UNIVERSIDADE DE LISBOA
FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE INFORMÁTICA

SEGURANÇA, PRIVACIDADE E TRATAMENTO DE DADOS: RGPD E A FACILITAÇÃO DO PROCESSO DE DIAGNÓSTICO EM CONTEXTO NACIONAL

Ricardo Miguel Cordeiro dos Santos

MESTRADO EM ENGENHARIA INFORMÁTICA
Especialização em Engenharia de Software

Trabalho de projeto orientado por:
Prof. Doutor José Carlos Medeiros de Campos

2020

Agradecimentos

Ao longo deste percurso tive a ajuda de muitas pessoas que sempre se preocuparam com o meu sucesso, esta secção serve como forma de agradecimento a todas elas.

Primeiramente gostava de agradecer ao Frederico Alves e à Mónica Cabaço por tudo o que fizeram por mim, sem eles não tinha sido possível concluir este projeto. Ao longo do percurso tive vários percalços e foram eles que me ajudaram a ultrapassá-los. Sem eles inverterem o sentido da marcha o projeto poderia ter ficado estagnado num dos vários becos sem saída que foram aparecendo. Agradeço-lhes a sua disponibilidade para me ajudar, a sua boa disposição e todo o conhecimento que me transmitiram.

Agradeço ao meu orientador, Professor José Campos, toda a sua disponibilidade, preocupação, paciência e conhecimento transmitido ao longo deste processo. As orientações ao longo do curso deste trabalho ajudaram, em muito, a manter-me no rumo certo e a conseguir desenvolver um trabalho com qualidade.

Outra pessoa muito importante neste percurso foi a Ana Guimarães, a minha supervisora. Agradeço-lhe toda a motivação que me deu para conseguir fazer um trabalho com a melhor qualidade possível. As suas palavras ajudaram-me em muito a superar algumas dificuldades ao longo deste trabalho e a sua crença no meu potencial também foi essencial. O seu rigor e preocupação em relação ao meu trabalho fizeram com que arranjasse motivação, em momentos por vezes difíceis.

Aos meus colegas da *Trust Systems* agradeço-lhes todos os momentos que me proporcionaram ao longo deste trajeto. Obrigado ao João Fonseca, ao André Tenda e ao Simão Ferreira pela paciência para me aturarem... Gostava também de agradecer a todos os meus colegas por proporcionarem todos os dias um ambiente de boa disposição, difícil de encontrar em muitos outros lugares.

Por último, gostava de agradecer à minha família, aos meus pais, ao meu irmão, aos meus avós, tias e ao meu tio. Um agradecimento especial ao Floyd por me ouvir nos dias menos bons! Todos eles foram fundamentais para concluir este trabalho e sem eles nada disto era possível. Muito obrigado!

A todos aqueles que sempre acreditaram em mim.

Resumo

O Regulamento Geral da Proteção de Dados (RGPD) surgiu como uma evolução da Diretiva 95/46/CE, que foi julgada antiquada por não considerar o aparecimento de novas tecnologias que estabeleceram a internet como *hub* de negócios e para uniformizar a forma como os dados são colecionados, armazenados e tratados, a nível europeu. Assim, existem agora diferenças fundamentais, na forma como os dados pessoais são tratados e protegidos, de forma a oferecer garantias de confidencialidade e integridade. Por ser uma realidade recente, as organizações revelam falta de preparação para a nova realidade. É, por isso, necessário realizar auditorias que revelem as não-conformidades com a norma. A execução destas auditorias é uma tarefa difícil, morosa, que produz uma grande quantidade de dados e que acarreta uma sobrecarga burocrática para os envolvidos. É um processo longo, exigindo muitas horas de trabalho de profissionais qualificados que cobram de forma valiosa essas horas. Como tal, estão associados orçamentos elevados à execução destas auditorias, dificultando o acesso a privacidade de dados de qualidade às organizações que dele necessitam.

A solução, foi construir um sistema capaz de automatizar partes repetitivas do processo, apto para reutilizar material de auditoria já produzido, que organiza a informação de forma estruturada, facilitando o acesso quando os dados escalam. Este sistema garante uma centralização do projeto RGPD, juntando toda a informação, todas as tarefas decorrentes, todos os artefatos produzidos no mesmo local, evitando o dispersar. Tornando a auditoria mais fácil de executar, com menos recursos, tornamos a mesma acessível em termos orçamentais, providenciamos resultados finais que mantêm a qualidade resolvendo o referido problema.

A avaliação qualitativa da solução proposta, mostrou uma ferramenta que diminuiu a duração de todas as fases inerentes à auditoria, agregou segurança aos processos, minorou a permeabilidade a erros, baixou os custos com pessoal, continuando a produzir auditorias de qualidade.

Palavras-chave: Confidencialidade; Proteção; Confiança; Privacidade; Segurança

Abstract

The General Data Protection Regulation (GDPR) emerged as an evolution of Directive 95/46 / EC, which was deemed outdated because it did not consider the emergence of new technologies that established the internet as a business hub and to standardize the way data they are collected, stored and processed at European level. Thus, there are now fundamental differences in the way personal data is viewed and protected, in order to offer guarantees of confidentiality and integrity. As it is a recent reality, organizations show a lack of preparation for the new reality. It is, therefore, necessary to carry out audits that reveal non-conformities with the standard. Performing these audits is a difficult, time-consuming task that produces a large amount of data and entails bureaucratic overhead for those involved. It is a long process, requiring many hours of work from qualified professionals who charge these hours in a valuable way. As such, high budgets are associated with the performance of these audits, making it difficult for organizations that need access to quality data privacy.

The solution was to build a system capable of automating repetitive parts of the process, able to reuse audit material already produced, which organizes the information in a structured way, facilitating access when the data escalates. This system guarantees a centralization of the GDPR project, gathering all the information, all the resulting tasks, all the artifacts produced in the same place, avoiding dispersion. By making the audit easier to perform, with fewer resources, we make it accessible in budgetary terms, providing final results that maintain quality by solving that problem.

The qualitative evaluation of the proposed solution, showed a tool, which reduced the duration of all the phases inherent to the audit, added security to the processes, reduced the permeability to errors, lowered the personnel costs, continuing to produce quality audits.

Keywords: Confidentiality; Protection; Trust; Privacy; Security

Conteúdo

Lista de Figuras

Lista de Tabelas

Abreviaturas

AIPD Avaliação de Impacto na Proteção de Dados.

API Application Programming Interface.

AWS Amazon Web Services.

BA Back Office de Administração.

BC Back Office de Cliente.

BD Base de Dados.

BE Back End.

CDN Content Delivery Network.

CNPD Comissão Nacional da Proteção de Dados.

CRUD Create, Read, Update and Delete.

CSRF Cross-Site Request Forgery.

DNS Domain Name System.

DPA Data Protection Authority.

DPO Data Protection Officer.

DTO Data Transfer Object.

EC2 Elastic Compute Cloud.

FE Front End.

GRC Governance, Risk and Compliance.

HTTP Hypertext Transfer Protocol.

IT Information Technology.

KPI Key Performance Indicator.

PIN Personal Identification Number.

RDS Relational Database Service.

REST Representational State Transfer.

RGPD Regulamento Geral da Proteção de Dados.

S3 Simple Storage Service.

SES Simple Email Service.

SM Gestor de Aplicação.

SMS Short Message Service.

SNS Simple Notification Service.

SO Sistema Operativo.

SQL Structured Query Language.

SYS Gestor de Sistema.

TS TypeScript.

TTL Time To Live.

XSS Cross-Site Scripting.

YAML YAML Ain't Markup Language.

Capítulo 1

Introdução

O facto de o RGPD ser uma realidade relativamente recente, leva a que muitos dos processos de auditoria e verificação de conformidade não estejam ainda sistematizados. A informação é gerida *ad hoc*, não é parte de procedimentos bem estabelecidos e padronizados capazes de serem replicados em ocasiões futuras, pelo que todos os processos de gestão e interpretação desta informação são permeáveis a erros, bastante morosos e com orçamentos elevados devido à senioridade dos profissionais envolvidos. As organizações diferem entre si, pelos processos executados, pelas suas finalidades, pela sua natureza pública ou privada, pela sua lógica de negócio, mais ou menos complicada ou até mesmo pelo impacto que têm na sociedade em geral através do emprego que providenciam. Se realizarmos uma categorização das organizações no que concerne à sua dimensão e à complexidade de exercício, chegamos a uma divisão em 4 quadrantes distintos, como é possível constatar através da figura 1.1:

- I – Organizações de grande dimensão e complexidade, frequentemente com forte exposição internacional e a mercados verticais muito regulados;
- II – Organizações de dimensão limitada à sua área de ação, com cariz solidário e/ou estadual, que lidam com elevada complexidade de operação;
- III – Organizações de serviço imediato pouco complexo com dimensão reduzida;
- IV – Organizações de dimensão considerável, com lógica de negócio simples.

1.1 Motivação

No quadrante I, assiste-se à presença de grandes empresas, com anos de negócio, com processos padronizados e que começaram a dar atenção à privacidade e à proteção de dados pessoais dos seus clientes já há algum tempo. São, portanto, um grupo consciencializado para a importância da proteção de dados, porque consideraram desde cedo que

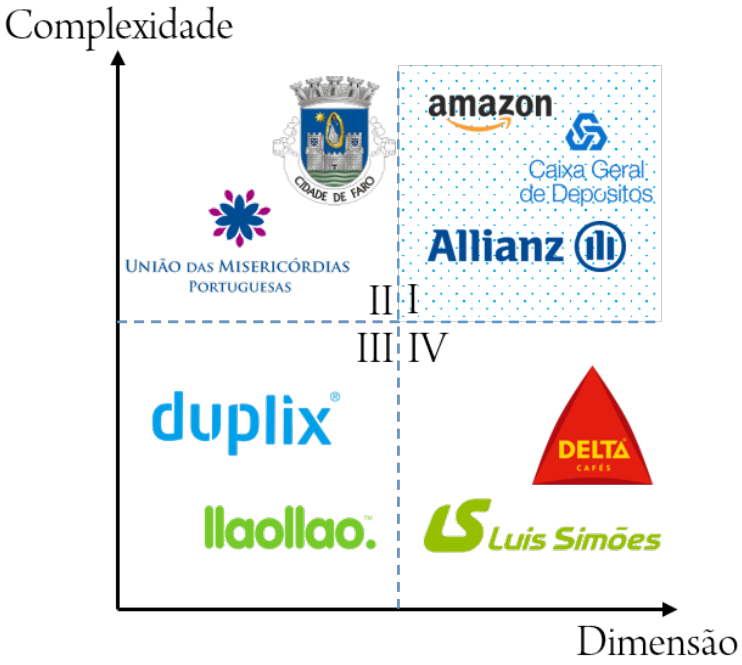

Figura 1.1: Quadrante Dimensão vs. Complexidade

esta era importante para fazer o seu negócio crescer e tornar-se robusto, associando-lhe confiança e fiabilidade.

Associadas ao quadrante IV, estão as empresas com lógica de negócio simples, mas que se tornaram referências nos seus mercados. Como a sua principal área de operação não se foca na recolha e processamento de dados pessoais, as organizações deste quadrante têm tendência a não julgar o assunto da proteção de dados como importante, apesar de terem recursos para montarem estruturas capazes de cuidar destes dados de forma apropriada. O maior desafio para estas empresas está em conseguir criar-lhes interesse nesta matéria e consciencializá-las para uma cultura de segurança da informação.

No quadrante III, temos as organizações com complexidade de operação diminuta e com uma dimensão reduzida, onde toda a sua lógica de negócio não requer, de todo, a recolha de dados pessoais. Contudo, a partir do momento em que haja recolhimento de dados, para eventuais programas de fidelização, por exemplo, é mais uma vez levantada a importância de proteger a privacidade de todos os envolvidos, apesar de haver menos dano associado a uma possível violação desses dados do que em organizações de dimensão superior, onde porventura se lida com dados financeiros e sociais capazes de comprometer a liberdade e os direitos dos seus titulares.

Por fim, temos o quadrante II, onde estão as organizações que lidam com elevada complexidade nos dados que tratam, mas devido ao seu contexto têm dimensão reduzida e recursos escassos, quando comparadas com organizações de outros quadrantes. Aqui, lida-se com dados sensíveis, que devem ser protegidos de uma forma ativa e reforçada.

Acontece que, em muitos dos casos estas organizações não têm os recursos para garantir que tal aconteça, existindo uma disparidade enorme entre o que estão dispostas a pagar e, o preço de garantir proteção de dados apropriada à sua conjuntura.

Assim, surgiu o estímulo necessário para encontrar uma forma mais eficaz e replicável de assegurar que organizações com menos recursos sejam capazes de aceder a proteção de dados de igual qualidade e seja mantido o direito à privacidade, de igual forma, em todos os quadrantes. Manifestou-se a intenção de construir um sistema capaz de atender a todas as necessidades RGPD, tanto do lado das organizações auditadas, como do lado de quem é responsável por realizar a própria auditoria. Na definição deste sistema, considerou-se indispensável desenvolver um módulo de gestão que facilitasse a administração da informação de auditoria, fornecendo uma interface para a mesma, e que implementasse premissas de segurança em todo o processo de gestão da mesma.

1.2 Contexto

Este projecto foi desenvolvido foi na *Trust Systems*[1], uma empresa do ecossistema *Inoweiser*[2], especializada em soluções no mercado de Segurança. Existia a intenção de implementar um sistema que agilizasse os processos de auditoria RGPD e o presente relatório surge no contexto desse projeto.

Desde que o RGPD entrou em vigor, a Trust Systems oferece serviços de auditoria, tendo executado projetos RGPD para organizações em vários setores e de várias dimensões. Por já haver alguma experiência de auditoria, foram detetadas dificuldades inerentes, quer a todo o processo, quer às atividades de *follow up*. Estas dificuldades redundaram num conjunto de particularidades consideradas *good-to-have* para a sua resolução ou diminuição de impacto, aquando da execução de projetos deste tipo.

Houve uma equipa multi-disciplinar alocada à realização da plataforma *Privacy*, que visava agilizar os processos inerentes às auditorias RGPD, tornando-as mais acessíveis e menos custosas em termos orçamentais e temporais, tendo eu integrado esta equipa como *developer full-stack*, sendo o responsável pela implementação do módulo de gestão. O projeto descrito neste documento decorreu em paralelo com o desenvolvimento da plataforma *Privacy*. Houve ainda a definição de mais 2 *developers*, especializados cada um em BE e FE, respetivamente, um *product owner* interno, um responsável pelo *reporting*, outro pelos *dashboards*, um *scrum master* e um responsável pela *quality assurance*. Desde o início de desenvolvimento, houve reuniões de sincronização, praticamente, todos os dias, onde se expunha o trabalho realizado, as dúvidas e as dificuldades, e se alinhavava o trabalho a realizar. Houve ainda o apoio da ferramenta Jira Agile[3] para organizar e atribuir as

[1] https://www.trustsystems.pt/ acedido a 11/2020
[2] https://www.inoweiser.com/ acedido a 11/2020
[3] https://www.atlassian.com/software/jira/agile acedido a 11/2020

issues a cada elemento da equipa, detalhando as partes integrantes de cada e controlando o seu estado de completude.

1.3 Objetivos

Para manter a plataforma (i.e., o *Privacy*) organizada, estruturada, com níveis de segurança elevados e usável para o utilizador comum, implementou-se um módulo de gestão responsável por realizar toda a administração dos dados de auditoria que circulassem na plataforma. Os objetivos deste módulo são:

- Ser conforme com o RGPD, por exemplo, minimizando os dados e não concedendo acessos a quem não os deve ter;
- Ter altos níveis de usabilidade, facilitando o uso de pessoal leigo na área, através de uma interface intuitiva;
- Ser seguro, oferecendo garantias de ser capaz de suportar e resistir a atos e influências hostis que destruam ou adulterem dados nucleares ou impeçam o sistema de funcionar de forma correta;
- Realizar as suas atividades num intervalo de tempo considerado aceitável, não consumindo muitos recursos;
- Ser escalável, adaptando-se bem ao aumento de dados na plataforma ou ao aumento do número de utilizadores;
- Melhoria significativa do desempenho e resultado em relação à solução manual;
- Impedir que aconteçam erros na gestão da informação, precavendo usos impróprios dos utilizadores;
- Reunir as funcionalidades de gestão de informação num único local, dando organização e estruturação ao sistema.

Assim, com a construção deste módulo é esperado que todo o processo de gestão dos dados se agilize e se torne menos permeável a falhas. Como tal, é expectável que exista uma melhoria do desempenho global, na realização deste tipo de projetos, em relação à solução prévia, quando se usa a ferramenta proposta.

1.4 Contribuições

A principal contribuição deste projeto é, no geral, a melhoria significativa do desempenho do processo de auditoria RGPD de organizações com complexidade de operação acima da média.

O desenvolvimento da ferramenta proposta, traz ao panorama de auditorias RGPD, um conjunto de mais-valias, para além dos objetivos descritos anteriormente. Existe agora uma *pool* de informação sistematizada e pronta a usar, uma estrutura que permite a construção de questionários de forma rápida e dinâmica e que possibilita a sua atribuição de forma inequívoca aos responsáveis. É possível manter um controlo maior sobre todos os processos e gerir as situações de risco em tempo real, de forma contínua, o que garante uma visão mais abrangente e precisa da situação RGPD. O sistema trouxe também economia de tempo de todos os envolvidos na auditoria, pois proporciona a oportunidade de reutilizar material e evitar tarefas repetidas. Toda sobrecarga burocrática que este tipo de projetos acarreta, é organizada e estruturada para que a informação seja mais fácil de gerir, ajudando os profissionais envolvidos a focarem-se nos seus conhecimentos do processo e nas suas competências centrais. A nível de segurança, a informação é guardada de uma forma própria com as defesas consideradas razoáveis para impedir ataques que impossibilitem o negócio do auditor e prejuízos para quem é auditado. Em suma, temos agora um sistema que facilita o processo RGPD e o torna mais rápido e acessível em termos orçamentais. Em particular, o módulo de gestão, facilita a administração da informação, tornando os processos que a integram mais fáceis e intuitivos de executar, e junta a estes a segurança apropriada à defesa da informação que circula dentro da plataforma.

1.5 Estrutura do documento

Este documento está organizado da seguinte forma:

- Capítulo 2 - **Trabalho Relacionado, Contexto e Ferramentas Utilizadas** - O propósito deste capítulo é fazer uma breve introdução aos temas diretamente relacionados com o âmbito deste projeto.

  O primeiro tema é a proteção de dados pessoais, sendo este tema uma base para os outros temas. Relacionado com o primeiro tema está o próprio RGPD. A aplicação do regulamento, bem como a mudança de entendimento de alguns conceitos relativos à área é também abordada neste capítulo. Algumas das ferramentas GRC consultadas são também alvo de uma breve referência e descrição, por terem feito parte do processo de decisão. Por último, é apresentada a ferramenta *Privacy* e é explicado o seu funcionamento, na ótica do utilizador.

- Capítulo 3 - **Módulo de Gestão** - Neste capítulo é descrito em detalhe o módulo de gestão do *Privacy*.

- Capítulo 4 - **Análise Qualitativa** - Neste capítulo é apresentada uma análise qualitativa do sistema desenvolvido, no seu todo, e em particular, do módulo de gestão, bem como uma discussão acerca das vantagens e das contribuições dadas na realização de projetos deste tipo.

- Capítulo 5 - **Conclusão** - Este capítulo contém um sumário do que foi feito neste projeto, recapitulando o que era o problema e como foi resolvido. Indicou-se alguns dos indicadores que guiarão a avaliação da ferramenta e do módulo (como integrante) em possíveis trabalhos futuros.

Capítulo 2

Trabalho Relacionado, Contexto e Ferramentas Consultadas

O sistema desenvolvido neste projeto tem como objetivo reduzir de forma considerável, a duração de um projeto típico de RGPD, bem como o orçamento que lhe está associado. Através da sistematização de alguns processos comuns, do uso de tecnologia para agilizar partes morosas, que permita organizar documentação, responsáveis departamentais, análises de riscos e planos de contingência, é possível garantir níveis elevados de conformidade com a regulamentação vigente. Neste capítulo é também feita uma introdução a diferentes conceitos relacionados com o RGPD e respetiva aplicação do mesmo em contexto empresarial.

Por fim, são descritas duas ferramentas de suporte à garantia de conformidade e de gestão de risco, bem como que tipo de influências podem ser retiradas destas para que ajudem a suportar uma aplicação do RGPD completa e bem estruturada.

2.1 Proteção de Dados Pessoais

Sendo este um projeto que se insere no âmbito de proteção de dados pessoais é necessária a devida contextualização. Nesta secção, são introduzidos os conceitos mais pertinentes que orbitam em torno da proteção de dados pessoais. Hoje em dia, o bem mais valioso, é a informação [3], que nos permite fazer escolhas ponderadas e em consciência, calcular riscos, fazer previsões e criar valor acrescentado para empresas e consumidores providenciando serviços, dificilmente imagináveis sem ela. Como um bem precioso e apetecível, devem ser tomadas precauções para que não caia nas mãos erradas. Isto, é uma tarefa de todos os envolvidos no ciclo de vida dessa informação, desde o titular da mesma até à organização que a gere e trata. Assim, é necessário rodear a comunidade que lida com dados pessoais e informações críticas, de uma cultura de segurança da informação, seguindo os seus conselhos.

Com a crescente desconfiança em relação à segurança dos seus dados pessoais, devido às intrusões e aos *leaks* de informação de várias organizações [4], surge a necessidade de

envolver regulamentação, de modo a tornar objetivo o processo de proteção e uniformizar a forma como estes dados são tratados, independentemente do tipo de instituição que os detém. Acredita-se que as melhorias que advêm de cumprir os regulamentos, causarão um aumento de confiança, por parte dos titulares, aquando da entrega dos seus dados [5].

Um dos principais conceitos associados a este projeto é o de **dado pessoal** que se define como: qualquer informação relacionada a uma pessoa singular, que pode ser usada direta ou indiretamente para identificar essa pessoa [6]. Previamente à implementação do RGPD, os dados pessoais eram pedidos em grande quantidade, sem qualquer tipo de justificação, com muita informação desnecessária à lógica de negócio das organizações, criando susceptibilidades a eventuais fugas de informação que porventura nem deveria ter sido recolhida, ou recolhida de forma mais parcimoniosa, cuidada e exata.

Na figura 2.1 é possível observar um esquema que exemplifica um pedido de informação por parte da organização.

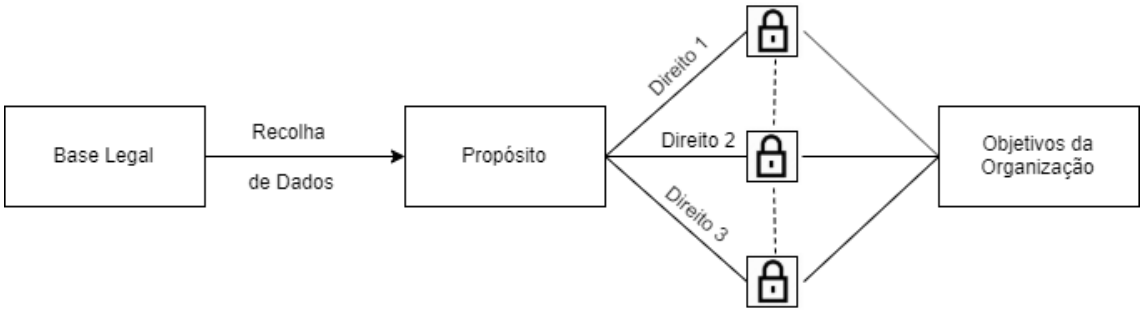

Figura 2.1: Esquema de pedido de informação

De forma a respeitar conformidade com RGPD, as informações e comunicações relacionadas com tratamento de dados pessoais devem ser de fácil acesso e compreensão, formuladas numa linguagem clara e simples. Devem haver procedimentos razoáveis para retificar, apagar ou deixarem de ser objeto de tratamento, os dados não necessários para a finalidade para a qual foram recolhidos/tratados [7]. E para que estes procedimentos sejam estabelecidos e concretizados é necessário haver uma catalogação dos dados pessoais, bem como o recolhimento de alguns metadados que ajudarão no processo de decisão em relação ao tratamento ou não, desses mesmos dados. Assim no processo de tratamento dos dados deve juntar-se aos mesmos as seguintes informações:

- Que informação foi recolhida?
- Porque foi recolhida?
- Como será usada?
- Quem recolheu?
- Como foi recolhida?

- Com quem será partilhada?

De acordo com o Artigo 30º do RGPD [8], é mandatório manter documentação de todas as atividades de processamento de dados, em detalhe: o propósito do processamento, as categorias dos assuntos e dados pessoais envolvidos, categorias dos destinatários, salvaguardas em todas as transferências de dados, os limites temporais para apagar e as descrições técnicas de todas as medidas de segurança na organização.

Existe então uma demarcação das categorias de dados pessoais [9], sendo estes divididos em:

- Internos
  - **Conhecimento e Crenças**: informação acerca de crenças religiosas, filosóficas e pensamentos.
  - **Autenticação**: informação que seja para autenticar através de senha de acesso, PIN, impressão digital.
  - **Preferência**: informação de interesses relacionados com cores, música e gostos.
- Externos
  - **Identificação**: informação que identifica uma pessoa singular através do nome, foto, dados biométricos e identificador único.
  - **Etnia**: informação que descreve a raça, origem e idiomas falados.
  - **Sexual**: informação que descreve a vida sexual e preferências pessoais.
  - **Comportamento**: informação que descreve atividades relativas a uma pessoa.
  - **Demografia**: informação que descreve as características partilhadas relativas a escalões de rendimento, faixas etárias e traços físicos.
  - **Médicos e Saúde**: informação que descreve condições de saúde relativas a tipo de sangue, ADN, resultados de testes, deficiências, prescrições e histórico clínico.
  - **Características físicas**: informação que descreve características como altura, peso, idade, cor do cabelo, pele, tatuagens e género.
- Históricos
  - **História da vida**: informação acerca do historial pessoal que pode ter influenciado a vida da pessoa.
- Financeiros

  - **Conta**: informação que identifica contas financeiras de uma pessoa, relativos com número de cartão de crédito e número de conta bancária.
  - **Propriedade**: informação de coisas que a pessoa tem, arrendou, emprestou ou possuiu.
  - **Transações**: informação das compras ou despesas relacionadas com vendas, créditos, receitas, empréstimos, transações, impostos e hábitos de compras.
  - **Crédito**: informação acerca de dinheiro para credibilidade, capacidade e posição de crédito.

- Sociais
  - **Profissional**: informação acerca da carreira académica ou profissional que descreve ficheiros de empregado, salário, avaliações, entrevistas e historial de trabalho.
  - **Criminal**: informação acerca de atividades criminais relacionadas com condenações e acusações.
  - **Vida pública**: informação acerca da vida pública relacionada com reputação, religião, filiações políticas e sindicais.
  - **Família**: informação acerca da família relativa à estrutura familiar, irmãos, primos, casamentos e divórcios.
  - **Redes Sociais**: informação relacionada com ligações sociais com amigos, conhecidos, associações e grupos.
  - **Comunicação**: informação comunicada por mensagem para 2 pessoas através de e-mail e voz.

- Rastreamento
  - **Computador**: informação acerca de um dispositivo para utilização pessoal relacionada com endereços IP e MAC.
  - **Contacto**: informação que fornece mecanismo para contactar através de e-mail e telefone.
  - **Localização**: informação acerca da localização relativa às coordenadas GPS e país.

