IEC 27001 e 27002 de 2022 (cláusulas 4 a 10 e controlos do anexo A) e a *framework* CIS *Controls*:

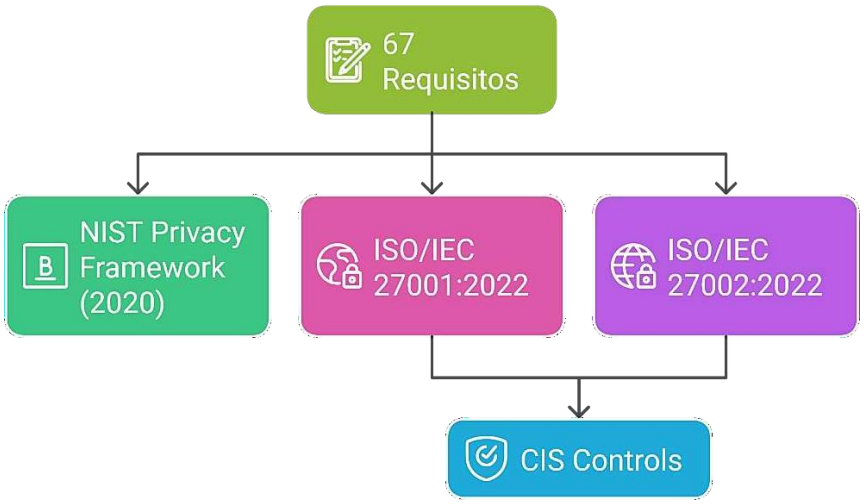

FIGURA 6 – PROCESSO DE MAPEAMENTO E HARMONIZAÇÃO DE REQUISITOS (2º PASSO)

Na Tabela 37 – *Framework* de resultados do mapeamento (2º passo) evidenciamos o total de requisitos da *framework* desenvolvida que têm correspondência com as *frameworks* e standards mencionadas na figura 6:

TABELA 37 – *FRAMEWORK* DE RESULTADO DO MAPEAMENTO (2º PASSO)

Nova *framework* total de requisitos com correspondência	***Frameworks*/standards**
62	NIST Privacy framework (2020)
60	ISO/IEC 27001:2022 & 27002:2022 Information Security Controls
54	CIS controls

No 3º passo realizado, efetuou-se o mapeamento entre os 54 requisitos da *framework* desenvolvida que tiveram correspondência com a *framework* CIS, com as seguintes *frameworks* e standards descritas na Figura 7 – Processo de mapeamento de requisitos por tipologia (3º passo):

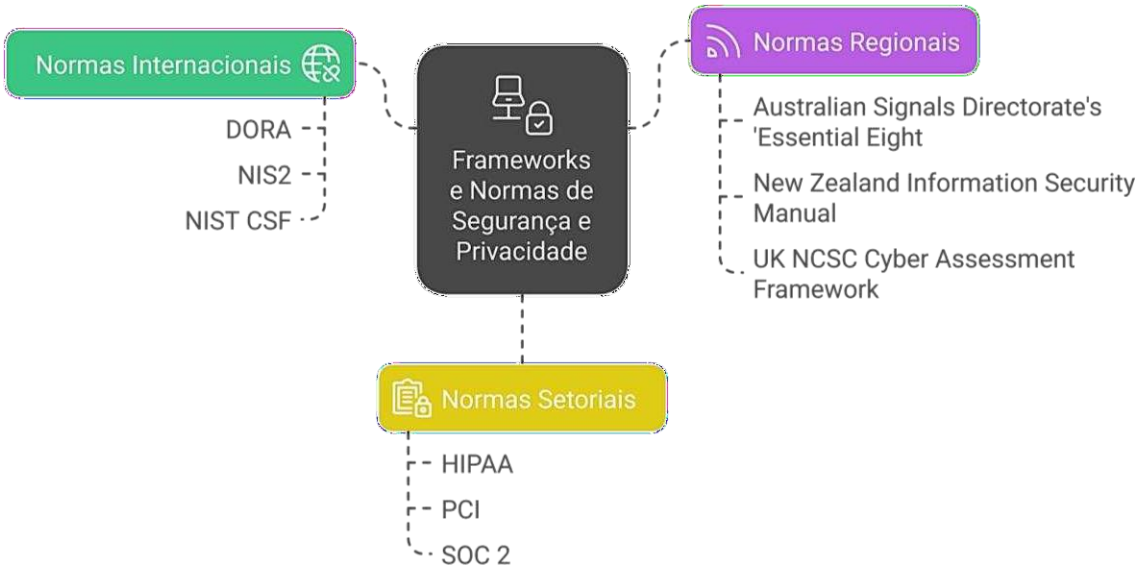

FIGURA 7 – PROCESSO DO MAPEAMENTO DE REQUISITOS POR TIPOLOGIA (3º PASSO)

