INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Privacidade e Proteção de Dados Pessoais – Desenho de Processos de Negócio Seguros e Privados nas Organizações

André Filipe Ferreira de Almeida

Mestrado em Engenharia de Telecomunicações e Informática

Orientador:
Professor Doutor Vítor Manuel Basto Fernandes, Professor Auxiliar com Agregação
Iscte – Instituto Universitário de Lisboa

Coorientador:
Professor Doutor Carlos José Corredoura Serrão, Professor Associado
Iscte – Instituto Universitário de Lisboa

Outubro, 2020

Agradecimentos

Em primeiro lugar, gostaria de agradecer aos meus orientadores, Prof. Doutor Vítor Manuel Basto Fernandes e Prof. Doutor Carlos José Corredoura Serrão, por confiarem em mim para realizar este trabalho e por toda a ajuda e ensinamentos ao longo do desenvolvimento da dissertação.

Aos meus colegas de curso por todos os bons momentos que passei neste percurso académico, por me fazerem companhia nos bons e maus momentos, nas noitadas a estudar na faculdade e também nas festas para descomprimir.

Aos meus amigos cientistas, Bianca, Sofia, Francisco e Rúben, por me mostrarem que não é necessário sermos colegas de curso para sermos bons amigos e que na FCUL também há boa gente.

Aos grandes amigos que a faculdade me trouxe, Gonçalo Caldeira, João Oliveira, Rita Peixoto e Rúben Silva, obrigado por acreditarem em mim e me ajudarem sempre que precisei. Foram uma parte importantíssima de todo o meu percurso desde o primeiro dia, em setembro de 2014.

E principalmente, à Beatriz Duarte, a companheira de uma vida. Obrigado por acreditares em mim, nas minhas capacidades e principalmente por não desistires de mim mesmo quando eu já o tinha feito. Sem ti não teria terminado a etapa mais importante da minha vida. Parte do meu sucesso serás sempre tu.

Por fim e não menos importante, obrigado à minha família, que sempre me proporcionou as melhores condições para atingir o sucesso tanto académico como pessoal. Muito obrigado mãe, pai e kika.

Resumo

Atualmente o conhecimento sobre o tema da privacidade e proteção de dados já é grande, mas a nível empresarial, a sua aplicação e tratamento ainda consiste num grande desafio. No presente, as empresas colocam cada vez mais esforços na investigação deste tema pois envolve variadas áreas do conhecimento, tais como processos de negócio, tecnologia, enquadramento legal, entre outros.

Esta dissertação tem como objetivo desenvolver uma nova metodologia de aplicação de boas práticas para tentar resolver estes novos problemas que vieram com o novo regulamente geral de proteção de dados, RGPD. Essa metodologia é dividida em três partes, o desenvolvimento de um modelo de processos de negócio em BPMN, a criação de *tags* de segurança em XSD e a incorporação das últimas no diagrama desenvolvido.

O trabalho desenvolvido nesta dissertação veio contribuir para o aumento do conhecimento acerca do desenho de processos de negócio seguros e privados nas organizações.

Com o trabalho desenvolvido foi possível compreender que ainda existe um caminho a percorrer de maneira a facilitar e simplificar o processo de analisar o cumprimento do RGPD nas organizações.

Palavras-Chave: RGPD, Dados Pessoais, Segurança, Informação, Privacidade, Proteção, XML, XSD.

Abstract

Nowadays the knowledge on the subject of privacy and data protection is already great, but at the business level, its application and treatment is still a great challenge. At present, companies are putting more and more efforts into the investigation of this topic as it involves various areas of knowledge, such as business processes, technology, legal framework, among others.

This dissertation aims to develop a new methodology for applying good practices to try to solve these new problems that came with the new general data protection regulation, GDPR. This methodology is divided into three parts, the development of a business process model in BPMN, the creation of security tags in XSD and the incorporation of the security tags in the developed diagram.

The work developed in this dissertation contributed to increase knowledge about the design of safe and private business processes in organizations.

With the work developed, it was possible to understand that there is still a way to go in order to facilitate and simplify the process of analyzing GDPR compliance in organizations.

Keywords: GDPR, Personal Data, Security, Information, Privacy, Protection, XML, XSD.

Índice

Índice de Figuras

Índice de Tabelas

Lista de Abreviaturas e Siglas

3DES - *Triple Data Encryption Standard*

AES - *Advance Encryption Standard*

BPD - *Business Process Diagram*

BPEL4WS - *Business Process Execution Language for Web Services*

BPMI - *Business Process Management Initiative*

BPML - *Business Process Modeling Language*

BPMN - *Business Process Modeling Notation*

BPQL - *Business Process Query Language*

CRUD – *Create, Read, Update, Delete*

DES - *Data Encryption Standard*

DPC – *Data Protection Coordinator*

DPO - *Data Protection Officer*

DSR - *Design Science Research*

DSR - *Design Science Research Methodology*

EDPS - *European Data Protection Supervisor*

EPD - Encarregado de Proteção de Dados

GDPR - *General Data Protection Regulation*

GPS – *Global Positioning System*

IBM - *International Business Machines Corporation*

IDE - *Integrated Development Environment*

IP - *Internet Protocol*

IPI - *Informação Pessoalmente Identificável*

IRS - *Imposto sobre o Rendimento das Pessoas Singulares*

IT - *Iinformation Technology*

MAC - *Media Access Control*

NIST - *National Institute of Standards and Technology*

OMG® - *Object Management Group*

PII - *Personal Identifying Information*

RGPD – Regulamento Geral de Proteção de Dados

SGML - *Standard Generalized Markup Language*

UML - *Unified Modeling Language*

W3C - *World Wide Web Consortium* (W3C

XML - *Extensible Markup Language*

XSD - *XML Schema Definition*

Capítulo 1 – Introdução

1.1. Enquadramento do tema

Desde 26 de Outubro de 1998, última regulamentação referente à proteção de dados (Assembleia da República, 1998), que não eram feitas alterações à legislação existente. Hoje em dia, o fluxo de informação é muito grande e sem a implementação de novas restrições e regulamentações tornar-se-ia extremamente difícil, senão mesmo impossível, manter controlo sobre os nossos dados pessoais dados às mais variadas instituições, *sites*, aplicações, entre outros (Regulamento (UE) 2016/679, 2016).

Em maio de 2018, foi criada uma regulamentação Europeia relativa à proteção de dados, chamada RGPD. Este novo regulamento contém todos os requisitos detalhados da nova política de proteção de dados, e das consequentes penalizações para as empresas que não o cumprem. O intuito, por parte da União Europeia, com a aprovação e implementação destas medidas é a aplicação de políticas de tratamento seguro de dados (McGavisk, 2019).

Atualmente, apesar de existir legislação (Regulamento (UE) 2016/679, 2016), e informação sobre este tema, cada organização é diferente, fazendo com que as suas responsabilidades face ao RGPD sejam também elas diferentes. Desta forma, mesmo já tendo chegado ao fim o período de dois anos de adaptação, as empresas ainda se encontram num período de dúvidas sobre o que fazer (Reis, 2018).

Num estudo realizado pela *Dell and Dimension Research* (SuperOffice, 2018), onde foram analizados cerca de 800 profissionais da área de IT, estando responsáveis pela proteção de dados em empresas, observou-se que cerca de 80% conheciam apenas superficialmente os detalhes do RGPD e ainda não finalizaram a implementação das medidas necessárias, tal como é possível observar na figura 1, somando as respostas “fase de implementação” e “ainda não iniciaram a fase de implementação”. Mais de 1 em cada 4 empresas estudadas não teriam começado a implementar o regulamento.

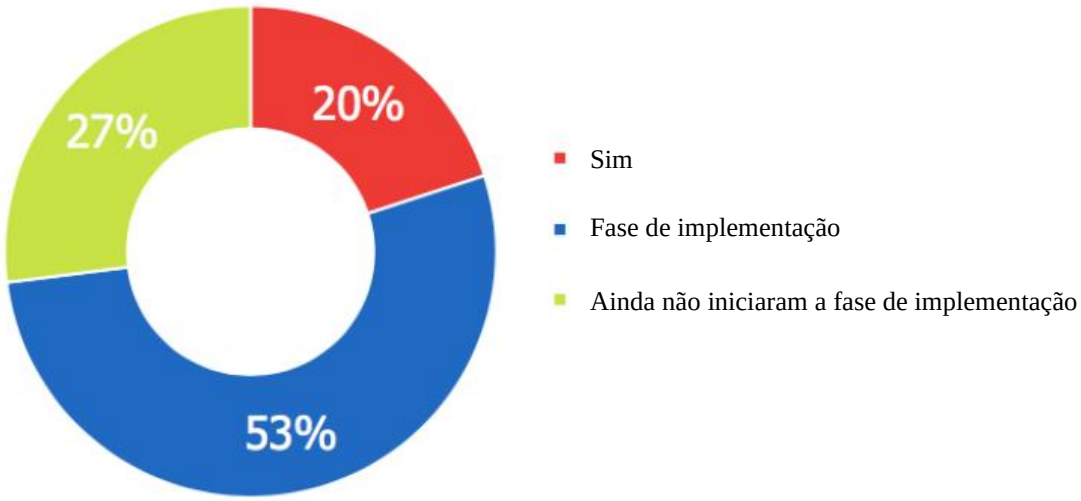


Figura 1 *- Percentagem de empresas, num estudo com 821, que responderam à pergunta "Está o seu negócio em concordância com o Regulamento Geral de Proteção de Dados da União Europeia?". Adaptado de (SuperOffice,2018).*

O incumprimento do RGPD tem consequências a vários níveis (SuperOffice, 2018):

1. **Económico:** Esta consequência é a que mais preocupa as empresas, pois podem ser aplicadas penalizações até 20 milhões de euros, ou 4% do rendimento anual da empresa. Esta sanção varia consoante o tipo de incumprimento, quer seja negligência, recorrência, entre outros aspetos, por exemplo, quantas pessoas afetadas ou quais os danos causados. Além de penalizações administrativas, as empresas correm o risco de sofrer repercursões financeiras devido a indeminizações pedidas pelos afetados.
2. **Reputacional:** O incumprimento do RGPD pode levar as empresas a sofrerem escrutínio público. A falta de confiança e publicidade negativa deverá ser um fator preocupante além das sanções.
3. **Comercial:** A possibilidade de os dados pessoais dos consumidores não estarem protegidos, pode levá-los a procurar uma outra alternativa que esteja de acordo com o RGPD. Este incumprimento pode afetar, também, parcerias com outras empresas.

1.2. Motivação e relevância do tema

Desta forma, cresce a necessidade de criar uma simples metodologia que torne mais fácil o cumprimento desta nova legislação que entrou em vigor a 25 de maio de 2018. Para tal, pretende-se aplicar boas práticas de forma a ajudar a resolver os desafios que advêm desta nova regulação de proteção de dados pessoais.

O objetivo deste trabalho é criar uma metodologia que permita analisar os dados pessoais e o respetivo cumprimento, ou não, do RGPD de um modelo de processo de negócio. Nesta dissertação, de forma a testar a metodologia criada, foi utilizado como caso de estudo, o processo de inscrição e matriculação dos alunos no Iscte-Instituto Universitário de Lisboa.

1.3. Questões e objetivos de investigação

Com esta dissertação serão levantadas algumas questões, incluindo o problema principal de investigação, abaixo descrito.

1.3.1. Problema de Investigação

O problema tratado nesta dissertação provém da falta de ferramentas que permitam a uma empresa analisar e melhorar a *compliance* do RGPD a modelos de negócio na linguagem BPMN. Deste modo pretende-se efetuar um acrescento à norma XML, criando um sistema de análise dos processos de negócio na linguagem BPMN através de *tags* de segurança, a fim de avaliar a extensão do cumprimento do RGPD.

Com este trabalho, pretende-se não só facilitar as empresas a melhor cumprirem o RGPD, assim como fomentar um maior respeito pela privacidade dos utilizadores assim como dos seus dados pessoais.

1.3.2. Questões de Investigação

A formulação do problema levanta a seguinte questão que foi utilizada como guia para a realização da dissertação:

Será possível melhorar o desenho de processos de negócios das organizações tendo em consideração requisitos de privacidade e de segurança, de forma a que os mesmos possam estar alinhados com as recomendações do RGPD?

1.3.3. Objetivos de Investigação

Sendo a motivação a contribuição para a protecção da informação da instituição, definiram-se os seguintes objectivos:

- Identificar ferramentas para edição de ficheiros XSD, XML e BPMN.
- Estruturar metodologia que torne mais fácil o cumprimento do RGPD.
- Estruturar um processo de modelo de negócio em BPMN que substituiria o modelo anteriormente escrito em texto simples.
- Incorporação das *tags* de segurança criadas no diagrama desenvolvido.

1.4.Abordagem metodológica

A metodologia *Design Science Research* (DSRM) foca-se na importância de criar, desenvolver e avaliar diferentes artefactos para atender e solucionar os objetivos e problemas propostos e relevantes (Peffers et al., 2008). *Design Science Research* (DSR) é um processo de resolução de problemas, o que significa que o seu objetivo principal é a aquisição de conhecimento e compreensibilidade dos problemas e suas respetivas soluções para permitir o desenvolvimento e a aplicação desses artefactos criados através da metodologia (Hevner et al., 2004). Assim, são propostas sete diretrizes de DSR a serem seguidas de modo a provar o sucesso de cada um dos artefactos:

1. ***Design as an Artifact*:** produzir artefactos viáveis e bem-sucedidos que podem ser definidos como de construção, modelo, método ou instanciação.
2. **Relevância do Problema:** desenvolver soluções capazes de resolver problemas tecnológicos ou problemas relevantes de negócios.
3. **Avaliação do Projeto:** a utilidade, qualidade e eficácia de cada um dos artefactos criados, deve ser demonstrada através de métodos de avaliação adequados.
4. **Contribuições de Pesquisa:** fornecer contribuições que possam ser verificadas nas áreas de foco de cada um dos artefactos.
5. **Rigor da Pesquisa:** aplicação de métodos rigorosos para desenvolver, demonstrar e avaliar os artefactos.
6. ***Design* como um Processo de Busca:** utilização de todos os meios disponíveis para alcançar um fim desejado, no âmbito do problema.
7. **Comunicação da Pesquisa:** apresentado tanto a audiências tecnológicas como administrativas.

A DSRM baseia-se em seis passos principais (Peffers et al., 2008):

1. Identificação do problema e motivação.
2. Definição dos objetivos.
3. *Design* e desenvolvimento da proposta de solução.
4. Demonstração da utilização da proposta desenvolvida.
5. Avaliação da proposta apresentada e dos seus resultados.
6. Comunicação.

Consoante o tipo de investigação em curso, a metodologia pode iniciar-se num ponto de entrada diferente do passo inicial (Figura 2). Em relação a esta dissertação, o ponto de entrada é o primeiro passo – identificação do problema e motivação (Huber et al., 2016) (Figura 3).