Existem dados cujo seu tratamento é proibido (Artigo 9º – 1) por se inserirem em categorias especiais e serem suscetíveis de causar dano no titular dos dados:

- Origem racial ou étnica.
- Opiniões políticas.

- Convicções religiosas e filosóficas.
- Filiação sindical.
- Dados genéticos.
- Dados biométricos capazes de identificar uma pessoa de forma inequívoca.
- Dados de saúde.
- Vida ou orientação sexual.

Com a entrada em vigor do RGPD, estabeleceu-se que os clientes são donos dos seus dados, não as organizações que os detêm. Com a mudança de entendimento acerca de quem é dono dos dados surgiu também nova regulamentação com os direitos que devem ser garantidos aos titulares dos mesmos:

- **Direito a ser informado (Artigo 15º)** [10]
  - Responder prontamente a pedidos dos indivíduos acerca dos seus dados pessoais que uma entidade controla, processa ou transfere. Têm direito a saber objetivos com que os dados são processados, as categorias de dados pessoais processados, destinatários ou as suas categorias que têm acesso aos dados, quanto tempo estarão gravados e a origem dos seus dados pessoais se estes não tiverem sido fornecidos por si.
  - Se dados são sujeitos a processamentos automáticos e definição de perfis, a entidade tem de providenciar informação acerca da lógica envolvida, bem como o significado e as consequências previstas desse processamento para o indivíduo.
  - O titular dos dados deve ser capaz de executar este direito facilmente com intervalos de tempo razoáveis para que lhe seja possível acompanhar o processamento e verificar a sua legalidade.
- **Direito à retificação (Artigo 16º)** [11]
  - Sempre que considerar que os seus dados pessoais (dados pessoais objetivos fornecidos por si) estão incompletos ou incorretos, pode requerer a sua retificação ou que os mesmos sejam completados.
  - As entidades terão de implementar uma integração entre todos os sistemas e processos de forma a assegurar a atualização automática, de dados alterados num sistema, em todos os sistemas dessa entidade.
- **Direito ao apagamento (Artigo 17º)** [12]

  - O indivíduo tem o direito de apagar permanentemente qualquer dado pessoal de acordo com condições específicas: retirada de consentimento (quando o mesmo foi a origem da recolha e processamento), dados pessoais processados de forma ilegal, dados pessoais deixarem de ser necessários para a finalidade que motivou o processamento.
  - Se esses dados tiverem sido tornados públicos por alguma razão, têm de ser tomadas ações razoáveis no sentido de informar os outros controladores de dados do pedido/direito de os apagar.

- **Direito de Restrição/Limitação de Tratamento (Artigo 18º)** [13]
  - A limitação do tratamento permite ao titular solicitar ao responsável que restrinja o acesso a dados pessoais ou que suspensa as atividades de tratamento.
  - Em casos de contestação da exatidão dos dados pessoais, de dados processados de forma ilegal sem pedido de apagamento, de já não serem precisos para fins de tratamento, mas ainda precisos para fins declarativos ou por simples oposição ao tratamento.

- **Direito à Portabilidade dos Dados (Artigo 20º)** [14]
  - O indivíduo "tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento".
  - Formato deve ser interoperável.

- **Direito à Oposição** [15]
  - Pode opor-se ao tratamento dos seus dados para fins de marketing direto, incluindo a definição de perfis que esteja relacionada com esse marketing.

- **Direito à retirada de consentimento** [16]
  - Nos casos em que o tratamento dos dados seja feito com base no seu consentimento, poderá retirar o consentimento a qualquer momento (com a mesma facilidade com que foi dado)

- **Direito à não Sujeição a Automação de Decisão (Artigo 22º)** [17]
  - Ter intervenção humana em processos de tomada de decisão, para que indivíduo não fique sujeito a definições estritamente automatizadas, que produzam efeitos na sua esfera jurídica ou o afetem de forma similar.

Com o aumento de poder sobre os dados, por parte dos titulares, surge também um conceito reforçado de **consentimento**, que é agora encarado com um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca e onde silêncio, opções pré-validadas e omissão não se constituem como um consentimento válido [18], como se vê na figura 2.2. Abrange todas as atividades de tratamento com a mesma finalidade, e em caso de fins múltiplos, cada um deverá ter um consentimento próprio elaborado de forma clara e concisa. O consentimento deve ser documentado para que possa ser demonstrado que foi dado.

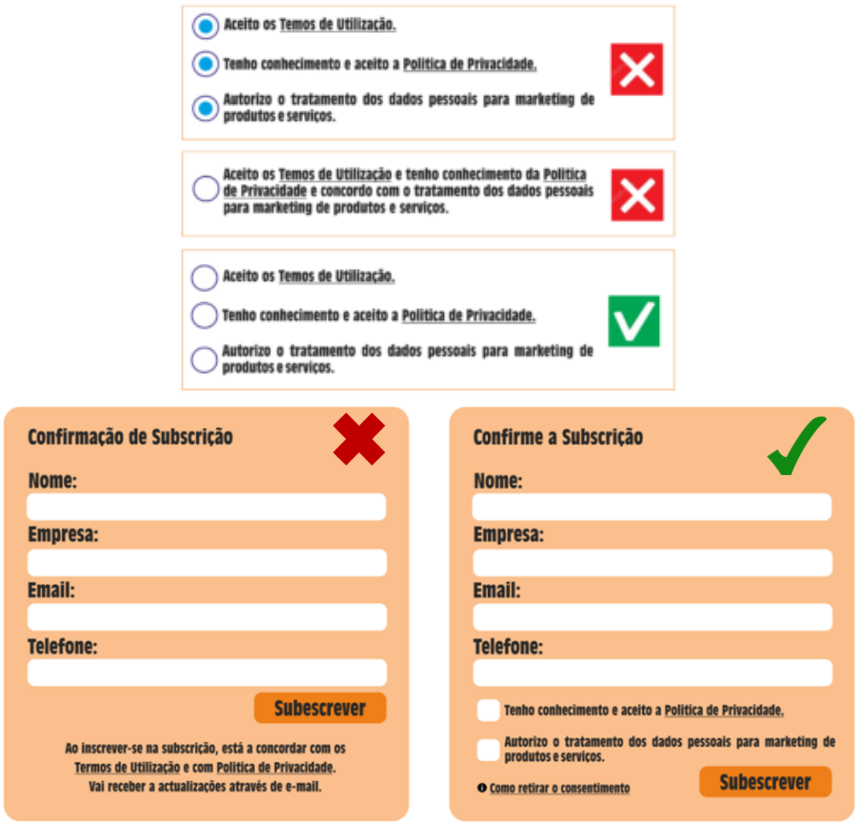

Figura 2.2: Formulários de consentimento [1]

Uma alteração relevante, no que concerne aos consentimentos, trazida pelo RGPD, prende-se por exemplo com o uso de *cookies*. No período pré-RGPD, a maneira mais comum de obter consentimento é um aviso com uma barra informativa para um "*cookie* de aceitação da política de *cookies*" que tinha um "TTL" de aproximadamente 1 ano. Após o RGPD é necessário obter consentimento por parte do utilizador em diferentes níveis de aceitação, ou seja, para cada tipo de *cookie* [19], expresso na figura 2.3:

- *Cookies* estritamente necessários: permitem a navegação no site usando áreas seguras. Sem estes, os serviços requeridos não podem ser apresentados.
- *Cookies* analíticos: usados anonimamente para efeitos de monitorizar e analisar estatísticas, sem nunca recolher informações de caráter pessoal.

- *Cookies* de funcionalidade: guardam preferências do utilizador relativamente à utilização do site, de modo a que não seja necessário voltar a configurar definições do site.
- *Cookies* de publicidade: direcionam a publicidade através de campanhas em função dos interesses e gostos de cada utilizador.
- *Cookies* de terceiros: medem o sucesso de aplicações e a eficácia da publicidade de terceiros.

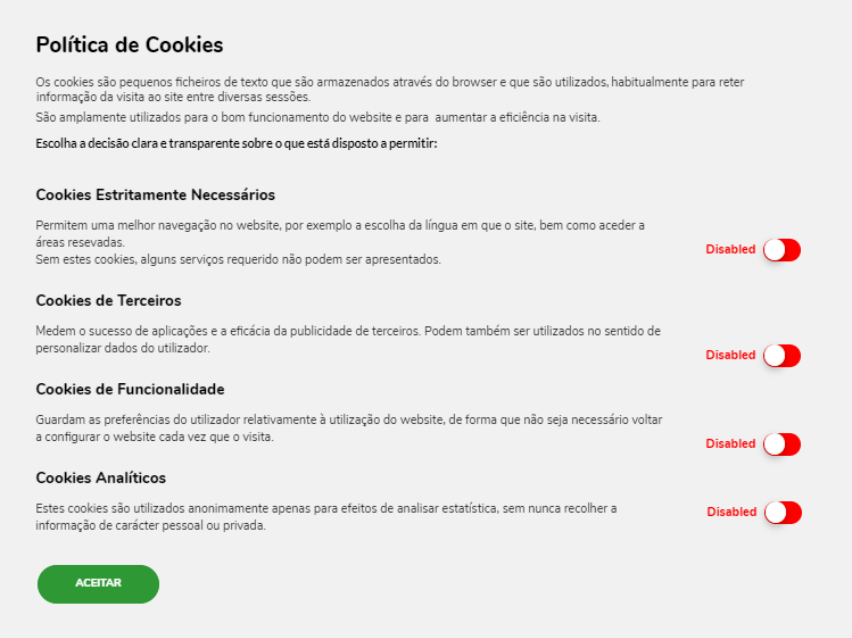

Figura 2.3: Exemplo de formulário de consentimento do uso de *cookies* bem construído [2]

Surgiram também novos *roles* no panorama da proteção de dados [20], com novos direitos e novas obrigações. Após a entrada em vigor do regulamento vigente, a divisão estabeleceu-se em:

- *Data Subject* (Titular dos dados)
  - Pessoa natural.
  - Cidadão ou residente de um estado membro da União Europeia.
  - Dono legítimo dos seus próprios dados.
- *Data Controller* (Possui os dados)
  - Organização que recolhe dados dos cidadãos ou residentes da UE.
  - Determinam os propósitos, condições e meios de processamento dos dados pessoais.

  - Obrigações
    * Licitude do tratamento com o consentimento livre, específico, informado e explícito (Artigo 6º-1) [7].
    * Assegurar a privacidade desde o padrão até ao desenho (Artigo 25º) [21].
    * Definir políticas, procedimentos e códigos de conduta adequados (Artigo 24º-2) [22].
    * Obter garantias adequadas do subcontratado (Artigo 28º) [23].
    * Proceder ao registo das atividades de tratamento, quando aplicável (Artigo 30º) [8].
    * Cooperar com as autoridades de controlo (Artigo 31º) [24].
    * Garantir a segurança do tratamento com medidas técnicas de pseudonimização (Artigo 32º-1) [25].
    * Assegurar a gestão de risco (Artigo 32º-2) [25].
    * Notificação à autoridade de controlo em 72 horas (Artigo 33º) [26] .
    * Proceder à AIPD (Artigo 35º) [27].
    * Designar o DPO (Artigo 37º) [28].

- *Data Processor* (Gere os dados)
  - Processa dados em nome do *Data Controller*.
  - Têm obrigações estatuárias e podem estar sujeitos a execução das leis pela autoridade supervisora.
  - O *Data Processor* pode ser a mesma figura que o *Data Controller* e possui responsabilidades equivalentes.

- *Data Protection Officer* (Encarregado da proteção de dados) [28] [29] [30]
  - É obrigatório nomear um DPO para autoridades públicas e entidades cujas atividades do seu "*core business*" consistem em processamento de dados que necessitam de monitorização sistemática e regular dos indivíduos em larga escala e que lidam com categorias de dados especiais. Isto também se aplica a empresas não-UE que estão sujeitas aos requisitos do RGPD.
  - Pode ser funcionário da entidade, representante para grupo de organizações ou um consultor externo.
  - Deve ter conhecimento das leis de proteção de dados.
  - Deve ter independência nas suas tarefas;
  - Deve informar e aconselhar responsáveis pelo tratamento, subcontratantes e trabalhadores acerca das suas responsabilidades decorrentes do RGPD, reportando ao nível mais alto da empresa.

  - Deve monitorizar conformidade e comunicar com a autoridade supervisora.

- *Data Protection Authority* (Autoridade supervisora) [31]
  - Autoridade nacional encarregada da proteção de dados.
  - Cada estado membro da EU tem de nomear uma ou mais DPAs para implementar a regulamentação.
  - Têm poderes de execução, incluindo a habilidade de emitir multas [32].
  - Organizações a operar através de vários estados podem ter que interagir com múltiplas DPAs.
  - Em Portugal, quem assume este papel é a Comissão Nacional de Proteção de Dados CNPD, que entre outras coisas, tem como responsabilidade, elaborar e publicitar a lista de tratamentos de dados pessoais sujeitos a AIPDs [33].

De forma a preservar a privacidade dos dados possuídos e processados, é recomendado o uso da **pseudonimização**, por forma a reduzir os riscos de exposição dos titulares dos dados e a possibilitar uma segurança adicional para os responsáveis pelo tratamento. Não remove informações de identificação dos dados, reduz a vinculação de um conjunto de dados com a identidade original usando criptografia ou funções de *hash*. Para pseudonimizar um conjunto de dado de forma eficiente, todas as informações adicionais devem ser mantidas separadamente e sujeitas a medidas técnicas que garantam a sua não atribuição a uma pessoa identificada ou identificável [18].

Associados a este projeto estão também os conceitos de **confidencialidade**, que se refere a proteger informação de ser acedida por partes não autorizadas, **integridade**, que trata de assegurar a autenticidade da informação, quer a nível de alterações da mesma, quer na verificação da genuinidade das fontes e, **disponibilidade**, que significa que a informação é acessível pelos utilizadores autorizados.

2.1.1 Auditorias RGPD

Um projeto típico de RGPD, normalmente, prende-se com a realização de uma auditoria de privacidade, que se foca nas comunicações externas, nas instruções internas, na gestão de risco e nos processos de privacidade vigentes, e em desenvolver um roteiro de como mitigar as lacunas encontradas.

As auditorias RGPD seguem um *workflow* já estabelecido e, possível de discriminar em várias etapas bem definidas.

Em primeiro lugar, num projeto destes, surge a **fase 0**, uma fase de preparação da auditoria e de reconhecimento das circunstâncias e do modo como a privacidade é endereçada na organização auditada, onde se inserem várias sub-fases:

- Fase de Estudo.

- Levantamento de Sistemas.
- Levantamento de Softwares.
- Levantamento de BDs.
- Levantamento de dados em papel.

De seguida, vem a **fase 1**, onde se procede à preparação dos questionários, por parte da equipa auditora, para avaliar e identificar as inconformidades com o RGPD, de acordo com o que a organização coloca em prática no momento da auditoria, na forma como gere e processa os dados pessoais que detém, as medidas que toma para os proteger e os riscos envolvidos. Os questionários devem ser construídos da forma mais completa e abrangente possível, onde preferencialmente se atinja uma cobertura que se aproxime dos 100%, no que concerne às operações da organização. Para que tal aconteça, é então fundamental realizar as sub-fases prévias de forma cuidada e atenta para que não escape nada ao escrutínio dos questionários.

Posteriormente, é a **fase 2**, o preenchimento dos questionários, por parte da organização auditada. Um preenchimento eficiente, objetivo e completo de um questionário bem construído, leva a uma boa avaliação e torna o processo de auditoria mais pragmático.

Segue-se a **fase 3**, onde se realiza a análise das respostas aos questionários. É aqui que os auditores começam o processo de avaliação, condensando as informações adquiridas nos questionários, com as obtidas previamente na fase 0.

De forma a mitigar possíveis incongruências, surge a **fase 4**, a fase de entrevistas, onde se pega nos resultados da análise aos questionários preenchidos e se tenta aclarar algumas respostas, chegar a conclusões mais concisas, atingir pontos de entendimento em áreas de operação não abrangidas pelos relatórios e verificar a veracidade daquilo que são conjuntos de respostas que não fazem sentido juntas.

Quase realizada de forma paralela, aparece a **fase 5**, a fase de dúvidas. Uma fase de tamanho variável, devido ao carácter volátil das operações das organizações auditadas. Aqui surgem as dúvidas que persistiram da fase anterior.

Por fim, surge a **fase 6**, a produção e a entrega do relatório e recomendações, onde existe uma enorme sensibilidade associada a este, pois será onde será baseado o destino RGPD da organização auditada, pelo que deve ser realizado de forma atenta, cuidada, completa, percetível e sem erros. Assim é uma atividade que pela sua complexidade e por condensar muita da informação recolhida anteriormente, assume um carácter de extrema importância e como tal deve ser reservado, para esta atividade, um intervalo de tempo considerável para que possa ser executada da melhor forma possível.

Tomou-se como exemplo um projeto RGPD anterior, realizado pela empresa, a uma organização de tamanho e complexidade de operação médios, a OTLIS[1]. Tendo este por

[1] https://www.portalviva.pt/pt/homepage/sobre-a-otlis/a-otlis.aspx acedido a 11/2020

base, estimou-se a duração média de um projeto deste nível de complexidade, expressa na tabela 2.1 em 2 a 3 meses, dependendo das variáveis associadas a tempos de resposta do cliente e às fases de dúvidas e entrevistas.

1. Preparação dos Questionários	**2. Questionários**	**3. Análise dos Questionários**	**4. Entrevistas**	**5. Fase de Dúvidas**	**6. Relatórios / Recomendações**
5-10 dias	Tempo do cliente	7-8 dias	10 dias	variável	15 dias

Tabela 2.1: Estimativa de duração de cada fase de um projeto de auditoria RGPD

Existem quatro critérios que influenciam o custo de estar conforme com a norma vigente, por parte da organização auditada:

1. *Indústria em que se está e que tipo de dados se processam.* Dados sensíveis são regulados muito mais estritamente do que outros tipos de dados e requerem conformidade com obrigações adicionais.

2. *Tamanho da empresa.* Empresas maiores detêm dados de mais pessoas, mais processos de tratamento, mais bases de dados que têm de cuidar.

3. *Começar do início ou adaptar processos existentes?* Quanto maior a empresa, maior a probabilidade de que já exista um programa de gestão dos dados, pelo que há que calcular custos correntes e os custos de algumas mudanças específicas (revisão de contratos, gestão de risco com vendedores, privacidade dos subcontratados). Caso não haja qualquer processo implementado, todos os custos serão os associados a colocar um programa de privacidade de pé (o que envolve a contratação de novo *staff*).

4. *Necessidade de investir em novos sistemas IT?* Para cada processamento que dependa de um consentimento, a empresa tem de trabalhar nos elementos discretos deste e oferecer consentimentos separados para esses elementos, o que irá impactar as escolhas apresentadas ao utilizador, pelo que o sistema também deverá ser capaz de refletir estas escolhas para que se possa honrar a retirada de consentimento.

Panorama das auditorias

As auditorias geram quantidades de informação gigantescas, difíceis de processar rapidamente. Muita desta informação é texto denso, de complexa análise, que se torna difícil de gerir. O *Excel* é usado como BD para, por exemplo, armazenar responsáveis pelas determinadas áreas da organização, para armazenar processos e dados pessoais que orbitam em torno dos mesmos e para produzir questionários. A comunicação entre auditores, DPO e responsáveis departamentais é pouco dinâmica o que dificulta a auditoria, tanto por haver atrasos nas respostas, explicações e descrições dos processos pouco precisas e

não coincidentes com a realidade que irão precisar de esclarecimentos adicionais. Existe também atribulações em manter o controlo sobre o que já foi feito e o que está por fazer, pois em muitos dos casos quem responde aos questionários não tem como prioridade a proteção de dados, pelo que pode descurar a necessidade de demonstrar a sinceridade que se pretende, por ser o seu trabalho que está em causa. Por tudo isto, realizar esta auditoria é um processo moroso, cansativo, difícil de controlar, com bastantes contrariedades e partes integrantes que oferecem resistência, que exige hoje que, em muitas partes deste, haja um *rework* constante, que processa e produz grandes quantidades de material pesado difícil de organizar, aumentando a permeabilidade a erros durante o mesmo.

2.1.2 Políticas de Privacidade / Termos e Condições de Segurança

Surgem para tornar mais transparente o tratamento e as finalidades da recolha de dados pessoais, sendo uma maneira de isentar o responsável pelo tratamento de qualquer responsabilidade [34]. É uma mais valia para a credibilidade junto dos utilizadores [35]. Deve conter informação acerca:

- Âmbito da política de privacidade;
- Dados pessoais recolhidos sobre o utilizador (de forma direta ou indireta);
- Categoria dos Dados Pessoais tratados;
- Finalidades do tratamento dos Dados Pessoais;
- Partilha e Divulgação dos Dados Pessoais;
- Políticas de *cookies*;
- Conservação de Dados Pessoais;
- Armazenamento dos Dados Pessoais;
- Direitos dos utilizadores sobre os dados;
- Aceitação de consentimento;
- Segurança dos Dados Pessoais;
- Sub-contratação / *Data Processors*;
- Hiperligações para outros *websites*;
- Contacto do Responsável pelo tratamento.

A supervisão dos códigos de conduta aprovados, pode estar sujeita a uma verificação periódica da conformidade por parte da autoridade de controlo, revendo as políticas, processos e documentação do responsável pelo tratamento [36].

2.1.3 Políticas de Segurança

Na operação diária, os funcionários devem estar sensibilizados para a política de segurança e com os procedimentos operacionais da segurança da informação, adotando cuidados [19]. Assim a política de segurança defende que:

1. Cada colaborador assume a responsabilidade no que respeita aos direitos e deveres, no uso de ferramentas informáticas, nos comportamentos do dia-a-dia e no cuidado com documentos físicos que contenham dados pessoais.

2. A cultura de Segurança da Informação deve ser incutida a partir do mais alto nível e fomentada todos os dias entre os colaboradores.

2.2 Ferramentas GRC

Uma das dificuldades sentidas, ao nível das empresas, na aplicação da nova regulamentação prende-se com a segmentação da informação de forma a assegurar que, aplicadas as metodologias e ferramentas disponíveis, se esteja de facto a cumprir o preceito legal. É dada grande importância a atividades e programas GRC para garantir que as empresas protegem as suas informações, que tenham coesão consistente por departamento e sigam todas as regulamentações governamentais. Existem muitos riscos no local de trabalho relacionados à garantia de administração, gestão de riscos e conformidade. Tome-se o conceito de GRC como uma abordagem estruturada para alinhar as Tecnologias da Informação com os objetivos de negócios, enquanto se gere os riscos associados e se atende aos requisitos de conformidade com os regulamentos [37].

O software GRC permite que empresas de capital aberto integrem e giram operações de IT sujeitas a regulamentação. Este software, geralmente, combina funcionalidades que gerem as principais funções do GRC num único pacote integrado. Na generalidade, os maiores componentes de um sistema GRC [38] são:

- Gestão de Políticas IT.
- Gestão de Riscos IT.
- Gestão de Conformidade.
- Gestão de Ameaças e Vulnerabilidades.
- Gestão de Incidentes.
- Gestão de Risco do Fornecedor.

2.2.1 Eramba

O **Eramba**[2] é uma plataforma GRC de nível empresarial de *open-source* e, inclui módulos para gestão de riscos, gestão de conformidade, auditorias e gestão de políticas. Esta ferramenta oferece uma API personalizada, permitindo que os *developers* criem ligações entre o si e produtos de terceiros. Realiza gestão de ativos, com análises aos seus ciclos de vida e ajuda a identificar o fluxo dos dados, o que se torna especialmente crítico no que toca ao RGPD, sendo um módulo necessário para ajudar as organizações a perceber como informação sensível circula através do seu ambiente, pessoas, processos e tecnologia [39].

Funciona também como repositório de políticas de segurança, de planos de contingência, de documentação e ainda ajuda a estabelecer controlo de acessos e a fazer a atribuição de responsabilidades aos devidos, sendo também uma ajuda no que concerne à realização de *Business Impact Analysis* (BIAs). Assume um papel de relevo na gestão de risco, através de classificações (probabilidade x impacto), ou através do estabelecimento de um *threshold* que atribui pontuações de risco e cores baseadas na combinação da classificação de risco.

No que toca à gestão de conformidade, permite fazer análises individuais de cada requisito de um dado pacote (ex. RGPD) de forma a determinar-se se se está em conformidade. Existem também operações de segurança, com campanhas de consciencialização, projetos relacionados a mitigar a deficiências e incidentes de segurança [40].

O Eramba mostrou acima de tudo funcionalidades promissoras de se ter numa ferramenta de gestão de conformidade mas revelou um conjunto de vulnerabilidades impeditivas de constar num tipo de projeto que tem de garantir a total segurança dos dados que transitam na plataforma usada. De resto, também foi considerado que esta ferramenta não agregava todas as funcionalidades pretendidas pelo *product owner*.

No que toca à segurança da ferramenta, foram descobertas vulnerabilidades em locais diferentes da aplicação [41]:

- **Stored XSS** no parâmetro 'descrição' da *tooltipbox* na página 'programScopes' com o *payload*: `lt;"img src="" onerror="alert(1);"gt;` ;
- **Reflected XSS** na página de erro de importação de ficheiros .CSV, onde basta colocar uma *tag* <script> dentro do ficheiro importado. O *payload* usado foi: `<script>alert(1)</script>` ;
- **Reflected XSS** no parâmetro '*advanced_filter*' nos parâmetros de procura, na página `<ip-address>/reviews/filterIndex/ThirdPartyRiskReview?`, com o *payload* `<script>alert(1)</script>`.

[2] https://www.eramba.org/ acedido a 11/2020

Estas vulnerabilidades, no geral, permitiam a inclusão de *scripts* maliciosos que correriam junto com o código, que poderiam ter como repercussões acessos indesejados, roubando a informações de sessão (através dos *cookies*) e alteração da própria página *web*, podendo reescrevê-la. Expondo os dados do sistema e permitindo acessos indevidos à informação que este contém, percebeu-se que estas fragilidades não eram desprezáveis num sistema que tenha como contexto o RGPD. Visto que este versa, sobretudo, em manter a privacidade dos dados e dar acessos a informação estritamente necessária para a execução das funções pretendidas e não estando essas duas premissas garantidas, a existência destas vulnerabilidades impediu que se usasse o Eramba.

2.2.2 SimpleRisk

O **SimpleRisk** [3] é um sistema *open-source* usado para atividades de gestão de risco. Permite aos gestores de risco, contabilizar os riscos, planearem medidas de mitigação, facilitar revisões de gestão, priorizar o planeamento do projeto e acompanhar revisões periódicas. Possibilita que as respostas da empresa possam ser priorizadas também de acordo com a gravidade das ameaças e vulnerabilidades que possam afetar o negócio. Possui um *dashboard* para submeter riscos para consideração pela equipa responsável, para criar relatórios de riscos, gráficos de níveis de risco e localizações. É altamente configurável, inclui relatórios e questionários dinâmicos e a capacidade de ajustar fórmulas de risco em tempo real [42].

O SimpleRisk é uma ferramenta que opera maioritariamente no ramo da gestão de risco e está claramente virado para isso pelo que as tentativas de modular a ferramenta num rumo de gestão de conformidade se revelaram infrutíferas por ser manifestamente insuficiente nesse aspeto.