Na Tabela 38 – *Framework* final harmonizada (3º passo), evidenciamos dos 54 requisitos da *framework* desenvolvida que tiveram correspondência com a *framework* CIS, o total dos que têm correspondência com as *frameworks* e standards mencionadas:

TABELA 38 – *FRAMEWORK* FINAL HARMONIZADA (3º PASSO)

Nova *framework* total de requisitos com correspondência	***Frameworks*/standards**
48	*Digital Operational and Resilience Act (DORA)*
52	*Network and Information Security Directive (NIS2)*
29	Australian Signals Directorate's 'Essential Eight'
53	Azure Security Benchmark v3
47	CISA Cross-Sector Cybersecurity Performance Goals
46	CISA Cybersecurity Performance Goals
53	CMMC v2.0
53	Criminal Justice Information Services (CJIS) Security Policy
53	CSA Cloud Controls Matrix v4
54	Cyber Risk Institute (CRI) Profile v1.2
54	Federal Financial Institutions Examination Council (FFIEC-CAT)
53	GSMA FS.31 Baseline Security Controls v2.0
52	HIPAA
52	ISACA COBIT 19
54	MITRE Enterprise ATT&CK v8.2
54	New Zealand Information Security Manual v3.5
54	NIST CSF
52	NIST SP 800-171
53	NIST SP 800-53 Revision 5 Low Baseline
53	NIST SP 800-53 Revision 5 Moderate Baseline
53	North American Electric Reliability Corporation-Critical Infrastructure Protection Standards (NERC-CIP Standards)

Nova *framework* total de requisitos com correspondência	*Frameworks*/standards
53	NYDFS Part 500
54	PCI v3.2.1
54	PCI v4.0
54	SOC 2
50	TSA Security Directive Pipeline-2021-02
53	UK NCSC Cyber Assessment Framework
40	UK NCSC Cyber Essentials v2.2

7.3.1 Abrangência

Na sequência do mapeamento efetuado no subcapítulo anterior, achamos também relevante partilhar o oposto, ou seja, o total dos requisitos das *frameworks* e standards mapeadas que tiveram correspondência com os requisitos da *framework* desenvolvida. No nosso entendimento, esta perspetiva materializa a abrangência e a utilidade que esta *framework* pode ter para a sociedade, para as organizações e para a própria academia nestas temáticas.

Selecionamos as seguintes *frameworks* e standards, sendo que no âmbito da:

- NIST *privacy framework* V1.0 de 2020 - é composta por 5 domínios, 18 subdomínios e 100 requisitos. Os 100 requisitos mapearam com 62 em 67 requisitos da *framework* desenvolvida;
- ISO/IEC 270001 e 27002 versões de 2022, o standard 27001 é composto pelas cláusulas 4 a 10 e o 27002 é composto por 4 tipologias de controlos, com um total de 93 controlos. Relativamente aos 93 controlos, 85 mapearam com 60 dos 67 requisitos da *framework* desenvolvida;
- CIS *controls*, a *framework* incorpora 153 controlos dos quais 129 mapearam com 54 em 67 requisitos da *framework* desenvolvida.

7.4 Avaliação dos requisitos

Adicionalmente, à questão do mapeamento dos requisitos, é também um objetivo para esta *framework*, que cada um dos 67 requisitos que a compõem possua indicadores de monitorização de risco, e/ou performance e/ou outros, disponíveis para os órgãos de gestão das organizações. E que sejam avaliados quanto aos níveis de conformidade e maturidade conforme espelhado nos títulos/ dimensão da Tabela 39 – Dimensão da avaliação dos requisitos por título das colunas:

TABELA 39 – DIMENSÃO DA AVALIAÇÃO DOS REQUISITOS POR TÍTULO DE COLUNAS

Req#ID	***Requirement***	***Indicators (KRI, KPI, ..)***	***Target (KRI, KPI, ..)***	***Formula to calculate***	***Compliat level***	***Maturity Level***

Neste subcapítulo constatar-se-á também o funcionamento da *framework* desenvolvida através dos exemplos apresentados em 7.4.1 a 7.4.3.