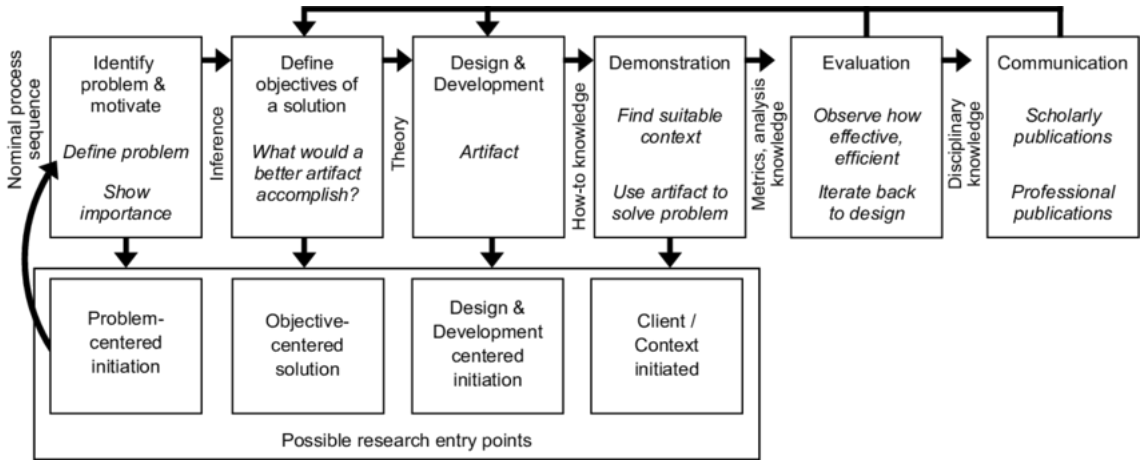


Figura 2 *- "Design Science Research Metodology". Adaptado de 9.*

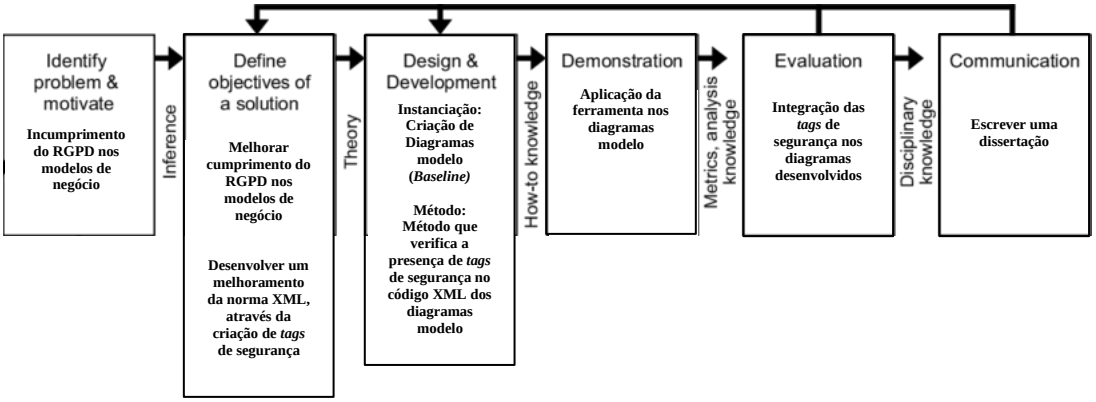


Figura 3 *- Adaptação da "Design Science Research Metodology" aplicada à dissertação.*

Nesta dissertação serão propostas extensões à norma BPMN para modelação de propriedades relacionadas com a privacidade e proteção de dados pessoais, e desenvolvidos artefactos, nomeadamente, um diagrama de processos que ocorrem no Iscte-Instituto Universitário de Lisboa, tal como o processo de matriculação dos alunos no Iscte-Instituto Universitário de Lisboa (*Baseline*). A utilização combinada desses artefactos, assim como a possibilidade de melhorias a partir desses modelos, permitem às organizações progredir de forma mais rápida e consistente para a desejada implementação do RGPD.

A demonstração dos artefactos é feita através da sua aplicação num diagrama relativo a processos que os alunos do Iscte-Instituto Universitário de Lisboa necessitam realizar, de modo a estarem corretamente inscritos no ano letivo correspondente.

1.5. Estrutura do documento

Este documento contém uma breve introdução sobre a proteção de dados pessoais. Esta é seguida por um capítulo onde é explicado o que são dados pessoais, são apresentadas processos de negócios e respetivas normas e são identificados algoritmos de cifragem. De seguida, encontra-se o caso de estudo, onde é explicado o desenvolvimento do diagrama de processo de modelo de negócio, assim como os seus vários componentes. São ainda apresentados os requisitos de segurança da informação. O capítulo seguinte expõe as *tags* de segurança desenvolvidas. Por fim, encontram-se o capítulo das conclusões e trabalho futuro.

Capítulo 2 – Revisão da Literatura

Neste capítulo serão apresentados os principais tópicos relativos ao RGPD, bem como o estado da arte sobre ferramentas de desenho de processos de negócio, adaptadas à privacidade e proteção de dados pessoais.

2.1.Dados Pessoais

2.1.1. O que são dados pessoais?

Segundo o artigo 4º do RGPD (Regulamento (UE) 2016/679, 2016), dados pessoais são dados que tornam possível identificar/tornar identificável uma pessoa singular. É considerada identificável uma pessoa que possa ser identificada direta ou indiretamente. Pode ser identificada através de um nome, número de identificação, localização, ou elementos de identidade física, cultural, fisiológica, económica, entre outros.

Para se saber se segundo o RGPD os dados tratados são dados pessoais, faz-se um "simples" teste que consiste em avaliar se através de mais do que um dado se consegue descobrir a identidade da pessoa, direta ou indiretamente. A identificação dá-se com dados diretos (por exemplo, nome ou fotografia do titular dos dados), ou através da combinação de diferentes dados indiretos (por exemplo, morada ou número de conta bancária). É importante ainda salientar que o regulamento se aplica aos dados pessoais pertencentes a pessoas singulares e não aos dados de uma empresa (pessoa coletiva).

O conceito de PII (*Personally Identifiable Information*) (Grimes, 2019) acompanhou o crescimento das tecnologias de informação e a Internet, através do aumento do seu número de utilizadores. Este crescimento facilitou a recolha deste tipo de informação, originando um mercado lucrativo baseado na recolha e revenda de PII (Kroft, 2014).

PII pode ser, ou não, informação sensível. A informação pessoal sensível é aquela que permite identificar uma pessoa singular com base em apenas uma informação, tal como o número de Cartão de Cidadão ou número de conta bancária. A informação não sensível é aquela que para identificar uma pessoa singular, é necessário juntar um conjunto de informações pessoais, tais como a morada, sexo e idade (Grimes, 2019).

Segundo um estudo realizado pela Universidade de Carnegie Mellon (Sweeney, 2000), apenas é necessário ter acesso aos dados pessoais sexo, data de nascimento e código postal para conseguir identificar 87% da população. Com este estudo facilmente

se percebe que apesar de existirem categorias diferentes de dados, todas devem ter o mesmo nível de proteção (Comissão Europeia, 2018a).

2.1.2. Categorias de Dados Pessoais

Os dados pessoais estão divididos em diferentes categorias (Nascimento, 2019):

- **Internos**
  - Conhecimento e Crenças: Dados relativos às opiniões de uma pessoa. Podem ser crenças religiosas, filosóficas. O que uma pessoa pensa/acredita.
  - Autenticação: Informação que o indivíduo sabe que pode ser usada para o autenticar. Podem ser PIN, nome dos filhos, número de animais de estimação, entre outros.
  - Preferência: Dados relativos às preferências, interesses e gostos de um indivíduo.
- **Externos**
  - Identificação: Informação relativa à identificação única ou semi-única da pessoa singular: nome, dados biométricos, identificador único, identificador de governo, fotografia, entre outros.
  - Etnia: Informação relativa à etnia e origens de uma pessoa: raça, linguagens faladas, sotaques, dialetos.
  - Sexual: Dados relativos à identidade sexual de um indivíduo, por exemplo: identidade de género, preferências e tendências.
  - Comportamento: Informação que descreve os hábitos comportamentais ou atividades de um indivíduo, quer seja *on-line* ou não.
  - Demografia: São as características que um indivíduo partilha com outros, tais como: faixa etária e escalão de rendimento.
  - Médica e Saúde: Dados que se referem à saúde de um indivíduo, por exemplo: historial clínico próprio ou de familiares, registos hospitalares, ADN.
  - Física: Dados relativos às características físicas do indivíduo, tais como: altura, tatuagens, peso e idade.

- **Históricos**
    - História da Vida: Informações sobre acontecimentos referentes à vida pessoal de um indivíduo, quer tenham acontecido diretamente ou indiretamente, tendo influenciado a sua vida.
- **Financeiros**
    - Conta: Dados que identificam a conta bancária de uma pessoa individual. Tanto pode ser número de cartão de crédito como número de conta.
    - Propriedade: Informações sobre bens que o indivíduo possui ou possuiu.
    - Transações: Dados referentes a compras, despesas ou receitas de um indivíduo. Por exemplo: impostos, transações ou hábitos de compras.
    - Crédito: Informação referente à credibilidade do indivíduo em questões financeiras. Pode ser registos de créditos, credibilidade ou capacidade de crédito.
- **Sociais**
    - Profissional: Dados referentes à carreira académica ou profissional. Podem ser dados de: títulos de cargos, salário, historial de projetos, escolas frequentadas ou entrevistas
    - Criminal: Informações sobre o historial criminal de um indivíduo. Condenações, acusações ou indultos.
    - Vida Pública: Informações que dizem respeito à vida pública de uma pessoa. Tanto pode ser informações sobre o carácter, posição social, estado cívil, entre outros.
    - Família: Dados relativos às relações familiares que uma pessoa tem. Podem ser dados sobre a estrutura familiar, familiares em si, divórcios ou casamentos.
    - Redes Sociais: Informações referentes aos amigos e as suas ligações sociais com esses mesmos amigos.
    - Comunicação: Dados de comunicações efetuadas ou recebidas pelo indivíduo. Podem ser comunicações via *email*, *voice* m*a*il ou gravações telefónicas.

- **De Rastreamento**
    - Computador: Informações referentes a um dispositivo utilizado por parte do indivíduo para uso pessoal tais como endereço IP (*Internet Protocol*) ou MAC (*Media Access Control)*, impressão digital do navegador.
    - Contacto: Dados com os quais é possível contactar um indivíduo endereço de e-*mail*, morada ou número de telefone.
    - Localização: Informação referente à localização do indivíduo. Coordenadas GPS (Global Positioning System), país ou morada.

2.1.3. Direitos que vêm com o novo regulamento

Com a implementação do novo RGPD, o titular dos dados pessoais tornou-se detentor de vários direitos que anteriormente não possuía (SuperOffice, 2018), entre os quais se destacam os seguintes (Comissão Nacional de Proteção de Dados, 2018):

- O direito de acesso - Os donos têm o direito de solicitar acesso aos seus dados pessoais e de perguntar como estes são utilizados pela empresa após a recolha. A empresa deve fornecer uma cópia dos dados pessoais, gratuitamente e em formato eletrónico, se solicitado.
- O direito ao esquecimento - Se os consumidores deixaram de ser clientes ou se os mesmos retiram o seu consentimento de uma empresa para a utilização dos seus dados pessoais, eles têm o direito de que os seus dados sejam apagados.
- O direito à portabilidade (de dados) - Os indivíduos têm o direito de transferir os seus dados de um provedor de serviços para outro. E isso deve acontecer num formato correntemente utilizado e legível por máquina.
- O direito de ser informado - Abrange qualquer recolha de dados efetuada por empresas, e os donos dos dados pessoais devem ser informados antes da recolha de dados. Os titulares dos dados precisam de aceitar que sejam recolhidos os seus dados e o seu consentimento deve ser concedido livremente e não de maneira implícita.
- O direito de corrigir as informações – Garante que os titulares dos dados possam ter os seus dados atualizados se estiverem desatualizados, incompletos ou incorretos.

- O direito à limitação de tratamento – Passa a ser possível que os titulares dos dados solicitem a não utilização dos seus dados para processamento. Ou seja, o registo dos seus dados pode permanecer armazenado, mas não pode ser utilizado.
- O direito à oposição – O titular dos dados pessoais tem o direito de se opor, em qualquer momento, ao tratamento dos seus dados, por motivos relacionados com a sua situação particular, sempre que esteja em causa: um tratamento necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública; a prossecução dos interesses legítimos do responsável ou de terceiro; uma reutilização dos dados para uma finalidade diferente daquela que o motivou a recolha inicial, incluindo a definição de perfis (Comissão Nacional de Proteção de Dados, 2018).
- O direito de ser notificado - se ocorrer uma violação de dados que comprometa os dados pessoais de uma pessoa, ela terá o direito de ser informada dentro de 72 horas após a primeira tomada de conhecimento da violação.

2.1.4. Dados Pessoais Especialmente Sensíveis

São classificados como dados pessoais especialmente sensíveis (Comissão Europeia, 2018b), quaisquer dados que sejam relativos aos direitos e liberdades fundamentais do ser humano. Estes dados estão sujeitos a condições de tratamento específicas, tais como uma maior necessidade de proteção.

Na categoria de dados pessoais especialmente sensíveis, inserem-se os seguintes:

- **Externos**
  - Etnia
  - Médica e Saúde
  - Sexual
- **Internos**
  - Conhecimento e Crença
  - Preferência

Os dados enumerados acima correspondem a dados pessoais que revelem a origem étnica ou racial (Externos, Etnia), opiniões políticas e convicções religiosas ou filosóficas (Internos, Conhecimento e Crença), filiação sindical (Internos, Preferência), dados genéticos, biométricos, e restantes dados relacionados com a saúde (Externos, Médica e

Saúde) e dados relativos à vida/orientação sexual (Externos, Sexual) do dono dos dados pessoais.

2.1.5. Encarregado de Proteção de Dados

Encarregado de Proteção de Dados (Regulamento (UE) 2016/679, 2016), EPD, em inglês *Data Protection Officer*, *DPO,* é o responsável máximo pela proteção dos dados de uma empresa.

A sua principal função (UE, 2016) é garantir que a organização, para a qual foi designado, processa os dados pessoais da sua equipa, clientes, fornecedores ou quaisquer outros indivíduos (também chamados de titulares de dados), em conformidade com as regras de proteção de dados aplicáveis. Nas instituições e órgãos da UE, o Regulamento de Proteção de Dados aplicável (Regulamento (UE) 2018/1725) obriga a nomeação de um DPO.

A nomeação de um DPO deve basear-se nas suas qualidades pessoais e profissionais, dando atenção especial ao seu conhecimento especializado em proteção de dados. É também recomendável um bom entendimento e conhecimento acerca da maneira como a organização opera.

O DPO é parte integrante da organização, tornando-o ideal para garantir a conformidade. No entanto, este deve poder desempenhar as suas funções de forma independente. Nas instituições e órgãos da UE, existem várias garantias que permitem essa independência (Simoncini, 2017):

- As regras (Parlamento Europeu, 2001) aplicáveis às instituições e órgãos da UE estabelecem expressamente que o DPO não receberá instruções sobre o desempenho de suas funções.
- Não deve existir qualquer conflito de interesses entre os deveres do indivíduo como DPO e os seus outros deveres, caso existam. Para evitar conflitos, é recomendável que:
    - Um DPO não deva controlar quaisquer atividades de processamento (por exemplo, se for chefe de Recursos Humanos).
    - O DPO não deva ser um empregado com contrato fixo ou de curto prazo.
    - Um DPO deva informar diretamente a direção ao mais alto nível do responsável pelo tratamento ou do subcontratante.
    - Um DPO deva ter a responsabilidade de gerir o seu próprio orçamento.

- A organização deve oferecer recursos, financeiros ou *staff*, para apoiar o DPO no desempenho de suas funções. A esse respeito, os DPOs das instituições e órgãos da UE podem destacar membros do seu *staff*, tais como um assistente ou vice-DPO para o representar e podem contar com os coordenadores de proteção de dados (DPCs (Simoncini, 2017) em cada secção da organização. O acesso aos recursos também inclui instalações para formação.
- O DPO deve ter autoridade para investigar, mantendo no desempenho das suas funções, a devida consideração pelos riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento.
- Um prazo mínimo de nomeação e condições restritas de demissão devem ser estabelecidos pela organização para um cargo de DPO. Nas instituições e órgãos da UE, o DPO é nomeado por um período entre 2 e 5 anos, podendo este período ser extendido até um máximo de 10 anos.

O DPO deve garantir que as regras de proteção de dados sejam respeitadas em cooperação com a autoridade de proteção de dados (para as instituições e órgãos da UE, esta é o EDPS (*European Data Protection Supervisor)* (Albinati, 2016).

Nas instituições e órgãos da UE, o DPO deve (Regulamento (UE) 2016/679, 2016):

- Garantir que tanto os titulares dos dados como quem os trata sejam informados sobre os seus direitos, obrigações e responsabilidades de proteção de dados e aumentem a consciencialização sobre eles.
- Dar conselhos e recomendações à instituição sobre a interpretação ou aplicação das regras de proteção de dados.
- Criar um registo das operações de processamento na instituição e notificar o EDPS sobre os que apresentam riscos específicos (os chamados controlos prévios).
- Garantir a conformidade da proteção de dados na sua instituição e ajudá-la a ser responsável a esse respeito.
- Lidar com consultas ou reclamações a pedido da instituição, do responsável pelo tratamento, de outra pessoa ou por sua própria iniciativa.
- Cooperar com o EDPS (responder aos seus pedidos sobre investigações, tratamento de reclamações, inspeções realizadas pelo EDPS, etc.).

- Chamar a atenção da instituição para qualquer falha no cumprimento das regras de proteção de dados.

2.1.6. Limitação de Conservação

Segundo o ponto 39, presente na página 7 (UE, 2016) do Regulamento Geral de Proteção de Dados pode ler-se a seguinte frase "A fim de assegurar que os dados pessoais sejam conservados apenas durante o período considerado necessário, o responsável pelo tratamento deverá fixar os prazos para o apagamento ou a revisão periódica.", onde é indicada uma medida que necessita obrigatoriamente de ser implementada pelo DPO.

Presente no artigo 5º (UE, 2016), intitulado "Princípios relativos ao tratamento de dados pessoais", encontra-se definido no ponto e), que apesar de ser necessário estabelecer um limite de tempo para que os dados pessoais possam ser tratados, estes podem ser armazenados durante períodos mais longos, desde que "sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos". Se este processo estiver de acordo com o artigo 89º, nº1 (UE, 2016), ou seja, "sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados" a limitação de conservação pode ser efetuada deste modo sem nenhum problema.