Para além da impossibilidade de configuração adequada ao problema, o SimpleRisk revelou ainda algumas vulnerabilidades no que toca à segurança da aplicação [43]:

- Ataque XSS CSRF no formulário de envio de e-mail de redefinição da *password* (`reset.php`) onde é possível injetar sequências XSS por via do parâmetro 'utilizador'.

Esta vulnerabilidade, iria permitir essencialmente que o atacante adulterasse os pedidos dos utilizadores legítimos, induzindo-os a realizar ações que não pretendessem. Por se lidar com informação extremamente sensível, que não pode ser perdida, adulterada ou consultada de forma indevida, seria muito arriscado permitir que esta vulnerabilidade persistisse num sistema cujo principal intuito é gerir e processar esse tipo de informações.

[3] https://www.simplerisk.com acedido a 11/2020

2.3 *Privacy*

Nesta secção é apresentada a solução proposta para resolver o problema anteriormente mencionado: o *Privacy*. Esta ferramenta foi desenvolvida com o intuito de agilizar os processos de auditoria RGPD, tornando-os mais rápidos na sua execução, menos custosos em termos orçamentais e menos permeáveis a erros humanos. Tudo isto, beneficia as organizações alvo das auditorias, que obtêm resultados mais expeditos, de melhor qualidade, com um custo mais acessível. Para além das contribuições trazidas ao panorama das auditorias, a ferramenta oferece ainda vantagens na logística das mesmas, por anular muitas despesas associadas a transportes, estadias, alimentação, *etc.*, dos profissionais envolvidos e na gestão dos recursos humanos da empresa. Iria aumentar os níveis de **produtividade** permitindo que cada profissional pudesse lidar com mais de um projeto RGPD em simultâneo. Por fim, ligado a todas as vantagens descritas anteriormente, surge o aumento da competitividade, alcançando novos segmentos de mercado, chegando a clientes antes inatingíveis. Associado, vem o aumento da margem de lucro da empresa, que aumenta a sua capacidade de assumir novos projetos, não aumentando de sobremaneira os custos, o que faz com que haja um maior *income* de capital.

Vantagens

Para o DPO, com Privacy consegue ter numa única solução a visão completa dos riscos de não conformidade em matéria de proteção dos dados pessoais da sua organização. Consegue igualmente partilhar essa visibilidade com a gestão de topo e tornar claro dentro da organização quais as áreas com maior e menor nível de risco de incumprimento. E consegue realizar esse acompanhamento, quer a nível agregado quer em detalhe, de forma fácil e intuitiva.

1. Acessos diferenciados e seguros.
2. Visão detalhada do risco e de fragilidades associadas aos seus departamentos.
3. Acompanhamento das medidas de redução de risco.
4. Geração automática dos relatórios da gestão de riscos.
5. Suporte do início ao fim às auditorias RGPD com registo da informação apresentada nas várias etapas do processo.

Para o Auditor, é uma ferramenta que gere todos os seus processos de RGPD, sem confusões, sem atrasos, totalmente configurável e com um vasto conjunto de relatórios gerados de forma automática.

1. Assegura auditorias a vários clientes, em paralelo, sem contaminação dos dados.

2. Oferece diferentes níveis de risco a cada fragilidade, de acordo com uma metodologia aceite em processos críticos de segurança.

3. Gera automaticamente os relatórios requeridos no enquadramento legal vigente.

4. Suporte do início ao fim às auditorias RGPD com registo da informação apresentada nas várias etapas do processo.

5. Poupança de tempo.

Roles do *Privacy*

Dentro da ferramenta é possível assumir vários papéis, quer a nível do cliente, quer a nível da empresa auditora. Cada *role* tem os seus privilégios bem definidos, para evitar a partilha de informação desnecessária, defendendo os princípios do RGPD, concedendo apenas o bastante para que cada profissional envolvido possa realizar o seu trabalho sem impedimentos, e para que cada cliente possa ter um *insight* da sua situação RGPD, sem prejuízo dos seus princípios.

Gestor de Aplicação (SM). O Gestor de Aplicação tem acesso global a toda a aplicação, tendo privilégios de leitura, escrita em todas as funcionalidades oferecidas pela ferramenta: acesso à lista de clientes e a cada um individualmente, tendo a possibilidade de adicionar novos, viabilidade de configuração de *templates* de questionários e da matriz de dados pessoais, acesso a todas as fragilidades e recomendações registadas na plataforma, acesso aos relatórios e *dashboards* com alguns dos KPIs usados no sistema. Um gestor de aplicação, em modo 'Administração', pode também inserir novos utilizadores na plataforma, podendo definir o seu nível de privilégio até um máximo de SM também. Em suma, é um nível de privilégio destinado a quem gere a informação na totalidade no *Privacy*.

Gestor de Sistema (SYS). O Gestor de Sistema tem privilégios de configuração da plataforma em si. É reservado apenas aos utilizadores responsáveis por gerir toda a instância da ferramenta, podendo assumir características de um *power user* da aplicação em termos estruturais, através de permissão de acesso aos Parâmetros HTML e Parâmetros Texto, podendo ainda inserir dados de referência (*reference data*) e novos utilizadores (o primeiro utilizador a ser criado é o *manager*, que é SYS). Pode ainda alterar as informações dos utilizadores, algo inalcançável por níveis de privilégio inferiores.

Cliente. O Cliente pode responder a questionários que lhe são colocados, preencher matrizes de dados, consultar as fragilidades de todos os departamentos e ver os gráficos. Tem acesso global dentro do si próprio, podendo consultar todas as informações a si relativas. É um *user* relativamente limitado, não tendo privilégios de configuração.

Entidade - Auditor / Advogado. A figura do Auditor vê todos os clientes que lhes estejam associados, e por consequência, tudo o que está associado ao cliente, possuindo

acesso às configurações, mas de forma limitada (*Templates* de fragilidades, Categorias, Perguntas, *Templates* de questionários), podendo apenas consultar, não interferindo com o estado das existentes, nem criando novas. É capaz de adicionar *templates* de questionário aos clientes, fazer análises individuais a cada pergunta respondida nos questionários, e possui acesso às ferramentas de produção do relatório final. Pode ainda alterar o estágio da Matriz de Dados, inserir fragilidades e gerar relatórios. O Advogado, é em si um género de auditor, assumindo, por isso, todos os privilégios de Auditor, só mudando a descrição atribuída à entidade, a pedido de quem vai assumir essas funções. Estes dois tipos de entidades estão reservados à empresa auditora.

Entidade - Departamento. Este tipo de entidade está reservado ao cliente, mais concretamente aos seus responsáveis departamentais. Apenas vê a informação pela qual é encarregue, onde se incluem as fragilidades, matriz de dados e recomendações, só consulta e responde a questionários atribuídos ao seu departamento, é capaz de criar e atribuir tarefas relativas à sua área de operação. Um departamento pode incluir vários utilizadores.

2.3.1 *Back Office* de Administração (BA)

O BA surge como um módulo de apoio à gestão da ferramenta, sendo apenas de acesso particular e restrito, destinado a pessoal técnico especializado na gestão e configuração da aplicação. É composto por três secções diferentes:

1. Parâmetros HTML.
2. Parâmetros Texto.
3. Gestão de Utilizadores.

Parâmetros HTML

A página de **Parâmetros HTML** surge para colmatar a necessidade de ter alguma customização nas páginas da ferramenta, através do uso de parâmetros que permitirão uma personalização das mesmas, em caso de, por exemplo, a venda de instâncias da ferramenta para uso particular. Utilizadores com privilégios de 'Gestor de Sistema' (SYS), têm controlo absoluto sobre o ciclo de vida destes parâmetros, podendo criar novos, atualizar os atuais e torná-los invisíveis, enquanto que um utilizador com nível 'Gestor de Aplicação' (SM), pode consultar a lista de parâmetros existentes e o detalhe de cada um, não podendo interagir com o estado dos mesmos, nem promover a criação de novos.

Parâmetros Texto

No que concerne aos **Parâmetros Texto**, surgem para automatizar ao máximo a produção de documentos como todo o tipo relatórios, bem como a montagem dos diversos e-mails

produzidos pela ferramenta. Quanto aos privilégios de leitura e escrita, mantêm-se, podendo o nível SYS assumir um controlo total sobre o ciclo de vida dos parâmetros, enquanto que o nível SM apenas pode ler da lista geral de parâmetros e consultar, individualmente, o detalhe de cada um.

Gestão de Utilizadores

Nesta secção, é tratado tudo o que é relativo à gestão dos utilizadores, desde a sua criação, através de um endereço de *e-mail*, até à definição do seu *role* na aplicação, passando pelos detalhes do mesmo, onde é possível consultar a lista de associações do utilizador com clientes, bem como as associações a entidades. Uma vez criado o utilizador, é impossível modificá-lo, para um utilizador com nível SM ou inferior.

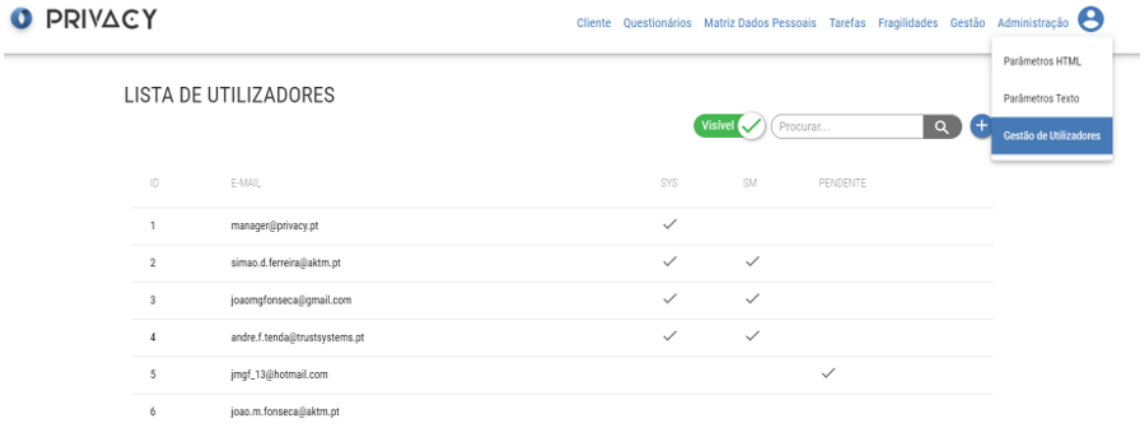

Figura 2.4: Lista de utilizadores da plataforma com representação do BA condensado no BC

2.3.2 *Back Office* de Cliente (BC)

O *Back Office* de Cliente, é a concretização da ferramenta em si. É aqui que se desenrolam todos os processos e particularidades inerentes à auditoria RGPD. Como foi referido anteriormente, um Gestor da Aplicação (SM) tem privilégios totais no que concerne à gestão da ferramenta, da informação que circula dentro desta, bem como dos conteúdos que fazem parte da mesma, pelo que a descrição do BC, se fará pelo ponto de vista de um Gestor de Aplicação, complementando a informação relativa a outros perfis com a secção de *roles*, descrita previamente.

Existe uma barra superior que coordena os acessos a todas as secções da ferramenta: Cliente, Questionários, Matriz de Dados Pessoais, Tarefas, Fragilidades, Gestão e Administração. Os dois últimos módulos são de acesso exclusivo a pessoal afeto à gestão da ferramenta e ao processo de auditoria, pelo que um perfil de cliente não tem acesso a estes. Perfis de auditor apenas acedem a um módulo de Gestão truncado, que é o estritamente necessário

ao desempenho das suas funções, podendo consultar os *templates* de questionários e fragilidades e as perguntas e categorias presentes na *pool* da ferramenta, não tendo acesso também ao menu da Administração (o *Back Office* de Administração, anteriormente referido).

Módulo de Cliente

A página do cliente surge em forma de menu com a informação relativa a si mesmo, toda condensada em sub-menus:

- **Detalhes** - Onde é possível consultar e alterar as informações do cliente e associar utilizadores que sejam pontos de contacto do cliente, bem como processos relativos à sua operação. Para além disto, existe a possibilidade de anexar documentos e notas considerados pertinentes ao processo de auditoria.

- **Template Cliente** - Nesta página é onde são disponibilizados todos os *templates* de questionários relativos ao cliente para, após a devida personalização, serem enviados para o mesmo. O Cliente não tem acesso a esta funcionalidade, sendo apenas de uso restrito ao pessoal afeto à auditoria, servindo como um estágio intermédio dos questionários, permitindo que a personalização seja efetuada, já dentro do contexto do cliente, como se observa na figura 2.5, ficando apenas associada a si, garantindo a privacidade e facilitando a gestão, não afetando os restantes *templates*, presentes na aplicação.

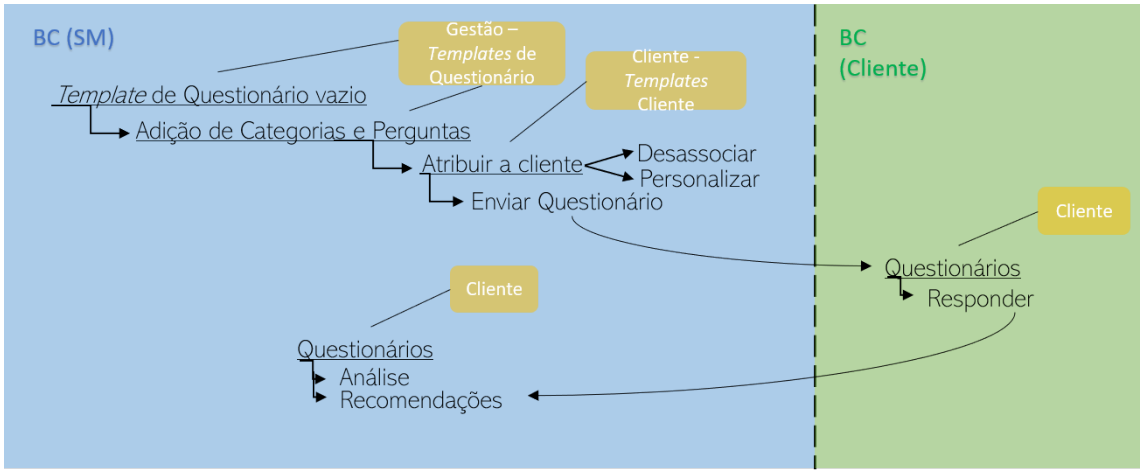

Figura 2.5: Ciclo de vida de um *template* de questionário

- **Questionários** - Nesta página estão presentes todos os *templates*, que foram concretizados em questionários, tendo sido enviados para o cliente. Após a sua criação, toda a gestão de questionários é feita aqui, incluindo a resposta, por parte do cliente, a análise, questão a questão, a recolha de informação pertinente para o relatório final e, a atribuição de recomendações relativas aos assuntos tratados em

cada questionário, tudo por parte do auditor. Para submeter o questionário, é necessário submeter a matriz de dados pessoais, referente ao processo ou tecnologia que o questionário trata.

- **Matriz Dados Pessoais** - Neste sub-menu, é possível consultar os dados pessoais envolvidos em cada processo ou tecnologia, pertencentes a departamentos da organização auditada. Cada entrada da tabela, corresponde a um processo ou tecnologia e após o clique, podemos definir, em detalhe, os dados pessoais que circulam em determinada operação da organização. A matriz tem vários estados que se alteram segundo as ações do utilizador, como é possível ver na figura 2.6.

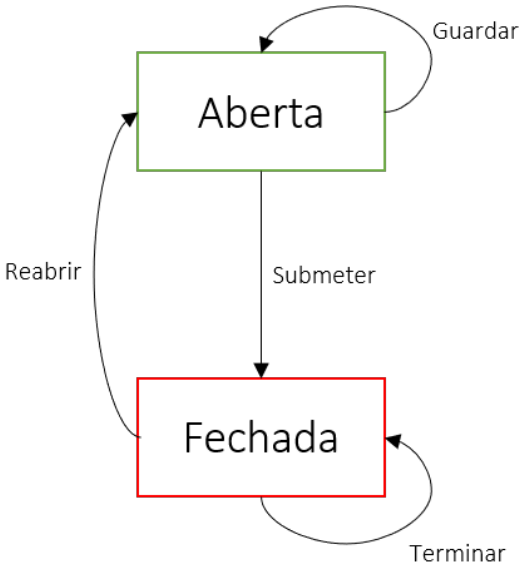

Figura 2.6: Estados da Matriz de Dados Pessoais

- **Fragilidades** - Nesta página, estão presentes todas as fragilidades imputadas ao cliente em questão. As fragilidades são a concretização das não conformidades com o RGPD, e assumem uma estrutura própria, tal como os questionários: Existem *templates* de fragilidades que contêm dentro de si, a falha potencial e uma descrição da fragilidade, bem como os tipos de fragilidades que lhes podem estar associados. Ainda dentro do *template* de fragilidade, existe uma lista de *templates* de recomendações para essa fragilidade em específico. Mais uma vez procedeu-se ao uso de *templates* por haver muitas fragilidades comuns às várias organizações, e como tal, agilizar o processo de levantamento destas, garantindo ainda assim uma certa personalização, adaptando-se ao contexto dos clientes. As fragilidades podem ser criadas neste sub-menu ou em alternativa, diretamente no questionário, relativo ao departamento e processo onde foram identificadas, anexando desde o momento da criação da fragilidade, uma recomendação para a sua mitigação. Na figura 2.7, é possível ver a relação entre os artefatos envolvidos na criação de fragilidades:

origens, origens funcionais e *templates* de fragilidades.

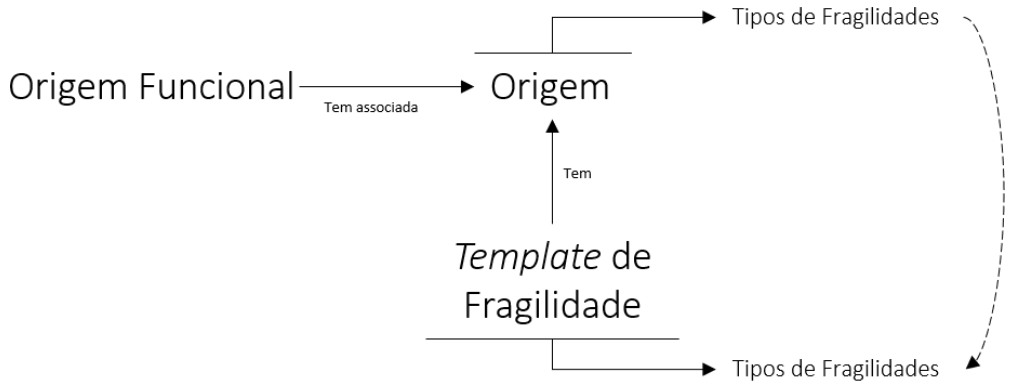

Figura 2.7: Relação entre Origens, Origens Funcionais e *Templates* de fragilidades

- **Relatórios** - Na página dos Relatórios, surge um *dashboard*, com vários gráficos dinâmicos, que depois se desdobram em informações mais detalhadas, relativos às fragilidades (número de fragilidades por departamento, número de fragilidades por processo e a evolução do número de fragilidades ao longo do tempo), ao risco (evolução do nível de risco por departamento e evolução do nível de risco por processo), recomendações (recomendações por estado por departamento e recomendações por estado por processo) e por fim, o orçamento por área de operação da organização. Existe também a possibilidade de gerar 4 tipos relatórios, um de dados pessoais, um relativo aos questionários, outra relativo aos riscos a que a organização está sujeita e o culminar de todo o processo de auditoria, o relatório final.

Módulo de Questionários, Matriz de Dados Pessoais, Fragilidades

Nestes módulos é possível ter uma visão geral sobre todos os questionários produzidos na ferramenta, todas as matrizes de dados pessoais construídas e todas as fragilidades levantadas, para utilizadores SM. Com perfil de auditor, é possível consultar todos os questionários, matrizes e fragilidades relativos a clientes aos quais o auditor é responsável por, enquanto que o Cliente vê todos os questionários, matrizes e fragilidades a si relativos. Os responsáveis departamentais, não têm acesso a esta visão geral, acedendo apenas a questionários alusivos ao seu departamento, através dos sub-menus do Cliente.

Módulo de Tarefas

Este módulo serve para dar suporte a todo o processo da auditoria e a atividades de *follow-up* da mesma, criando tarefas e concretizando recomendações em ações específicas para resolver alguns dos problemas detetados e indicar a forma como certas fragilidades devem ser endereçadas, juntando ao processo, as atualizações dos vários estágios da tarefa, permitindo *tracking* do estado da mesma, possibilitando a quem de direito, man-

ter uma perceção precisa acerca dos estado das circunstâncias pelas quais é responsável. Cada perfil tem um tipo de tarefas que pode criar, adaptado às suas necessidades, podendo criar incumbências para si, ou para responsáveis diretos que lhes estejam associados.

- Gestor de Aplicação (SM) produz tarefas do tipo:
  - *Software Manager*
  - Cliente
  - Departamento
- Cliente produz tarefas do tipo:
  - Departamento
- Auditor produz tarefas do tipo:
  - Auditor
- Departamento produz tarefas do tipo:
  - Departamento
- Advogado produz tarefas do tipo:
  - Advogado

Módulo de Administração

Este módulo é a concretização da condensação do BA no contexto do BC, formando uma única ferramenta, com tudo no mesmo domínio. Mais uma vez, é de acesso restrito a pessoal com perfil SM e SYS.

2.3.3 Arquitetura

A ferramenta apresenta uma arquitetura em camadas, visto haver 3 bem distintas que comunicam entre si: uma **camada de apresentação (FE)** que interage diretamente com o utilizador e é responsável por recolher os pedidos do mesmo, uma **camada de lógica de negócio (BE)** que é onde se processam os pedidos recolhidos na camada acima, segundo as regras do negócio, e, por fim, uma **camada de dados (BD)**, que serve para persistir todos os dados considerados necessários manter.

Em concreto, a plataforma *Privacy* é uma solução *cloud-based* que utiliza máquinas virtuais AWS EC2 com Docker instalado para abstrair o SO usado no momento da execução da ferramenta, fornecendo uma base própria para a sua execução. Tanto o BE como o FE executam em instâncias Docker distintas. O BE tem o apoio de uma cache implementada

pelo Redis, que também executa numa instância Docker própria. Diretamente ligado ao BE, está também o servidor de relatórios, mais uma imagem Docker, que serve para gerar relatórios Jasper. Com o apoio do Traefik, os pedidos são recebidos e reencaminhados para o sítio certo, havendo lugar a um balanceamento de carga caso seja necessário. Existe a presença do AWS S3 Buckets que servem para guardar a diversa documentação que circula no sistema. Existe ainda suporte de serviços AWS no envio de mensagens SMS e de *e-mails*, através do AWS SNS e AWS SES, respetivamente. É usado o AWS CloudFront como serviço de CDN e como *firewall* aplicacional, o AWS Cloud Watch como ferramenta de *logs* do sistema e o AWS Route 53 como servidor de DNS. Por fim, a camada de dados utiliza o AWS RDS para estabelecer uma base de dados PostgreSQL. Utiliza ainda, o Google reCAPTCHA como forma de mitigar acessos indesejados à plataforma.

Na generalidade do sistema, foram usadas diferentes tecnologias e serviços, para atender às diversas necessidades:

- **Google reCAPTCHA**: é um serviço gratuito da Google que visa proteger os *sites* de *spam* e de possíveis tentativas de DDoS. Essencialmente, um 'CAPTCHA' é um teste de Turing para diferenciar humanos de *bots*. Adicionando o reCAPTCHA ao site, ganha-se a possibilidade de bloquear *software* automatizado ao mesmo tempo que se permite a entrada de utilizadores legítimos, com mais facilidade que anteriormente, através de provas fornecidas involuntariamente por estes (endereços IP, *cookies*, ...), associadas a análises dos movimentos efetuados pelo rato no momento de aproximação à *checkbox* a clicar, comparadas com modelos que contêm padrões comportamentais de seres humanos, juntando análises de riscos avançadas, que acrescentam mais uma camada de filtragem a potenciais ameaças ao bom uso e funcionamento do sistema.

- **Serviços AWS**:

  - **AWS EC2**: O Amazon Elastic Compute Cloud (Amazon EC2) é um serviço Web que disponibiliza capacidade computacional segura e redimensionável na nuvem. Foi projetado para facilitar a computação em nuvem em escala na web para os *developers*. A interface de *web service* simples do EC2 permite que se obtenha e configure a capacidade com o mínimo de esforço. Oferece um controle completo dos recursos computacionais disponibilizados.

  - **AWS RDS**: Facilita a configuração, a operação e a escalabilidade de BD relacionais na nuvem. O serviço oferece capacidade económica e redimensionável e automatiza tarefas demoradas de administração, como provisionamento de *hardware*, configuração de BD, aplicação de *patches* e *backups*. Dessa forma, pode-se concentrar na performance rápida, alta disponibilidade, segurança e conformidade que os aplicativos precisam.

Benefícios

* Fácil de administrar;
* Altamente escalável;
* Disponível e resiliente;
* Rápido;
* Baixo custo;
* Seguro.

– **AWS S3 Bucket**: Recurso de armazenamento em núvem pública que armazena objetos (ficheiro + metadados). Os metadados são uma série de informações sobre o próprio objeto, como última data de modificação, tamanho do arquivo e outros metadados específicos de HTTP. É possível criar versões para os objetos guardados e é excelente em garantir disponibilidade, segurança, escalabilidade e performance.

– **AWS SES**: O Amazon Simple E-mail Service (SES) é um serviço de *e-mail* eficaz, flexível e dimensionável. Tem diversos casos de uso: *e-mails* de transacionais, de marketing e de comunicação em massa e é usado no *Privacy* para enviar notificação via *e-mail*.

Benefícios

* Rápida integração;
* Envio de mensagens com eficiência;
* Otimiza a capacidade de entrega;
* Dimensiona com segurança;

– **AWS SNS**: O Amazon Simple Notification Service (SNS) é um serviço de notificação. Fornece uma infraestrutura de baixo custo para a entrega em massa de mensagens, principalmente para utilizadores móveis. Pode enviar mensagens por SMS para 200+ países e é usado, no *Privacy*, para enviar notificações por esta via.

– **AWS Cloud Front (CDN)**: O Amazon CloudFront é um serviço rápido de rede de entrega de conteúdo (CDN) que entrega dados, vídeos, aplicativos e APIs a clientes em todo o mundo com segurança, baixa latência e altas velocidades de transferência. No caso do Privacy, para além dos serviços de CDN, usa o AWS Shield como *firewall* aplicacional em conjunto com o EC2.

Benefícios

* Acessos rápidos e globais;

    - Altamente programável;
    - Segurança no ponto de presença;
    - Forte integração com outros serviços AWS;

- **AWS Cloud Watch (Logs)**: O CloudWatch coleciona dados de monitorização e operações na forma de *logs*, métricas e eventos, oferecendo uma visualização unificada dos recursos, dos aplicativos e dos serviços executados na AWS e em servidores locais. Pode-se usar o CloudWatch para detectar comportamento anómalo nos ambientes, definir alarmes, visualizar *logs* e métricas lado a lado, executar ações automatizadas, resolver problemas e descobrir *insights* para manter os sistemas em perfeita execução.

  Benefícios

    - Capacidade de observação de uma única plataforma em vários aplicativos e infraestruturas;
    - A maneira mais fácil de recolher métricas na AWS e no local;
    - Adquirir *insights* e visibilidade operacional;
    - Extrair *insights* acionáveis com base em *logs*;
    - Melhorar o desempenho operacional e a otimização de recursos;

- **AWS Route 53 (DNS)**: O Amazon Route 53 é um *web service Domain Name System* (DNS) na nuvem altamente disponível e escalável. Foi projetado para oferecer aos *developers* e empresas uma maneira altamente confiável e económica de direcionar os utilizadores finais às aplicações *web*.