7.4.1 Indicadores

A forma como foi desenvolvida esta *framework*, sugere que sejam identificados por cada requisito, um, ou um conjunto de indicadores de monitorização que possam ser utilizados pelos órgãos de gestão das organizações de forma a garantir a prossecução dos objetivos corporativos e evitar riscos em matérias de privacidade, segurança de informação e cibersegurança.

TABELA 40 – AVALIAÇÃO DOS REQUISITOS POR INDICADOR E FÓRMULA DE CÁLCULO

Req#ID	***Requirement***	***Indicators (KRI, KPI,…)***	***Target (KRI, KPI..)***	***Formula to calculate***	***Compliant level***	***Maturity Level***

Para este efeito, 3 parâmetros têm de ser definidos por cada indicador conforme espelhado na Tabela 40–Avaliação dos requisitos por indicador e fórmula de cálculo, os quais são os seguintes:

- Definição do indicador (*Indicator's*);
- Os objetivos do indicador (*Target*);
- Fórmula de cálculo do indicador (*Formula to Calculate*).

No entanto, recomendamos que a tipologia e o objetivo do indicador fiquem à consideração de cada organização que possa vir a utilizar esta *framework*, uma vez que entendemos que esta decisão está relacionada com a maturidade da organização nestas temáticas, bem como com o nível de exposição ao risco que a organização pretende incorrer. Não obstante, a *framework* disponibilizará pelo menos um indicador por cada requisito, que por opção do autor será um *Key Risk Indicators* (KRI's).

Ao nível das tipologias de indicadores sugerimos que sejam utilizados KRI's ou *Key Perfomance Indicator* (KPI's), no entanto outros tipos de indicadores podem ser utilizados como os *Key Goal Indicators* (KGI's), ou outros.

Com o objetivo de clarificação fundamentamos os conceitos de KRI's e KPI's com base em publicações científicas:

- KPI's são fontes de informação baseadas em dados históricos, pelo que não são apropriados para a avaliação de riscos futuros. Em contrapartida, os KRI's partem da premissa de uma visão futura do risco, e as métricas são desenvolvidas para dar suporte às atividades de gestão de risco (Beasley et al., 2010);
- Os KPI's são ferramentas essenciais para medir a eficiência e a eficácia de uma organização na prossecução dos seus objetivos estratégicos. Estes indicadores fornecem uma visão do desempenho organizacional e ajudam a identificar as áreas que precisam de ser melhoradas. Por outro lado, os KRI's são utilizados para identificar e monitorizar os riscos que podem ter um impacto negativo no desempenho organizacional. Estes

indicadores fornecem sinais de alerta precoce, permitindo que as organizações tomem medidas preventivas para gerir os riscos, antes de estes se tornarem problemas importantes (Ionescu et al., 2024).

De seguida, apresentamos de forma não exaustiva, exemplos de KRI's que o autor da dissertação identificou para três diferentes requisitos. O primeiro caso, na Tabela 41, refere-se ao requisito com o ID G.A.PS.3, do Domínio *Governance*, em que se identificou o KRI, *"% of legal entities entitled with a required DPO appointed*":

TABELA 41 – KRI, REQUISITO ID G.A.PS.3

Req#ID	***Requirement***	***Indicators (KRI, KPI,…)***	***Target (KRI, KPI..)***	***Formula to calculate***	***Compliant level***	***Maturity Level***
G.A.PS.3	*The Data Protection Officer (DPO) is appointed and is an independent, expert in data protection and related topics, adequately resourced, and reporting to the highest management level.*	*'% of legal entities entitled with a required DPO appointed*	*X%*	*[#legal entities with DPO/#total number of legal entities requiring a DPO] * 100*	*Not Compliant*	*Managed and Preliminary*

O segundo caso, na Tabela 42, refere-se ao requisito com o ID O.UD.3, do Domínio *Data Treatment*, em que se identificou o KRI, *"% Parental authorization rate*":

TABELA 42 – KRI, REQUISITO ID O.UD.3

Req#ID	***Requirement***	***Indicators (KRI, KPI,…)***	***Target (KRI, KPI..)***	***Formula to calculate***	***Compliant level***	***Maturity Level***
O.UD.3	*The organization should analyze based on the legal environment, whether necessary prior to the processing of personal data related to minors, the collection of parental authorization, or others.*	*% Parental authorization rate*	*X%*	*[# of data processing with valid authorization/# Total number of data processing related to minor's] * 100*	*Not Compliant*	*Managed and Preliminary*