2.1.7. Finalidade

Quando algum dado pessoal é recolhido é necessário indicar qual a finalidade para a qual este é necessário (artigo 13º e 14º, nº1, alínea c) (Regulamento (UE) 2016/679, 2016), assim como muitos outros fatores, tal como o período de conservação desses mesmos dados pessoais.

Aquando dos pedidos de recolha, estes por norma envolvem mais do que apenas uma finalidade, mas pode ocorrer que a recolha não seja feita através de boas práticas, ou seja, que não seja completamente explícito qual a motivação para a qual se está a solicitar a recolha dos dados pessoais.

Com esses exemplos acima indicados, pode perceber-se que para que seja legal a recolha dos dados pessoais, tem de ser indicado de maneira inequívoca qual a intenção e motivação para a recolha dos mesmos.

Tal como descrito anteriormente, existem diferentes tipos de finalidades (Alfonso Rodriguez et al., 2007) para os quais pode ser feito o pedido de recolha de dados pessoais, entre os quais se destacam os seguintes:

- *Marketing*.
- Cumprimento do Serviço.
- Gestão Fiscal/Administrativa.
- Gestão do Contencioso.
- Controlo da Segurança da informação.
- Cumprimento das Obrigações Legais.
- Deteção de Fraude/Auditorias.
- Emissão de Certificados/Diplomas de Formação.
- Emissão de Declarações para efeitos de IRS.

Os exemplos acima indicados são apenas alguns dos muitos tipos de finalidade existentes (CECOA, 2018).

2.1.8. Fundamento

Tal como na subsecção anterior, a finalidade, aquando da recolha de dados pessoais, é necessário indicar qual o fundamento pelo qual se está a solicitar a recolha e tratamento dos dados (Vollmer, 2018).

A aplicação de um dos 6 fundamentos base (Grupo de Trabalho do Artigo 29.º, 2018, p. 679) abaixo indicados deve ser estabelecida antes da atividade de recolha e tratamento e em relação a uma finalidade específica.

Existem 6 fundamentos base:

- Consentimento.
- Contrato.
- Obrigação Jurídica.
- Interesses Vitais.
- Interesse Público.
- Interesses Legítimos.

Através de análise do artigo 6º, nº3 do RGPD (Vollmer, 2018), percebe-se que o tratamento dos dados pessoais recolhidos apenas é valido se servir o fundamento apresentado no momento da recolha - "o responsável pelo tratamento não pode passar do

consentimento para outros fundamentos legais. Por exemplo, não lhe é permitido utilizar retroativamente o fundamento do interesse legítimo para justificar o tratamento, se forem detetados problemas com a validade do consentimento." (Grupo de Trabalho do Artigo 29.º, 2018, p. 679).

2.2. Processos de Negócio

Um processo de negócio é utilizado com o intuito de definir o funcionamento e os objetivos de uma certa organização e consiste num conjunto de atividades que criam algo de valor (um produto ou um serviço) para os clientes dessa organização (Caldas, 2003).

Para modelação de processos de negócios, existem várias linguagens e notações, abaixo descritas. No entanto, o BPMN (*Business Process Modeling Notation*) é considerada um dos principais padrões (A. Rodriguez et al., 2007).

2.2.1. Normas/Notações

Tal como indicado no ponto 2.2., de seguida apresentam-se vários exemplos de notações para modelação de processos de negócios.

2.2.1.1. BPMN

O *Business Process Model and Notation* (BPMN) é uma notação da metodologia de gestão de processos de negócio e trata-se de uma linguagem e série de ícones padrão para o desenho de processos, o que facilita o entendimento do utilizador.

Esta notação, apesar de ser considerada padrão para processos de negócio, possui uma lacuna, relativamente aos aspectos de segurança, pois estes não estão incluídos na Modelação de Processos de Negócio na primeira versão do BPMN realizada pela empresa BPMI (Business Process Management Initiative) ou na nova versão já pertencente à OMG®, consórcio tecnológico internacional sem fins lucrativos, resultante da junção das duas entidades (A. Rodriguez et al., 2007).

O BPMN consiste numa notação que considera um diagrama único para a representação de processos, *Business Process Diagram* (BPD). Este diagrama foi projetado de modo a simplificar o seu uso e tornar mais simples a sua compreensão e para oferecer uma força expressiva que nos permita modelar negócios complexos, atribuindo-os de maneira natural a linguagens de execução, como o BPEL4WS (*Business Process Execution Language for Web Services*). Para fazer isso, a notação é suportada por uma linguagem de modelagem, *Business Process Modeling Language* (BPML) e uma

linguagem de consulta, *Business Process Query Language* (BPQL) (A. Rodriguez et al., 2007).

Outra característica bastante interessante do BPMN é que esta notação oferece uma técnica de modelagem que todos os utilizadores facilmente compreendem, desde analistas de negócios que fazem rascunhos dos processos para utilizadores mais técnicos que são responsáveis pela implementação tecnológica desses mesmo processos, assim como pessoas de negócios que serão responsáveis por controlar e gerir esses processos. Para além disso, estabelece uma padronização que associa o *design* com a implementação de processos de negócios (A. Rodriguez et al., 2007), (White, 2004).

2.2.1.2. XML

XML (*Extensible Markup Language*) foi desenvolvido por um grupo de trabalho XML formado sob os auspícios do *World Wide Web Consortium* (W3C) em 1996 (W3C, 2008), para gerar linguagens de marcação para necessidades especiais.

É um dos subtipos da SGML (*Standard Generalized Markup Language*) com a capacidade de descrever diversos tipos de dados. O seu propósito principal é a facilidade de partilha de informações através da internet.

Os dados XML são conhecidos como sendo autodescritivos ou autodefinidos, o que significa que a estrutura dos dados é incorporada nos próprios dados, assim, quando estes chegam, não existe a necessidade de pré-construir a estrutura para os armazenar, ou seja, é entendido dinamicamente dentro do próprio XML.

O formato XML pode ser utilizado por qualquer indivíduo, grupo de indivíduos ou empresas que desejam partilhar informações de maneira consistente. XML é, na verdade, uma simplificação do SGML, que é o padrão a utilizar para criar uma estrutura de um documento (Rouse, 2015a).

O corpo básico de um documento XML é um elemento, definido por *tags*. Um elemento tem uma *tag* de começo e uma *tag* final. Todos os elementos num documento XML estão contidos num elemento externo conhecido como o elemento raiz. O XML também pode suportar elementos aninhados (*nested*) ou elementos dentro de elementos. Essa capacidade torna possível ao XML suportar estruturas hierárquicas. Os nomes dos elementos descrevem o conteúdo do elemento e a estrutura descreve o relacionamento entre os seus elementos.

Um documento XML é considerado formado corretamente (é possível ser lido por um analisador XML) se o seu formato estiver em conformidade com a especificação XML, se estiver devidamente marcado e se os elementos estiverem adequadamente aninhados. O XML suporta também a capacidade de definir atributos para elementos e descrever características dos mesmos na sua *tag* inicial (W3C, 2008).

A principal utilidade do XML reside na sua simplicidade. Esta linguagem é capaz de transportar grandes quantidades de informação e consolidá-la num estado mais estruturado e organizado (Rouse, 2015a).

2.2.1.3. XSD

XSD (*XML Schema Definition*) é uma recomendação do W3C que especifica a maneira de estruturar e descrever, formalmente, os elementos num documento XML.

A versão 1.1 foi aprovada pela W3C em abril de 2012 (W3C, 2013).

O XSD pode ser usado para gerar documentos XML que podem ser tratados como objetos de programação. Além disso, várias ferramentas de processamento XML também podem gerar documentação legível por humanos, o que torna mais simples a compreensão de documentos XML mais complexos.

Um esquema XML representa a relação entre os atributos e elementos de um objeto XML.

O processo de criação de um esquema para um documento envolve a análise da sua estrutura e definição de cada elemento estrutural encontrado.

Por exemplo, para criar um esquema para um documento que descreve um *site* é necessário definir um elemento "*site*", um elemento "página web" assim como qualquer outro elemento que descreva possíveis divisões de conteúdo em qualquer página desse *site*. O mesmo acontece com as linguagens XML e HTML, os elementos são definidos num conjunto de *tags* (Rouse, 2015b).

Algumas das vantagens da utilização do XSD, para além da correta estruturação do ficheiro XML, são a possibilidade de:

- Definição de tipos de dados específicos, tal como definir dados como dias da semana, em que os dados podem tomar um dos sete dias da semana, depois de definir estes mesmos sete nomes dos dias da semana como valores enumerados.

Após essa definição, o ficheiro XML indicaria erros de validação para qualquer outro valor que não estivesse definido anteriormente.

- Testar corretamente a hierarquia dos elementos do ficheiro XML, ou seja, qual a ordem pelos quais os "progenitores" e "filhos" aparecem. Por exemplo, um "filho" não pode estar antes do seu "progenitor".
- Implementar restrições na ocorrência dos elementos, utilizando os indicadores *minOccurs* e *maxOccurs*, que têm o valor "1" por pre-definição.

2.3. Ferramentas

2.3.1. Eclipse

Eclipse é um *Integrated Development Environment* (IDE), um ambiente de desenvolvimento integrado, ou seja, é uma plataforma onde é possível criar aplicações através do desenvolvimento de *software*.

Figura 4 *- Logótipo da ferramenta Eclipse IDE - integrated development environment.*

Um dos principais aspetos desta plataforma é a variedade de *plug-ins* possíveis de instalar, tornando-a uma plataforma muito abrangente a nível de linguagens que podem ser utilizadas e trabalhadas. Consoante os *plug-ins* que forem instalados, pode-se trabalhar com variadas linguagens, tais como Java, C/C++, Python, Ruby, BPMN, entre outras (Tutorialspoint, 2006).

De forma a complementar este IDE, existe um *plug-in* denominado "Eclipse BPMN2 Modeler 1.5.0", pertencente ao *Object Management Group* (OMG), com o intuito de tornar possível e simples a especificação de processos de negócio. O principal objetivo do BPMN2 Modeler 1.5.0 é fornecer uma estrutura gráfica que torna possível a edição de fluxo de trabalho, que pode ser facilmente aplicado em qualquer mecanismo de execução que seja compatível com a linguagem BPMN 2.0 (Brodt, 2018).

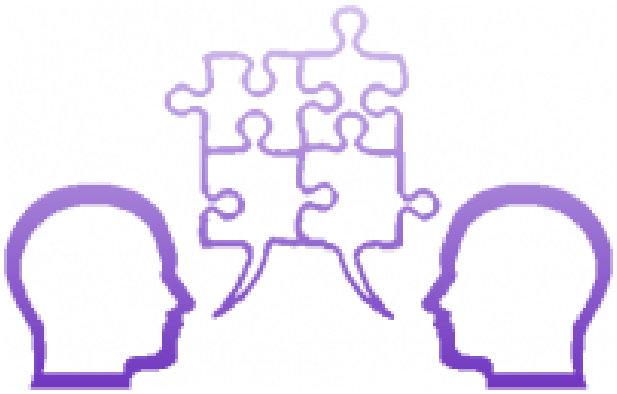


Figura 5 *- Logótipo do plug-in utilizado - Eclipse BPMN2 Modeler 1.5.0.*

2.3.2. Bizagi Modeler

Este é um *software* baseado totalmente na notação BPMN (Brodt, 2018), cuja principal vantagem é a simplicidade com que é utilizado. Baseia-se na ideologia de *drag and drop*, ou seja, a interação com o programa funciona com o arrastar do que se quer para o local de trabalho, que é significativamente mais simples do que escrever o código completo (Brodt, 2018).

Figura 6 *- Logótipo da ferramenta bizagi modeler.*

Apesar de ter sido uma opção para o desenvolvimento do trabalho, este não foi o *software* escolhido, uma vez que não suporta o sistema operativo Mac OS. Apenas sendo possível a sua utilização para os sistemas operativos seguintes: *Windows* 10, *Windows* 8.1, *Windows* 7, *Windows Server* 2016, *Windows Server* 2012 R2 (Bizagi, 2019).

Uma possível solução para o problema apresentado seria a utilização de um ambiente *Windows* numa máquina virtual (Bizagi, 2012).

2.3.3. Activiti

É um *software open-source* com a capacidade de executar processos de negócio descritos em BPMN (Hub, 2015).

A ideia de utilização deste *workflow* proveio da sua possibilidade de integração com o programa Eclipse, que viria a aumentar o leque de opções de ferramentas para a construção dos modelos de negócio pretendidos.

Figura 7 *- Logótipo da ferramenta Activiti.*

O problema detetado com este programa reside na sua difícil instalação, assim como apenas ser possível trabalhar numa versão de teste, *free trial*.

2.3.4. Modelio

É um ambiente de modelagem *open-source* que suporta uma vasta gama de modelos e diagramas, assim como bastantes linguagens, entre as quais BPMN2, UML2, XMI, entre outros (Modelio, 2011).

Figura 8 *- Logótipo da ferramenta modelio.*

As funcionalidades necessárias para o correto desenvolvimento dos diagramas de modelo de negócio presentes nesta ferramenta são bastante semelhantes às presentes no *plug-in* "Eclipse BPMN2 Modeler 1.5.0" utilizado no programa Eclipse, ocupando, no entanto, mais espaço de memória e não tendo uma interface tão simplificada, gerando alguma confusão na concepção dos diagramas.

2.3.5. BPMN.IO

Esta é uma ferramenta *online* (BPMN.i0, 2018), que serve o propósito de criar e editar diagramas BPMN, tendo a vantagem de não ocupar espaço de memória, e a desvantagem da obrigatoriedade da ligação à Internet para a sua utilização.

Figura 9 *- Logótipo da ferramenta online bpmn.io.*

2.4. Extensões para Segurança e Privacidade

As ferramentas apresentadas acima servem o propósito de criar e editar programas. De forma a desenvolver o diagrama e as *tags* de segurança são necessários adicionar critérios de segurança e privacidade, para tal é necessário a inclusão de extensões de forma a incluir nos artefactos a desenvolver as características desejadas relativas a segurança e privacidade.

Algumas das soluções encontradas eram apenas parcialmente terminadas e não era possível implementá-las em tempo útil.

Um desses casos é o sistema elaborado por Wadha Labda, Nikolay Mehandjiev e Pedro Sampaio, da Universidade de Manchester, em (Labda et al., 2014) onde é proposta uma representação da semântica das extensões de reconhecimento de privacidade para BPMN e permitir o uso de ferramentas de raciocínio que suportam a verificação e aplicação de restrições de privacidade durante o tempo de execução.

Privacy Requirement		Icon	Description	BPMN Mapping
Access Control	allow		Specify access control requirements on the resources it is attached to.	Pool, Lane
	Prevent			
	Limited			
Separation of Tasks			Separate the tasks of each role if more than one user is required to successfully complete the process	Lane, Pool, Data Object, and Activity
Binding of Taks			Same user with different assigned roles needs to execute several tasks of a process	Lane, Pool, Data Object, and Activity
User Consent			Personal information and resources can only be accessed if the user consent is provided	Lane, Pool, Data Object, and Activity, sequence and message flow
Necessity to know	High		A user should only be able to access the information that is strictly necessary for completing a certain task	Lane, Pool, Data Object, Activity, sequence and message
	medium			
	low			

Figura 10 *- Descrição e anotações dos requisitos de privacidade por parte de Wadha Labda, Nikolay Mehandjiev e Pedro Sampaio da Universidade de Manchester.*

Outra solução encontrada é a apresentada por Per H˚akon Meland e Erlend Andreas Gjære do SINTEF ICT, *Software Engineering, Safety and Security* da Noruega, (Meland & Gjære, 2012) onde são apresentadas opções e os benefícios de representar ameaças de segurança da informação em BPMN 2.0. Neste caso representam ameaças com diferentes construções simbólicas e diagramas encontrados no BPMN 2.0, nomeadamente como eventos de erro, ou seja, como excepções, que invocam novas atividades.