  Benefícios

    - Altamente disponível e confiável
    - Flexível
    - Desenvolvido para uso com outros serviços a AWS
    - Simples
    - Económico
    - Seguro
    - Simplifica a nuvem híbrida
    - Rápido
    - Escalável

Muitos dos serviços AWS funcionam em conjunto fornecendo outras funcionalidades resultantes da sua combinação:

  - Armazenar *templates* de CloudFormation;
  - Armazenar *templates* para serem usados nas notificações SES e SNS;
  - Usar o Route53 para direcionar tráfego web para páginas estáticas *hosted* no S3;
  - Quando um objeto é adicionado, alterado ou removido num *bucket* pode ser gerada uma entrada no CloudWatch que pode acionar numa notificação SNS;

- **Redis**: Redis é um armazenamento de estrutura de dados *in-memory open source*, usado como BD, cache e *broker* de mensagens. No *Privacy*, é usado como *cache*, para acelerar os tempos de resposta da aplicação e ajudar o sistema a escalar colocando os dados frequentemente necessários muito próximos da aplicação. Providencia alta disponibilidade via Redis Sentinel, e particionamento automático via Redis Cluster.

- **Traefik (Docker)**: Traefik é um *reverse proxy* e *load balancer* que facilita a implantação de microsserviços. O Traefik integra-se com os componentes de infraestrutura existentes e configura-se automática e dinamicamente.

- **Docker**: É uma ferramenta projetada para tornar mais fácil criar, implantar e executar aplicativos usando containers. Os containers permitem que um *developer* empacote um aplicativo com todas as partes de que precisa, como bibliotecas e outras dependências, e o implante como um pacote.

2.3.4 Falta de um Módulo de Gestão

A quantidade e complexidade de informação que circula na plataforma aumentou de sobremaneira e tornou-se difícil de gerir. Para popular a BD com dados de auditoria teria de se usar um conjunto de *scripts*, para fazer a criação de novo material, atualização do existente e a remoção de qualquer tipo de informação teria de se recorrer a *scripts* específicos também, tornaria muito difícil a construção de *templates* de questionários e de fragilidades, fazendo com que a complexidade de uso da ferramenta aumentasse, diminuindo a sua usabilidade e tornaria difícil o estabelecimento de associações entre as diversas informações. Para gerir a informação, com tudo o que envolve, era preciso ser especialista da ferramenta ou ter formação em BD para poder executar ações que se querem simples e intuitivas. Como é que os utilizadores processariam as suas ações? Teriam *scripts* pré-feitos? E tinham acesso direto à BD? Como se faria a segurança?

Surgiu assim a necessidade de criar um módulo de gestão e adicioná-lo à ferramenta, para tornar toda a gestão do material de auditoria, um assunto algo mais do que simples *scripts* de BD. Havendo um módulo capaz de gerir a informação com lógica de negócio própria no BE e uma interface no FE, adicionaram-se algumas verificações e validações

à informação que chega à BD e adicionou-se uma camada de usabilidade, facilitando as ações do utilizador, através de uma linguagem mais percetível para ele, que anula a necessidade de o mesmo ter que colocar as mãos em código aquando do uso da plataforma, focando-se só nos aspetos inerentes às suas funções.

2.4 Sumário

Este capítulo introduziu conceitos relacionados com a proteção de dados e as novas formas como esta deve ser endereçada, para manter a privacidade dos titulares, abordou alguns aspetos das auditorias RGPD, e algumas das boas práticas decorrentes de um bom tratamento de dados, tais como o estabelecimento de políticas de privacidade (para o cliente da organização) e segurança (para consumo interno à organização).

Foram também descritas ferramentas GRC que fizeram parte do processo geral de produção da solução, tendo sido feita uma avaliação para verificar se com as configurações certas podiam resolver o problema proposto. Apesar de terem sido excluídas como resposta ao problema, algumas das suas funcionalidades foram cogitadas para inspirarem funções da ferramenta a implementar.

Por fim, foi descrita a solução implementada, havendo lugar a um olhar global sobre a mesma, as suas funcionalidades, os seus usos e perfis de utilização, bem como uma visão geral da arquitetura, das tecnologias usadas e a motivação para a falta / existência do Módulo de Gestão.

O próximo capítulo apresenta o Módulo de Gestão em mais detalhe.

Capítulo 3

Módulo de Gestão

No capítulo anterior foram descritos vários conceitos que giram em torno da proteção de dados pessoais, informações acerca das auditorias RGPD, ferramentas de suporte à garantia de conformidade e a ferramenta *Privacy*. O maior enfoque neste capítulo, é no **módulo de gestão**. A implementação foi dividida em *backend* (BE) e *front end* (FE), tendo sido utilizadas as linguagens Java e Angular3 + TypeScript, respetivamente.

Neste capítulo, descreve-se o módulo de gestão, de forma completa, os requisitos do módulo e de explicar o *flow* de implementação nas duas camadas de implementação referidas anteriormente (BE e FE).

3.1 Descrição

O módulo de gestão é relativo à gestão da informação do processo de auditoria que circula dentro da plataforma e é integrado pelo sub-menus relativos a essa: *templates* de questionário, categorias, perguntas, entidades, processos, dados pessoais, tipos de fragilidades, origens, origens funcionais e *templates* de fragilidades. É neste módulo que se faz toda a inserção da informação anterior, bem como as suas atualizações de estado. Acrescentar novo material, não só contribui para aumentar a *pool* de informação de auditoria existente, o que poderá ajudar em futuros projetos, como permite à ferramenta manter-se atual, customizável e sujeita a mudanças na regulamentação, possibilitando a sua evolução em conjunto e concordância com as suas circunstâncias. Por se tratar de material usado para realizar a auditoria é de acesso exclusivo a pessoal afeto à mesma, apesar de não ter todas as funcionalidades acessíveis a pessoal não-SM. Assim, apenas os perfis SM têm acesso a criar e a modificar informações contidas no módulo de gestão, para gerirem a informação presente na instância, garantindo o controlo da mesma no que toca à quantidade e qualidade do material de auditoria que integra a mesma, não deixando capacidades potencialmente perigosas na mão de quem não deve.

Veio fornecer uma interface para ajudar a estabelecer ligações entre informações presentes na ferramenta, adicionar novo material, renovar o desatualizado e remover/desa-

tivar aquele considerado ultrapassado, tornando este tipo de gestão muito mais intuitiva, imediata e de fácil execução.

3.1.1 Arquitetura

O módulo de gestão divide-se pelas 3 camadas descritas anteriormente, tendo uma interface própria para interagir no FE, as suas regras de negócio no BE e dados a si relativos persistidos na BD. Caracteriza-se por ser o módulo que permite o arranque do uso ferramenta, pois é através deste que se insere a informação vital para todas as partes inerentes aos processos de auditoria que passam pelo sistema. O módulo de gestão, por ser aquele que fornece material para todos os outros, tem ligações com todos os outros módulos:

- ***Templates* de Questionário** fornece dados ao módulo de questionários;
- **Categorias e Perguntas** fornecem dados ao módulo de Cliente e ao próprio módulo de gestão aquando da construção ou atualização de *templates* de questionário;
- **Entidades e Processos** fornecem dados ao módulo de cliente aquando do estabelecimento dos processos da empresa, bem como na definição dos seus departamentos, de pessoal de âmbito legal e de pessoal auditor como diferentes tipos de entidades, dentro da organização, o que alimentará por si, o módulo de tarefas;
- **Dados Pessoais** providencia dados ao módulo das matrizes de dados pessoais, que por sua vez fornece o módulo de questionários;
- **Tipos de Fragilidades, Origens, Origens Funcionais e *Templates* de Fragilidades** trocam dados entre si, alimentando por isso não só o próprio módulo de gestão, mas também o módulo de fragilidades, através do fornecimento dos *templates*, que incluem os tipos de fragilidades e *templates* de recomendações, tudo associado à própria fragilidade.

3.2 Requisitos do Módulo

Qualquer módulo de *software* tem um conjunto de características que deve reunir, tanto a nível de funcionalidades do próprio (funcionais), como a nível do uso da aplicação (não funcionais). As funções do sistema integram os requisitos funcionais e conceitos como eficiência, fiabilidade e usabilidade fazem parte dos requisitos não funcionais, que evocam premissas de qualidade na execução do *software* não diretamente relacionadas com a presença, ou não, de determinada funcionalidade. Como tal foram definidos os requisitos do módulo.

3.2.1 Requisitos Funcionais

Nesta secção define-se os requisitos funcionais de todos os sub-módulos pertencentes ao módulo de gestão e exprime-se os diagramas de casos de uso referentes a cada sub-módulo.

Templates de Questionário

Tabela 3.1 lista os requisitos funcionais do sub-módulo '*Templates de Questionário*' e a figura 3.1 exprime o diagrama de casos de uso do sub-módulo '*Templates* de Questionário'.

Tabela 3.1: Requisitos funcionais dos Templates de Questionário.

ID	Requisito	Descrição
TQ-L-1	Consultar os *templates* existentes	Deve ser possível consultar os *templates* com o mínimo de informação: Código, Versão, Idioma, Nome e Descrição
TQ-L-2	Procurar *templates* por campo	Deve ser possível fazer uma procura por qualquer um dos campos referidos anteriormente
TQ-L-3	Alternar visão da lista	Deve ser possível alternar entre uma visão geral e uma visão que contemple apenas os templates ativos
TQ-L-4	Criar novos *templates* de questionário	Deve ser possível criar novos *templates* de questionário definindo seu idioma e nome
TQ-L-5	Clonar *templates* existentes	Deve ser possível clonar *templates* existentes, mantendo todas as particularidades do original (categorias e perguntas)
TQ-D-1	Consultar detalhes do *template*	Deve ser possível consultar no detalhe do *template* todas as suas informações de forma completa
TQ-D-2	Alterar detalhes do *template*	Deve ser possível alterar o Nome e a Descrição do *template*
TQ-D-3	Desativar *template*	Deve ser possível desativar o *template*, através de um *toggle* no início do detalhe do mesmo
TQ-D-4	Gerir categorias do questionário	Deve ser possível adicionar ou remover categorias (existentes ou novas), bem como consultar a lista de categorias já associadas ao *template* e alterar a sua ordem
TQ-D-5	Gerir perguntas do questionário	Deve ser possível adicionar ou remover perguntas (existentes ou novas) e alterar a sua ordem, alterando o conteúdo do questionário
TQ-D-6	Consultar lista de clientes associados	Deve ser possível consultar a lista de clientes a que dado *template* foi associado, com a possibilidade de filtrar por todos os campos da tabela: Código e Nome

Continua na próxima página

Tabela 3.1 – continuação da página prévia

ID	Requisito	Descrição
TQ-D-7	Consultar versões do *template*	Deve ser possível consultar as diferentes versões de dum dado *template*

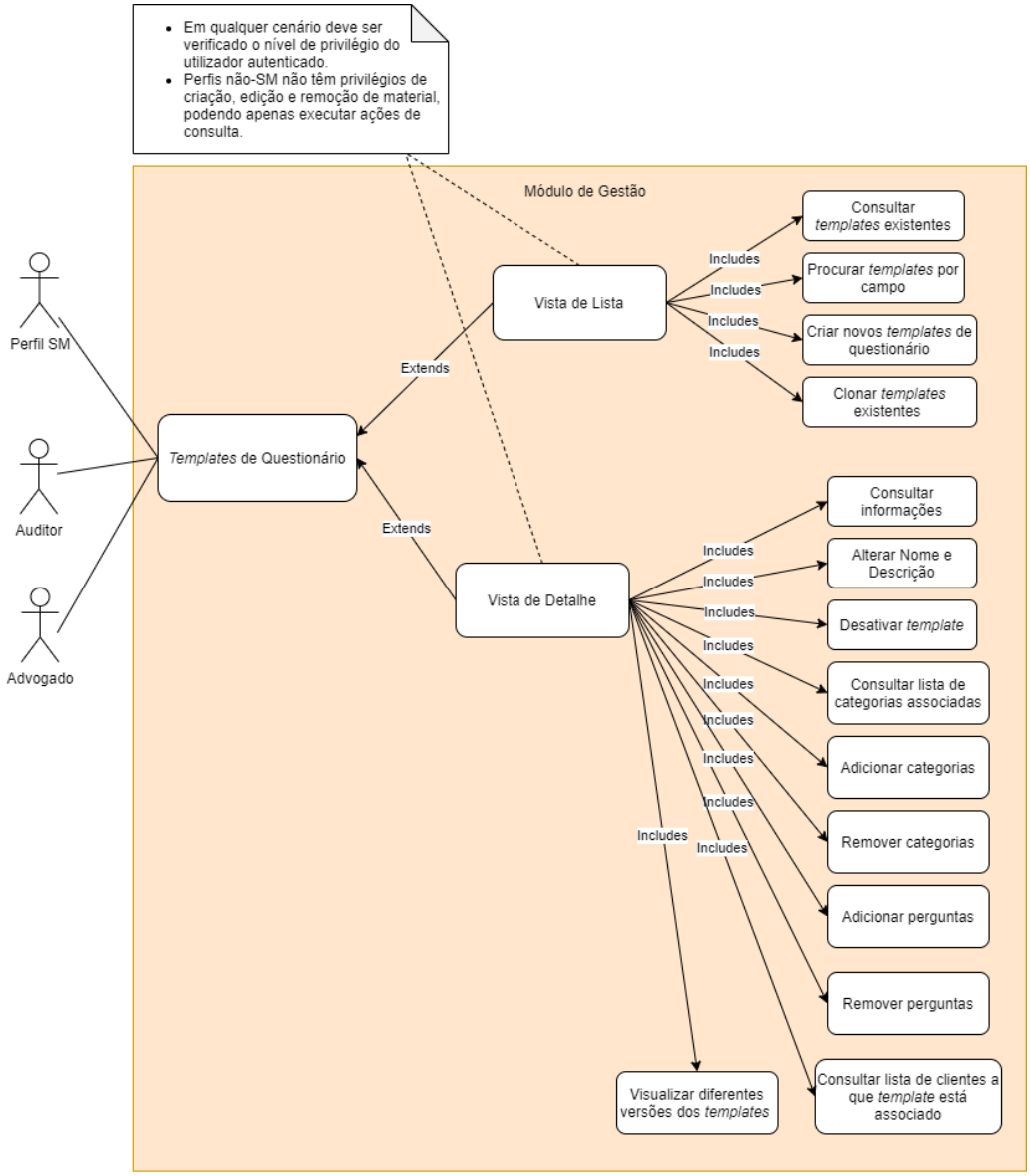

Figura 3.1: Diagrama de Casos de Uso dos *Templates* de Questionário

Categorias

Tabela 3.2 lista os requisitos funcionais do sub-módulo 'Categorias' e a figura 3.2 exprime o diagrama de casos de uso do sub-módulo 'Categorias'.

Tabela 3.2: Requisitos funcionais das Categorias.

ID	Requisito	Descrição
C-L-1	Consultar as categorias existentes	Deve ser possível consultar as categorias existentes com o mínimo de informação: Código, Idioma, Nome e Descrição
C-L-2	Filtrar categorias por campo	Deve ser possível fazer uma filtragem por qualquer um dos campos referidos anteriormente
C-L-3	Alternar visão da lista	Deve ser possível alternar entre uma visão geral e uma visão que contemple apenas as categorias ativas
C-L-4	Criar novas categorias	Deve ser possível criar novas categorias definindo seu idioma e nome
C-D-1	Consultar detalhes da categoria	Deve ser possível consultar no detalhe da categoria todas as suas informações de forma completa
C-D-2	Alterar detalhes da categoria	Deve ser possível alterar o Nome e a Descrição da categoria
C-D-3	Desativar categoria	Deve ser possível desativar a categoria, através de um *toggle* no início do detalhe da mesma
C-D-4	Gerir perguntas associadas	Deve ser possível consultar uma lista de perguntas associadas a dada categoria, com possibilidade de filtragem por todos os campos da tabela: Código, Estado e Descrição
C-D-5	Consultar metadados da categoria	Deve ser possível consultar metadados da categoria: Último utilizador a alterar e Data da última alteração

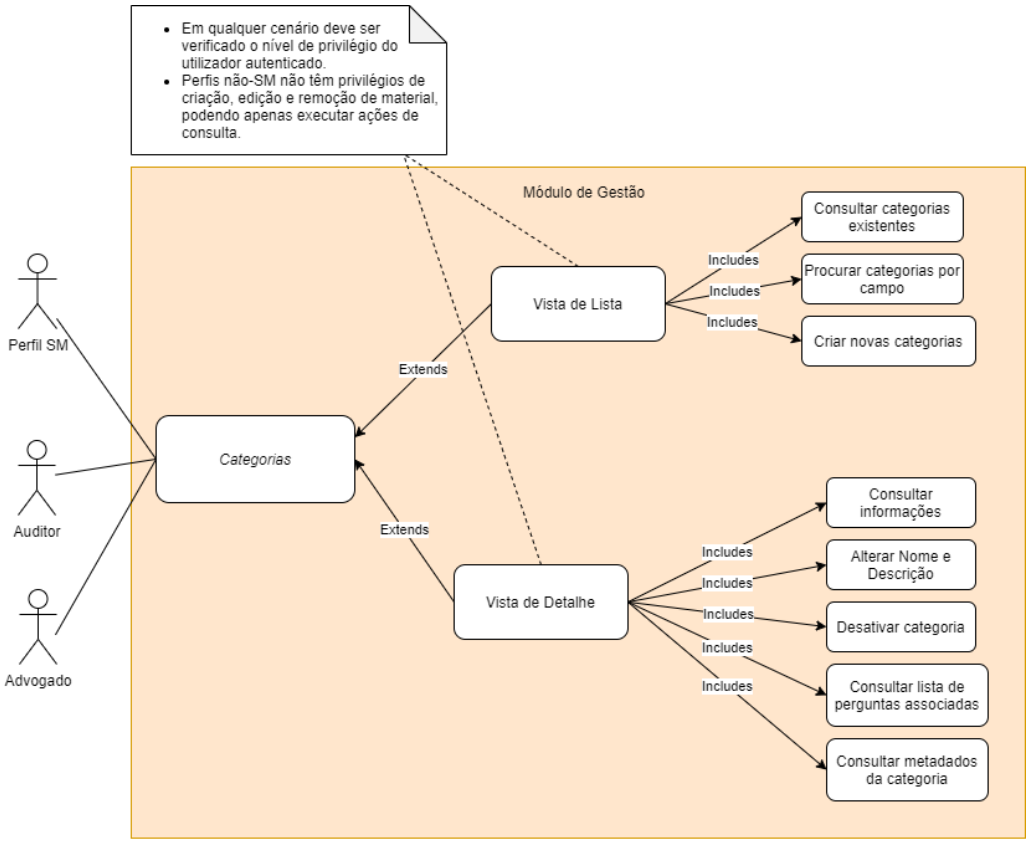

Figura 3.2: Diagrama de Casos de Uso das Categorias

Perguntas

Tabela 3.3 lista os requisitos funcionais do sub-módulo 'Perguntas' e a figura 3.3 exprime o diagrama de casos de uso do sub-módulo 'Perguntas'.

Tabela 3.3: Requisitos funcionais das Perguntas.

ID	Requisito	Descrição
P-L-1	Consultar as perguntas existentes	Deve ser possível consultar as perguntas existentes com o mínimo de informação: Código, Idioma e Resumo
P-L-2	Procurar perguntas por campo	Deve ser possível fazer uma procura por qualquer um dos campos referidos anteriormente
P-L-3	Alternar visão da lista	Deve ser possível alternar entre uma visão geral e uma visão que contemple apenas as perguntas ativas
P-L-4	Criar novas perguntas	Deve ser possível criar novas perguntas definindo seu idioma e conteúdo
P-L-5	Clonar perguntas existentes	Deve ser possível clonar perguntas existentes mantendo as características da original

Continua na próxima página

Tabela 3.3 – continuação da página prévia

ID	Requisito	Descrição
P-D-1	Consultar detalhes da pergunta	Deve ser possível consultar, no detalhe da pergunta, todas as suas informações de forma completa
P-D-2	Alterar detalhes da pergunta	Deve ser possível alterar o Resumo e o texto relativo ao conteúdo da pergunta
P-D-3	Desativar pergunta	Deve ser possível desativar a pergunta, através de um *toggle* no início do detalhe da mesma
P-D-4	Gerir categorias associadas	Deve ser possível consultar uma lista de categorias associadas a dada pergunta, com possibilidade de alternar vista geral e vista das categorias com associação ativa à pergunta. Deve haver também a possibilidade de filtragem por todos os campos da tabela: Código, Estado, Descrição e Nome
P-D-5	Associar categoria existente	Deve ser possível associar uma categoria (existente), bem como alterar o estado de associação com categorias que tenham sido associadas anteriormente
P-D-6	Consultar metadados da pergunta	Deve ser possível consultar metadados da pergunta: Último utilizador a alterar e Data da última alteração

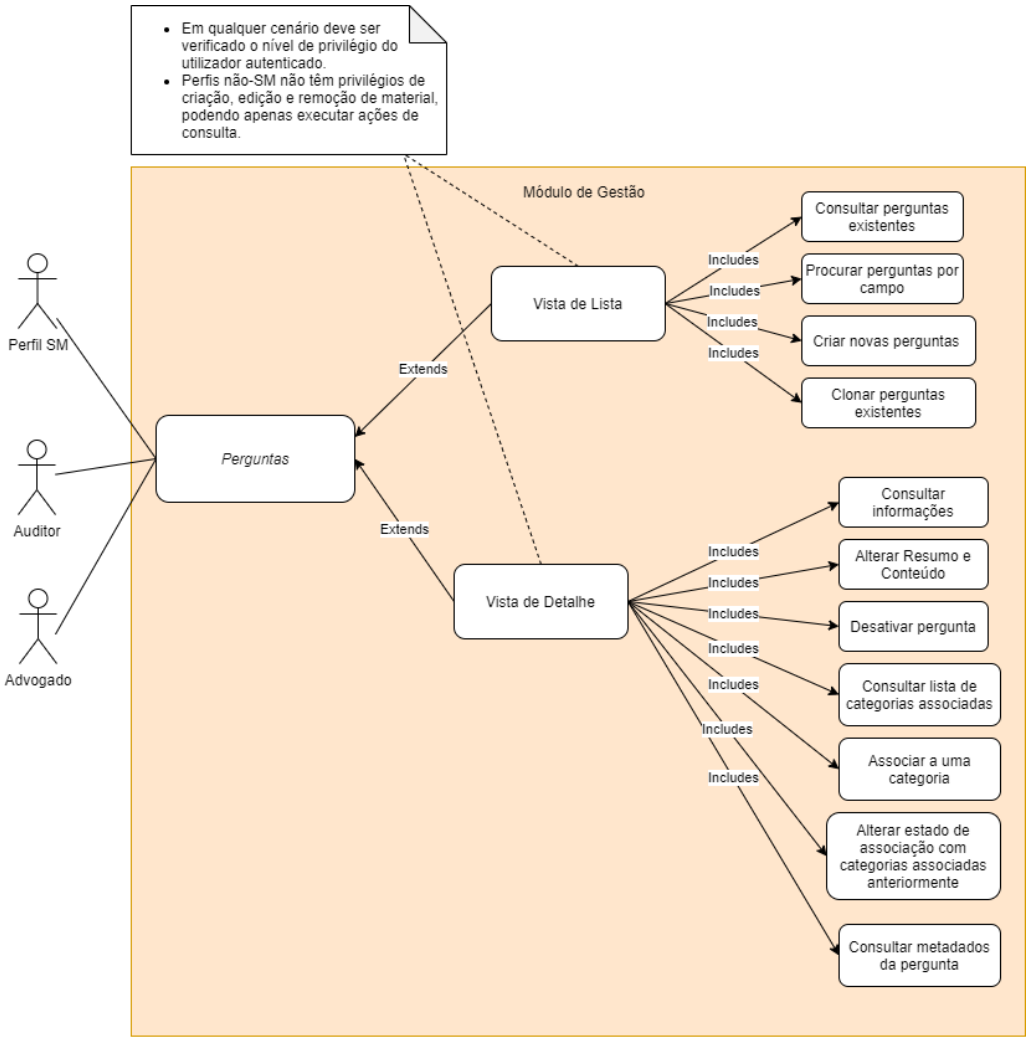

Figura 3.3: Diagrama de Casos de Uso das Perguntas

Entidades

Tabela 3.4 lista os requisitos do sub-módulo 'Entidades' e a figura 3.4 exprime o diagrama de casos de uso do sub-módulo 'Entidades'.

Tabela 3.4: Requisitos funcionais das Entidades.

ID	Requisito	Descrição
E-L-1	Consultar as entidades existentes	Deve ser possível consultar as entidades existentes, com um mínimo de informação: Código, Nome e Tipo
E-L-2	Procurar entidades por campo	Deve ser possível fazer uma procura por qualquer um dos campos referidos anteriormente
E-L-3	Alternar visão da lista	Deve ser possível alternar entre uma visão geral e uma visão que contemple apenas as entidades ativas

Continua na próxima página

Tabela 3.4 – continuação da página prévia

ID	Requisito	Descrição
E-L-4	Criar novas entidades	Deve ser possível criar novas entidades e definir o seu nome e tipo no momento da criação
E-D-1	Consultar detalhes da entidade	Deve ser possível consultar, no detalhe da entidade, todas as suas informações de forma completa
E-D-2	Alterar detalhes da entidade	Deve ser possível alterar o Nome da entidade
E-D-3	Desativar entidade	Deve ser possível desativar a entidade, através de um *toggle* no início do detalhe da mesma
E-D-4	Gerir utilizadores e clientes associados	Deve ser possível consultar uma lista de utilizadores e clientes associados a dada entidade, com possibilidade de alternar vista geral e vista dos utilizadores e clientes com associação ativa à entidade. Deve haver também a possibilidade de filtragem por todos os campos da tabela: ID, Estado, E-mail
E-D-5	Associar utilizador e/ou cliente existente	Deve ser possível associar um utilizador e um cliente, bem como alterar o estado de associação de utilizadores e clientes que tenham sido associados anteriormente
E-D-6	Consultar metadados da entidade	Deve ser possível consultar metadados da entidade: Último utilizador a alterar e Data da última alteração
E-D-7	Associar notas	Deve ser possível associar notas de texto à entidade

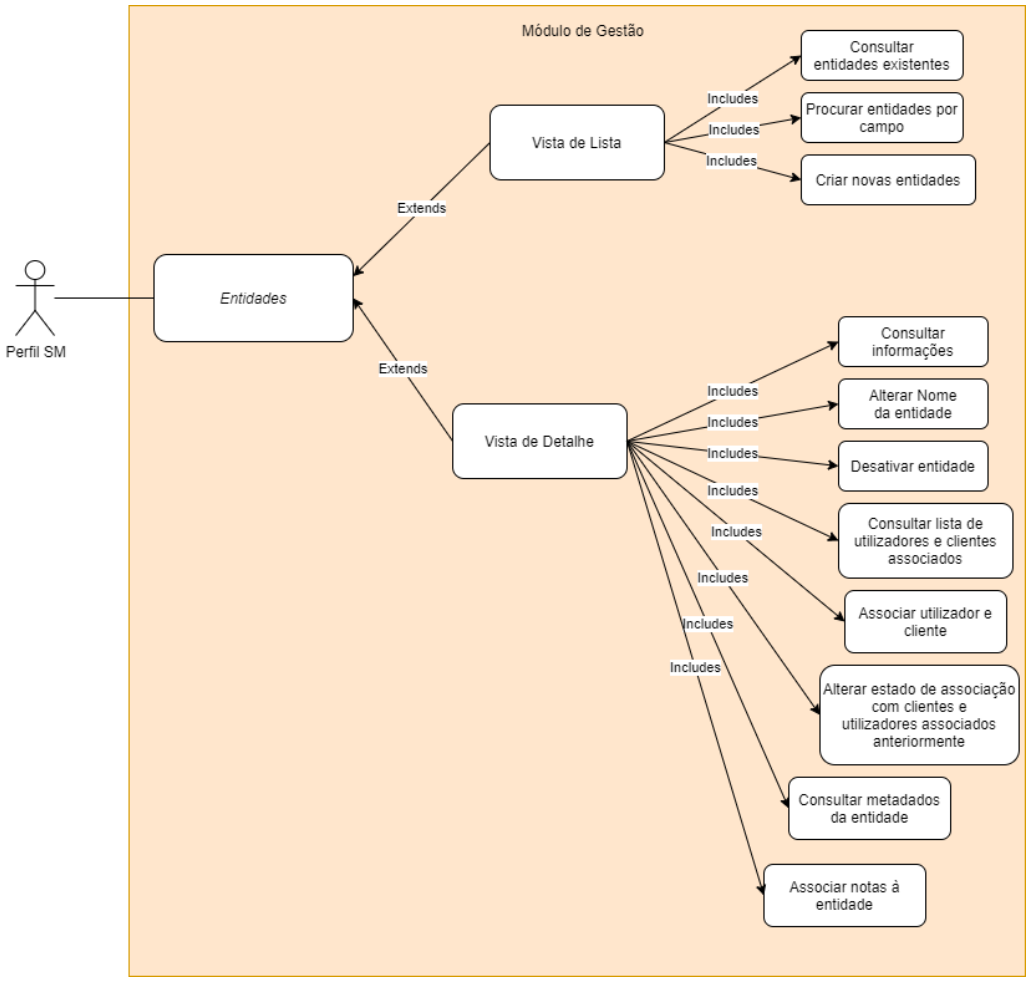

Figura 3.4: Diagrama de Casos de Uso das Entidades

Processos

Tabela 3.5 lista os requisitos funcionais do sub-módulo 'Processos' e a figura 3.5 exprime o diagrama de casos de uso do sub-módulo 'Processos'.