O terceiro caso, na Tabela 43, refere-se ao requisito com o ID I.BM.4, do Domínio *Information Security*, em que se identificou os seguintes KRI's:

- *"Post Mortem analysis completion rate";*
- *"Incident response plan testing frequency";*
- *"Timeliness and Frequency of incidents/data breaches reported to top management".*

TABELA 43 – KRI, REQUISITO ID G.A.PS.3

Req#ID	***Requirement***	***Indicators (KRI, KPI,…)***	***Target (KRI, KPI..)***	***Formula to calculate***	***Compliant level***	***Maturity Level***
I.BM.4	*The organization, related to incident and breach management should promote: - A post-mortem analysis of the root causes of the incidents/breaches; - A periodic testing of the incident/breach plan; - A periodic internal reporting on incidents/breaches to top management (i.e. Risk Management, Exco, AC, and BoD meetings.*	*- Post Mortem analysis completion rate - Incident response plan testing frequency - Timeliness and Frequency of incidents/data breaches reported to top management*	*- X% - quarterly - X%*	*- [total of incidents/data breaches with completed post-mortem analysis/#total of incidents/data breaches detected] * 100 - Frequency of incident response plan testing (quarterly, bi-annual, etc.) - [total of incidents/data breaches reported to top management/total of incidents/data breaches detected] * 100*	*Not Compliant*	*Managed and Preliminary*

Reforçando novamente a ideia de que a escolha do indicador ou indicadores a utilizar por requisito nas organizações que adotarem a *framework* deverá ser baseada em função de vários pressupostos. Por exemplo, os objetivos da organização, o sector de atividade onde se insere, a legislação existente que impacta o sector, o grau de maturidade em matérias de privacidade, segurança de informação e cibersegurança, o apetite ao risco que pretende incorrer, de entre outros pressupostos.

7.4.2 Conformidade (*Compliant level*)

A avaliação do nível de conformidade por cada requisito será baseada num modelo que dispõe de quatro estágios diferentes:

- *Not Applicable;*
- *Not Compliant;*

- *Partial Compliant;*
- *Totally Compliant.*

A descrição dos atributos relativos aos níveis de conformidade é detalhada na Tabela 44 – Descrição dos atributos do nível de conformidade, e destina-se a suportar as decisões de classificação por cada requisito:

TABELA 44 – DESCRIÇÃO DOS ATRIBUTOS DO NÍVEL DE CONFORMIDADE

Compliant attributes		
Level	***Description***	***Key Attributes***
0	***Not Applicable***	*The requirement is not applicable.*
1	***Not Compliant***	*The management of risk is undocumented, in flux, and depends on individual improvised practices, ad hoc, and often chaotic.*
2	***Partial Compliant***	*Risk is defined in different ways and managed in silos. Process discipline is unlikely to be rigorous. Practices are defined and managed, though sometimes informally.*
3	***Totally Compliant***	*A common risk assessment/response framework is in place. An organization-wide view of risk is provided to executive leadership and the board in the form of a list of 'top' risks. Action plans are implemented in response to high-priority risks. Practices are formally documented and consistently managed.*

Na Tabela 45 – Avaliação do nível de conformidade, partilhamos um exemplo da aplicação prática dos níveis para um requisito:

TABELA 45 – AVALIAÇÃO DO NÍVEL DE CONFORMIDADE

Req#ID	***Requirement***	***Indicators (KRI, KPI,…)***	***Target (KRI, KPI..)***	***Formula to calculate***	***Compliant level***	***Maturity Level***
G.A.PS.3	*The Data Protection Officer (DPO) is appointed and is independent, expert in data protection and related topics, adequately resourced, and reporting to the highest management level.*	*'% of legal entities entitled with a required DPO appointed*	*X%*	*[#legal entities with DPO/#total number of legal entities requiring a DPO] * 100*	*Not Compliant*	*Managed and Preliminary*

7.4.3 Maturidade (*Maturiy Level*)

Existem vários modelos de maturidade que podem ser utilizados pelas organizações como por exemplo OPM3, P6CMM, CMMI, OPMMM, TMM, P3M3, SPICE, BPMM, FAAiCMM, (PM)2, Kerzner's *Project Management Maturity Model*, Ibbs e Kwak *Maturity Model,* RMMM, TMM, etc. Os modelos de maturidade são usados na melhoria do desempenho organizacional. Os modelos de maturidade podem ser utilizados para identificar os pontos fortes e fracos da organização, para além de fornecerem informações para *benchmarking* (Khoshgoftar & Osman, 2008).