	Interrupting Error Start Event
	Boundary Catch Error Intermediate event
	Error End Event
	Escalation Start Event
	Non-interrupting Escalation Start Event
	Catch Escalation Intermediate Event
	Non-interrupting Boundary Catch Escalation Intermediate Event
	Throw Escalation Intermediate Event
	Escalation End Event

Figura 11 *- Símbolos de evento de erro e escalonamento no BPMN 2.0 utilizados por Per H˚akon Meland e Erlend Andreas Gjære do SINTEF ICT, Noruega.*

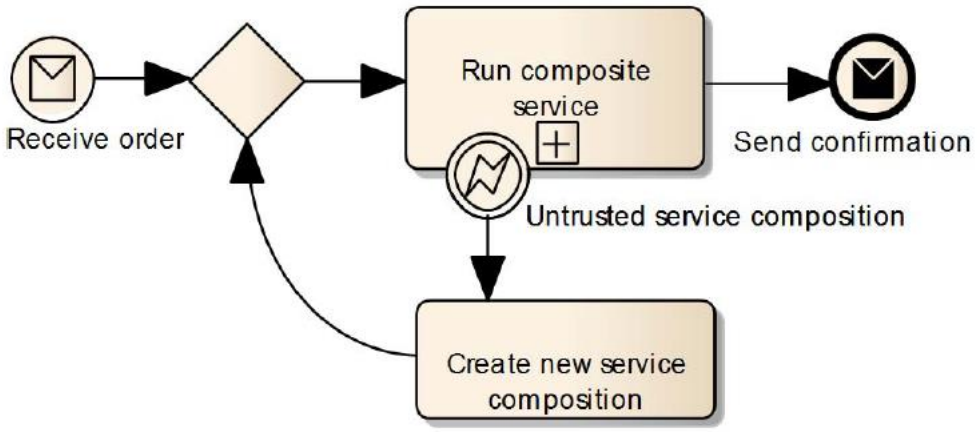


Figura 12 *- Utilização de um evento intermediário de erro de captura de limite num diagrama de processo para representar uma ameaça, invocando a nova atividade "Create new service composition".*

Num estudo realizado por Koh Song Sang e Bo Zhou, do departamento de Ciência da Computação da Universidade John Moores de Liverpool, é fornecida uma solução para modelar os conceitos de segurança em BPMN, estendendo-os com novos elementos de segurança projetados, que podem ser integrados com o diagrama BPMN (Sang & Zhou, 2015).

Element	Type	Design
Security Task	Task	
Authentication	Boundary Event	
Access Control	Boundary Event	
Authorization	Boundary Event	
Harm Protection	Boundary Event	
Encrypted Message	Intermediate Event	
Non Repudiation	Intermediate Event	
Secure Communication	Intermediate Event	

Figura 13 *- Elementos estendidos para requisitos de segurança, utilizados por Koh Song Sang e Bo Zhou, do departamento de Ciência da Computação da Universidade John Moores de Liverpool.*

Security Indicator	Low	Medium	High
Confidentiality			
Integrity			
Availability			

Figura 14 *- Elementos estendidos para requisitos de segurança, utilizados por Koh Song Sang e Bo Zhou, do departamento de Ciência da Computação da Universidade John Moores de Liverpool.*

Como se pode ver pelos exemplos apresentados, existem muitos estudos sobre a criação de representações e projeções de elementos de segurança e privacidade em BPMN, mas nenhum chegou a ser completamente implementado, pelo que ficaram pela teoria, não podendo ser utilizados na resolução do objetivo que é proposto nesta dissertação.

2.5. Algoritmos Criptográficos

2.5.1. DES

O DES (*Data Encryption Standard*) é um algoritmo de chave simétrica, que usa uma única chave de 64 *bits* para criptografar um bloco de texto de 64 *bits* num bloco de texto cifrado de 64 *bits*. Com um *bit* de paridade para cada byte da chave, a força da chave é de apenas 56 *bits*, o que se mostrou ser reduzido perante as variadas tentativas de ataque registadas a este algoritmo. O DES realiza uma permutação inicial, seguido de dezasseis rondas de cifragem e uma permutação final.

2.5.2. 3DES

3DES *(Triple Data Encryption Standard)* foi publicado pela primeira vez em 1998 e é um melhoramento do algoritmo DES. A principal diferença para com o seu precedente é que este aplica o algoritmo DES três vezes seguidas utilizando três chaves diferentes, uma para cada aplicação, obtento uma chave com 168 *bits* (três vezes 56 *bits*) e ocupa três vezes mais CPU.

2.5.3. AES

O algoritmo AES (*Advance Encryption Standard*) (*Advanced Encryption Standard (AES)*, 2001) é uma cifra de bloco de chave simétrica, desenvolvido em 1998 por *Joan Daemen* e *Vincent Rijmen* (Aleisa, 2015) .

O AES é baseado no algoritmo de *Rijndael*, que é uma combinação de um algoritmo forte com uma chave forte. Este algoritmo pode ser utilizado com três chaves com tamanhos diferentes, 128 *bits*, 192 *bits* e 256 *bits*. Esta versatilidade pode produzir cifras de bloco simétricas mais rápidas e mais seguras.

2.5.4. RSA

RSA (*Rivest, Shamir e Adleman*) é um algoritmo de chave pública, assimétrica. O RSA utiliza um bloco de criptografia assim como uma chave de tamanho variável (Singh & Supriya, 2013).

O algoritmo utiliza dois números primos para gerar as chaves pública e privada. Essas duas chaves diferentes são utilizadas para criptografar e descriptografar.

Este algoritmo possui duas versões, que diferem no tamanho das chaves utilizadas. Estas podem ter o tamanho de 1024 e 2048 *bits*, onde a última é mais segura que a primeira, sendo necessário muito mais tempo para a quebrar (Quora, 2013).

2.5.4.1.Blowfish

Blowfish é um algoritmo com chave de tamanho variável, com cifras em bloco de 64 *bits*, introduzido pela primeira vez em 1993 e ainda não foi quebrado (Singh & Supriya, 2013).

2.5.5. Twofish

O Twofish (*Twofish Explained*, 1998) é um algoritmo que até hoje, ainda não foi quebrado (Rizvi et al., 2011).

Este é um algoritmo de criptografia de bloco de chave simétrica derivado de blowfish. Utiliza blocos com 128 *bits* e chave com 128, 192, 256 *bits*.

2.5.6. Comparações entre algoritmos

Supondo que se consegue analizar 50 mil milhões de chaves por segundo, utilizando o AES com uma chave de 128 *bits*, seriam necessários 5 x 1021 anos, ao passo que utilizando o 3DES (que já é um melhoramento do DES), com as suas chaves de 56 *bits*, seriam necessários apenas 400 dias (Aleisa, 2015), assim como é apresentado um estudo (Alanazi et al., 2010) onde se chega a conclusões de que este é o algoritmo mais indicado.

Como apresentado em cima, compreende-se que AES é mais rápido e mais eficiente que os algoritmos Twofish, DES, 3DES.

2.6. Análise de Lacunas

2.6.1. Em que Consiste

Análise de lacunas é um processo que compara o desempenho ou os resultados reais com o que era esperado ou desejado (Smartsheet, 2019).

Esta análise pode ser realizada a dois níveis (Smartsheet, 2019):

1. **Estatégico**: Comparar o estado atual da empresa com o dos padrões do setor.

2. **Operacional**: Comparar o estado atual ou o desempenho da empresa com o desejado.

Para realizar este processo são necessários quatro principais passos (Lucidchart Blog, 2018):

1. Análise do estado atual.
2. Análise dos objetivos futuros.
3. Análise das ações necessárias para transitar de um estado para o outro.
4. Realizar as ações estabelecidas no passo 3.

Aplicando a análise de lacunas ao cumprimento do RGPD, é possível imaginar o cenário em que uma empresa foi contratada para realizar uma análise de lacunas no Iscte-Instituto Universitário de Lisboa, relativamente ao cumprimento do RGPD nos seus processos de negócio, como por exemplo o processo de matriculação dos seus alunos.

O primeiro passo seria essa empresa analisar o que já existe feito pela organização que solicitou a análise, verificando que processos de negócio existem e se estão de acordo com o regulamento geral de proteção de dados, assim como também poderia abranger um levantamento dos seus trabalhadores, em que projetos é que estes se encontram, de modo a obter assim uma figura mais clara do seu estado atual. Caso os processos de negócio existentes não cumpram o desejado, seria então realizado o segundo passo da análise de lacunas.

O segundo passo corresponde à realização de um estudo sobre quais as condições necessárias a realizar para que se atinja o objetivo, ou seja, de a organização que solicitou a análise estar num estado de cumprimento da regulação.

O terceiro passo é o passo onde se realiza a avaliação de quais as ações necessárias realizar, de modo a transitar do estado/ponto inicial para o estado/ponto desejado, que neste caso é o de cumprimento do RGPD relativamente aos processos de negócio. Uma das ações poderia ser a alocação de alguns funcionários de um projeto menos importante para a mais rápida realização do tratamento dos modelos de negócio.

Por último, o quarto passo corresponde à realização das ações previamente analisadas, o que leva ao fechar da lacuna que se a análise propunha fechar.

2.6.2. Definição/Especificação do Ponto de Partida

Este é o ponto em que a empresa, ou entidade que deseja realizar a análise de lacunas, se encontra aquando do início da avaliação.

É através do primeiro passo da análise de lacunas que se estabelece o ponto de partida da empresa. Para se chegar a esse ponto de partida realiza-se uma recolha de informação, tanto qualitativa (quais os projetos da empresa ou a sua metodologia de trabalho) como quantitativa (toda a informação que pode ser contada e medida).

2.6.3. Definição/Expecificação do Ponto de Chegada/Desejável/Objetivo

O objetivo da análise de lacunas é facilitar o processo de uma empresa atingir o ponto de chegada. De modo a definir esse ponto, têm de se estabelecer as condições que a empresa, ou organização, ambiciona atingir, assim como perceber onde a empresa está a falhar.

2.7. Requisitos de Segurança da Informação

Requisitos de segurança são os principais componentes de um processo organizado e estruturado que permite preservar a confidencialidade, integridade e a disponibilidade da informação. Não existe apenas um responsável pela segurança de informação, todos nós temos um papel a cumprir. "Todos nós somos os responsáveis pela segurança da informação e todos temos a responsabilidade de proteger os nossos dados e os que nos são confiados" (Vicente, 2017).

Figura 15 *- Pilares da Segurança da Informação. Adaptado de (CNCS,2017).*

2.7.1 Integridade

Integridade é um dos pilares da segurança de informação. O seu foco é em garantir a veracidade e complementaridade da informação, assim como os seus métodos de processamento. O seu conteúdo não pode ser modificado inesperadamente (Vicente, 2017).

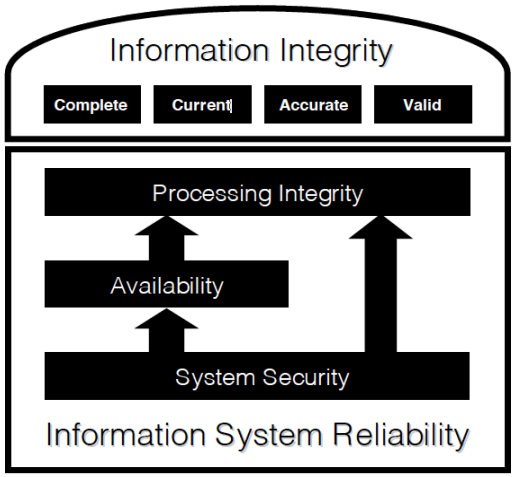


Figura 16 *- Relação entre integridade da informação, integridade de processamento e confiabilidade do sistema. Adaptado de (Boritz, 2005).*

Tal como se pode observar na figura 16 (Boritz, 2005) a integridade da informação é melhorada pela integridade do processamento. Na verdade, o nível de integridade de processamento do sistema é o que vai determinar o limite da integridade da informação. A integridade do processamento do sistema, por sua vez, depende da disponibilidade e segurança do sistema (Carnaghan, 2006).

A segurança também contribui para a disponibilidade, reforçando o ponto de que a segurança desempenha um papel crítico como facilitador da integridade das informações (Carnaghan, 2006).

Integridade da informação foi definida como a fidelidade representacional da informação à condição ou assunto que está sendo representado pela informação.

2.7.2. Disponibilidade

Disponibilidade tem como função assegurar o acesso à informação e bens associados por quem devidamente autorizado. A informação deve estar acessível sempre que necessário (Vicente, 2017).

Para que a informação esteja completa e atual, é necessário estar disponível e acessível aos utilizadores de acordo com as especificações do negócio e ser recuperadas de uma forma utilizável quando necessário. As informações que não são possíveis de aceder quando necessárias não teriam quaisquer consequências práticas para as atividades ou decisões dos utilizadores, exceto no sentido negativo de limitar a qualidade das informações e as decisões dos usuários com base nessas informações (Low & Mohr, 2001). Para que as informações sejam consideradas acessíveis, os utilizadores necessitam de ser capazes de trabalhar com as informações de uma forma que cumpra as suas necessidades (Wang & Strong, 1996). Na prática, para que a afirmação acima seja cumprida, é necessária a utilização de um sistema robusto, capaz de fornecer as informações. Esse sistema tem de estar disponível sempre que necessário, assim como permitir que os utilizadores o alterem (ou seja, sem alterações de programação) para atender às suas necessidades, funcionar com eficiência e eficácia e ser capaz de acomodar a necessidade crescente de informações dos utilizadores (Nelson et al., 2005).

Segurança da Informação e Disponibilidade são dissociáveis e complementares no sentido em que a segurança tem como objetivo restringir o acesso (não autorizado) à informação, enquanto a disponibilidade visa facilitar o acesso (autorizado) à informação.

2.7.3. Controlo de Acessos

Controlo de acessos está localizado dentro do pilar da segurança da informação "Confidencialidade", uma vez que é uma ferramenta para evitar que exista um acesso à informação por parte de quem não está autorizado a realizar essa ação.

O controlo de acesso, físico e lógico, serve para salvaguardar a informação, tanto em movimento como em repouso, de atos da natureza, através de um acidente ou uma catástrofe natural e de atos maliciosos intencionais, tais como a criação, modificação ou destruição não autorizada, bem como erros não intencionais que podem comprometer sua integridade.

Outro aspecto da segurança envolve a proteção da confidencialidade das informações, ou seja, protegendo-a contra ações como a visualização ou disseminação não autorizada. Embora a confidencialidade seja um aspecto importante da segurança, é conceitualmente diferente da fidelidade representacional (Carnaghan, 2006).

No projeto desenvolvido, a implementação da confidencialidade, através do controlo de acessos foi pensada em ser composta pela introdução de dois principais campos, um registo de *logs* e atribuição de permissões CRUD (*Create, Read, Update, Delete).*

O primeiro item, o registo de *logs* é composto por *logs* de nome, ip utilizado, porto utilizado, dados acedidos, data de acesso e utilização dos dados acedidos. Estes *logs* têm como objetivo manter a confidencialidade uma vez que responsabilizam quem efetua as ações potencialmente prejudiciais para a informação.

O segundo item, as permissões CRUD têm também como objetivo manter a confidencialidade da informação e controlo de acessos, uma vez que são o mecanismo que dita quem pode ou não aceder, modificar ou apagar informação, implementado um sistema de *roles* em que os diferentes *roles* possuem diferentes níveis de acesso à informação. O *role* de *dataOwner* possui diferentes permissões do que o de *dataProcessor*. O *dataOwner* possui permissões de criar, ler e atualizar informação. O *dataProcessor* possui permissões de ler, atualizar e apagar informação.

2.7.4. Não Repúdio

O não repúdio implica que uma parte de uma ação não pode negar ter realizado uma ação. Por exemplo, um interveniente de uma transação não pode negar ter recebido uma transação, assim como o outro interveniente não negar ter enviado uma transação (McCarthy, 2006).

Apesar de ser extremamente útil na melhoria da segurança da informação, não é suficiente para mostrar que uma mensagem corresponde a uma assinatura digital assinada com a chave privada do remetente e, portanto, apenas o remetente poderia ter enviado a mensagem e ninguém mais poderia alterá-la em trânsito (integridade dos dados).

O não repúdio é uma tentativa de impedir qualquer negação da transmissão / criação de qualquer informação pelo remetente.

Capítulo 3 - Especificação de Extensão de Segurança ao BPMN

Neste capítulo encontra-se especificada a metodologia que se propôs implementar assim como cada um dos seus passos.