Tabela 3.5: Requisitos funcionais dos Processos.

ID	Requisito	Descrição
Pr-L-1	Consultar os processos existentes	Deve ser possível consultar os processos existentes, com um mínimo de informação: Código, Idioma e Nome
Pr-L-2	Filtrar processos por campo	Deve ser possível fazer uma filtragem por qualquer um dos campos referidos anteriormente
Pr-L-3	Alternar visão da lista	Deve ser possível alternar entre uma visão geral e uma visão que contemple apenas os processos ativos

Continua na próxima página

Tabela 3.5 – continuação da página prévia

ID	Requisito	Descrição
Pr-L-4	Criar novos processos	Deve ser possível criar novos processos e definir o seu idioma e nome no momento da criação
Pr-D-1	Consultar detalhes do processo	Deve ser possível consultar, no detalhe do processo, todas as suas informações de forma completa, bem como os metadados do processo: Último utilizador a alterar e Data da última alteração
Pr-D-2	Alterar detalhes do processo	Deve ser possível alterar o Nome e Descrição do processo
Pr-D-3	Desativar processo	Deve ser possível desativar o processo, através de um *toggle* no início do detalhe do mesmo

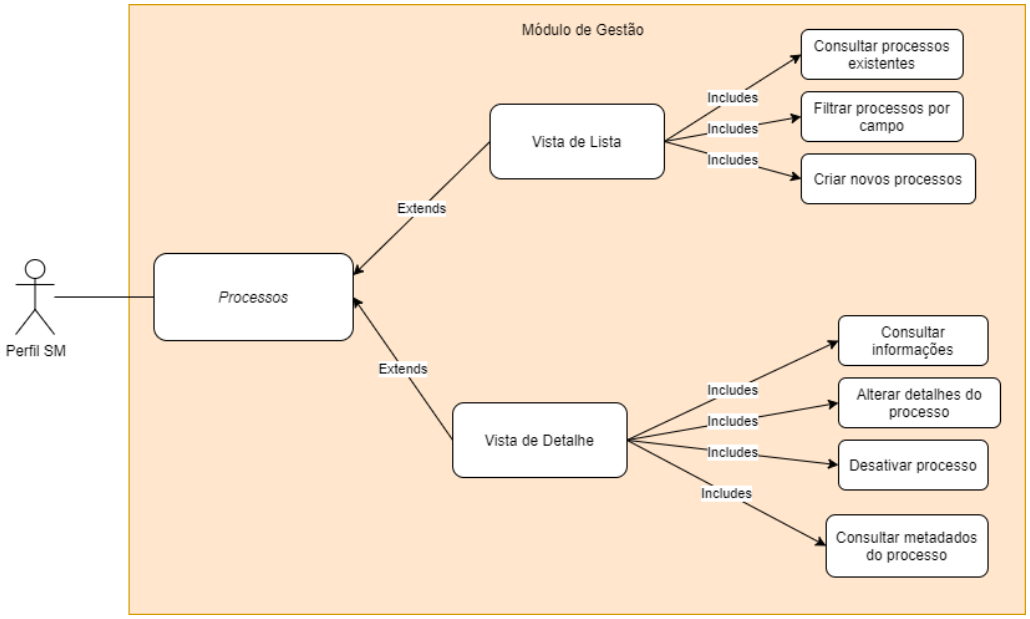

Figura 3.5: Diagrama de Casos de Uso dos Processos

Dados Pessoais

Tabela 3.6 lista os requisitos funcionais do sub-módulo 'Dados Pessoais' e a figura 3.6 exprime o diagrama de casos de uso do sub-módulo 'Dados Pessoais'.

Tabela 3.6: Requisitos funcionais dos Dados Pessoais.

ID	Requisito	Descrição
DP-L-1	Consultar os dados pessoais existentes	Deve ser possível consultar os dados pessoais existentes, com um mínimo de informação: Código, Idioma, Criticidade, Nome e Grupos e Categorias
DP-L-2	Filtrar dados pessoais por campo	Deve ser possível fazer uma filtragem por qualquer um dos campos referidos anteriormente
DP-L-3	Alternar visão da lista	Deve ser possível alternar entre uma visão geral e uma visão que contemple apenas os dados pessoais ativos
DP-L-4	Criar novos dados pessoais	Deve ser possível criar novos dados pessoais e definir o seu nome e idioma no momento da criação
DP-D-1	Consultar detalhes do dado pessoal	Deve ser possível consultar, no detalhe do dado pessoal, todas as suas informações de forma completa, bem como os metadados do dado pessoal: Último utilizador a alterar e Data da última alteração
DP-D-2	Alterar detalhes do dado pessoal	Deve ser possível alterar o Nome, o nível de Criticidade e a Ordem do dado pessoal
DP-D-3	Desativar dado pessoal	Deve ser possível desativar o dado pessoal, através de um *toggle* no início do detalhe do mesmo
DP-D-4	Gerir grupos e categorias	Deve ser possível consultar a listagem de grupos e categorias em que certo dado pessoal se insere, e filtrar a lista por esses dois campos
DP-D-5	Associar dado pessoal a grupos e categorias diferentes	Deve ser possível adicionar o dado pessoal a diferentes grupos e categorias

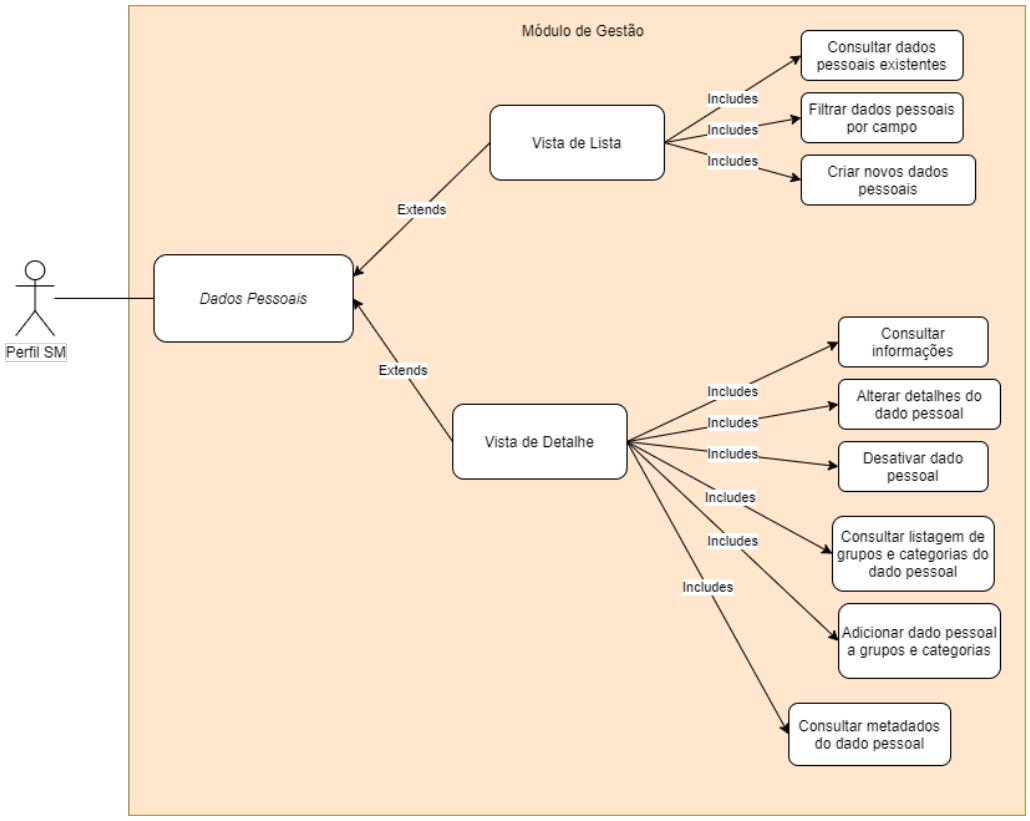

Figura 3.6: Diagrama de Casos de Uso dos Dados Pessoais

Tipos de Fragilidades

Tabela 3.7 lista os requisitos funcionais do sub-módulo 'Tipos de Fragilidades' e a figura 3.7 exprime o diagrama de casos de uso do sub-módulo 'Tipos de Fragilidades'.

Tabela 3.7: Requisitos funcionais dos Tipos de Fragilidades.

ID	Requisito	Descrição
TiF-L-1	Consultar os tipos de fragilidades existentes	Deve ser possível consultar os tipos de fragilidades existentes, com um mínimo de informação: Código, Idioma e Nome
TiF-L-2	Filtrar tipos de fragilidades por campo	Deve ser possível fazer uma filtragem por qualquer um dos campos referidos anteriormente
TiF-L-3	Alternar visão da lista	Deve ser possível alternar entre uma visão geral e uma visão que contemple apenas os tipos de fragilidades ativos
TiF-L-4	Criar novos dados pessoais	Deve ser possível criar novos tipos de fragilidades e definir o seu nome e idioma no momento da criação

Continua na próxima página

Tabela 3.7 – continuação da página prévia

ID	Requisito	Descrição
TiF-D-1	Consultar detalhes do tipo de fragilidade	Deve ser possível consultar, no detalhe do tipo de fragilidade, todas as suas informações de forma completa, bem como os metadados do tipo de fragilidade: Último utilizador a alterar e Data da última alteração
TiF-D-2	Alterar detalhes do tipo de fragilidade	Deve ser possível alterar o Nome do tipo de fragilidade
TiF-D-3	Desativar tipo de fragilidade	Deve ser possível desativar o tipo de fragilidade, através de um *toggle* no início do detalhe do mesmo

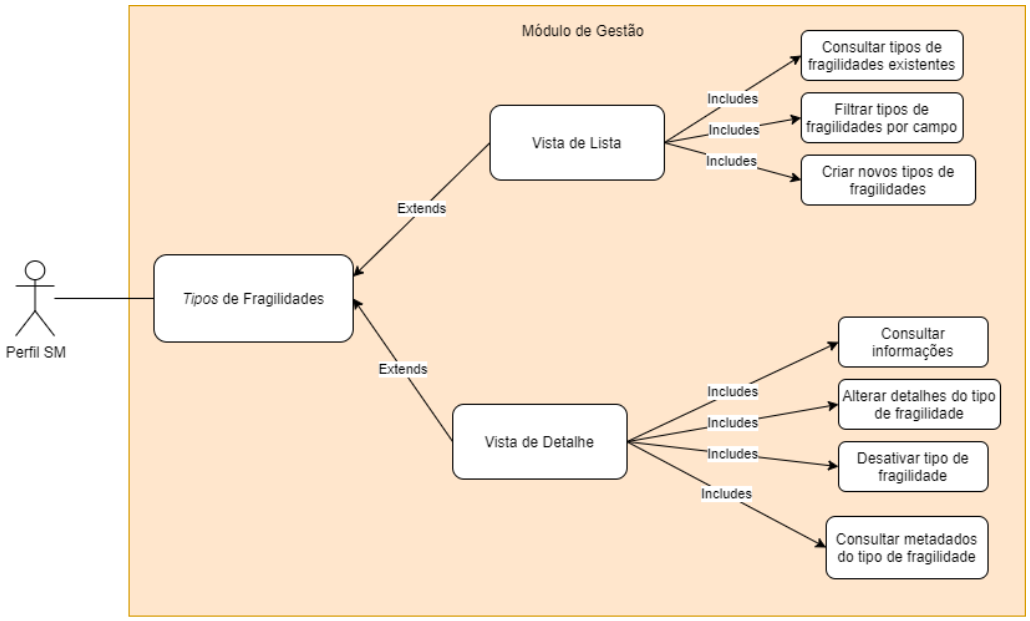

Figura 3.7: Diagrama de Casos de Uso dos Tipos de Fragilidades

Origens

Tabela 3.8 lista os requisitos funcionais do sub-módulo 'Origens' e a figura 3.8 exprime o diagrama de casos de uso do sub-módulo 'Origens'.

Tabela 3.8: Requisitos funcionais das Origens.

ID	Requisito	Descrição
O-L-1	Consultar as origens existentes	Deve ser possível consultar as origens existentes, com um mínimo de informação: Código, Idioma e Nome
O-L-2	Filtrar origens por campo	Deve ser possível fazer uma filtragem por qualquer um dos campos referidos anteriormente
O-L-3	Alternar visão da lista	Deve ser possível alternar entre uma visão geral e uma visão que contemple apenas as origens ativas
O-L-4	Criar novas origens	Deve ser possível criar novas origens e definir o seu nome e idioma no momento da criação
O-D-1	Consultar detalhes da origem	Deve ser possível consultar, no detalhe da origem, todas as suas informações de forma completa
O-D-2	Alterar detalhes da origem	Deve ser possível alterar o Nome e definir o Tipo de Fragilidade da origem
O-D-3	Desativar origem	Deve ser possível desativar a origem, através de um *toggle* no início do detalhe da mesma
O-D-4	Consultar metadados da origem	Deve ser possível consultar metadados da origem: Último utilizador a alterar e Data da última alteração

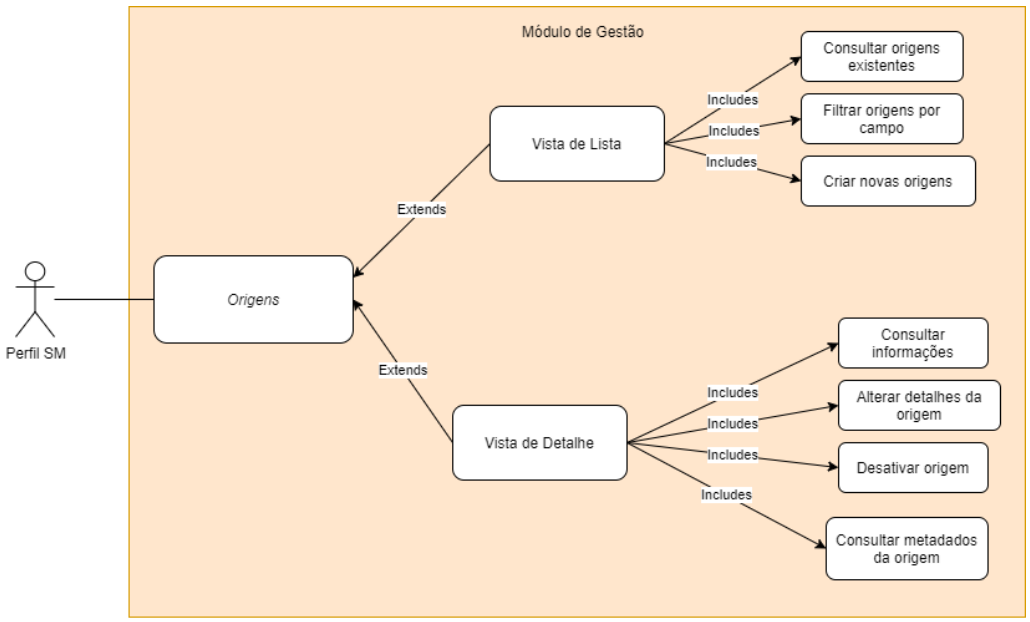

Figura 3.8: Diagrama de Casos de Uso das Origens

Origens Funcionais

Tabela 3.9 lista os requisitos funcionais do sub-módulo 'Origens Funcionais' e a figura 3.9 exprime o diagrama de casos de uso do sub-módulo 'Origens Funcionais'.

Tabela 3.9: Requisitos funcionais das Origens Funcionais.

ID	Requisito	Descrição
OF-L-1	Consultar as origens funcionais existentes	Deve ser possível consultar as origens existentes, com um mínimo de informação: Código, Idioma, Nome e Origem Associada
OF-L-2	Filtrar origens funcionais por campo	Deve ser possível fazer uma filtragem por qualquer um dos campos referidos anteriormente
OF-D-1	Consultar detalhes da origem funcional	Deve ser possível consultar, no detalhe da origem funcional, todas as suas informações de forma completa
OF-D-2	Alterar detalhes da origem funcional	Deve ser possível alterar o Nome e definir que Origem está associada à origem funcional
OF-D-3	Consultar metadados da origem funcional	Deve ser possível consultar metadados da origem funcional: Último utilizador a alterar e Data da última alteração

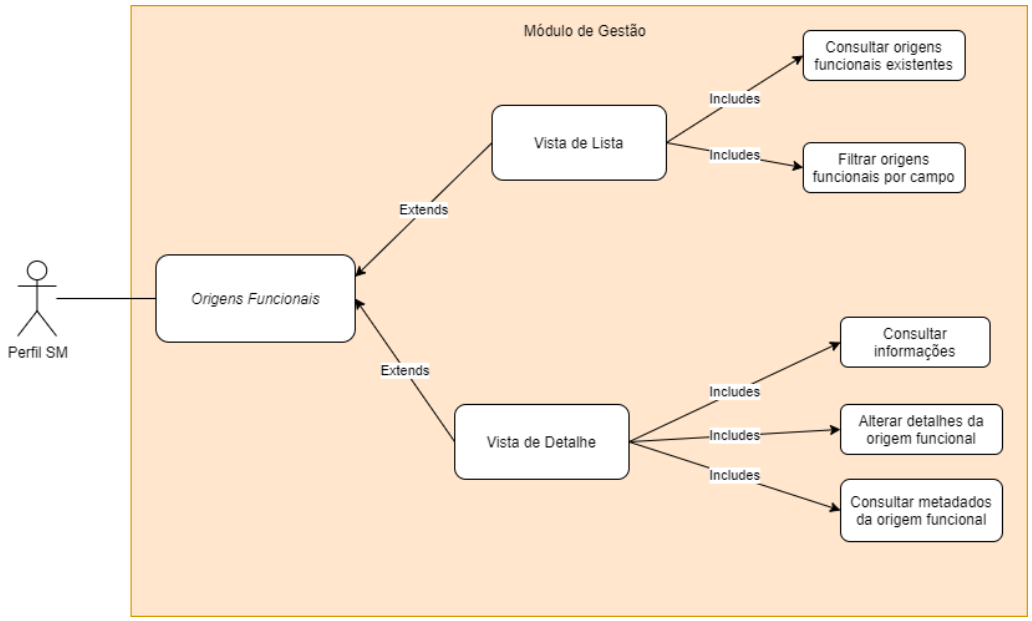

Figura 3.9: Diagrama de Casos de Uso das Origens Funcionais

Templates de Fragilidades

Tabela 3.10 lista os requisitos funcionais do sub-módulo '*Templates* de Fragilidades' e a figura 3.10 exprime o diagrama de casos de uso do sub-módulo '*Templates* de Fragilidades'.

Tabela 3.10: Requisitos funcionais dos *Templates* de Fragilidades.

ID	Requisito	Descrição
TeF-L-1	Consultar os *templates* de fragilidades existentes	Deve ser possível consultar os *templates* de fragilidades existentes, com um mínimo de informação: Código, Idioma e Falha Potencial
TeF-L-2	Filtrar os *templates* de fragilidades por campo	Deve ser possível fazer uma filtragem por qualquer um dos campos referidos anteriormente
TeF-L-3	Alternar visão da lista	Deve ser possível alternar entre uma visão geral e uma visão que contemple apenas os *templates* de fragilidades ativos
TeF-L-4	Criar novos *templates* de fragilidades	Deve ser possível criar novos *templates* de fragilidades e definir o seu idioma, falha de potencial e tipos de fragilidades no momento da criação
TeF-D-1	Consultar detalhes do *template* de fragilidade	Deve ser possível consultar, no detalhe do *template* de fragilidade, todas as suas informações de forma completa
TeF-D-2	Alterar detalhes do *template* de fragilidade	Deve ser possível alterar a Falha Potencial, a Descrição e os Tipo de Fragilidades que lhe estão associados
TeF-D-3	Gerir *templates* de recomendações associadas	Deve ser possível consultar uma lista com *templates* de recomendações associadas existentes, e criar novos, definindo a ação corretiva e uma descrição; Deve ainda estar disponível uma forma de filtrar a lista pelos campos existentes: Açãao Corretiva e Descrição, podendo ainda filtrar a lista pelo estado da associação entre *template* de fragilidade e *template* de recomendação
TeF-D-4	Alterar estado da associação entre *templates* de fragilidade e de recomendação	Deve ser possível alterar o estado da associação entre *templates* de fragilidade e de recomendação
TeF-D-5	Desativar *template*	Deve ser possível desativar o *template* de fragilidade, através de um *toggle* no início do detalhe da mesma
TeF-D-6	Consultar metadados do *template* de fragilidade	Deve ser possível consultar metadados do *template* de fragilidade: Último utilizador a alterar e Data da última alteração

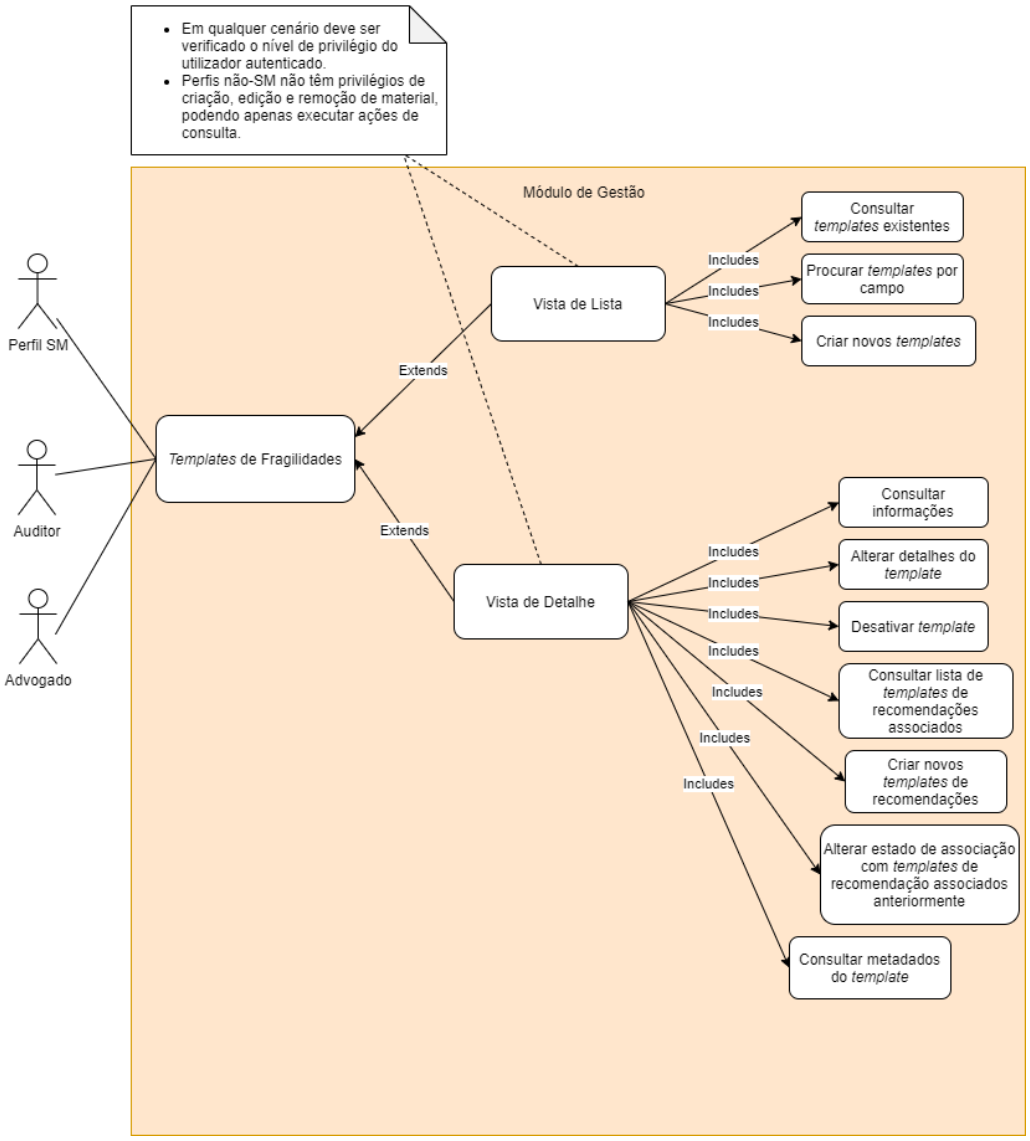

Figura 3.10: Diagrama de Casos de Uso dos *Templates* de Fragilidades

Geral

Em geral, existem alguns requisitos que são comuns a todos os sub-módulos referidos anteriormente. Assim, não deve ser possível a utilizadores sem privilégios para tal, consultar, adicionar, remover e atualizar material contido no módulo de gestão. Para perfis de Auditor, apenas deve ser possível consultar e usar a informação contida neste módulo, sem poder proceder a alterações. Para perfis de Cliente, o módulo de gestão não deverá ser visível.