Para a *framework* desenvolvida, dos modelos acima mencionados selecionamos o *Capability Maturity Model Integration* (CMMI), um modelo desenvolvido pela *Software Engineering Institute* (SEI) que é, atualmente, gerido pela CMMI *Institute*, uma organização pertencente à ISACA (Khoshgoftar & Osman, 2008)(ISACA, 2024a).

O CMMI é um modelo que promove uma cultura de melhoria contínua que incorpora dois níveis de avaliação. Um sobre capacidade (*capability*), e um outro sobre maturidade (*maturity*). No entanto, centraremos a análise apenas no nível da avaliação de maturidade (ISACA, 2024a) (Margarido et al., 2012).

A avaliação da maturidade do CMMI comporta 6 níveis, conforme descrito na Tabela 46:

TABELA 46 - CMMI NÍVEL DE AVALIAÇÃO DE MATURIDADE

Maturity		
Level	***Description***	***Key Attributes***
0	***Incomplete***	*Ad hoc and unknown. Work may or may not get completed.*
1	***Initial***	*Unpredictable and reactive. Work gets completed but is often delayed and over budget*
2	***Managed***	*Managed on the project level. Projects are planned, performed, measured, and controlled.*
3	***Defined***	*Proactive, rather than reactive. Organization-wide standards provide guidance across projects, programs, and portfolios*
4	***Quantitatively Managed***	*Measured and controlled. Organization is data-driven with quantitative performance improvement objectives that are predictable and align to meet the needs of internal and external stakeholders.*
5	***Optimizing***	*Stable and flexible. Organization is focused on continuous improvement and is built to pivot and respond to opportunity and change. The organization's stability provides a platform for agility and innovation.*

Para a *framework* desenvolvida, escolhemos um modelo de avaliação do nível de maturidade de cada requisito semelhante ao do CMMI. Dispõe de seis diferentes estágios:

- *Not Applicable;*
- *Initial/Ad-hoc;*
- *Managed and Preliminary;*
- *Consistent and Defined;*
- *Integrated and Measured;*
- *Optimized.*

A descrição dos atributos é detalhada na Tabela 47 – Descrição dos atributos do nível de maturidade e destinam-se a suportar a classificação por cada requisito:

TABELA 47 – DESCRIÇÃO DOS ATRIBUTOS DO NÍVEL DE MATURIDADE

Maturity		
Level	***Description***	***Key Attributes***
0	***Not Applicable***	*The requirement is not applicable.*
1	***Initial/Ad-hoc***	*The management of risk is undocumented, in flux, and depends on individual improvised practices, ad hoc, and often chaotic.*
2	***Managed and Preliminary***	*Risk is defined in different ways and managed in silos. Process discipline is unlikely to be rigorous. Practices are defined and managed, though sometimes informally.*
3	***Consistent and Defined***	*A common risk assessment/response framework is in place. An organization-wide view of risk is provided to executive leadership and the board in the form of a list of 'top' risks. Action plans are implemented in response to high-priority risks. Practices are formally documented and consistently managed.*
4	***Integrated and Measured***	*Activities are coordinated across business areas. Common risk management tools and processes are used where appropriate, with enterprise-wide risk monitoring, measurement, and reporting. Alternative responses are analyzed with scenario planning and other techniques, such as Monte Carlo simulation. Process metrics are in place. But the emphasis remains on managing a list of risks. Discussion of risk at executive committee and board levels is separate from the discussion of strategy and performance. Practices are measured and managed with data-driven evidence.*
5	***Optimized***	*The focus shifts from managing a list of risks outside the context of enterprise objectives to managing for the successful achievement of objectives. The consideration of what might happen is embedded in*

Maturity		
Level	***Description***	***Key Attributes***
		strategic planning, capital allocation, and other processes, as well as in daily strategic and tactical decision-making. There is a reasonable level of assurance that decision-makers are taking the right level of the right risks necessary for success and not just to avoid failure. Early-warning systems exist to notify board and management both of specific risks above established risk appetite or risk-capacity thresholds – and where the likelihood of achieving enterprise objectives is less than acceptable. Reporting to management and the board integrates performance reporting (where we are now) and risk (what might happen) to project the likelihood of achieving each enterprise objective. Discussion of risk at top management and board levels (what might happen) is not separate from the discussion of strategy and performance. Practices are consistently improved over time.