3.1. Metodologia

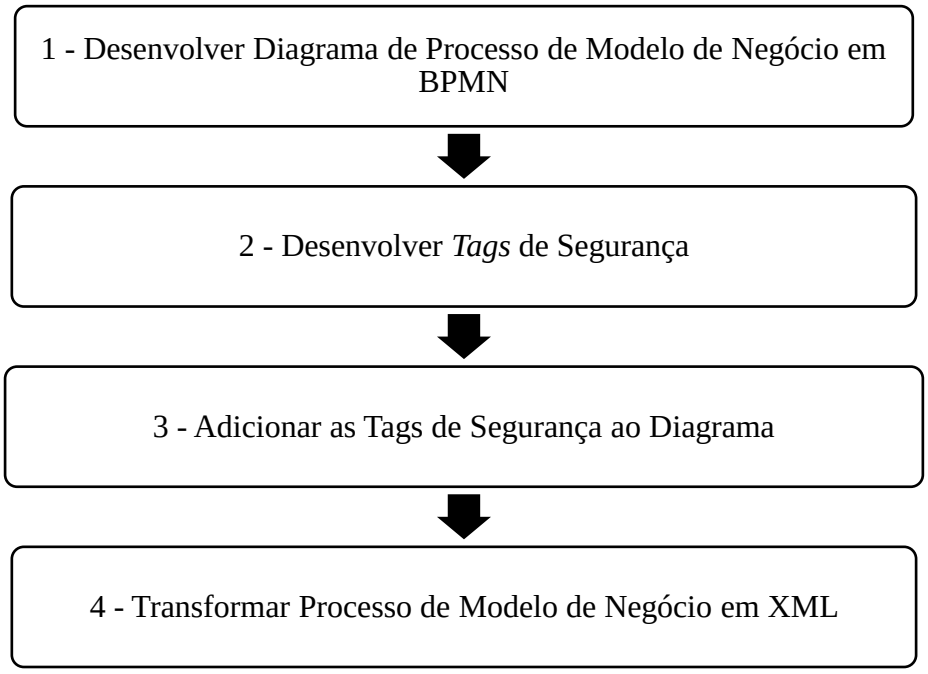


Figura 17 *- Demonstração dos passos da metodologia proposta realizada.*

Como se pode observar pela figura 17, a metodologia é composta por quatro principais passos.

3.2. Diagrama

De maneira a desenvolver os diagramas de processo de modelos de negócio, tendo em conta os aspetos de segurança e proteção de dados pessoais, foi necessário incluir nos mesmos, características de segurança e privacidade.

De forma a desenvolver o diagrama foi necessário identificar um processo para modular. O processo escolhido apenas existia em linguagem natural, pelo que o primeiro passo foi o de transformar a linguagem natural em linguagem BPMN. Esta transformação decorreu da seguinte forma: identificação dos intervenientes, identificação do ponto de início, identificação dos componentes do diagrama, identificação dos dados pessoais utilizados, identificação do percurso do fluxo do processo e identificação do ponto de fim do fluxo.

3.3. Componentes do diagrama

O diagrama desenvolvido é composto por variados elementos, os quais são distinguidos em seguida assim como a função de cada.

3.3.1. Pool

Este componente corresponde a uma representação gráfica de um participante presente numa colaboração ou de uma entidade própria, tal como se pode ver na *pool* de cima que representa o "Aluno" (Camunda.org, 2018a). Existe uma versão simplificada de uma *pool*, chamada de *lane* mas que apenas é utilizada quando não é parte ativa do processo, ex: apenas receber uma mensagem (Paradigm, 2004).

3.3.2. Start Event

O *start event* pertence à família dos eventos. Estes são a representação em modelação de que "algo aconteceu" durante o processo (Camunda.org, 2018d). Existem variados tipos de eventos, podendo estes ocorrer no início, durante ou no final de um processo.

O *start event* é um dos vários tipos de eventos e é onde se dá início a todo o processo ou sub-processo, é o ponto de arranque do diagrama (SYDLE, 2020).

3.3.3. Timer Event

O *timer event* pertence à família dos eventos. Tal como explicado em cima, os eventos são a representação em modelação de que "algo aconteceu" durante o processo.

Os *timer events* (Camunda.org, 2015), ou eventos temporais, são eventos disparados por um cronómetro definido. Eles podem ser usados como evento inicial, intermediário ou limite de processo. Os eventos de limite podem ser interrompidos ou não.

Uma das particularidades deste tipo de eventos é que necessita de definir um elemento temporal para que seja eficaz, quer seja ele um tempo cronometrado, uma data específica ou um ciclo de tempo que pode ser repetitivo. No primeiro exemplo, o evento seria despoletado e duraria um certo período de tempo definido, no segundo caso seria ativado quando se atingi-se a data definida e no último exemplo pode ser ativado por um certo período de tempo de cada vez (*Edraw Max*, 2019).

3.3.4. Exclusive Gateway

Este tipo de *gateway* é um dos vários existentes. A função dos *gateways* é de definir qual o caminho a seguir quando o processo se depara tanto com uma convergência ou com uma divergência (Camunda.org, 2018c).

O *exclusive gateway* é utilizado para modular uma decisão no decorrer do processo. Quando a execução do processo chega a este tipo de *gateway*, todos os fluxos de sequência de saída são avaliados consoante a ordem em que foram definidos (Camunda.org, 2018b). O fluxo de sequência cuja condição é avaliada como "verdadeira" é selecionado para continuar o processo. Se nenhum fluxo de sequência puder ser selecionado por não ter sido declarado como "verdadeiro" resultará numa "*runtime exception*" a menos que seja definido um outro percurso, tal como um "*End Event*" terminando o processo ou sub-processo (SYDLE, 2020).

3.3.5. Parallell Gateway

Tal como o *exclusive gateway*, o *parallell gateway* pertence à mesma família, mas este apresenta as suas especificidades.

Ao contrário do *gateway* (Camunda.org, 2018c) explicado anteriormente, este é utilizado para introduzir concorrência no processo, ou seja, permite a bifurcação (*fork*) em vários caminhos de execução ou a união (*join*) de vários caminhos de execução de entrada.

O *fork* corresponde à bifurcação de fluxos de sequência de saída são seguidos em paralelo, criando uma execução simultânea para cada fluxo de sequência. Já o *join* corresponde a todas as execuções simultâneas que chegam ao *gateway* paralelo (Camunda.org, 2015) e que aguardam até que todas tenham chegado, podendo depois continuar o processo ou sub-processo.

Ambos os comportamentos, *fork* e *join*, podem ocorrer no mesmo *gateway*, realizando o *join* primeiro na chegada e realizando o *fork* em seguida.

3.3.6. Task

Este elemento é o responsável pela representação das tarefas que o processo modela. É uma atividade dentro de um fluxo de processo. A criação de uma atividade pressupõe que não é possível dividir a atividade em partes mais detalhadas, ou seja, é a versão mais simplificada ao nível do detalhe de uma atividade (SYDLE, 2020).

Estas são normalmente executadas por uma pessoa ou uma aplicação.

Existem várias sub-categorias de *tasks.*

3.3.7. Send Task

Este tipo de *task* é o responsável por enviar uma mensagem para outra *lane* ou *pool*. Esta atividade fica concluída assim que a mensagem for enviada (*Edraw Max*, 2019), (Camunda, 2015).

3.3.8. Receive Task

As *receive task* são muito semelhantes às descritas acima, com a diferença de que estas tarefas são de receber mensagens e as de cima são para enviar mensagens (*Edraw Max*, 2019).

Este tipo de *task* é o responsável por receber uma mensagem vinda de outra *lane* ou *pool*. Esta atividade encontra-se em espera até que receba a mensagem e fica concluída assim que a mensagem for recebida (Camunda, 2015).

3.3.9. Service Task

A *service task* é utilizada quando se pretende invocar um serviço no processo (Camunda, 2015). Esse serviço utilizado pode ser um serviço *web*, uma aplicação automatizada, ou qualquer outro tipo de serviço.

3.3.10. DataObject

Este tipo de objeto existe fora do fluxo de sequência do processo, mas estão disponíveis para todos os objetos de fluxo numa determinada instância de processo. Os *DataObject* permitem visualizar graficamente o fluxo de informação que ocorre de/para as atividades. Objetos de dados são a construção primária para modelar dados dentro do fluxo do processo. São objetos com um ciclo de vida e estrutura bem definidos.

Um Objeto de Dados pode aparecer várias vezes na sequência de um processo, cada um referenciando a mesma instância do Objeto de Dados. Essas referências são usadas para simplificar as ligações do diagrama.

Os fluxos representados por estes objetos não são de sequência, mas sim de associações de dados (*Edraw Max*, 2019).

Estes objetos podem ser variados tipos de informação, entre eles, *emails*, documentos, ficheiros, cartas, etc.

3.4.Tags de Segurança

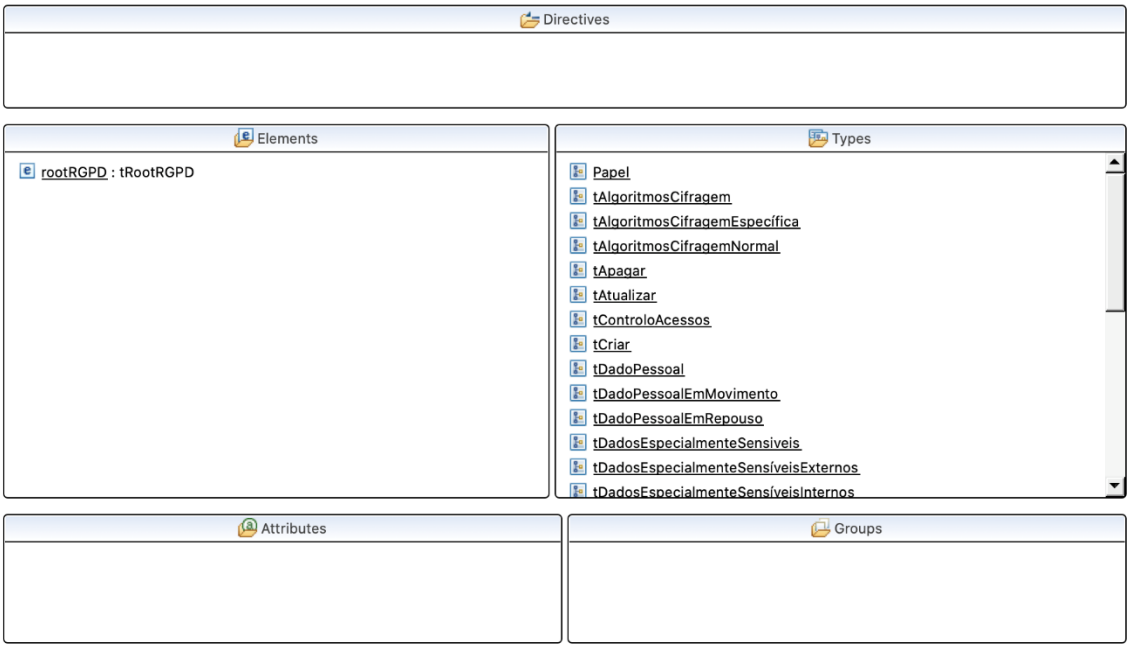
Tags de segurança são conjuntos de anotações sobre os dados escritas em XSD, onde são definidos os comportamentos de cada conjunto de tarefas que se desejam implementar.

No decorrer desta dissertação foram definidas variadas *tags* relativas aos princípios de segurança da informação: integridade, disponibilidade e confidencialidade.

Após análise do RGPD foi necessário identificar as novas regras por ele impostas. De seguida devenvolveram-se *tags* de segurança correspondentes às regras identificadas.

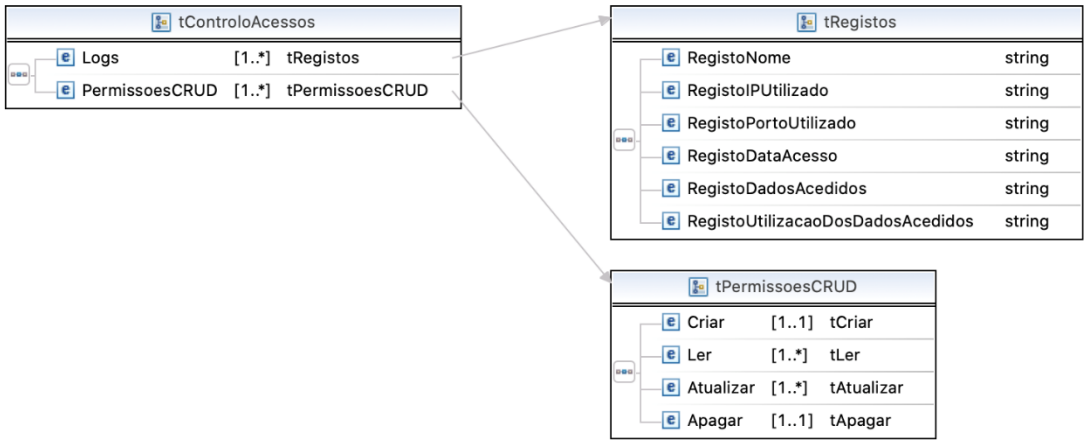
No desenvolvimento das *tags* foi tido em conta que cada uma destas seria parte de um conjunto de várias *tags* que teriam dependências entre si, de modo a aumentar o seu poder de fazer crescer a *compliance* do RGPD. Desta forma, a análise é mais confiável.

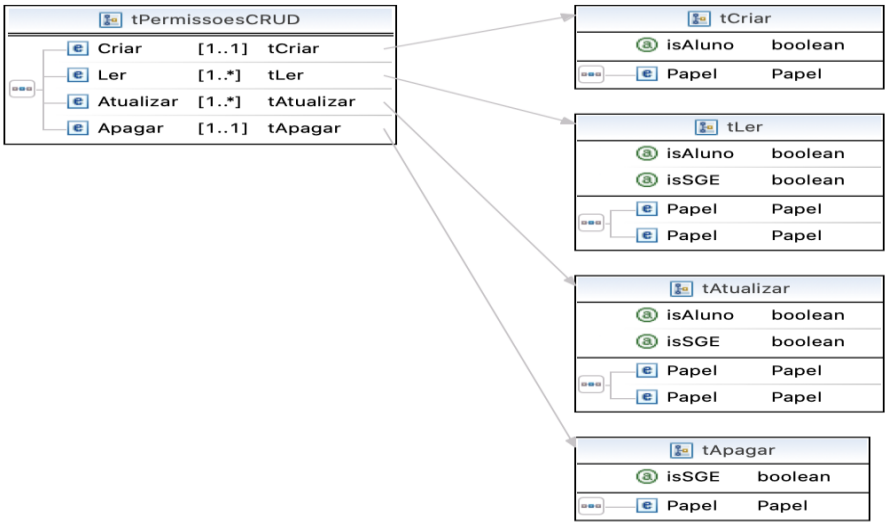
Em seguida apresenta-se a página principal do esquema gráfico de modelação das *tags* de segurança.



A figura 18 tem como elemento chave o separador “Types”, onde se encontram todas as *tags* de segurança criadas. É através desta página que é possível aceder e editar qualquer uma das *tags* e respetivos parâmetros e atributos.

As *tags* criadas pertencem a uma ferramenta onde é possível visualizá-las graficamente. Em seguida é demonstrado duas das vantagens da visualização das *tags* graficamente, a simplicidade de compreensão do que cada *tag* pretende analisar e quais as necessárias utilizar de modo a testar se certa característica está salvaguardada segundo o RGPD ou não.





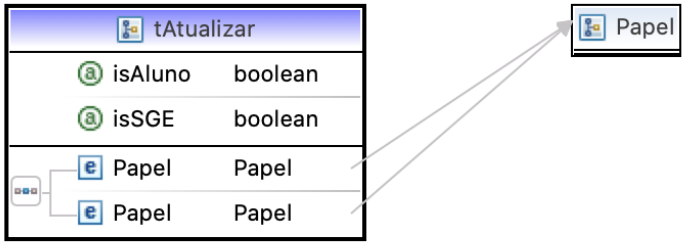


***Figura 21** - Parte final do percurso necessário percorrer para chegar à tag* tAtualizar.

Uma das vantagens deste tipo de apresentação, em árvore, é a facilidade de compreensão dos caminhos necessários de modo a testar se uma característica do processo de modelo de negócio se encontra de acordo com o RGPD ou não. Neste caso, facilita a compreensão de quais as *tags* envolvidas na confirmação, ou não, de quem pode realizar atualizações nos dados pessoais apenas pode ser alguém que tenha o Papel de *DataOwner* ou de *DataProcessor*. Neste exemplo, facilmente se percebe que o caminho começa em tControloAcessos, passando para tPermissoesCRUD, terminando na *tag* tAtualizar.

Em seguida apresentam-se as *tags* criadas assim como uma explicação do seu propósito.

3.4.1. tDadoPessoal

Esta *tag* tem o propósito de definir um objeto dado pessoal, onde é indicado que este

```
<complexType name="tDadoPessoal">
    <sequence>
        <element name="Finalidade" type="tns:tFinalidadeDosDados"></element>
        <element name="PeriodoDeConservacao" type="tns:tPeriodoDeConservacao"></element>
        <element name="NivelDeAcesso" type="tns:tControloAcessos"></element>
        <element name="TipoDeDadoPessoal" type="tns:tDadosPessoais"></element>

        <element name="DataObjectTypeDataAtRest"type="tns:tDataObjectAtRest"></element>
        <element name="DataObjectTypeDataAtMovement"type="tns:tDataObjectAtMovement"></element>

    </sequence>
</complexType>
```

tipo de objetos deve possuir uma finalidade, fundamento, período de conservação, nível de acesso, tipo de dado pessoal e o seu estado, se é um dado pessoal em movimento ou em descanso.