3.2.2 Requisitos Não Funcionais

Para além das cores que a ferramenta deveria apresentar, que seriam da palete de cores da empresa, não foram definidos requisitos não funcionais específicos. Ainda assim, para uma aplicação deste contexto, foram garantidas implicitamente algumas premissas de qualidade no uso do módulo, tais como **usabilidade**, que se define como a facilidade que um utilizador pode aprender a operar, preparar *inputs*, interpretar *outputs* de um sistema ou componente, **escalabilidade**, que versa acerca da facilidade com que o sistema pode crescer em tamanho, mantendo as suas propriedades e qualidades, **segurança**, que é a capacidade de um sistema gerir e proteger a informação sensível e resistir a utilizações não autorizadas, **disponibilidade**, que é a probabilidade de o sistema estar a operar corretamente quando requerido e por fim, a **portabilidade**, que é a facilidade com que se pode correr o sistema noutros ambientes de execução.

A definição explícita e implementação deste tipo de requisitos ficou reservada para trabalho futuro.

3.3 Implementação

A construção do *Privacy* foi baseada num projeto anterior da empresa, que também lidava com garantias de conformidade e normas específicas, para atingir níveis de certificação. Por já haver uma estrutura capaz de suportar as exigências que advêm desse tipo de áreas, foi decidido que a ferramenta a desenvolver iria ter uma estrutura semelhante e componentes similares à ferramenta anterior, adaptando funcionalidades já existentes para que se adequassem ao contexto RGPD. Assim, a implementação dividiu-se em *back end* e *front end*, com uma estrutura "imposta" pelo projeto anterior produzindo as devidas adaptações. O módulo de gestão seguiu a linha de implementação do resto do projeto.

3.3.1 *Back End*

O desenvolvimento do *back end* seguiu um *flow* de implementação bem específico. Primeiro, para cada funcionalidade implementada, houve lugar a um estabelecimento de regras Swagger para desenvolver APIs REST. Dentro do ficheiro YAML, definia-se o tipo de método a gerar, o nome, os parâmetros e os seus tipos e o tipo de resposta a receber, como é possível constatar na figura 3.11, e quando o ficheiro era executado, era gerado automaticamente um conjunto de artefatos, contendo a API respetiva com diverso código gerado, bem como o seu *Controller*, e modelos para os novos tipos de dados também definidos no mesmo.

O Swagger é um conjunto de regras (especificação) para um formato que descreva APIs REST. Pode ser usado para partilhar documentação entre gestores de produto, *testers* e *developers*, mas também pode ser usado por várias ferramentas para automatizar

processos relacionados à API. Cada entrada do Swagger apresentava uma estrutura bem demarcada:

API / Versão / Objeto de Tratamento / Função / {Argumentos}

```
/gdpr/v1/weaknesstemplate/associate/{recommendationId}:
   post:
     tags:
       - gdpr weakness template
     summary: Create a link between a weakness template and
       a recommendation
     description: Create a link between a weakness template
       and a recommendation
     operationId: createLinkWTR
     parameters:
       - in: path
         name: recommendationId
         schema:
           type: integer
           format: int64
         description: Id da recomendao
         required: true
     requestBody:
       required: true
       description: weakness template id
       content:
         application/json:
           schema:
             type: integer
             example: 2
     responses:
       '200':
         $ref: '#/components/responses/
           GdprAssociatedRecommendationsRestListHolder'
```

Figura 3.11: Exemplo de entrada Swagger para criar associação entre *template* de fragilidade e de recomendação

Procedeu-se ao uso do Swagger para definir desde logo um contrato de implementação e estabelecendo desde o início que regras devem ser cumpridas, no que toca a *inputs* e *outputs* de tudo o que é implementado para frente, o que permitiu estruturar o código a desenvolver. Definiu-se os métodos HTTP possíveis de executar: GET, para consultas, POST, para *updates* e PUT, para novas inserções.

De seguida, regra geral, procedeu-se ao desenvolvimento dos scripts de BD para construir os artefatos de base de dados necessários (tabelas, vistas, ...), de acordo com certo tipo de dados definido anteriormente no Swagger.

O próximo passo foi olhar as assinaturas do métodos definidos na API gerada, e fazer *override* dos mesmos no *controller* correspondente, em que apenas se retorna o resultado de um método correspondente de um serviço REST, responsável por receber pedidos do *front end* e entregá-los ao *back end* para o devido processamento.

Depois surgiu a criação de serviço REST referido anteriormente. Sempre seguindo as regras que vêm de trás, começou-se a implementação propriamente dita. Começou-se a

criar o método responsável por se endereçar à funcionalidade explícita no *controller* e de seguida por se estabelecer um objeto *holder*, por regra imposta pelo Swagger, que contém dentro de si dois parâmetros: *Result*, para definir o resultado do pedido e *Data*, para armazenar os dados a transmitir. De resto, o método criado era responsável por passar os parâmetros que recebeu para uma nova camada de implementação (*Data Service*) e popular os parâmetros referidos anteriormente, como é possível ver na figura 3.12 nas linhas 11 a 15, definindo em altura própria o resultado do pedido, fornecendo ou não os dados que se exigem.

```
1  public GdprAssociatedRecommendationsRestListHolder linkRecommendation(Long
       recommendationId, Integer weaknesstemplateId){
2     GdprAssociatedRecommendationsRestListHolder result = new
          GdprAssociatedRecommendationsRestListHolder();
3     try {
4        List<GdprAssociatedRecommendationData> gdprAssociatedRecommendationDataList =
             gdprWeaknessTemplateDataService.link(recommendationId, weaknesstemplateId);
5        if (gdprAssociatedRecommendationDataList == null) {
6           result.setResult(appStatusRestService.getFail("Problem with creating link
                weakness template-recommendation"));
7        } else {
8           result.setData(new GdprAssociatedRecommendationsRestListHolderData());
9           result.getData().setRecommendations(gdprWeaknessTemplateRestMapper.
10             toGdprAssociatedRecommendationRestListFromDataList(
11             gdprAssociatedRecommendationDataList));
12          result.setResult(appStatusRestService.getSuccess());
13       }
14    } catch (Exception e) {
15       log.error("Error creating link between weakness template and recommendation", e);
16       result.setResult(appStatusRestService.getError(e));
17    }
18    return result;
19 }
```

Figura 3.12: Método de um serviço REST

De seguida surgiu a implementação de um *Data Service*, que tinha como principais funções, fazer valer a lógica de negócio associada à funcionalidade em questão e comunicar com a camada de persistência, quer para recolher informação, quer para persisti-la. Preencheu-se os DTOs criados e processou-se o resultado consoante a função, como se pode comprovar pela figura 3.13, nas linhas 7 a 12.

```
1  public List<GdprAssociatedRecommendationData> link (Long recommendationId, Integer
       weaknesstemplateId) {
2     GdprWeaknessTemplateData gdprWeaknessTemplateData =
          gdprWeaknessTemplateDataPersistence.getWeaknessTemplate(
3        Long.valueOf(weaknesstemplateId));
4     if (gdprWeaknessTemplateData != null) {
5        GdprLinkData gdprLinkData = gdprLinkDataPersistence.getAssociation(
6           Long.valueOf(weaknesstemplateId), recommendationId);
7        if (gdprLinkData == null) {
8           GdprLinkData gdprLinkDataNew = new GdprLinkData();
9           gdprLinkDataNew.setId(null);
10          gdprLinkDataNew.setEnabled(Boolean.TRUE);
11          gdprLinkDataNew.setWtid(Long.valueOf(weaknesstemplateId));
12          gdprLinkDataNew.setRid(recommendationId);
13          gdprLinkDataPersistence.linkUnlink(gdprLinkDataNew);
14       } else if (!gdprLinkData.getEnabled()) {
15          gdprLinkData.setEnabled(Boolean.TRUE);
16          gdprLinkDataPersistence.linkUnlink(gdprLinkData);
17       }
18       return gdprLinkDataPersistence.listRecommendationsAssociated(Boolean.TRUE,
             gdprWeaknessTemplateData.getId());
19    }
20    return null;
21 }
```

Figura 3.13: Método do serviço de Dados

Foi criado para cada novo tipo de dados estabelecido no Swagger, um objeto do tipo Data para servir de DTO e facilitar a transferência de dados entre processos.

Toda esta comunicação era feita através de um *Entity Service* que implementava uma interface que definia os métodos necessários para a interação, após a adição de mais alguma lógica de negócio, com a camada de persistência como se vê na figura 3.14, na linha 8. Este serviço estava intimamente ligado à classe *Repository* correspondente (que estende CRUDRepository), que era a encarregue de concretizar as comunicações com a BD, possibilitando a implementação métodos de consulta com a própria *query* na anotação do método, como se constata na figura 3.15, nas linhas 1 a 5, fornecendo métodos de interação com a entidade construída, tais como *save*, *delete*, *existsByID*, *findAll*, entre outros.

A criação de uma determinada entidade foi feita através da ligação com a tabela correspondente na BD, e definia métodos *get* e *set* para cada parâmetro.

```
1  @Override
2  public GdprLinkData linkUnlink(GdprLinkData qLink) {
3     GdprLinkWeaknesstemplateRecommendationEntity
          gdprLinkWeaknesstemplateRecommendationEntity =
          gdprLinkEntityMapper.toEntityFromGdprLinkData(qLink);
4     gdprLinkWeaknesstemplateRecommendationEntity.setUdate(usmSession.getUdate());
5     gdprLinkWeaknesstemplateRecommendationEntity.setUid(usmSession.getUid());
6     return gdprLinkEntityMapper.toLinkDataFromEntity(gdprLinkEntityRepository.
7        save(gdprLinkWeaknesstemplateRecommendationEntity));
8  }
```

Figura 3.14: Método de um serviço de Entidade

```
@Query(nativeQuery = true,
       value = "select * " +
               "from gdpr_link_weaknesstemplate_recommendation " +
               "where wtid = :wtId " +
               "and rid = :rId")
GdprLinkWeaknesstemplateRecommendationEntity getAssociation(@Param("wtId") Long wtId,
    @Param("rId") Long rId);
```

Figura 3.15: Método de um Repositório

Em alguns casos foi usada uma camada de implementação extra denominada *Logic*, que continha lógica de negócio mais complexa.

Mappers

Cada vez que se mudava de camada de implementação era necessário colocar os dados que circulam no formato pretendido para que fossem lidos, processados e interpretados. Surgiu assim a necessidade de ter vários tipos de *mappers*, para efetuar a conversão de dados entre camadas.

Em primeira instância houve a necessidade de *REST Mapper*s, capazes de transformar objetos *REST* em objetos *Data* realizando também a conversão contrária, *Data* para *REST*. Este tipo de *mappers* foram usados no serviços REST, tanto para converter informações que vinham nesse formato para alimentar os métodos de camadas abaixo, como para converter dados resultantes da execução do pedido para o formato pretendido.

Depois, surgiu a necessidade de mapear objetos do tipo *Data* para objetos do tipo *Entity* e vice-versa, para colocar os dados num formato que as classes entity fossem capazes de interpretar e usar, devolvendo os resultados à camada acima já convertidos num formato percetível para si.

A definição dos *mappers* foi feita numa interface com a anotação `@Mapper`. A implementação dos *mappers* foi feita maioritariamente de forma automática numa classe à parte, por cortesia do Spring Boot, só havendo intervenção da equipa de programação quando a lógica de conversão não era tão simples, que pudesse ser automatizada.

O uso do Spring facilitou de sobremaneira algumas partes da implementação, ajudando a criar um serviço web RESTful, sem esforços de maior. Através desta *framework*, foi construído muito do que é a estrutura do sistema, tendo a equipa de programação a incumbência de preencher essa estrutura com a lógica de negócio inerente ao contexto da ferramenta. Através de um conjunto de anotações, o Spring providencia diversos serviços de forma automatizada, gerindo transações, criando serviços e entidades e injetando dependências.

O Módulo de Gestão seguiu esta linha de implementação, esquematizada na figura 3.16, no que concerne ao *back end*.

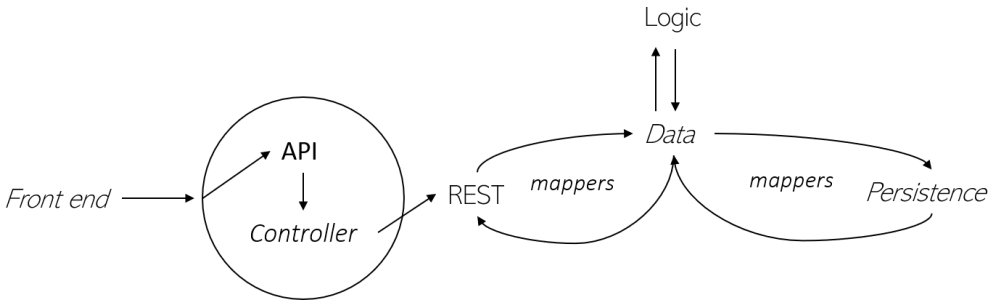

Figura 3.16: Esquema de implementação do *back end*.

3.3.2 *Front End* para programadores

Para servir de interface com o utilizador, surgiu a necessidade de implementar um *front end*, concretizado em Angular3 com o apoio de TypeScript para dar alguma inteligência às páginas construídas. Por se inserir, no projeto que já utilizava estas tecnologias, foi decidido continuar a usar as mesmas tecnologias na implementação do FE para facilitar a integração do módulo de gestão.

A implementação dividiu-se em vistas gerais, vistas de detalhes, *modals* e serviços.

Primeiro, criou-se o componente, que tinha dois ficheiros essenciais à sua composição, um .html, que definia a estrutura da página, invocava funções e era responsável por fazer aparecer ou desaparecer elementos consoante determinados privilégios e um .ts, responsável por tratar os dados e garantir a ligação ao *back end*.

Os ficheiros TS continham dentro de si várias funções comuns a todos deste tipo:

- `ngOnInit()` era o método de arranque do componente, responsável por chamar o initRequests() e o getData();
- `initRequests()` preparava para receber a resposta através do método *subscribe*;
- `getData()` fazia a chamada ao *back end* de modo a obter os dados necessários;
- `dataArrived()` verificava se tinha toda a informação necessária do lado do *front end*;
- `initForms()` era responsável por inicializar os formulários presentes na página e chamar o método initTable();
- `initTable()` inicializa as tabelas da página, organizava a paginação das mesma e carregava os diversos filtros existentes (*filterByPage*, *filterByText*, *sortTable*, *filterTableVisibleAll*);
- `validateForm(:FormGroup)` validava o formulário passado no argumento;

- `ngOnDestroy()` era o responsável por anular a subscrição feita no initRequests() terminando a execução do componente.

Dentro dos ficheiros TypeScript, existiam ainda alguns métodos essenciais à lógica da ferramenta, a definir o *routing* dos componentes, a implementar *rights* de acessos a elementos do componente, firmando os requisitos de segurança e a abrir *modals*, para inserir ou editar conteúdos:

- `goToItemDetails(itemData)` (Lista) direcionava para as páginas de detalhes de determinado elemento da lista;
- `closeForm()` (Detalhe) fechava a página de detalhes de determinado elemento redirecionando para a lista geral desse tipo de elementos;
- `openDialog[function]()` abria o *modal* responsável por executar [function];
- `canAdd()` controlava se dado utilizador tinha o privilégio de adicionar novos elementos à lista, tornando o botão de adicionar visível e invisível consoante o valor do *right*;
- `canViewToggle()` (Lista) controlava se dado utilizador tinha o privilégio de consultar todos os elementos da lista (ativos e inativos), tornado o *toggle* que permite alterar essa vista da tabela, visível ou invisível consoante o valor do *right*;
- `canViewList()` controlava se dado utilizador poderia aceder ao conteúdo da lista aquando do momento de carregamento da página, mostrando ou não a lista consoante o valor do *right*;
- `canUpdate()` controlava se um utilizador conseguia alterar as informações de um determinado elemento, através de tornar o botão de 'guardar' visível ou invisível consoante o valor do *right*;
- `canViewToggle()` (Detalhe) controlava se um dado utilizador poderia ou não desativar o elemento tornado o *toggle* que controla essa funcionalidade visível ou invisível consoante o valor do *right*;
- `canViewDetails()` controlava se um utilizador pode consultar os detalhes de dado elemento, eliminando as informações da página consoante o valor do *right*.

Serviços

Os serviços surgiram no *front end* para fazer a ligação com a lógica implementada no *back end*. Dividiam-se em dois tipos: o tipo de serviço gerado automaticamente através do Swagger **(através generate_bc)** e os serviços implementados com a lógica necessária

desenvolvida pela equipa, que utilizavam os anteriores, fornecendo-lhes dados e recolhendo os resultados da sua execução, usando já objetos dos tipos de dados definidos no Swagger.

No serviço implementado, era chamado no construtor o serviço gerado e eram definidos vários argumentos que iriam guardar as diversas informações passíveis de serem recolhidas pelo serviço, com o tipo Subject<[tipo de dados da informação]>. Isto define o argumento como um *Observer* sobre esse tipo de informação. Para fornecer um novo valor ao Subject, usava-se o método *next(value)* e era *multicasted* para os *Observers* registados para escutarem o Subject, à espera de nova informação.

Os serviços implementados tinham em geral quatro métodos em comum, essenciais ao funcionamento das funcionalidades implementadas:

- `getItems(all:boolean)` devolve a lista completa com items visíveis ou com todos os existentes;
- `getItem(id:number)` devolve item correspondente ao id fornecido;
- `addItem(itemToAdd:[tipo de dados do item])` adiciona item;
- `updateItem(itemToUpdate:[tipo de dados do item])` atualiza item.

Routing, *Rights*, Limitações de *input* e Mensagens de Erro

Importante a todo o processo de construção desta interface, foi estabelecimento de um ficheiro responsável (*app-routing.module.ts*) por gerir os *routings* entre os diferentes componentes do *front end*, definindo o *path* e o componente a que este se referia. Em algumas páginas foi implementado um *breadcrumb* que também beneficiou do apoio deste ficheiro de *routing*.

Num ficheiro próprio também (*auth-rights.ts*), implementou-se os *rights* existentes no uso da plataforma. Os métodos responsáveis por analisar o tipo de privilégio de um dado utilizador dependem da consulta deste ficheiro para ajuizar que informação e/ou funcionalidades devem ser mostradas.

As limitações de *input* foram definidas em *base-class.ts*, onde foi definida a zona do input como nome do objeto, com os devidos argumentos limitados a certo tamanho, como se vê na figura 3.17, nas linhas 2 e 3.

```
1 public tablesSizes_BC_Weakness_Templates = {
2    potentialfailure: 300,
3    description: 300,
4 }
```

Figura 3.17: Exemplo de entrada na *Base Class*

Por fim, as mensagens de erros foram desenvolvidas em *error-handler.ts*, que implementa a função DelegateErrorMessage (errorId:String), interpretando o código fornecido, devolvendo a devida mensagem e adaptando também o ícone a mostrar na mensagem.

Assim é possível esquematizar o FE, como se demonstra na figura 3.18:

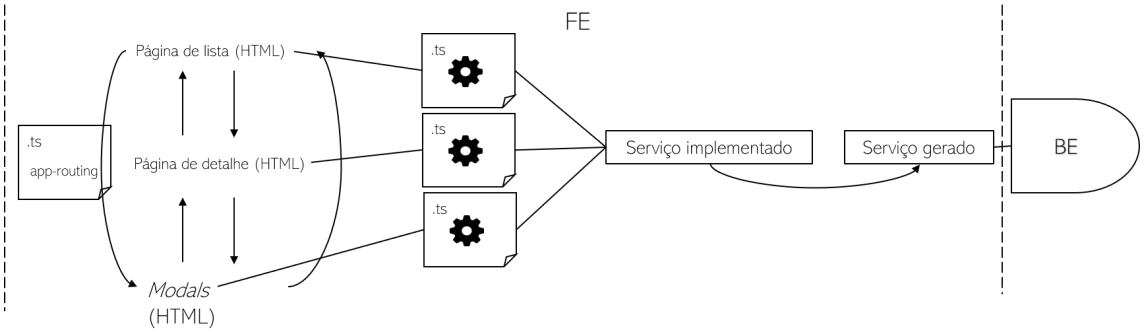

Figura 3.18: Esquema de implementação do *front end*

O Módulo de Gestão seguiu esta linha de implementação no *front end*.

Decisões de implementação

Foi decidido implementar *templates* de questionário de modo a contornar as diferenças inevitáveis entre os contextos das diversas organizações. Alguns questionários, apesar de modo geral serem semelhantes em grande parte do seu conteúdo, necessitavam de uma customização própria para atender a essas diferenças, tais como departamentos específicos, processos exclusivos e dados pessoais que não tinham sido tratados anteriormente. O facto de se ter criado *templates* promoveu a reutilização questionários, através da sua clonagem, o que permitiu economizar tempo aos responsáveis por construir esses questionários evitando que tenham de os produzir de base, limando apenas algumas arestas no *template* clonado.

Permitir que associe perguntas a categorias, permitiu também que se contribuísse para a poupança de tempo e organização dos conteúdos que se pretendem com o uso do *Privacy*. A partir desta definição podíamos ter acesso às perguntas dessa categoria aquando da construção do *template* de questionário, evitando ter que redigir as perguntas de novo, conseguindo estruturar os mesmos de forma mais fácil quando a quantidade de informação se tornar avassaladora, o que iria dificultar a sua gestão.

A criação de Entidades e a associação de clientes e utilizadores a estas foi a forma como os diferentes acessos e privilégios foram concedidos ou retirados aos diversos utilizadores da plataforma, fornecendo uma interface para este processo, facilitando-o.

Nos Dados Pessoais, foi permitido definir o nível de criticidade o que ajudou a tornar a elaboração dos relatórios mais automatizada. Este componente do sistema em conjunto com outros permite que a informação seja introduzida de forma progressiva e que seja

reutilizada na elaboração dos relatórios finais, anulando a necessidade de reescrever elementos já presentes na auditoria.

Os *Templates* de Fragilidades foram produzidos pelas mesmas razões que os anteriores, evitar *rework* de artefatos produzidos anteriormente, poupando tempo aos utilizadores, e definir logo um conjunto de propriedades comuns à fragilidade que serão assumidas quando o *template* for usado, na criação de uma nova fragilidade, herdando as falhas potenciais e os templates de recomendações

O estabelecimento de Origens Funcionais e Origens surgiu como uma forma de armazenar a origem das fragilidades e promover desde logo uma catalogação no que toca ao tipo de fragilidades que podem vir dessa origem. Estas origens ajudam também na criação de uma nova fragilidade que herda, precisamente, os tipos de fragilidades.

Os 3 sub-módulos anteriores tornam o processo de criação de uma fragilidade mais rápido, fácil e intuitivo.

3.3.3 *Front End* para utilizadores

Enquanto que na secção anterior, se descreveu o FE do módulo de gestão de uma perspetiva de *developer*, procura-se agora exprimir os modos de uso da plataforma do ponto de vista de um utilizador. Em cada sub-módulo existe um uso específico da parte do utilizador.

No sub-módulo de '*Templates* de Questionário', temos acesso a uma lista dos *templates* criados, onde é possível alternar entre uma vista dos atualmente ativos e uma vista de todos os presentes, através de cliques no *toggle*. Para clonar os *templates*, basta clicar no botão que se apresenta no final da linha a que correspondem. Para criar um *template* carrega-se no botão '+' e em primeira instância define-se o idioma e o nome do mesmo. Tudo isto é possível observar na figura 3.19.

Após ficar na lista, carrega-se no *template* e procede-se à sua edição, onde é possível alterar (se se tiver privilégios para tal) Nome e Descrição, substituindo o texto presente pelo pretendido, onde se podem adicionar as categorias e as perguntas subsequentes, através de botões similares ao anterior ('+'). Em qualquer altura a ordem das perguntas e das categorias pode ser alterada através de um *drag and drop*. Para completar a edição clica-se no botão 'Guardar'. Para consultar as versões anteriores do *template* em questão, avançamos até ao fundo da página e clicamos no botão 'Visualizar' da versão pretendida. Por fim, é possível desativar o *template* clicando no *toggle*, junto do título da página, como é possível constatar através da figura 3.20.

No sub-módulo das 'Categorias', temos uma visão de lista e um modo de uso similar ao sub-módulo anterior. Para alternar entre a visão de categorias entre ativas e todas deve proceder-se ao clique no *toggle* para o efeito. Para adicionar uma nova categoria, clica-se no botão '+', e definindo-se primeiramente o idioma e o nome da categoria. Para editar, carrega-se na entrada da lista que corresponde à categoria pretendida, abrindo o detalhe

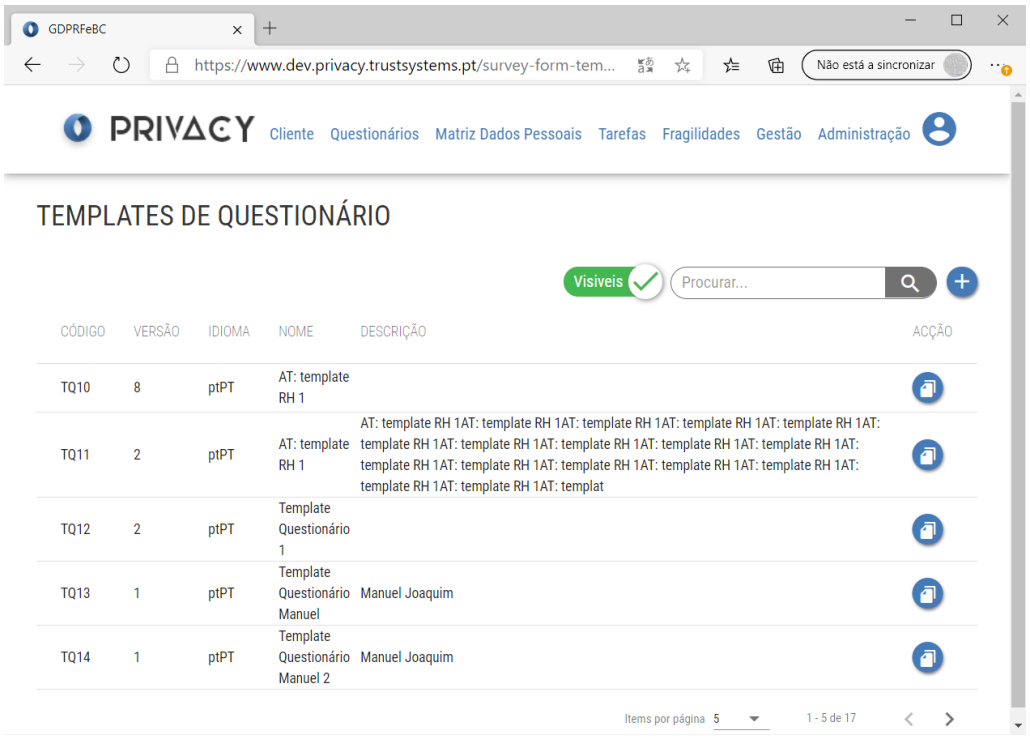

Figura 3.19: Vista da lista de *templates* de questionário

da categoria. No detalhe da categoria, pode então proceder-se à edição do Nome e da Descrição, substituindo o seu conteúdo pelo pretendido. Todas as informações estão presentes na página, pelo que um *scroll* por esta chegará para consultar todas as informações pretendidas. Por fim, é possível desativar a categoria clicando no *toggle*, junto do título da página.