Na Tabela 48 – Avaliação do nível de maturidade, partilhamos um exemplo da aplicação prática dos níveis para um requisito:

TABELA 48 – AVALIAÇÃO DO NÍVEL DE MATURIDADE

Req#ID	***Requirement***	***Indicators (KRI, KPI,…)***	***Target (KRI, KPI..)***	***Formula to calculate***	***Compliant level***	***Maturity Level***
G.A.PS.3	*The Data Protection Officer (DPO) is appointed and is independent, expert in data protection and related topics, adequately resourced, and reporting to the highest management level.*	*'% of legal entities entitled with a required DPO appointed*	*X%*	*[#legal entities with DPO/#total number of legal entities requiring a DPO] * 100*	*Not Compliant*	*Managed and Preliminary*

TABELA 48 – AVALIAÇÃO DO NÍVEL DE MATURIDADE

8 Conclusão

A densificação de obrigações legais em matérias como a privacidade, a segurança da informação e a cibersegurança, é uma realidade que não se espera que abrande nos anos

vindouros. Mediante esta conjuntura, as organizações vão enfrentar dificuldades acrescidas na gestão de riscos e dos seus recursos.

É igualmente verdade, que existem várias *frameworks* ou standards sobre estes temas que podem ser usadas pelas organizações. Por exemplo, a NIST *Privacy framework* no âmbito da privacidade. No âmbito da segurança de informação, as ISO/IEC 27001 e 27002 que teremos de complementar com a ISO/IEC 27701 se quisermos endereçar questões de privacidade. Ao nível da cibersegurança, a NIST *cybersecurity framework* ou a CIS *framework*, de entre outras.

Pelo exposto, defendemos que a relevância desta *framework* harmonizada de privacidade, segurança de informação e cibersegurança assenta na forma como foram identificados os seus requisitos, usando fontes como o RGPD e as *frameworks* Nymity e ENISA.

Com esta orientação, asseguramos o conceito da privacidade muito para além do entendimento generalizado, de que a privacidade consiste apenas em proteger os dados pessoais. No âmbito da privacidade, com o RGPD, as organizações têm a obrigação de proteger os dados pessoais, mas, cumulativamente, também têm de ter um fundamento legal e cumprir com um conjunto de obrigações legais não relacionadas com a segurança da informação e a cibersegurança, que se encontram espelhadas nos requisitos da *framework*.

Na perspetiva da proteção dos dados pessoais, em termos da segurança da informação e cibersegurança, com o objetivo de obter granularidade em termos dos requisitos, utilizamos as *frameworks* da Nymity e da ENISA para atingir rigor e robustez ao nível dos mesmos.

E ainda, para cada requisito da *framework* partilhámos indicadores para o seu seguimento, uma visão de conformidade e ainda um nível de maturidade, que a maioria de outras *frameworks* e standards não acomoda na sua plenitude.

Procedemos igualmente ao mapeamento dos requisitos da *framework* com requisitos de outros standards e *frameworks*.

Por estes pressupostos, é nossa convicção que conseguimos desenvolver uma *framework* harmonizada de requisitos sobre estas temáticas assente numa única ferramenta, que poderá ajudar as organizações na gestão dos seus recursos e dos seus riscos nestas matérias.

8.1 *Framework* – potenciais melhorias

Existem variadíssimas *frameworks* e standards em múltiplas matérias, no entanto subsistem ainda oportunidades significativas de investigação com o objetivo de continuar a dotar e a ajudar a sociedade e as organizações no aumento da eficiência e da eficácia na gestão das temáticas de privacidade, segurança de informação e cibersegurança.

Como potenciais áreas de enriquecimento da *framework* identificamos as seguintes:

- Estabelecimento de critérios que ajudem a identificar quais requisitos da *framework* devem ser prioritários em termos de implementação. Esta abordagem poderá passar pelo desenvolvimento de uma matriz de impacto regulatório, pela definição do custo-benefício da implementação de cada requisito ou por dependências lógicas entre requisitos. No entanto, outras abordagens são igualmente válidas, como o desenvolvimento de um *Toolkit* ou a definição de um *Roadmap* para auxiliar na implementação.
- Acomodação de requisitos decorrentes de obrigações legais não consideradas, entretanto atualizadas ou que venham a surgir (e.g. AI act, etc.);
- Mapeamento dos requisitos com outras *frameworks* ou standards não considerados;
- Exploração do conceito de "*risk tolerance*" e "*risk capacity*";
- A ligação do modelo "MITRE *Enterprise* ATT&CK" v8.2 inserido na *framework* com a base de dados de *Common Vulnerabilities and Exposures* (CVE).