3.4.2. tDadoPessoalEmRepouso

```
<complexType name="tDadoPessoalEmRepouso">
    <sequence>
        <element name="CifraUtilizada" type="tns:tAlgoritmosCifragem"></element>
        <element name="GestãoValidade" type="tns:tPeriodoDeConservacao"></element>
        <element name="Mascaramento_Anonimização_Cifra" type="tns:tAlgoritmosCifragem"></element>
        <element name="RealizarBackUp" type="tns:tRealizarBackUp"></element>
    </sequence>
    <attribute name="isBackUpRealizado" type="boolean"></attribute>
</complexType>
```

Esta *tag* possui uma estrutura semelhante à da figura 22, uma vez que possui a particularidade de possuir dois atributos. Esta diferença deve-se à não obrigatoriedade de o *complexType* utilizado necessitar de possuir os atributos sempre, o mesmo não acontece com os elementos, que são obrigatórios.

O objetivo desta *tag* é a criação de um *dataObject* que se encontra em repouso. Este *dataObject* possui os seguintes elementos: CifraUtilizada, PeriodoConservação, Mascaramento_Anonimização_Cifra e RealizarBacUp.

3.4.3. tDadoPessoalEmMovimento

```
<complexType name="tDadoPessoalEmMovimento">
    <sequence>
        <element name="RegistoAcessos" type="tns:tControloAcessos"></element>
        <element name="CifraUtilizada" type="tns:tAlgoritmosCifragem"></element>
    </sequence>
    <attribute name="isTLS_Utilizado" type="boolean"></attribute>
</complexType>
```

A *tag* especificada neste ponto é muito semelhante à anterior, uma vez que representa um *dataObject* em movimento enquanto que a anterior era em repouso. Esta *tag* define que os objetos do tipo tDadoPessoalEmMovimento necessitam de ter definidos um RegistoAcessos e uma CifraUtilizada, assim como possuem um atributo booleano que define se o objeto utiliza TLS, ou seja, *Transport Layer Security*.

3.4.4. tFinalidadeDosDados

```
<simpleType name="tFinalidadeDosDados">
    <restriction base="string">
        <enumeration value="Marketing"></enumeration>
        <enumeration value="CumprimentoDoServiço"></enumeration>
        <enumeration value="GestaoFiscal"></enumeration>
        <enumeration value="GestãoAdministrativa"></enumeration>
        <enumeration value="GestãoDoContencioso"></enumeration>
        <enumeration value="ControloDaSegurançaDaInformaçao"></enumeration>
        <enumeration value="CumprimentoDasObrigaçoesLegais"></enumeration>
        <enumeration value="EmissãoDeCertificados"></enumeration>
        <enumeration value="EmissãoDiplomasDeFormaçao"></enumeration>
        <enumeration value="DeteçaoDeFraude"></enumeration>
        <enumeration value="EmissãoDeDeclaraçõesParaEfeitosDeIRS"></enumeration>
        <enumeration value="Auditoria"></enumeration>
    </restriction>
</simpleType>
```

***Figura 25** - Tag de Segurança "tFinalidadeDosDados".*

A *tag* apresentada neste ponto especifica apenas um conjunto de enumerados para a finalidade dos dados recolhidos, ou seja, o seu propósito é o de permitir indicar qual das finalidades é escolhida para poder efetuar a recolha dos dados pessoais.

As finalidades possíveis são as seguintes: *marketing*, cumprimento do serviço, gestão fiscal, gestão administrativa, gestão do contencioso, controlo da segurança da informação, cumprimentos das obrigações legais, emissão de certificados, emissão de diplomas de formação, deteção de fraude, emissão de declarações para efeitos de IRS (Imposto sobre o Rendimento das Pessoas Singulares) e auditoria.

3.4.5. tFundamentoDosDados

```
<simpleType name="tFundamentoDosDados">
    <restriction base="string">
        <enumeration value="Consentimento"></enumeration>
        <enumeration value="Contrato"></enumeration>
        <enumeration value="ObrigaçãoJurídica"></enumeration>
        <enumeration value="InteressesVitais"></enumeration>
        <enumeration value="InteressePúblico"></enumeration>
        <enumeration value="InteressesLegítimos"></enumeration>
    </restriction>
</simpleType>
```

***Figura 26** - Tag de Segurança "tFundamentoDosDados".*

Esta *tag* possui a mesma funcionalidade da anterior, uma vez que também representa um enumerado que tem a função de permitir indicar qual das seguintes opções é a escolhida para o fundamento da recolha de dados pessoais.

Os fundamentos possíveis são os seguintes: consentimento, contrato, obrigação jurídica, interesses vitais, interesse público e interesses legítimos.

3.4.6. tPeriodoDeConservacao

```
<complexType name="tPeriodoDeConservacao">
    <choice>
        <element name="PeriodoConservação" type="date"></element>
    </choice>
    <attribute name="isPermanente" type="boolean"></attribute>
</complexType>
```

Figura 27 *- Tag de Segurança "tPeriodoDeConservacao".*

Neste *complexType* encontra-se definido o comportamento do período de conservação dos dados pessoais. É necessário indicar qual o período de conservação dos mesmos, através do elemento apresentado, tendo ainda um atributo booleano onde se pode indicar que a conservação será permanente.

3.4.7. tRequisitosSegurança

```
<complexType name="tRequisitosSegurança">
    <sequence>
        <element name="Permanente"
        type="boolean"></element>
        <element name="PeríodoPermanência"
        type="date"></element>
        <element name="RequisitoSegurançaUtilizado"
        type="tns:tRequisitoSegurançaUtilizado"></element>
        <element name="Confidencialidade"
        type="tns:tAlgoritmosCifragem"></element>
    </sequence>
</complexType>
```

Figura 28 *- Tag de Segurança "tRequisitosSegurança".*

A *tag* aqui presente especifica os requisitos de segurança que se encontram presentes no dado pessoal recolhido.

3.4.8. tRequisitoSegurançaUtilizado

```
<complexType name="tRequisitoSegurançaUtilizado">
    <sequence>
        <element name="Integridade" type="boolean"></element>
        <element name="NãoRepúdio" type="boolean"></element>
        <element name="ControloAcessos" type="boolean"></element>
    </sequence>
</complexType>
```

Figura 29 *- Tag de Segurança "tRequisitoSegurançaUtilizado".*

Esta *tag* tem como função especificar os requisitos de segurança a utilizar para proteger os dados pessoais recolhidos, nomeadamente integridade, não repúdio e controlo de acessos.

3.4.9. tNãoRepúdio

```
<complexType name="tNãoRepúdio">
    <sequence>
        <element name="AdicionarNãoRepúdio" type="anySimpleType"></element>
    </sequence>
</complexType>
```

Figura 30 *- Tag de Segurança "tNãoRepúdio".*

Nesta *tag* é pensado definir o comportamento a adotar quando se decide utilizar o requisito de segurança de não repúdio. Apesar do esforço, não foi possível implementar o comportamento.

3.4.10. tAlgoritmosCifragem

```
<complexType name="tAlgoritmosCifragem">
    <choice>
        <element name="AlgoritmosCifragemNormal"
        type="tns:tAlgoritmosCifragemNormal" maxOccurs="1" minOccurs="1">
        </element>
        <element name="AlgoritmosCifragemEspecífica"
        type="tns:tAlgoritmosCifragemEspecífica" maxOccurs="1" minOccurs="1">
        </element>
        <element name="Outro" type="string"></element>
    </choice>
</complexType>
```

Figura 31 *- Tag de Segurança "tAlgoritmosCifragem".*

A *tag* tAlgoritmosCifragem serve o propósito de especificar que tipo de algoritmos de cifragem a utilizar para proteger os dados pessoais. Os algoritmos de cifragem encontram-se separados em três categorias, os algoritmos de cifragem normal, os algoritmos de cifragem específica e os outros. Estas categorias encontram-se explicadas nas *tags* seguintes.

3.4.11. tAlgoritmosCifragemNormal

```
<simpleType name="tAlgoritmosCifragemNormal">
    <restriction base="string">
        <enumeration value="AES128"></enumeration>
        <enumeration value="AES192"></enumeration>
        <enumeration value="TripleDES"></enumeration>
        <enumeration value="Blowfish"></enumeration>
    </restriction>
</simpleType>
```

Figura 32 *- Tag de Segurança "tAlgoritmosCifragemNormal".*

Tal como dito anteriormente, os algoritmos de cifragem encontram-se divididos em três categorias, esta *tag* tem como objetivo definir quais são os algoritmos de cifragem normal, ou seja, não são tão fortes como os algoritmos de cifragem específica. Estes algoritmos são utilizados para cifrar dados pessoais que não são especialmente sensíveis. Os algoritmos escolhidos são os seguintes: AES128, AES192, TripleDES e Blowfish.

3.4.12. tAlgoritmosCifragemEspecífica

```
<simpleType name="tAlgoritmosCifragemEspecífica">
    <restriction base="string">
        <enumeration value="AES256"></enumeration>
        <enumeration value="RSA1024"></enumeration>
        <enumeration value="RSA2048"></enumeration>
        <enumeration value="Twofish"></enumeration>
    </restriction>
</simpleType>
```

Figura 33 *- Tag de Segurança "tAlgoritmosCifragemEspecífica".*

A *tag* aqui presente, serve um propósito semelhante à anterior, ou seja, tem o propósito de definir quais os algoritmos de cifragem a utilizar quando se lida com dados pessoais especialmente sensíveis, sendo necessário utilizar cifras que garantam uma melhor segurança da informação. Os algoritmos de cifragem escolhidos são os seguintes: AES256, RSA1024, RSA2048 e Twofish.

3.4.13. tControloAcessos

```
<complexType name="tControloAcessos">
    <sequence>
        <element name="Logs" type="tns:tLogs"
        maxOccurs="unbounded" minOccurs="1"></element>
        <element name="PermissoesCRUD" type="tns:tPermissoesCRUD"
        maxOccurs="unbounded" minOccurs="1"></element>
    </sequence>
</complexType>
```

Figura 34 *- Tag de Segurança "tControloAcessos".*

Esta *tag* especifica o funcionamento do controlo de acessos. Para se poder utilizar este elemento da segurança da informação é necessário implementar um sistema de registos (logs) e também definir as permissões CRUD.

3.4.14. tRegistos

```
<complexType name="tRegistos">
    <sequence>
        <element name="RegistoNome" type="string"></element>
        <element name="RegistoIPUtilizado" type="string"></element>
        <element name="RegistoPortoUtilizado" type="string"></element>
        <element name="RegistoDataAcesso" type="string"></element>
        <element name="RegistoDadosAcedidos" type="string"></element>
        <element name="RegistoUtilizacaoDosDadosAcedidos" type="string"></element>
    </sequence>
</complexType>
```

Os logs dos utilizadores a ser guardados, de modo a aumentar o grau de segurança da informação são os seguintes: nome, ip utilizado, porto utilizado, data de acesso, dados acedidos e qual a utilização dos dados acedidos. Ou seja, cada vez que alguém acede aos dados, são registadas essas informações.

3.4.15. tPermissoesCRUD

```
<complexType name="tPermissoesCRUD">
    <sequence>
        <element name="Criar" type="tns:tCriar" maxOccurs="1"   minOccurs="1"></element>
        <element name="Ler" type="tns:tLer" maxOccurs="unbounded" minOccurs="1"></element>
        <element name="Atualizar" type="tns:tAtualizar" maxOccurs="unbounded" minOccurs="1"> </element>
        <element name="Apagar" type="tns:tApagar" maxOccurs="1" minOccurs="1"></element>
    </sequence>
</complexType>
```

As permissões CRUD são definidas nesta *tag*, onde se define que apenas se pode criar um dado uma só vez, que se pode ler os dados no mínimo uma vez e sem limite de vezes, o mesmo para o update e que tal como o criar, apenas se pode apagar um dado uma só vez.

As próximas quatro *tags* definem cada um dos componentes das permissões CRUD.

3.4.16. tCriar

```
<complexType name="tCriar">
    <sequence>
        <element name="Papel" type="tns:Papel"></element>
    </sequence>
    <attribute name="isAluno" type="boolean"></attribute>
</complexType>
```

A *tCreate* trata a definição da atribuição da permissão de criar. Para atribuir esta permissão é necessário indicar qual o papel do utilizador, assim como um atributo booleano onde se indica se o utilizador é ou não o dono dos dados pessoais. Apenas se define um papel pois apenas o *data owner* pode criar os dados pessoais sobre si mesmo.

3.4.17. tLer

```
<complexType name="tLer">
    <sequence>
        <element name="Papel" type="tns:Papel"></element>
        <element name="Papel" type="tns:Papel"></element>
    </sequence>
    <attribute name="isAluno" type="boolean"></attribute>
    <attribute name="isSGE" type="boolean"></attribute>
</complexType>
```

A *tag* tLer define a atribuição da permissão para ler um dado pessoal. Esta permissão pode ser atribuída tanto ao dono dos dados como à pessoa que vai realizar o tratamento dos dados pessoais.

3.4.18. tAtualizar

```
<complexType name="tAtualizar">
    <sequence>
        <element name="Papel" type="tns:Papel"></element>
        <element name="Papel" type="tns:Papel"></element>
    </sequence>
    <attribute name="isAluno" type="boolean"></attribute>
    <attribute name="isSGE" type="boolean"></attribute>
</complexType>
```

Muito semelhante à *tag* anterior, a tAtualizar define a atribuição da permissão para atualizar um dado pessoal. Esta permissão pode ser atribuída tanto ao dono dos dados como à pessoa que vai realizar o tratamento dos dados pessoais.

3.4.19. tApagar

```
<complexType name="tApagar">
    <sequence>
        <element name="Papel" type="tns:Papel"></element>
    </sequence>
    <attribute name="isSGE" type="boolean"></attribute>
</complexType>
```

Similarmente à tCriar, a tApagar trata a definição da atribuição da permissão de apagar dados pessoais. Para atribuir esta permissão é necessário indicar qual o papel do utilizador, assim como um atributo booleano onde se indica se o utilizador é ou não quem realiza o tratamento dos dados pessoais. Apenas se define um papel pois apenas o *data processor* pode realizar a ação de apagar os dados pessoais.

3.4.20. tDadosEspecialmenteSensiveis

```
<complexType name="tDadosEspecialmenteSensiveis">
    <sequence>
        <element name="DadosEspecialmenteSensíveisInternos"
            type="tns:tDadosEspecialmenteSensíveisInternos"
            maxOccurs="unbounded" minOccurs="1">
        </element>
        <element name="DadosEspecialmenteSensíveisExternos"
            type="tns:tDadosEspecialmenteSensíveisExternos"
            maxOccurs="unbounded" minOccurs="1">
        </element>
    </sequence>
</complexType>
```

Figura 41 *- Tag de Segurança "tDadosEspecialementeSensiveis".*

Esta *tag* tem o simples propósito de especificar se os dados especialmente sensíveis em questão são de natureza interna ou externa.

3.4.21. tDadosEspecialmenteSensíveisInternos

```
<complexType name="tDadosEspecialmenteSensíveisInternos">
    <choice>
        <element name="ConhecimentoECrença" type="string"
            maxOccurs="unbounded" minOccurs="1">
        </element>
        <element name="Preferência" type="string"
            maxOccurs="unbounded" minOccurs="1">
        </element>
    </choice>
</complexType>
```

Figura 42 *- Tag de Segurança "tDadosEspecialementeSensiveisInternos".*

Nesta *tag* são definidos os diferentes tipos de dados pessoais especialmente sensíveis internos que existem, sendo eles: conhecimento e crença e preferência.

3.4.22. tDadosEspecialmenteSensíveisExternos

```
<complexType name="tDadosEspecialmenteSensíveisExternos">
    <choice>
        <element name="Etnia" type="string" maxOccurs="unbounded"
            minOccurs="1">
        </element>
        <element name="MédicaESaúde" type="string"
            maxOccurs="unbounded" minOccurs="1">
        </element>
        <element name="Sexual" type="string" maxOccurs="unbounded"
            minOccurs="1">
        </element>
    </choice>
</complexType>
```

Figura 43 *- Tag de Segurança "tDadosEspecialementeSensíveisExternos".*

Tal como a *tag* anterior, a *tag* tDadosEspecialmenteSensíveisExternos tem o propósito de definir os dados especialmente sensíveis externos, que são os seguintes: etnia, médica e saúde e sexual.