Estando no sub-módulo de 'Perguntas', podemos adicionar novas através do botão '+', definindo o idioma e a pergunta em si, podemos alternar a vista entre a geral e a das perguntas ativas através de cliques no 'toggle'. Para clonar a pergunta, clica-se no botão que encerra cada entrada da lista e para editar clica-se na própria entrada, abrindo o detalhe de pergunta, como se vê na figura 3.22. Aqui, podemos alterar o Resumo e a Pergunta, substituindo o seu conteúdo pelo pretendido. Para associar categorias à pergunta clica-se no botão '+', presente no cimo da tabela que mostra as categorias associadas, e surge um *modal* em que ou se seleciona uma categoria da lista das existentes ou se se produz (em texto) uma nova categoria, finalizando o processo clicando no botão 'Adicionar'. No fim de cada entrada da tabela, existe um *toggle* que controla o estado de associação da categoria com a pergunta, pelo que basta um clique para alterá-lo. Por fim, é possível desativar a pergunta clicando no *toggle*, junto do título da página, como se demonstra na figura 3.23.

Chegando ao sub-módulo de 'Entidades', criamos novas clicando no botão '+', definindo o nome e o tipo logo no momento da criação. Para alternar entre visão geral e visão das entidades ativas, usa-se novamente o *toggle* para esse efeito, como se constata na figura 3.24. Clicando em dada entrada da lista, temos acesso ao detalhe da entidade onde é

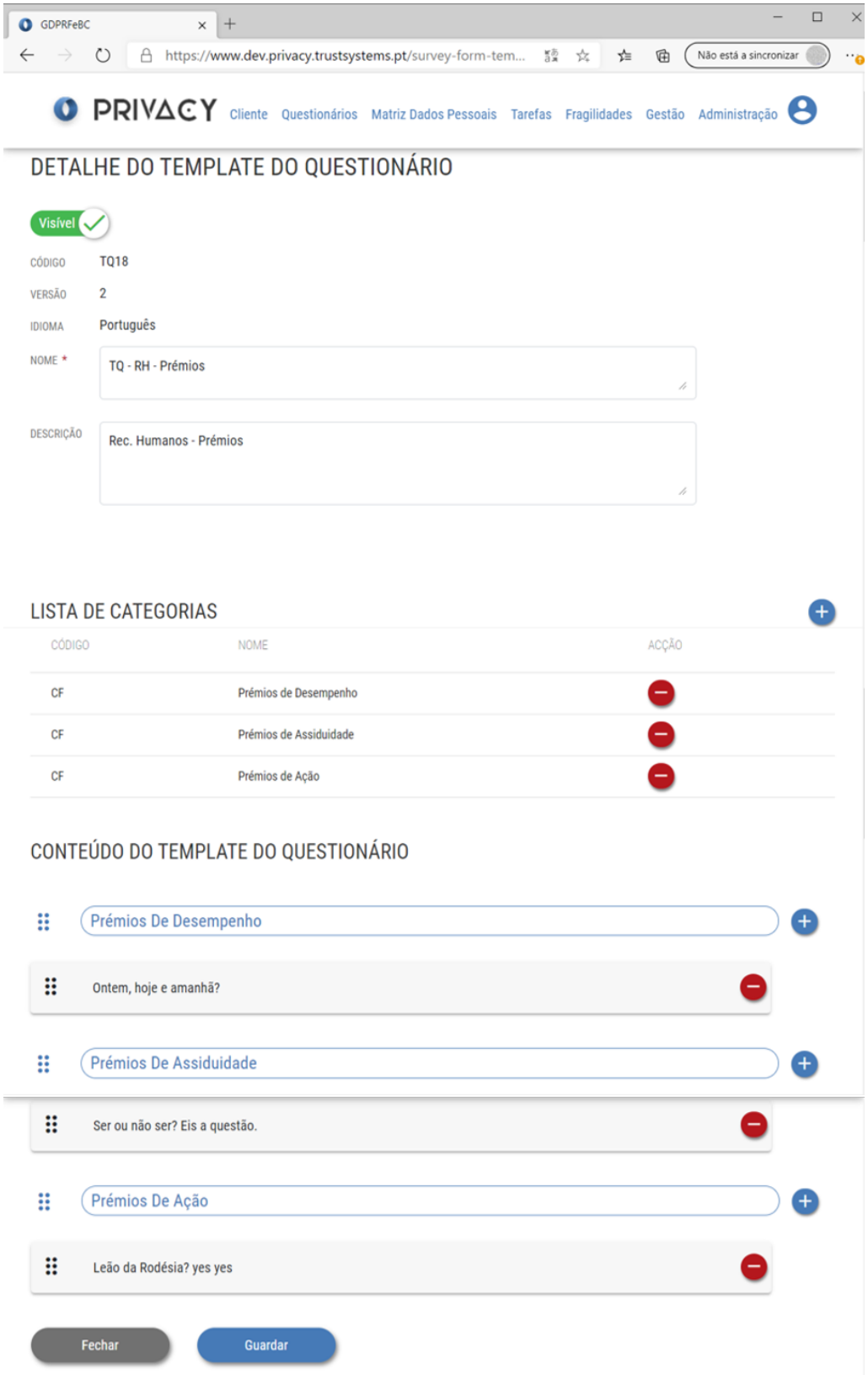

Figura 3.20: Vista de detalhe de *template* de questionário (1)

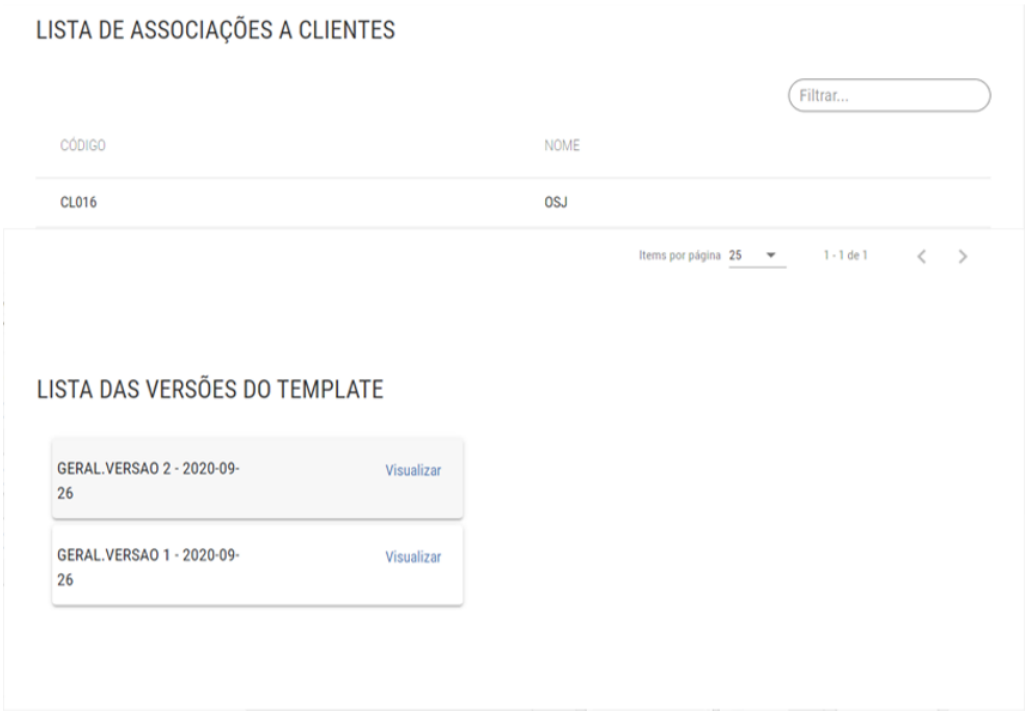

Figura 3.21: Continuação da figura anterior - Vista de detalhe de *template* de questionário (2)

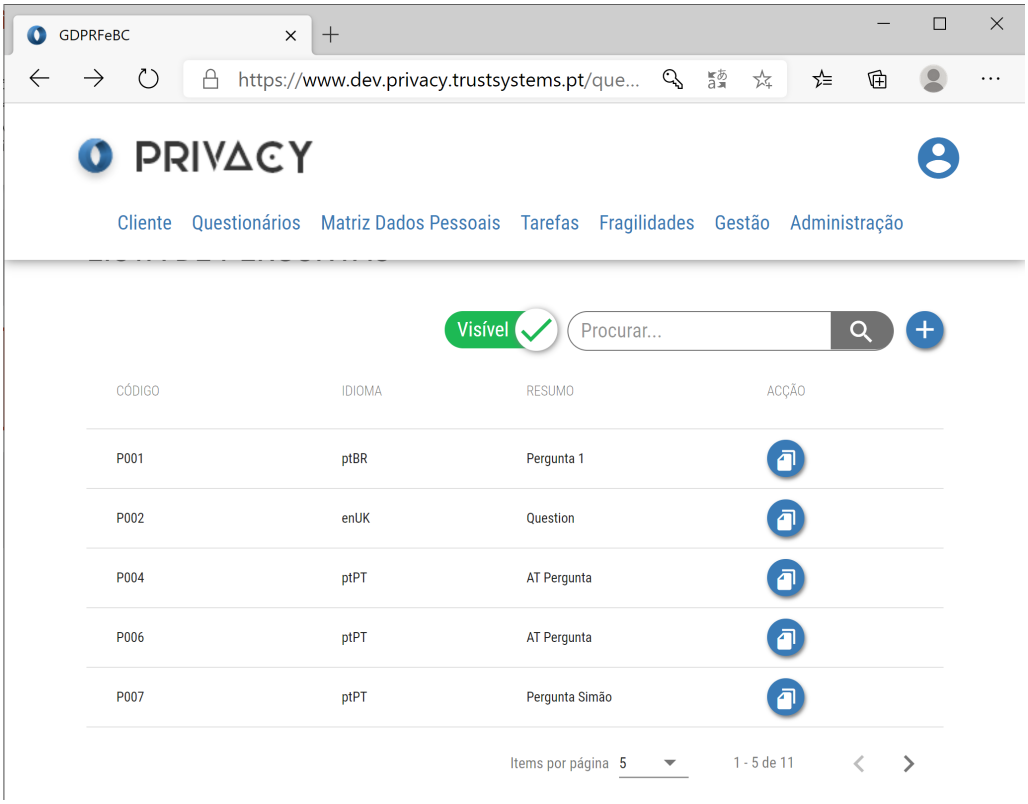

Figura 3.22: Vista de lista das perguntas

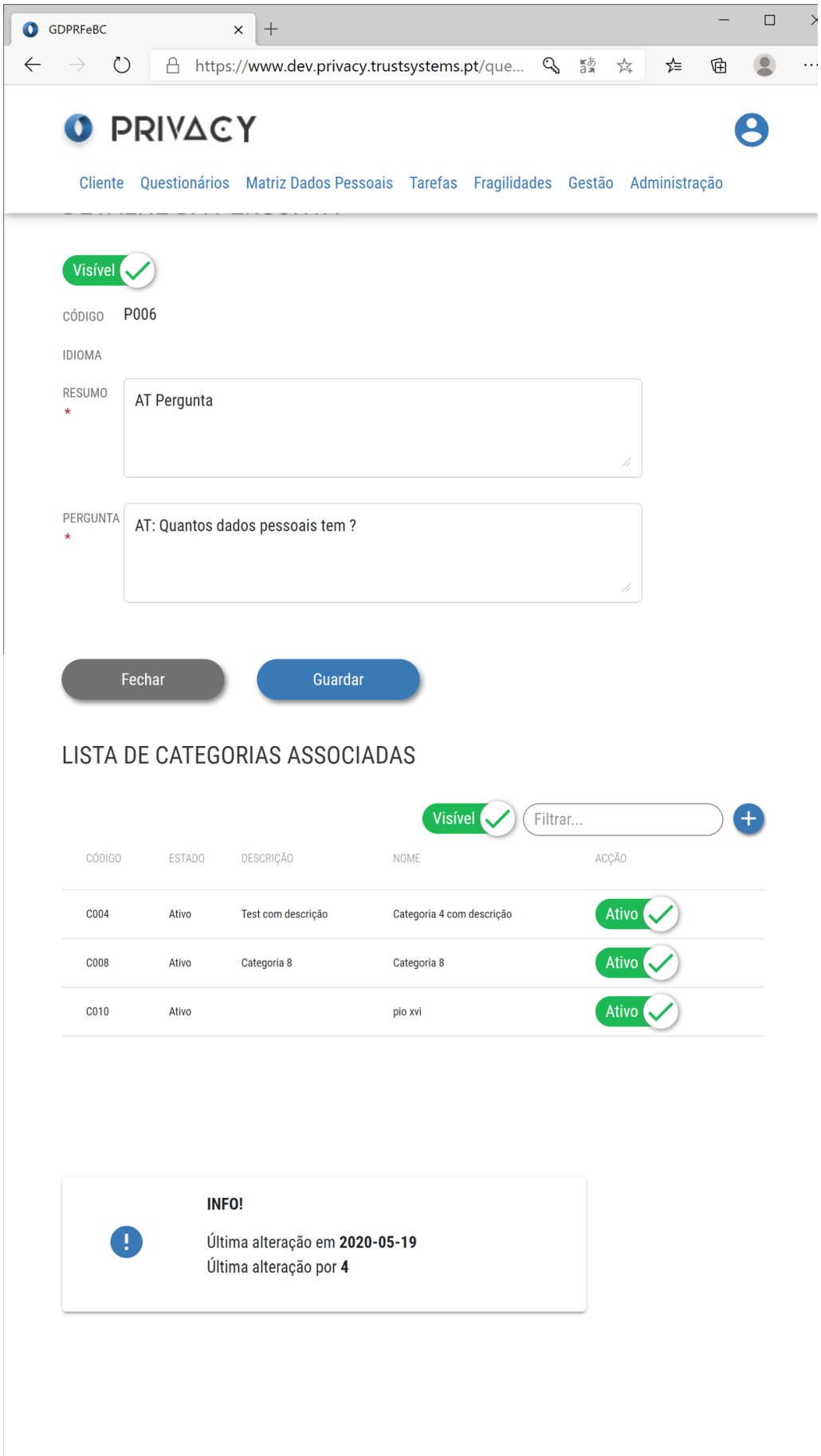

Figura 3.23: Vista de detalhe da pergunta

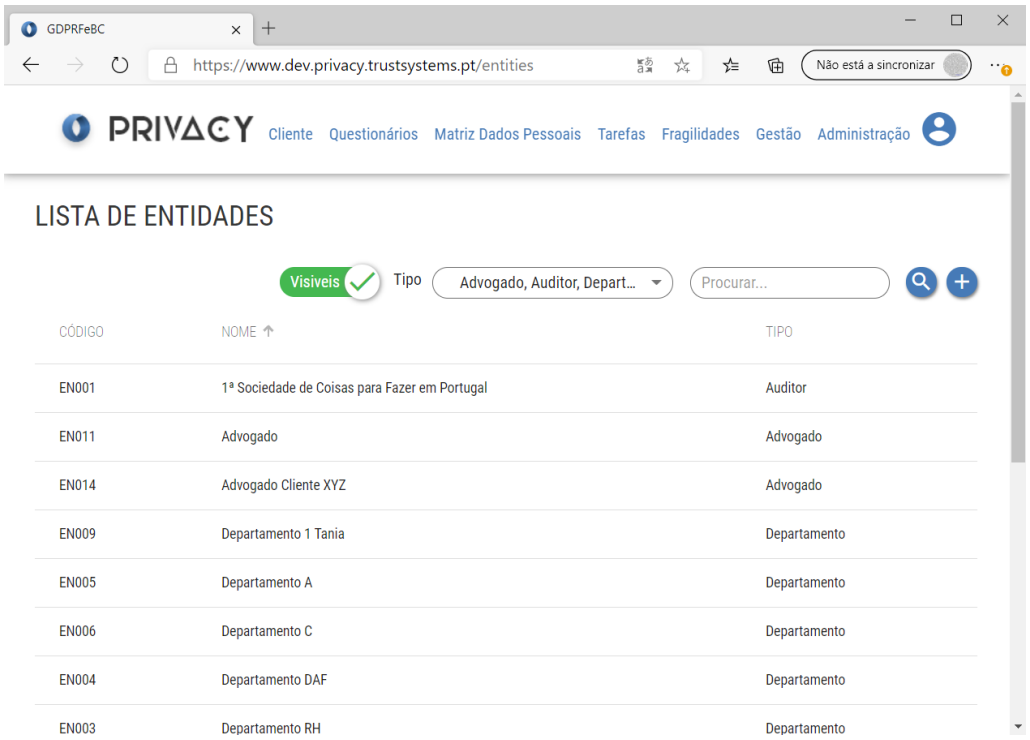

Figura 3.24: Vista de lista das entidades

possível proceder à edição da mesma. Pode-se alterar o Nome da entidade, substituindo o conteúdo prévio pelo novo. Para associar clientes e utilizadores, navega-se até à zona da página das listas correspondentes e clica-se no botão '+', escolhendo da lista de clientes e utilizadores existentes, finalizando o processo com um clique no botão 'Adicionar'. Para alterar o estado de associação, clica-se no *toggle* apropriado, no fim de cada entrada da lista de clientes e utilizadores associados. Para adicionar notas, também é através de um botão '+', que abre um *modal* com uma caixa de texto para o efeito. Pode-se editar e consultar o histórico da nota, através do clique nos botões presentes nas colunas para o efeito. Por fim, é possível desativar a entidade clicando no *toggle*, junto do título da página. Estas informações podem ser corroboradas pela figura 3.25.

No sub-módulo de 'Processos', podemos criar novos através do botão '+', definindo no *modal* que se abre, o Idioma e o Nome. Para alternar entre vista geral e vista de processos ativos, clica-se no *toggle* que controla essa particularidade. Clicando numa entrada da lista, abre-se o detalhe de processo, onde é possível proceder à edição do processo em si, alterando o Nome e a Descrição, finalizando o processo de edição, carregando no botão 'Guardar'. É ainda possível desativar o processo no *toggle* que surge logo a seguir ao título da página, clicando no mesmo para alterar o seu estado.

No sub-módulo de Dados Pessoais, podemos alternar a vista entre ativos e todos através de um clique no *toggle* para o efeito, podendo adicionar novos através de um botão '+', que abre um *modal*, onde se define o Idioma e o Nome. Clicando numa entrada da lista abre-se o detalhe de dado pessoal, onde se pode editar o mesmo, alterando cam-

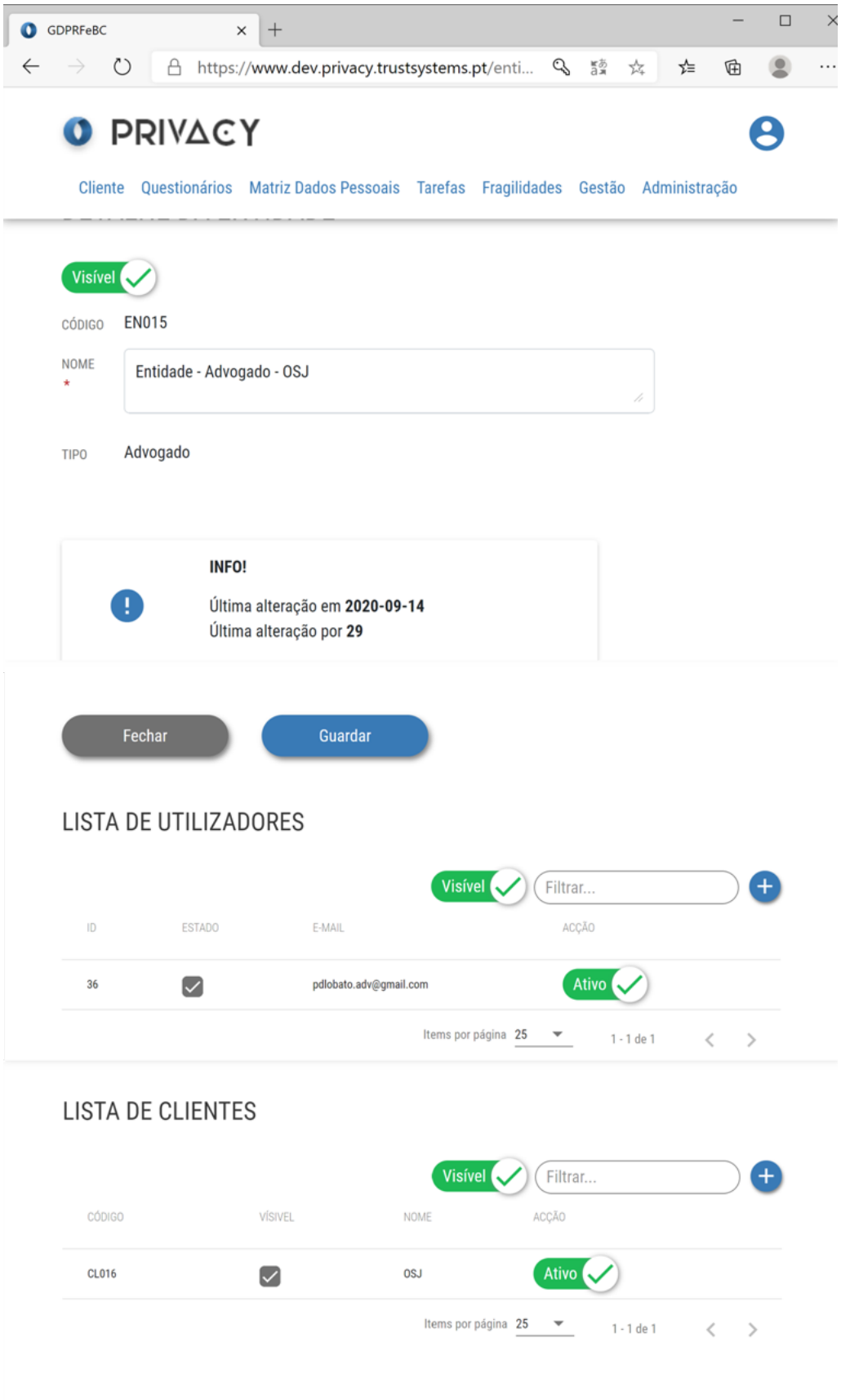

Figura 3.25: Vista de detalhe da entidade (1)

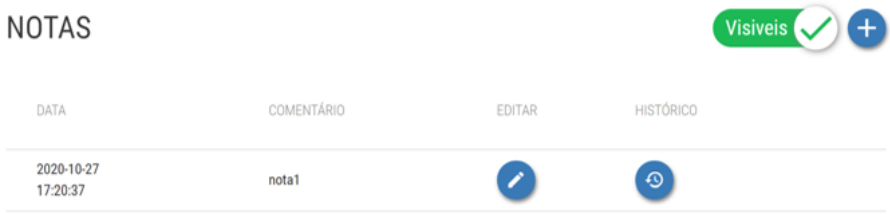

Figura 3.26: Continuação da figura anterior - Vista de detalhe da entidade (2)

pos como o Nome, Criticidade e Ordem, substituindo os valores anteriores pelos novos, finalizando o processo, clicando em 'Guardar'. Para adicionar o dado pessoal a grupos e categorias, navega-se até à zona da página adequada e clica-se em '+', abrindo-se um *modal* para concretizar essa associação. É ainda possível desativar o dado pessoal através de um *toggle* próprio, junto ao título da página.

Nos 'Tipos de Fragilidades', podemos alterar a vista entre ativos e todos os existentes através de um clique no *toggle* para o efeito, podendo adicionar novos através do botão '+', que abre um *modal*, onde se define o Idioma e Nome. Clicando numa entrada da lista, abre-se o detalhe de tipo de fragilidade, onde se pode editar o mesmo, alterando Nome, substituindo o conteúdo prévio pelo pretendido, clicando em 'Guardar' para finalizar a edição. Para desativar o tipo de fragilidade, clica-se no *toggle*, por baixo do título da página.

Nas 'Origens', podemos alterar a vista entre ativas e todas as existentes através de um clique no *toggle* para o efeito, podendo adicionar novas através do botão '+', que abre um *modal*, onde se define o Idioma e Nome. Clicando numa entrada da lista, abre-se o detalhe de origem, onde se pode editar a mesma, alterando Nome, substituindo o conteúdo prévio pelo pretendido, e alterando os Tipos de Fragilidades associados, marcando a *checkbox* a que correspondem, clicando em 'Guardar' para finalizar a edição. Para desativar a origem, clica-se no *toggle*, por baixo do título da página.

Nas Origens Funcionais, podemos abrir o detalhe das mesmas clicando numa entrada da lista, onde se pode editar o Nome, substituindo o anterior pelo novo, e a Origem Associada, concluindo a edição através do clique no botão 'Guardar'.

Nos '*Templates* de Fragilidade', podemos alterar a vista entre ativos e todos os existentes através de um clique no *toggle* para o efeito, podendo adicionar novos através do botão '+', que abre um *modal*, onde se define o Idioma, a Falha Potencial e os Tipos de Fragilidades. Clicando num dado *template* abre-se o detalhe de *template* de fragilidade, onde é possível editar a Falha Potencial e a Descrição, substituindo o conteúdo anterior

pelo novo e os Tipos de Fragilidades, marcando ou desmarcando as respetivas *checkboxes*. É ainda possível criar *templates* de recomendações através do clique no botão '+', que promove a abertura de um *modal* onde se define a Ação Corretiva e a Descrição da recomendação. Em cada entrada da lista de *templates* de recomendações associadas, na última coluna é possível controlar o estado desta associação através do clique no *toggle* próprio para o efeito. Para desativar o referido *template*, clica-se no *toggle*, junto ao título da página.

Em todas as listas é possível ordenar os componentes pelos valores de determinadas colunas bastando para isso clicar no nome da coluna para ordenar por ordem ascendente ou descendente.

3.4 Sumário

Neste capítulo foi apresentado o módulo de gestão, responsável por gerir toda a informação e material de auditoria presentes na plataforma, tornando essa gestão mais fácil e intuitiva, aumentando os níveis de usabilidade da plataforma. Foram descritos os requisitos funcionais, a arquitetura de forma breve, bem como as ligações do módulo com os outros módulos e o processo de implementação, tanto no BE como no FE, influenciado por uma estrutura já montada, de um projeto anterior que também orbitava em torno de noções como garantia de conformidade, normas e gestão de riscos. O próximo capítulo refere-se à análise qualitativa feita à ferramenta como um todo e mais em específico, ao módulo de gestão.

Capítulo 4

Análise Qualitativa

No capítulo anterior, descreveu-se o *Privacy* e o módulo de gestão em detalhe, passando pela sua implementação e uso por parte do utilizador. Neste capítulo, fazemos a avaliação da ferramenta produzida, e mais concretamente do módulo de gestão. Fez-se uma análise qualitativa à ferramenta como um todo, explicando as contribuições para o panorama das auditorias RGPD nos dias de hoje, fazendo previsões acerca dos melhoramentos trazidos pelo uso do sistema desenvolvido.

4.1 Comparação entre auditorias pré-*Privacy* e pós-*Privacy*

Antes da implementação do *Privacy*, realizar auditorias RGPD era um processo moroso, no qual as empresas auditoras encontravam muitas dificuldades, pela facto de ser uma realidade recente e ainda não haver estruturas próprias que suportassem projetos deste tipo de uma forma que diminuíssem as dificuldades que advêm dos mesmos, como foi descrito na secção 2.1.1.

Apesar de se dar as boas vindas a normas que aumentam a segurança dos clientes das organizações, realizar auditorias deste tipo, é um trabalho burocrático e repetitivo, tanto para os auditores como para os próprios DPOs. Dar início a ciclos iguais para clientes diferentes, repetir trabalho já efetuado, produzir grandes quantidades de informação difícil de ler e processar e realizar todo este processo, um cliente de cada vez, dada a dimensão de todos os elementos produzidos.

O *Privacy* vem por isso tentar mitigar essas contrariedades das auditorias, tentando tornar a conformidade com o RGPD, um processo mais rápido, eficiente, menos monótono e menos permeável a erros, evitando a sobrecarga burocrática inerente aos processos de garantia de conformidade.