9 Bibliografia

Almuhammadi, S., & Alsaleh, M. (2017). *Information Security Maturity Model for Nist Cyber Security Framework*. 51–62. https://doi.org/10.5121/csit.2017.70305

Arfelt, E., Basin, D., & Debois, S. (2019). *Monitoring the GDPR. In: European Symposium on Research in Computer Security. Cham: Springer International Publishing*, 2019. p. 681-699.

Assembleia da República. (2018). *Lei 46/2018 - Estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União*.

Assembleia da República. (2019). *Lei n.º 58/2019 - Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*.

Ayala-Rivera, V., & Lero@ucd, L. P. (2018). *"The Grace Period Has Ended": An Approach to Operationalize GDPR Requirements*.

Beasley, M. S., Branson, B. C., & Hancock, B. V. (2010). *"Developing Key Risk Indicators to Strengthen Enterprise Risk Management."*

Becker, J., Niehaves, B., Poeppelbuss, J., Simons, A., Becker, J. ;, Niehaves, B. ;, & Poeppelbuss, J. ; (2010). *Maturity Models in IS Research*. http://aisel.aisnet.org/ecis2010/42

Center for Internet Security. (2024). *CIS Critical Security Controls*. https://www.cisecurity.org/controls

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). *Technology Innovation Management Review Defining Cybersecurity*. www.timreview.ca

De Castro, E. T. V., Silva, G. R. S., & Canedo, E. D. (2022). Ensuring privacy in the application of the Brazilian general data protection law (LGPD). *Proceedings of the ACM Symposium on Applied Computing*, 1228–1235. https://doi.org/10.1145/3477314.3507023

Deng, Q., & Ji, S. (2018). A Review of Design Science Research in Information Systems: Concept, Process, Outcome, and Evaluation. *Pacific Asia Journal of the Association for Information Systems*, 1–36. https://doi.org/10.17705/1pais.10101

European Union Agency for Cybersecurity. (2020). *On-line tool for the security of personal data processing*. https://www.enisa.europa.eu/risk-level-tool

Ghorashi, S. R., Zia, T., Bewong, M., & Jiang, Y. (2023). An Analytical Review of Industrial Privacy Frameworks and Regulations for Organizational Data Sharing. *Applied Sciences*, *13*(23), 12727. https://doi.org/10.3390/app132312727

Huth, D., & Matthes, F. (2019). *Privacy Engineering Approaches for GDPR Requirements "Appropriate Technical and Organizational Measures": Identifying Privacy Engineering Approaches to Meet GDPR Requirements Completed Research*.

International Association of Privacy Professionals (IAPP). (2024). *Definition of Privacy*. https://iapp.org/about/what-is-privacy/

Ionescu, Ștefan, Dumitrescu, G., Ioanăș, C., & Delcea, C. (2024). Mapping the Landscape of Key Performance and Key Risk Indicators in Business: A Comprehensive Bibliometric Analysis. *Risks*, *12*(8). https://doi.org/10.3390/risks12080125

ISACA. (2024a). *CMMI Institute - CMMI Levels of Capability and Performance*. https://cmmiinstitute.com/learning/appraisals/levels

ISACA. (2024b). *CMMI: What is the purpose of a maturity level?* https://support.isaca.org/s/article/What-is-the-purpose-of-a-maturity-level-1598331747435

ISACA. (2024c). *COBIT | Control Objectives for Information Technologies*. https://www.isaca.org/resources/cobit#1

ISO/IEC. (2018). *ISO 31000:2018(en), Risk management — Guidelines*. https://www.iso.org/obp/ui/en/#iso:std:iso:31000:ed-2:v1:en

ISO/IEC. (2019). *ISO/IEC 27701 - Security Techniques-Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management -Requirements and guidelines*. www.iso.org

ISO/IEC. (2022a). *ISO/IEC 27001 - Information security, cybersecurity and privacy protection-Information security management systems-Requirements*.

ISO/IEC. (2022b). *ISO/IEC 27002 - Information security, cybersecurity and privacy protection-Information security controls*.