3.4.23. tDadosPessoais

```
<complexType name="tDadosPessoais">
    <choice>
        <element name="Internos" type="tns:tInternos" maxOccurs="unbounded" minOccurs="1"></element>
        <element name="Externos" type="tns:tExternos" maxOccurs="unbounded" minOccurs="1"></element>
        <element name="Históricos" type="tns:tHistóricos" maxOccurs="unbounded" minOccurs="1"></element>
        <element name="Financeiros" type="tns:tFinanceiros" maxOccurs="unbounded" minOccurs="1"></element>
        <element name="Sociais" type="tns:tSociais" maxOccurs="unbounded" minOccurs="1"></element>
        <element name="Rastreamento" type="tns:tRastreamento" maxOccurs="unbounded" minOccurs="1"></element>
    </choice>

    <attribute name="EspecialmenteSensível" type="boolean" use="prohibited"></attribute>
    <attribute name="AcessoPúblico" type="boolean"></attribute>
    <attribute name="AcessoInternoGeralizado" type="boolean"></attribute>
    <attribute name="AcessoInternoRestrito" type="boolean"></attribute>
</complexType>
```

Figura 44 *- Tag de Segurança "tDadosPessoais".*

A *tag* tDadosPessoais define quais as categorias de dados pessoais existentes assim como indica se esses dados são especialmente sensíveis, e depois qual o tipo de acesso que devem ter, facilitando a atribuição de permissões. As categorias de dados pessoais são as seguintes: internos, externos, históricos, financeiros, sociais e de rastremento.

3.4.24. tInternos

```
<simpleType name="tInternos" final="restriction">
        <restriction base="string">
            <enumeration value="ConhecimentoECrença"></enumeration>
            <enumeration value="Autenticação"></enumeration>
            <enumeration value="Preferência"></enumeration>

            <enumeration value="Outras"></enumeration>

        </restriction>
</simpleType>
```

Figura 45 *- Tag de Segurança "tInternos".*

Esta *tag* tem como função definir quais os diferentes tipos de dados existentes dentro da categoria de dados pessoais internos. São eles conhecimento e crença, autenticação, preferência e foi adicionado um campo "Outras" para quando a situação não permitir indicar facilmente o tipo de dados.

3.4.25. tExternos

```
<simpleType name="tExternos" final="restriction">
        <restriction base="string">
            <enumeration value="Identificação"></enumeration>
            <enumeration value="Etnia"></enumeration>
            <enumeration value="Sexual"></enumeration>
            <enumeration value="Comportamento"></enumeration>
            <enumeration value="Demografia"></enumeration>
            <enumeration value="MédicaESaúde"></enumeration>
            <enumeration value="Física"></enumeration>


            <enumeration value="Outras"></enumeration>

        </restriction>
</simpleType>
```

Figura 46 *- Tag de Segurança "tExternos".*

Tal como o exemplo anterior, neste caso são definidos quais os diferentes tipos de dados existentes dentro da categoria de dados pessoais externos. São eles: identificação, etnia, sexual, comportamento, médica e saúde, demografia e física.

3.4.26. tHistóricos

```
<simpleType name="tHistóricos" final="restriction">
        <restriction base="string">

            <enumeration value="HistóriaDaVida"></enumeration>

        </restriction>
</simpleType>
```

Figura 47 *- Tag de Segurança "tHistóricos"*

O mesmo acontece para esta *tag*, onde são definidos quais os diferentes tipos de dados existentes dentro da categoria de dados pessoais históricos. Neste caso apenas são os dados história da vida.

3.4.27. tFinanceiros

```
<simpleType name="tFinanceiros" final="restriction">
        <restriction base="string">

            <enumeration value="Conta"></enumeration>
            <enumeration value="Propriedade"></enumeration>
            <enumeration value="Transações"></enumeration>
            <enumeration value="Crédito"></enumeration>

        </restriction>
</simpleType>
```

Figura 48 *- Tag de Segurança "tFianceiros".*

Assim como os anteriores, a *tag* tFinanceiros definine quais os diferentes tipos de dados existentes dentro da categoria de dados pessoais financeiros, sendo eles: conta, propriedade, transações e crédito.

3.4.28. tSociais

```
<simpleType name="tSociais" final="restriction">
        <restriction base="string">

            <enumeration value="Profissional"></enumeration>
            <enumeration value="Criminal"></enumeration>
            <enumeration value="VidaPública"></enumeration>
            <enumeration value="Família"></enumeration>
            <enumeration value="RedesSociais"></enumeration>
            <enumeration value="Comunicação"></enumeration>

        </restriction>
</simpleType>
```

Figura 49 *- Tag de Segurança "tSociais".*

Existe ainda a *tag* tSociais onde são definidos os diferentes tipos de dados existentes dentro da categoria de dados pessoais sociais, sendo os seguintes: profissional, criminal, vida pública, família, redes sociais e comunicação.

3.4.29. tRastreamento

```
<simpleType name="tRastreamento" final="restriction">
        <restriction base="string">

            <enumeration value="Computador"></enumeration>
            <enumeration value="Contacto"></enumeration>
            <enumeration value="Localização"></enumeration>

        </restriction>
</simpleType>
```

Figura 50 *- Tag de Segurança "tRastreamento".*

Por fim temos a *tag* referente aos dados pessoais de rastreamento, onde são definidos os diferentes tipos de dados existentes dentro da categoria de dados pessoais de rastreamento, que são os seguintes: computador, contacto e localização.

3.5.Integração das *Tags* de Segurança no Diagrama

Após a realização, quer do diagrama, quer do conjunto das *tags* de segurança, foi necessário integrar as *tags* no diagrama. Esta integração ocorreu da seguinte forma: identificação das *tags* necessárias que vão ao encontro das novas regras definidas no RGPD, para cada componente do diagrama, seguidas da sua adição aos componentes.

Capítulo 4 – Caso de Estudo e Validação do Sistema

Neste capítulo está descrita a aplicação da metodologia desenvolvida no capítulo anterior. Os procedimentos de inscrição e matriculação dos alunos do Iscte-Instituto Universitário de Lisboa, foram o caso de estudo escolhido para a aplicação da metodologia desenvolvida.

Em relação aos procedimentos acima referidos, procurou-se verificar se estes estavam a ser desenvolvidos no sentido de:

- Demonstrar os esforços do Iscte-Instituto Universitário de Lisboa, para organizar e melhorar a gestão dos processos por parte do seu *staff*.
- Oferecer uma visão compartilhada do Processo de inscrição e matriculação dos alunos, pela organização dos seus processos internos e possibilidade de comunicá-lo com uma linguagem universal, realizando para tal a modelação com BPMN.

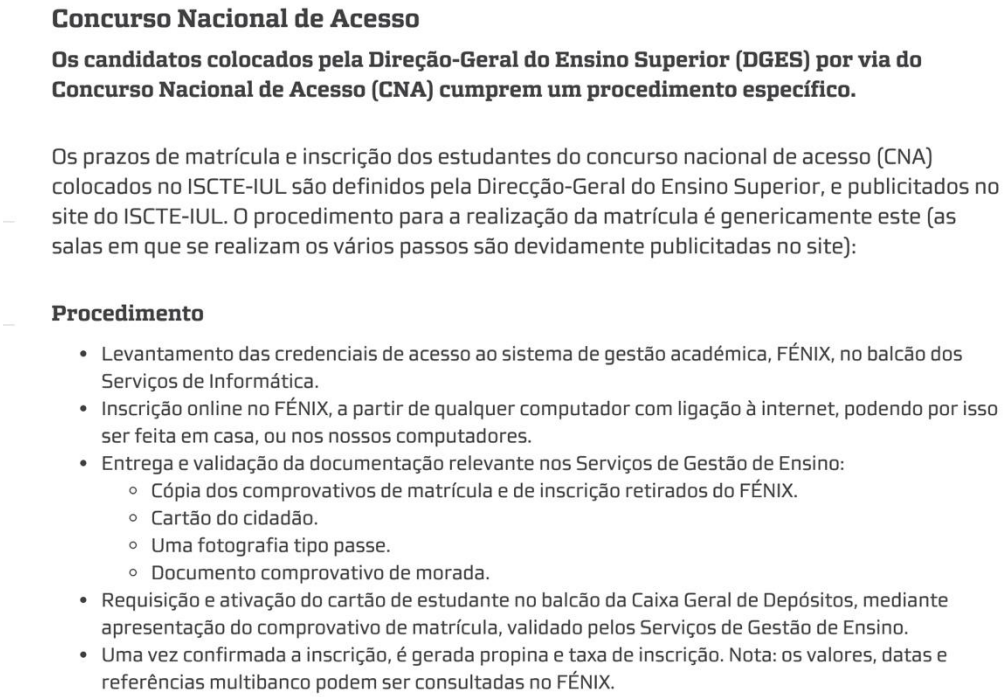
- Melhorar a segurança e privacidade da informação utilizada no Processo de inscrição e matriculação dos alunos.

O primeiro passo no sentido de realizar o estudo proposto foi a tomada de decisão sobre quais os processos a analisar. Através de pesquisa no site do Iscte-Instituto Universitário de Lisboa, foi decidido desenvolver processos modelados em BPMN sobre o seguinte processo, "Inscrição e Matriculação dos Alunos no Iscte-Instituto Universitário de Lisboa", seguindo (Harmon, 2007) quando sugere que as alterações nos processos começam pela decisão de melhorar um processo de negócio específico.

De modo a realizar as alterações, foram considerados os seguintes três critérios para escolher o processo:

1- Identificação de processos com contacto com dados pessoais. O processo de inscrição e matriculação é um dos principais processos onde é envolvida a cedência de dados pessoais por parte dos alunos ao Iscte-Instituto Universitário de Lisboa.
2- Importância dos processos com maior impacto sobre os clientes, que neste caso são os alunos. Para além da inscrição que os alunos têm de fazer quando ingressam o Iscte-Instituto Universitário de Lisboa, todos os anos é necessário realizar a inscrição, de modo a estarem aptos a usufruir das aulas necessárias para realizarem o seu processo escolar.
3- Viabilidade, que considerou se o processo era exequível ou não. O processo selecionado numa primeira análise ao site do Iscte-Instituto Universitário de Lisboa foi aprovado por estes três critérios, pelo que foi decidido avançar com o seu melhoramento.

Para tal foi realizado um levantamento e especificação com BPMN dos processos referentes à matriculação e inscrição dos alunos, dado que não existiam modelações utilizando esta linguagem. As modelações existentes foram feitas com recurso a linguagem natural e estruturada conforme a figura 51.



Concurso Nacional de Acesso

Os candidatos colocados pela Direção-Geral do Ensino Superior (DGES) por via do Concurso Nacional de Acesso (CNA) cumprem um procedimento específico.

Os prazos de matrícula e inscrição dos estudantes do concurso nacional de acesso (CNA) colocados no ISCTE-IUL são definidos pela Direcção-Geral do Ensino Superior, e publicitados no site do ISCTE-IUL. O procedimento para a realização da matrícula é genericamente este (as salas em que se realizam os vários passos são devidamente publicitadas no site):

Procedimento

- Levantamento das credenciais de acesso ao sistema de gestão académica, FÉNIX, no balcão dos Serviços de Informática.
- Inscrição online no FÉNIX, a partir de qualquer computador com ligação à internet, podendo por isso ser feita em casa, ou nos nossos computadores.
- Entrega e validação da documentação relevante nos Serviços de Gestão de Ensino:
  - Cópia dos comprovativos de matrícula e de inscrição retirados do FÉNIX.
  - Cartão do cidadão.
  - Uma fotografia tipo passe.
  - Documento comprovativo de morada.
- Requisição e ativação do cartão de estudante no balcão da Caixa Geral de Depósitos, mediante apresentação do comprovativo de matrícula, validado pelos Serviços de Gestão de Ensino.
- Uma vez confirmada a inscrição, é gerada propina e taxa de inscrição. Nota: os valores, datas e referências multibanco podem ser consultadas no FÉNIX.

Figura 51 *- Dados relativos aos procedimentos de inscrição e matriculação dos alunos no Iscte-Instituto Universitário de Lisboa.*

Os dados utilizados para começar este projeto foram obtidos através da consulta do *site* do Iscte-Instituto Universitário de Lisboa (*Página principal - Iscte – Instituto Universitário de Lisboa*, 2020), dentro do sector "Estudar", "Candidaturas". Atualmente o *site* já foi reformulado, pelo que já não existe o local onde os dados iniciais foram consultados, tendo este sido substituído (*Matrícula e inscrição dos candidatos colocados no ISCTE-IUL na 1.ª fase*, 2020).

Deste modo, decidiu-se criar um modelo simples, de matriculação e inscrição dos alunos, através da utilização de um editor BPMN (que pode estar disponível num IDE).

Os IDE's encontrados não suportam as notações definidas nas normas BPMN assim como as normas também não suportam as especificações das propriedades de segurança desejadas, como tal não se adotou nenhuma proposta já existente para o desenvolvimento do diagrama, pelo que tanto o modelo de processo de negócio como as *tags* de segurança foram criadas do zero. Na figura 52 é possível observar o diagrama desenvolvido aplicado

ao processo de inscrição e matriculação dos alunos no Iscte-Instituto Universitário de Lisboa.

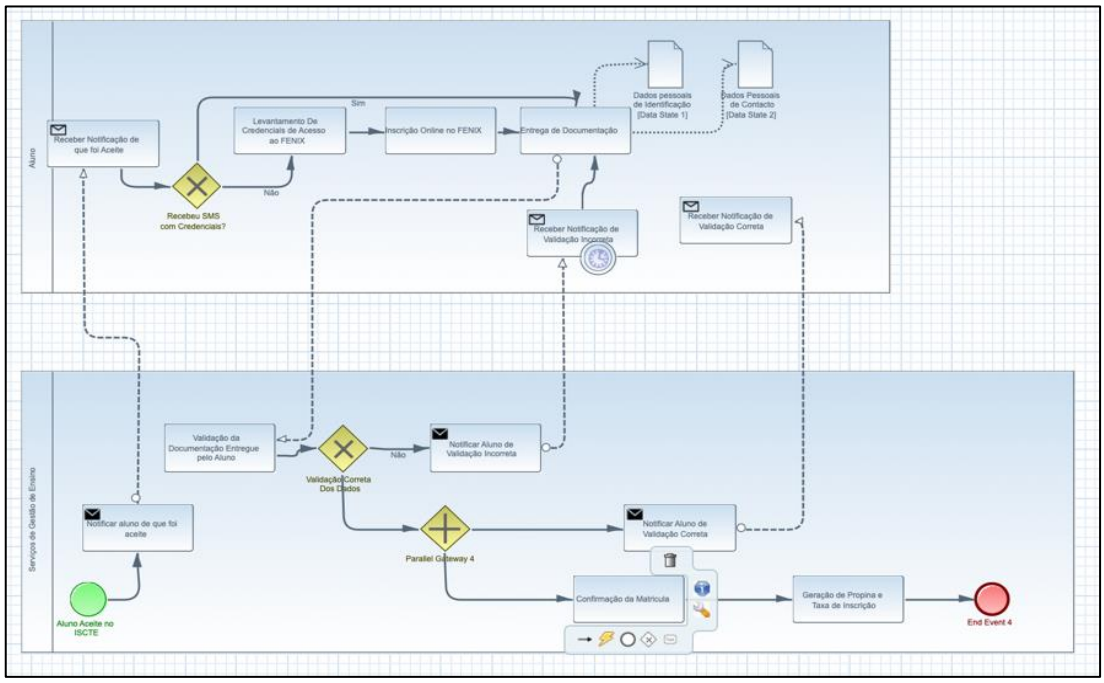


***Figura 52** - Diagrama BPMN final "ProcessoMatriculaçãoeInscriçãoNoISCTE".*

O diagrama teve o seu desenvolvimento afetado pela necessidade de ser facilmente exportado tanto como ficheiro BPMN como XML. Para tal, foi necessário simplificar o processo de modelo de negócio, não o deixando perder as suas características principais, como as ações necessárias para realizar a inscrição e matriculação dos alunos. Assim, foi adotada a decisão de não introduzir demasiados elementos capazes de "prender" ou tornar demasiado complexo o diagrama, de modo a que fosse facilmente compreendido tanto por técnicos como por qualquer outra pessoa fora da área de tecnologias de informação.