Hoje, com o *Privacy*, temos uma ferramenta de gestão de conformidade poderosa, capaz de suportar vários processos de auditoria ao mesmo tempo, sem contaminação dos dados. Temos uma interface adequada à gestão de todo o material e informação da auditoria, permitindo que esta se faça de forma clara, concisa e organizada, sem que o aumento

da quantidade da mesma influencie a realização e os resultados de todo o processo.

Deixou-se de utilizar o Excel como ferramenta nuclear às auditorias, abandonando todas as premissas de insegurança que vêm do seu uso, bem como a manifesta falta de preparação para cruzar informações de forma dinâmica e produzir questionários. Com a plataforma desenvolvida, temos bases de dados seguras, com dados verificados e validados, possuímos formas de aceder às informações pretendidas de forma mais rápida e direta sem ter que a procurar em tabelas intermináveis, havendo ainda a capacidade de cruzar dados que facilitem o processo de auditoria, sendo interpretados para retirar conclusões como o risco a que se está sujeito.

No presente, os questionários são construídos de forma robusta em local próprio por quem de direito, são altamente customizáveis e são diretamente atribuídos ao cliente a que se referem através da ferramenta, anulando-se a necessidade de recorrer a ambientes externos para promover a realização dos mesmos. São construídos, atribuídos, respondidos e analisados, questão a questão, no sistema e o facto de se conseguir concretizar esta realidade, promove que haja menos confusões e atrasos.

Os auditores, hoje em dia, podem focar-se nas suas competências centrais, nos seus conhecimentos essenciais do processo deixando as tarefas recorrentes serem automatizadas. Existem *templates* que visam promover a reutilização de material para organizações em que o contexto seja semelhante, existem elementos que ajudam a direcionar o preenchimento de muito material com opções pré-formatadas, das quais só tem que se escolher as que mais se ajustam ao pretendido, evitando enganos e erros, tendo um processo mais guiado e mais estruturado do que anteriormente.

Tanto para a equipa auditora, como para a equipa responsável por assegurar a conformidade da organização, existe hoje uma plataforma central que agrega todas as particularidades deste processo com funcionalidades próprias, o que suprime todas as necessidades de recorrer a aplicações estranhas ao âmbito da auditoria. O facto de existir esta centralização facilita a comunicação entre equipas, permite atribuir responsabilidades de forma inequívoca, viabiliza a associação quase imediata de material a dado cliente, possibilita um controlo constante do estado das coisas, permite manter a documentação de apoio anexada nos devidos locais e facilita no pós-auditoria as atividades de acompanhamento das medidas propostas, contendo tudo no mesmo sítio, evitando o dispersar de dados.

Existe também um módulo de tarefas para concretizar as medidas propostas e as incumbências intermédias do processo e acompanhar o estado das mesma, garantindo um maior controlo sobre todos os processos, quando antes a visão sobre o panorama RGPD era pouco abrangente, difícil de controlar o que se fez e o que falta fazer. Hoje o DPO pode ter fácil acesso às tarefas e aos seus responsáveis e pressionar para que tudo ande mais rápido e para que todo este processo não se arraste para além do estritamente necessário.

Temos também agora uma plataforma que ela própria cumpre com a norma vigente, separando acessos, dando os privilégios mínimos para que cada utilizador execute as suas funções sem prejuízo das mesmas, situação esta que previamente não se verificava, por haver integrantes do processo a lidar com muita informação que não era fulcral às suas funções, tanto do lado da equipa auditora, como do lado da equipa responsável pela proteção de dados.

A atribuição níveis de risco a cada fragilidade, de acordo com uma metodologia aceite em processos críticos de segurança também integrou a ferramenta, permitindo manter gráficos e estatísticas que espelham a situação do risco em tempo real e permitem consultar a evolução do mesmo, proporcionando que se possa agir em conformidade mais em cima do acontecimento.

Temos ainda a possibilidade de gerar relatórios rapidamente de forma automática, permitindo usar os dados recolhidos ao longo de todo o processo, o que permite que na altura de os produzir, muito do trabalho já esteja feito, reduzindo de sobremaneira o tempo dedicado a estes, mas mantendo a qualidade do resultado final.

Em suma, tudo o que é relativo ao processo RGPD, pode agora ser concretizado numa única plataforma, com organização, estruturação, segurança, economizando tempo a todos os participantes, atingindo à facilidade, rapidez e eficiência que se pretendiam alcançar.

4.1.1 *Research Questions*

Produziu-se um conjunto de questões que levam em conta os objetivos da ferramenta ao mesmo tempo que promovem uma forma de a avaliar, as *research questions*:

1. *O tempo despendido pela equipa de auditoria foi diminuído em todas as fases do processo?*

   Espera-se que em todas as fases de auditoria haja melhorias neste aspeto, diminuindo o tempo total para a realização completa de uma auditoria, como é possível comprovar nas previsões efetuadas na tabela 4.1.

2. *O custo com o pessoal é diminuído?*

   Havendo a possibilidade de automatizar muito do que são os processos repetitivos, de reutilizar material já produzido e realizar as auditorias de forma mais rápida, muitos dos custos associados irão diminuir. As horas dos profissionais da auditoria serão agora divididas em vários projetos RGPD, serão menos custosas para cada processo individualmente, havendo menos *rework*, fruto da quantidade diminuta de erros que podem surgir, o custos só tendem a reduzir.

3. *Os erros no processo são minorados?*

Como já foi dito anteriormente, com o *Privacy* temos uma ferramenta que permite construir auditorias de forma guiada e sustentada com o mínimo de intervenção humana possível, fornecendo o seu apoio nas diversas fases do processo. Com as ajudas dadas pela ferramenta no preenchimento de elementos, em cruzar dados, em fazer atribuições com uma interface intuitiva os erros irão rarear, melhorando o processo de auditoria, neste aspeto, em toda a linha.

4. *A qualidade do resultado final diminui, mantém-se ou aumenta?*

   As auditorias são construídas de forma sustentada, com passos firmes e validações exigentes que propiciam um crescimento sólido das mesmas. Por haver menos erros associados a todo o processo de auditoria, a qualidade aumenta, sendo o resultado final mais preciso e adequado. O aumento de qualidade promove uma auditoria o mais completa possível que se dirige a todos os pontos fulcrais no que toca à privacidade de dados nas diversas operações das organizações auditadas.

4.2 Nova forma de realizar auditorias

O primeiro uso da ferramenta será o mais lento, pela necessidade de popular a mesma com os materiais de auditoria necessários, mas auditoria após auditoria, este uso permite o crescimento da ferramenta, por vai enriquecendo a *pool* de conteúdos, tornando os processo efetivamente mais rápidos. Quando a ferramenta estiver praticamente estabilizada em termos de materiais e tiver elementos de auditoria (questionários, fragilidades, ...) suficientes, aproximamos-nos então de um uso mais constante e linear, de onde é possível estimar uma redução de mais de 60% do tempo necessário para realizar esta auditoria (para empresas de complexidade de operação média).

Na secção 2.1.1, na figura 2.1 explicitou-se uma estimativa da duração de um projeto RGPD, da fase 1 à fase 6. Com a influência do *Privacy*, prevê-se agora melhorias em todas as fases do processo.

Temos uma fase 1 que diminui de forma considerável, passando dos anteriores 5-10 dias úteis para um dia útil apenas. Isto é explicado com a forte componente de questionários que integra o *Privacy*, que oferece maior dinamismo na sua construção e a possibilidade de clonar existentes, replicando os mesmos para contextos idênticos.

Na fase 2, apesar de ser tempo do cliente, é expectável que este seja mais rápido a responder. Para isto contribui o facto de a plataforma ser *user-friendly*, o que facilita o seu preenchimento. Para além disso, por parte do DPO (que é o ponto de contacto com o cliente), é possível poupar tempo ao ter uma perceção exata do estado dos questionários, o que anula a necessidade de contatar os responsáveis pelo seu preenchimento, para saber do estado dos mesmos, podendo desde logo pressionar para que sejam preenchidos. Anulando esta necessidade de contato, anula-se o tempo perdido nessas comunicações, anula-se as demoras na resposta (só para saber o estado), dando mais controlo ao DPO.

Entrando na fase 3, a análise aos questionários diminui também de forma considerável, dos anteriores 7-8 dias úteis para 5 dias úteis, por haver uma estrutura analítica já montada, permitindo uma análise questão a questão de questionários específicos, bem atribuídos e bem organizados, não havendo a necessidade de procurar por eles nas pilhas de artefatos produzidos pela auditoria. O facto de poder sistematizar as dúvidas decorrentes das respostas em notas próprias do questionário, ajuda a manter a organização e ajuda a que essa dúvida seja imediatamente recuperada na fase de entrevistas, poupando em si tempo.

Na fase 4, prevê-se uma melhoria residual, passando dos 10 dias úteis para 9 dias úteis. Esta fase costuma ser presencial pelo que o sistema não pode ajudar muito na sua execução. Ainda assim se atá aqui todas informações e dúvidas estiverem sistematizadas de forma correta, é possível arrecadar um conjunto de informação organizada que indubitavelmente facilitará o trabalho de quem tem que conduzir essas entrevistas. Esta fase é extremamente importante, pois é aqui que se retiram a maioria das ilações acerca das reais situações RGPD das organizações auditadas, anulando contradições nas respostas anteriores e chegando a pormenores acerca da operação diária que um questionário pode não chegar. Esta é a fase em que existe uma interação humano-humano que não pode ser descurada e como tal espera-se que a melhoria temporal não seja assim tanta.

A fase 5, regra geral, é das fases mais demoradas das auditorias por ser aquela em que existe maior indefinição e por isso maior *rework*, juntando tudo isso a uma quantidade de informação absurda que torna muito difícil de processar. Com o *Privacy*, acredita-se numa construção da auditoria sustentada, pensada, com passos bem definidos e por isso com tudo o que foi feito nas fases anteriores, ao chegar ao fim da fase de entrevistas já não pode haver dúvidas e todo o trabalho feito para trás é sólido ao ponto de ser considerado final. Assim, espera-se que a fase de dúvidas seja anulada, sendo esta a maior contribuição temporal que o *Privacy* pode oferecer.

Por fim, na fase 6, existe uma diminuição significativa, passando dos anteriores 15 dias úteis para apenas 3 dias úteis. O facto de não se ter de escrever textos densos e extensos reduz em muito a duração desta fase. Os relatórios são agora construídos ao longo de todo o processo de auditoria, sendo a informação que contêm, sistematizada ao longo do mesmo. Hoje, estando em qualquer fase do projeto, o auditor pode começar a retirar apontamentos, alinhavar recomendações, avaliar riscos, para os relatórios oferecidos pela plataforma, gerados de forma automática, tendo aquilo que se espera que sejam os tais 3 dias para limar arestas e finalizar tudo aquilo que considere pertinente.

4.3 *Privacy* sem módulo de gestão vs. *Privacy* com módulo de gestão

Após as descrições dos melhoramentos trazidos pela ferramenta, como um todo, focamo-nos agora na avaliação do módulo de gestão.

1. Preparação dos Questionários	2. Questionários	3. Análise dos Questionários	4. Entrevistas	5. Fase de Dúvidas	6. Relatórios / Recomendações
Sem *Privacy*					
5-10 dias	Tempo do cliente	7-8 dias	10 dias	variável	15 dias
Com *Privacy*					
1 dia	Tempo do cliente	5 dias	9 dias	–	3 dias

Tabela 4.1: Estimativa de duração de cada fase de um projeto de auditoria RGPD com e sem o *Privacy*

Se o módulo de gestão não existisse, toda a administração de dados na plataforma seria extremamente difícil de executar. Os utilizadores teriam que inserir dados diretamente na base de dados, sendo que essa inserção não passaria nunca pelos filtros da interface e da lógica de negócio onde existem alguns passos de verificação e validação dessa mesma informação. Ora, a inexistência deste módulo traria muitos problemas.

A nível de segurança, sem as devidas validações poderiam haver ataques aos dados, dando origem a *leaks* que contém conhecimentos de negócio e informações pessoais bastante sensíveis, e ataques à própria base de dados, podendo adulterar ou destruir elementos integrantes, estragando o negócio da auditora. Seria uma tarefa muito difícil cumprir com a confidencialidade, a integridade e a disponibilidade a que a ferramenta se propunha.

A um nível de usabilidade, os utilizadores seriam obrigados a colocar as mãos em código, prolongando a curva de aprendizagem, dificultando em muito o uso da plataforma. Haveria a necessidade de os utilizadores terem de aprender competências novas para usar a ferramenta, tendo que, por exemplo, um auditor da parte legal, ter noções de SQL para usar a ferramenta. Ou seja, seria uma tarefa difícil inserir e cruzar dados no sistema. Sem a devida validação, a ferramenta estaria exposta também a que erros fossem introduzidos frequentemente, pois os utilizadores também não têm as noções de tipos de dados e toda a sua experiência de utilização é difícil de prever pelo seria de esperar que o sistema despertasse muitos erros, difíceis de analisar para o utilizador leigo no ramo de informática, que acaba por ser o público-alvo da ferramenta.

Com o módulo de gestão, temos uma interface que coloca toda a lógica de negócio numa linguagem *high-level* a que o utilizador é familiar e é capaz de compreender, suprimindo-se a necessidade de formação para além do uso da ferramenta, tornando-a de fácil uso, intuitiva e organizada, podendo os profissionais da auditoria focarem-se nas suas competências centrais e no valor que aportam ao resultado final da mesma.

Temos também que, com o módulo de gestão, todas as premissas de segurança são asseguradas, sendo os dados protegidos de acessos indevidos e sendo o sistema protegido de ataques à sua integridade. As validações e o controlo de acessos provenientes da implementação deste módulo ajudam a que, a ferramenta em si, cumpra com a norma vigente.

Em suma, o módulo de gestão aumenta os níveis de usabilidade e segurança da ferramenta, tornando-a acessível e robusta.

4.4 Sumário

Neste capítulo avaliou-se o módulo de gestão e a ferramenta produzida como um todo sob a perspetiva dos melhoramentos trazidos ao próprio sistema e ao panorama das auditorias, respetivamente. Detalhou-se a importância do módulo de gestão no sistema e comparou-se a execução de auditorias pré e pós-*Privacy*, fazendo algumas previsões acerca do aprimoramento do processo RGPD. Concluiu-se que o uso do *Privacy* facilita em toda a linha a condução das auditorias, agregando às mesmas valor através do uso de ferramentas adequadas, adaptadas às necessidades que surgem e que cumprem em si as premissas de segurança, qualidade, organização e estruturação necessárias ao seu contexto. O próximo capítulo apresenta as conclusões retiradas de todo o projeto e o trabalho futuro a desenvolver.

Capítulo 5

Conclusão

Neste capítulo, fala-se acerca do que era o problema e como o sistema produzido veio solucioná-lo. Indicou-se também alguns indicadores que poderão guiar o processo de avaliação da ferramenta no futuro.

5.1 O Problema vs. A solução

O problema identificado foi a manifesta incapacidade, a nível orçamental, de organizações com grande complexidade de operação e pequena dimensão terem projetos de RGPD executados de forma correta e completa com alta qualidade no seu resultado final. O *Privacy* surgiu com a motivação de levar premissas de qualidade a todos os segmentos do mercado, a baixo custo, para que em todos haja uma avaliação da privacidade precisa, que trará inúmeras mais valias à atuação das organizações, defendendo-as dos demais riscos a que estão sujeitas. Não só riscos de coimas avultadas, por não conformidade com a norma, como também riscos de segurança, por ter informações sensíveis expostas que prejudicarão o negócio e os titulares dos dados caso caiam nas mãos erradas.

A solução para o problema identificado, foi automatizar o processos de auditoria, onde eles podiam ser automatizados. O *Privacy* veio providenciar uma ferramenta de apoio para os dois lados da auditoria: a equipa de privacidade de dados da organização auditada e a equipa de auditoria.

Através da possibilidade de reutilizar material, de produzir artefatos como questionários de forma rápida e dinâmica, de apontar fragilidades construídas de forma robusta com origens e recomendações bem definidas, de gerar relatórios rapidamente, de promover auditorias sucintas a vários clientes ao mesmo tempo, podemos concluir que todo este processo RGPD se torna mais rápido e mais barato, pois existe menos intervenção humana em cada processo, o que irá, inevitavelmente, reduzir o orçamento. A necessidade dessa intervenção pode ser dividida também por vários casos em simultâneo diluindo o valor da hora dos profissionais envolvidos por diversos projetos, o que tornará também cada projeto, individualmente, mais barato e acessível.

Com projetos mais baratos e executados de forma mais expedita seria de esperar que a qualidade dos mesmos diminuísse, mas mais uma vez o *Privacy*, resolve o problema agregando ainda mais qualidade a este tipo de auditorias. Hoje, temos a possibilidade de:

- Acompanhar quase em tempo real a situação da auditoria;
- Avaliar a situação de risco e agir em conformidade de forma imediata;
- Ter mais controlo sobre todos os processos que a auditoria abarca;
- Ter uma ferramenta exclusivamente focada no que processos deste tipo exigem;
- Ter menos permeabilidade a erros por haver uma construção da auditoria de forma guiada, sustentada e intervenção humana em situações puramente necessárias;
- Ter toda a informação inerente à auditoria centralizada num único sítio o que facilita a sua análise, impedindo que disperse por vários locais;
- Anular as perdas de tempo que eram associadas às demoras a preencher elementos da auditoria;
- Facilitar a comunicação entre as equipas e responsáveis departamentais;
- Acrescer todo este processo de muito mais segurança e confiabilidade;
- Introduzir melhoramentos incontestáveis em relação à solução manual prévia, com a sua evidente falta de preparação para se endereçar a projetos deste género.

Associado à construção do *Privacy*, surgiu o problema de gerir toda a informação de auditoria. Implementou-se o módulo de gestão, que garantiu uma interface fácil de usar, estruturada e organizada, com segurança associada, que evitou as inúmeras contrariedades que a sua não implementação traria, como por exemplo, a necessidade de formações para lá do âmbito de uso da ferramenta e as possibilidades de ataques que seriam possíveis se não houvessem as validações presentes no mesmo.

A inserção de dados de auditoria na BD é hoje acessível ao utilizador comum, que não tem noções de programação, e é feita de forma segura, precavendo usos impróprios das funcionalidade contidas no módulo e ataques à informação contida no mesmo.

5.2 Trabalho futuro

Por falta de um caso de estudo, devido à pandemia COVID-19, foi difícil recolher dados que comprovem os melhoramentos trazidos pela plataforma desenvolvida. A inexistência de indicadores bem construídos deixa a estratégia organizacional à deriva, sem

se saber se estamos a conseguir alcançar aquilo a que nos propusemos. Assim foram recolhidos alguns indicadores pertinentes de avaliar numa ferramenta deste tipo.

Analisando de forma mais objetiva, em primeiro lugar surge a **produção** que se pode definir como o número médio de tarefas executadas pelo utilizador da ferramenta. De seguida vem a **produtividade**, que é a medição da produção em relação aos recursos utilizados para um projeto, ou seja o número médio de tarefas realizadas por cada membro de *staff*.

Em termos de conceitos mais abstratos, a **qualidade** é também um indicador importante, que se define como o grau em que dado *software* possui uma combinação desejada de atributos. Versa por isso em conseguir manter um *software* que não se cinge só em cumprir as suas funcionalidades, mas sim em reunir um conjunto de características que elevam o seu patamar, quer de forma externa, visíveis ao utilizador em *run-time*, como de forma interna, visíveis à equipa de desenvolvimento, ajudando-a a atingir as qualidades externas. Por fim, a **inovação**, cuja intenção é verificar se os esforços de inovação estão a gerar resultados positivos; caso não estejam, o gestor pode utilizar as informações para reavaliar sua metodologia e reverter a situação. Assim, podemos reunir vários subindicadores, tais como a taxa de sucesso das ideias implementadas, o investimento em *R&D* (*Research and Development*), a quantidade de ideias geradas em determinado produto, a quantidade de inovações trazidas ao contexto do produto e redução de custos trazida pelo artefato fornecido.

Como consequência da pandemia, o projeto de desenvolvimento sofreu alguns atrasos e foi também impossível encontrar uma organização capaz de servir como caso de estudo admissível para avaliar de forma sustentada a ferramenta produzida e como tal a aplicação e resultados destes indicadores ficaram destinados para um caso de estudo reservado para trabalho futuro.

Bibliografia

[1] "Portal do dpo - obtenção do consentimento." https://www.portaldodpo.pt/blog/service/consentimento/, 2018. [Online] Acedido a 11/2020.

[2] "Portal do dpo - *Cookies*." https://www.portaldodpo.pt/blog/service/cookies/, 2018. [Online] Acedido a 11/2020.

[3] "The world's most valuable resource is no longer oil, but data." https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data, 2017. [Online] Acedido a 11/2020.

[4] RSA, "RSA Data Privacy & Security Report." https://www.rsa.com/content/dam/en/e-book/rsa-data-privacy-report.pdf, 2018. [Online] Acedido a 11/2020.

[5] M. Nadeau, "General Data Protection Regulation (GDPR): What you need to know to stay compliant." https://www.csoonline.com/article/3202771/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html, 2020. [Online] Acedido a 11/2020.

[6] Netsparker, "The Road to GDPR Compliance." https://www.netsparker.com/whitepaper-general-data-protection-regulations-gdpr/, 2018. [Online] Acedido a 11/2020.

[7] P. Europeu, "Regulamento geral da protecao de dados (artigo 6º).," *Jornal Oficial da União Europeia*, vol. L 119/1, 2016-04-27.

[8] P. Europeu, "Regulamento geral da protecao de dados (artigo 30º).," *Jornal Oficial da União Europeia*, vol. L 119/1, 2016-04-27.

[9] "Categorias dos dados pessoais." https://www.portaldodpo.pt/categorias-de-dados/, 2018. [Online] Acedido a 11/2020.

[10] P. Europeu, "Regulamento geral da protecao de dados (artigo 15º).," *Jornal Oficial da União Europeia*, vol. L 119/1, 2016-04-27.

[11] P. Europeu, "Regulamento geral da protecao de dados (artigo 16º).," *Jornal Oficial da União Europeia*, vol. L 119/1, 2016-04-27.

[12] P. Europeu, "Regulamento geral da protecao de dados (artigo 17º).," *Jornal Oficial da União Europeia*, vol. L 119/1, 2016-04-27.

[13] P. Europeu, "Regulamento geral da protecao de dados (artigo 18º).," *Jornal Oficial da União Europeia*, vol. L 119/1, 2016-04-27.

[14] P. Europeu, "Regulamento geral da protecao de dados (artigo 20º).," *Jornal Oficial da União Europeia*, vol. L 119/1, 2016-04-27.

[15] P. Europeu, "Regulamento geral da protecao de dados (artigo 21º).," *Jornal Oficial da União Europeia*, vol. L 119/1, 2016-04-27.

[16] P. Europeu, "Regulamento geral da protecao de dados (artigo 19º).," *Jornal Oficial da União Europeia*, vol. L 119/1, 2016-04-27.

[17] P. Europeu, "Regulamento geral da protecao de dados (artigo 22º).," *Jornal Oficial da União Europeia*, vol. L 119/1, 2016-04-27.

[18] P. Europeu, "Regulamento geral da protecao de dados (artigo 4º).," *Jornal Oficial da União Europeia*, vol. L 119/1, 2016-04-27.

[19] E. Politou, E. Alepis, and C. Patsakis, "Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions," *Journal of Cybersecurity*, vol. 4, 03 2018. tyy001.

[20] "Gdpr attack plan - 02 the roles of gdpr." `https://info.varonis.com/thank-you/course/gdpr-attack-plan?`, 2017. [Online] Acedido a 11/2020.

[21] P. Europeu, "Regulamento geral da protecao de dados (artigo 25º).," *Jornal Oficial da União Europeia*, vol. L 119/1, 2016-04-27.

[22] P. Europeu, "Regulamento geral da protecao de dados (artigo 24º).," *Jornal Oficial da União Europeia*, vol. L 119/1, 2016-04-27.

[23] P. Europeu, "Regulamento geral da protecao de dados (artigo 28º).," *Jornal Oficial da União Europeia*, vol. L 119/1, 2016-04-27.

[24] P. Europeu, "Regulamento geral da protecao de dados (artigo 31º).," *Jornal Oficial da União Europeia*, vol. L 119/1, 2016-04-27.

[25] P. Europeu, "Regulamento geral da protecao de dados (artigo 32º).," *Jornal Oficial da União Europeia*, vol. L 119/1, 2016-04-27.

[26] P. Europeu, "Regulamento geral da protecao de dados (artigo 33º).," *Jornal Oficial da União Europeia*, vol. L 119/1, 2016-04-27.

[27] P. Europeu, "Regulamento geral da protecao de dados (artigo 35º).," *Jornal Oficial da União Europeia*, vol. L 119/1, 2016-04-27.

[28] P. Europeu, "Regulamento geral da protecao de dados (artigo 37º).," *Jornal Oficial da União Europeia*, vol. L 119/1, 2016-04-27.

[29] P. Europeu, "Regulamento geral da protecao de dados (artigo 38º).," *Jornal Oficial da União Europeia*, vol. L 119/1, 2016-04-27.

[30] P. Europeu, "Regulamento geral da protecao de dados (artigo 39º).," *Jornal Oficial da União Europeia*, vol. L 119/1, 2016-04-27.

[31] P. Europeu, "Regulamento geral da protecao de dados (artigo 51º).," *Jornal Oficial da União Europeia*, vol. L 119/1, 2016-04-27.

[32] P. Europeu, "Regulamento geral da protecao de dados (artigo 58º).," *Jornal Oficial da União Europeia*, vol. L 119/1, 2016-04-27.

[33] "Proposta de lei nº120/xiii (3ª)," 2018.

[34] "Portal do dpo - criação de uma política de privacidade." `https://www.portaldodpo.pt/blog/service/criacao-de-politica-de-privacidade/`, 2018. [Online] Acedido a 11/2020.

[35] C. Tankard, "What the gdpr means for businesses," *Network Security*, vol. 2016, pp. 5–8, 06 2016.

[36] P. Europeu, "Regulamento geral da protecao de dados (artigo 41º).," *Jornal Oficial da União Europeia*, vol. L 119/1, 2016-04-27.

[37] "Grc (governance, risk management and compliance) software." `https://searchcio.techtarget.com/definition/GRC-governance-risk-management-and-compliance-software`, 2010. [Online] Acedido a 11/2020.

[38] "Major components of it grc solutions." `https://www.cisoplatform.com/m/blogpost?id=6514552%3ABlogPost%3A37019`, 2015. [Online] Acedido a 11/2020.

[39] "Eramba: Taking the complexity and cost out of grc." `https://dryve.cc/2018/12/eramba-taking-the-complexity-and-cost-out-of-grc/`, 2018. [Online] Acedido a 11/2020.

[40] "Eramba documentation." https://www.eramba.org/documentation. [Online] Acedido a 11/2020.

[41] "Eramba vulnerabilities." https://www.cvedetails.com/vulnerability-list/vendor_id-17757/Eramba.html, 2018. [Online] Acedido a 11/2020.

[42] "Simplerisk documentation." https://simplerisk.freshdesk.com/support/solutions/articles/6000190811-simplerisk-feature-roadmap. [Online] Acedido a 11/2020.

[43] "Simplerisk vulnerabilities." https://www.cvedetails.com/vulnerability-list/vendor_id-13286/Simplerisk.html, 2017. [Online] Acedido a 11/2020.