ISO/IEC. (2022c). *ISO/IEC 27005 - Information security, cybersecurity and privacy protection-Guidance on managing information security risks*.

Khoshgoftar, M., & Osman, O. (2008). *Comparison of Maturity Models*.

Lachaud, E. (2020). ISO/IEC 27701 - Threats and Opportunities for GDPR Certification. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3521250

Laura, A., Diniz, B., & Pelicano Diniz, D. (2021). *A ABNT NBR ISO/IEC 27701:2019 E A SEGURANÇA DA INFORMAÇÃO*.

Lukács, A. (2016.). *What is privacy? The history and definition of privacy*.

Margarido, I. L., Vidal, R. M., & Vieira, M. (2012). Lessons learnt in the implementation of CMMI® maturity level 5. *Proceedings - 2012 8th International Conference on the Quality of Information and Communications Technology, QUATIC 2012*, 47–56. https://doi.org/10.1109/QUATIC.2012.37

Mario Draghi. (2024). *The future of European competitiveness (Part A)*.

Markopoulou, D., Papakonstantinou, V., & de Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law and Security Review*, *35*(6). https://doi.org/10.1016/j.clsr.2019.06.007

Moore, A. D. (2003). PRIVACY: ITS MEANING AND VALUE. In *Source: American Philosophical Quarterly* (Vol. 40, Issue 3).

National Institute of Standards and Technology. (2020). *NIST PRIVACY FRAMEWORK:* https://doi.org/10.6028/NIST.CSWP.01162020

National Institute of Standards and Technology (NIST). (2024a). *Definition of Cyber Security*. https://csrc.nist.gov/glossary/term/cyber_security

National Institute of Standards and Technology (NIST). (2024b). *Definition of privacy*. https://csrc.nist.gov/glossary/term/privacy

National Institute of Standards and Technology (NIST). (2024c). *Definition of Risk*. https://csrc.nist.gov/glossary/term/risk

Parlamento Europeu e do Conselho. (2016a). *Diretiva (UE) 2016/1148, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União*.

Parlamento Europeu e do Conselho. (2016b). Regulamento (UE) 2016/679, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. *Jornal Oficial Da União Europeia*.

Parlamento Europeu e do Conselho. (2022a). Diretiva (UE) 2022/2555, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União. *Jornal Oficial Da União Europeia*.

Parlamento Europeu e do Conselho. (2022b). *Regulamento (UE) 2022/2554, relativo à resiliência operacional digital do setor financeiro (DORA)*.

Parlamento Europeu e do Conselho. (2024). *Regulamento (UE) 2024/1689, que cria regras harmonizadas em matéria de inteligência artificial*. http://data.europa.eu/eli/reg/2024/1689/oj

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Popchev, I., Radeva, I., & Nikolova, I. (2021). Aspects of the Evolution from Risk Management to Enterprise Global Risk Management. *Engineering Sciences*, *LVIII*(1). https://doi.org/10.7546/engsci.lviii.21.01.02

Population Data BC. (2024). *Eligibility and the Five SAFEs model*. https://www.popdata.bc.ca/data_access/requirements/eligibility

Presidência do Conselho de Ministros. (2021). *Decreto-Lei 65/2021 - Regime Jurídico de Segurança do Ciberespaço*.

Privacy Protection Agency, C. (2018). *California Privacy Protection Agency - California Consumer Privacy Act*.

Selzer, A. (2021). The appropriateness of technical and organizational measures under article 32 GDPR. In *European Data Protection Law Review* (Vol. 7, Issue 1, pp. 120–128). Lexxion Verlagsgesellschaft mbH. https://doi.org/10.21552/edpl/2021/1/16

Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. In *Electronics (Switzerland)* (Vol. 11, Issue 14). MDPI. https://doi.org/10.3390/electronics11142181

TrustArc. (2023). *Nymity - Privacy Management Accountability Framework*.

US Congress. (1996). *HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996*.

US Congress. (2014). *Federal Information Security Modernization Act of 2014*.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Wallis, T., & Johnson, C. (2020, June 1). Implementing the NIS Directive, driving cybersecurity improvements for Essential Services. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2020*. https://doi.org/10.1109/CyberSA49311.2020.9139641

Whitman, M. E. (2011). *Principles of Information Security Fourth Edition*.

World Economic Forum. (2023). *The global risks report 2023*. World Economic Forum.

10 Anexos