O diagrama acima apresentado, é composto por diferentes componentes, sendo estes apresentados na tabela 1:

Tabela 1 *- Componentes do Diagrama BPMN "ProcessoMatriculaçãoeInscriçãonoISCTE", aplicado ao Caso de Estudo, com os respetivos nomes.*

Componente do Diagrama	Nome
Pool	"Aluno" "Serviços de Gestão de Ensino"
Start Event	"Levantamento de Credenciais"
Timer Event	"Receber Notificação de Validação Incorreta"
Exclusive Gateway	"Recebeu SMS com Credenciais?" "Validação Correta dos Dados"
Parallell Gateway	"Validação Positiva"
Task	"Levantamento de Credenciais de Acesso ao FENIX" "Inscrição Online no FENIX" "Entrega de Documentação" "Validação da Documentação Entregue pelo Aluno" "Confirmação da Matrícula" "Geração de Propina e Taxa de Inscrição" "Requisição do Cartão de Aluno" "Apresentação do Comprovativo de Matrícula"
Send Task	"Notificar o Aluno de Validação Incorreta" "Notificar o Aluno de Validação Correta"
Receive Task	"Receber Notificação de Validação Incorreta" "Receber Notificação de Validação Correta" "Receber Notificação de que foi Aceite"
Service Task	"Ativação do Cartão de Aluno"
DataObject	"Dados Pessoais de Identificação" "Dados Pessoais de Contacto"

Os riscos existentes no processo escolhido são relacionados com o RGPD, uma vez que este regulamento veio trazer a necessidade de implementação de variadas características, entre as quais os novos direitos que os utilizadores, neste caso os alunos, possuem sobre os seus dados, por exemplo o direito ao esquecimento, direito de limitação de tratamento, direito à portabilidade, entre outros direitos, assim como a necessidade de proteção e tratamento sobre dados pessoais, que com o RGPD foram atribuídos a novas categorias, as quais têm diferentes requisitos de segurança.

Após a aplicação da metodologia desenvolvida, foi facilitada a colmatação de vários riscos inicialmente encontrados, uma vez que foram criadas as ferramentas necessárias para a verificação da violação das novas regras provenientes do RGPD, definidas no ficheiro XSD.

As *tags* de segurança encontram-se inseridas dentro dos componentes do diagrama (tabela 1), sendo este depois transformado em XML.

Tal como descrito acima, as *tags* de segurança encontram-se localizadas dentro dos componentes do diagrama, no campo *Documentation*, como se apresenta na figura 53.

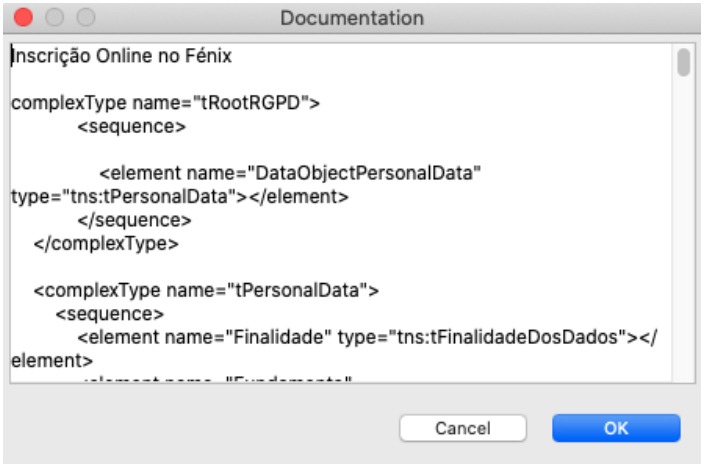


Figura 53 *- Demonstração da presença das tags de segurança inseridas nos componentes do diagrama no campo documentation.*

O passo seguinte é a transformação do diagrama para XML, onde é possível identificar a presença destas *tags*, tal como se apresenta na figura 54.

```
    <bpmn2:task id="EntregaDocumentacao" name="Entrega de Documentação">
      <bpmn2:documentation id="Documentation_10">Entrega da documentação relevante nos servicos de gestão de ensino.
-Cópia dos comprovativos de matrícula e de inscrição retirados do FÉNIX.
-Cartão do cidadão.
-Uma fotografia tipo passe.
-Documento comprovativo de morada.

complexType name=&quot;tRootRGPD&quot;>
            &lt;sequence>

                &lt;element name=&quot;DataObjectPersonalData&quot; type=&quot;tns:tPersonalData&quot;>&lt;/element>
            &lt;/sequence>
    &lt;/complexType>

    &lt;complexType name=&quot;tPersonalData&quot;>
        &lt;sequence>
            &lt;element name=&quot;Finalidade&quot; type=&quot;tns:tFinalidadeDosDados&quot;>&lt;/element>
            &lt;element name=&quot;Fundamento&quot; type=&quot;tns:tFundamentoDosDados&quot;>&lt;/element>
            &lt;element name=&quot;PeriodoDeConservacao&quot; type=&quot;tns:tPeriodoDeConservacao&quot;>&lt;/element>
            &lt;element name=&quot;NivelDeAcesso&quot; type=&quot;tns:tControloAcessos&quot;>&lt;/element>
            &lt;element name=&quot;TipoDeDadoPessoal&quot; type=&quot;tns:tDadosPessoais&quot;>&lt;/element>

            &lt;element name=&quot;DataObjectTypeDataAtRest&quot; type=&quot;tns:tDataObjectAtRest&quot;>&lt;/element>
            &lt;element name=&quot;DataObjectTypeDataAtMovement&quot; type=&quot;tns:tDataObjectAtMovement&quot;>&lt;/element>
        &lt;/sequence>
    &lt;/complexType>
```

Figura 54 *- Demonstração da presença das tags de segurança no ficheiro XML.*

Deste modo é possível verificar que o diagrama do processo de modelo de negócio desenvolvido contém as especificações desenvolvidas de modo a representar uma maior segurança e privacidade da informação, ajudando a facilitar o aumento da *compliance* do RGPD.

Capítulo 5 – Conclusões e Trabalho Futuro

A dissertação realizada teve como principais objetivos efetuar um acrescento à norma XML, ao criar um sistema de análise dos processos de negócio na linguagem BPMN, através de *tags* de segurança assim como o desenvolvimento de uma metodologia que torne mais fácil o cumprimento do RGPD.

Durante a realização da dissertação incluiu-se uma amostra reduzida, tendo apenas sido desenvolvido um processo de modelo de negócio de uma instituição. Desde modo apenas é possível estimar resultados sobre este processo desenvolvido.

Tal como explicado em 4.1, segundo (Harmon, 2007), de modo a melhorar um processo de negócio, a primeira decisão tem de ser melhorar esse mesmo processo. Para realizar essa melhoria, à luz do RGPD, a solução proposta nesta dissertação é a adoção da metodologia desenvolvida. Esta é composta por quatro passos principais, onde se garante que o processo de modelo de negócio passa a conter as novas regras do RGPD, definidas no esquema XSD. Desta forma garante-se que, aquando de uma análise de lacunas, o ficheiro XML originado através da conversão do diagrama BPMN, não é violado pela ausência dessas novas regras definidas.

Qualquer empresa ou organização que utilize a metodologia proposta poderá ver melhorias no desenho de processos de negócios, e ao nível de *compliance*, através da utilização das ferramentas desenvolvidas. No entanto, a utilização da metodologia e das ferramentas não resolve o problema da *compliance* por si só, apenas ajuda a resolver.

O projeto e investigação desenvolvidos permitiram criar valor pessoal e académico e também para a instituição através dos componentes desenvolvidos: uma metodologia de criação de *tags* de segurança, as *tags* de segurança e o diagrama que retrata o processo de modelo de negócio de inscrição e matriculação de alunos no Iscte-Instituto Universitário de Lisboa.

O trabalho futuro pode começar com a integração de uma ferramenta de análise de lacunas assim como a integração de testes para a comprovação dos resultados. Pode também ser implementado um maior grau de abrangência, tanto de maior número de processos para modelar como de modelar os processos mais detalhadamente, tendo em conta que poderá ter efeitos negativos ao nível da facilidade da compreensão.

Referências

Advanced Encryption Standard (AES). (2001). 51.

Alanazi, H., Bahaa, B., Zaidann, A. A., & Jalab, H. A. (2010). New Comparative Study Between DES, 3DES and AES within Nine Factors. *ResearchGate*. https://www.researchgate.net/publication/45907472_New_Comparative_Study_Between_DES_3DES_and_AES_within_Nine_Factors

Albinati, F. (2016). *European Data Protection Supervisor*. European Data Protection Supervisor - European Data Protection Supervisor. https://edps.europa.eu/data-protection/data-protection/glossary/e_en

Aleisa, N. (2015). A Comparison of the 3DES and AES Encryption Standards. *International Journal of Security and Its Applications*, *9*(7), 241–246. https://doi.org/10.14257/ijsia.2015.9.7.21

Assembleia da República. (1998). *Lei nº 67/98*.

Bizagi. (2012). *How do I install Bizagi Process Modeler on my Mac?* https://feedback.bizagi.com/en/topic/how-do-i-install-bizagi-process-modeler-on-my-mac

Bizagi. (2019). *Bizagi Modeler User Guide—A Business Process Modeling Tool*. https://help.bizagi.com/process-modeler/en/index.html?bm_requirements.htm

Boritz, J. E. (2005). IS practitioners' views on core concepts of information integrity. *International Journal of Accounting Information Systems*, *6*(4), 260–279. https://doi.org/10.1016/j.accinf.2005.07.001

BPMN.i0. (2018). *BPMN editor*. https://demo.bpmn.io/

Brodt, B. (2018). *Eclipse BPMN2 Modeler | The Eclipse Foundation*. https://www.eclipse.org/bpmn2-modeler/

Caldas, M. P. (2003). Management information systems: Managing the digital firm. *Revista de Administração Contemporânea*, *7*(1), 223–223. https://doi.org/10.1590/S1415-65552003000100014

Camunda. (2015). *Receive Task*. https://docs.camunda.org/manual/7.4/reference/bpmn20/tasks/receive-task/

Camunda. (2015). *Service Task*. https://docs.camunda.org/manual/7.4/reference/bpmn20/tasks/service-task/

Camunda. (2015). *Tasks*. https://docs.camunda.org/manual/7.4/reference/bpmn20/tasks/

Camunda.org. (2015). *Parallel Gateway*. https://docs.camunda.org/manual/7.4/reference/bpmn20/gateways/parallel-gateway/

Camunda.org. (2015). *Timer Events*. https://docs.camunda.org/manual/7.9/reference/bpmn20/events/timer-events/

Camunda.org. (2018a). *Call Activity*. https://docs.camunda.org/manual/7.4/reference/bpmn20/subprocesses/call-activity/

Camunda.org. (2018b). *Data-based Exclusive Gateway (XOR)*. https://docs.camunda.org/manual/7.4/reference/bpmn20/gateways/exclusive-gateway/

Camunda.org. (2018c). *Gateways*. https://docs.camunda.org/manual/7.4/reference/bpmn20/gateways/

Camunda.org. (2018d). *The Camunda BPM Manual*. https://docs.camunda.org/manual/7.13/

Carnaghan, C. (2006). *International Journal of Accounting Information Systems*. ResearchGate. https://www.researchgate.net/journal/1467-0895_International_Journal_of_Accounting_Information_Systems

CECOA. (2018). *Política De Privacidade De Tratamento De Dados Pessoais*.

Comissão Europeia. (2018a). *O que são dados pessoais?* Comissão Europeia - European Commission. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_pt

Comissão Europeia. (2018b). *Que dados pessoais são considerados sensíveis?* Comissão Europeia - European Commission. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_pt

Comissão Nacional de Proteção de Dados. (2018). *Direitos dos titulares*. https://www.cnpd.pt/home/direitos/direitos.htm

Edraw Max. (2019). https://www.edrawsoft.com/pt/ad/edraw-max.html?gclid=CjwKCAjwn9v7BRBqEiwAbq1Ey11V5mBga_Kq2iawN2viqEkdRJPH8joYhsk71sEDU15f27uXXHEi2xoCmAYQAvD_BwE

Grimes, R. A. (2019). *What is personally identifiable information (PII)? How to protect it under GDPR*. CSO Online. https://www.csoonline.com/article/3215864/how-to-protect-personally-identifiable-information-pii-under-gdpr.html

Grupo de Trabalho do Artigo 29.º. (2018). *Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679*.

Harmon, P. (2007). *Business Process Change: A Guide For Business Managers and BPM and Six Sigma Professionals*.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). *Design Science in Information Systems Research*. 33.

Hub, A. (2015). *Workflow with Activiti*. Alfresco Hub. https://hub.alfresco.com/t5/alfresco-content-services-hub/workflow-with-activiti/ba-p/290770

Huber, S., Mühlroth, C., Zagel, C., Schwarz, S., & Bodendorf, F. (2016). *Agile Innovation Management*. 116.

Kroft, S. (2014). *The Data Brokers: Selling your personal information*. https://www.cbsnews.com/news/data-brokers-selling-personal-information-60-minutes/

Labda, W., Mehandjiev, N., & Sampaio, P. (2014). Modeling of privacy-aware business processes in BPMN to protect personal data. *Proceedings of the 29th Annual ACM Symposium on Applied Computing*, 1399–1405. https://doi.org/10.1145/2554850.2555014

Low, G. S., & Mohr, J. J. (2001). Factors affecting the use of information in the evaluation of marketing communications productivity. *Journal of the Academy of Marketing Science, 29*(1), 70. https://doi.org/10.1177/0092070301291005

Lucidchart Blog. (2018). *What Is Gap Analysis | Lucidchart Blog*. /blog/what-is-gap-analysis

Matrícula e inscrição dos candidatos colocados no ISCTE-IUL na 1.ª fase. (2020). Iscte. www.iscte-iul.pt

McCarthy, C. (2006). *Digital Libraries: Security and Preservation Considerations*. Wiley. https://www.oreilly.com/library/view/handbook-of-information/9780471648307/14_chapter-04.html

McGavisk, T. (2019). *The Positive and Negative Implications of GDPR*. https://www.timedatasecurity.com/blogs/the-positive-and-negative-implications-of-gdpr

Meland, P. H., & Gjære, E. A. (2012). Representing threats in BPMN 2.0. *ResearchGate*. Availability, Reliability and Security (ARES). https://doi.org/10.1109/ARES.2012.13

Modelio. (2011). *Features within Modelio the open source modeling environment*. Modelio Open Source. https://www.modelio.org/about-modelio/features.html

Nascimento, T. (2019). Categorias de Dados. *Portal do DPO - Encarregado de Protecção de Dados*. https://www.portaldodpo.pt/categorias-de-dados/

Nelson, R. R., Todd, P. A., & Wixom, B. H. (2005). Antecedents of Information and System Quality: An Empirical Examination within the Context of Data Warehousing. *Journal of Management Information Systems*, *21*(4), 199–235. JSTOR.

Página principal—Iscte – Instituto Universitário de Lisboa. (2020). https://www.iscte-iul.pt/

Paradigm, V. (2004). *Drawing BPMN Pools and Lanes*. https://www.visual-paradigm.com/support/documents/vpuserguide/2821/286/56993_poolandlane.html

Parlamento Europeu. (2001). *Th regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data*.

Regulamento (UE) 2016/679, Pub. L. No. 32016R0679, 119 OJ L (2016). http://data.europa.eu/eli/reg/2016/679/oj/por

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2008). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, 45–77.

Quora. (2013). *How many times is RSA-2048 or RSA-4096 slower than RSA-1024? - Quora*. https://www.quora.com/How-many-times-is-RSA-2048-or-RSA-4096-slower-than-RSA-1024

Reis, D. (2018). Cinco meses de rgpd—Um primeiro balanço em 9 pontos. *Observador*. https://observador.pt/opiniao/cinco-meses-de-rgpd-um-primeiro-balanco-em-9-pontos/

Rizvi, S. A. M., Hussain, S. Z., & Wadhwa, N. (2011). Performance Analysis of AES and TwoFish Encryption Schemes. *2011 International Conference on Communication Systems and Network Technologies*, 76–79. https://doi.org/10.1109/CSNT.2011.160

Rodriguez, A., Fernandez-Medina, E., & Piattini, M. (2007). A BPMN Extension for the Modeling of Security Requirements in Business Processes. *IEICE Transactions on Information and Systems*, *E90-D*(4), 745–752. https://doi.org/10.1093/ietisy/e90-d.4.745

Rodriguez, Alfonso, Piattini, M., & Férnandez-Medina, E. (2007). Finalidades e períodos do tratamento de dados. *IEIC Transactions on Information and Systems*. http://www.nos.pt/institucional/PT/politica-de-privacidade/Paginas/finalidades-periodos-tratamento-dados.aspx

Rouse, M. (2015a). *What is XML (Extensible Markup Language)? - Definition from WhatIs.com*. WhatIs.Com. https://whatis.techtarget.com/definition/XML-Extensible-Markup-Language

Rouse, M. (2015b). *What is XSD (XML Schema Definition)? - Definition from WhatIs.com*. WhatIs.Com. https://whatis.techtarget.com/definition/XSD-XML-Schema-Definition

Sang, K. S., & Zhou, B. (2015). BPMN Security Extensions for Healthcare Process. *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, 2340–2345. https://doi.org/10.1109/CIT/IUCC/DASC/PICOM.2015.346

Simoncini, N. (2017). *Data Protection Officer (DPO)*. European Data Protection Supervisor - European Data Protection Supervisor. https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en

Singh, G., & Supriya. (2013). A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security. *International Journal of Computer Applications*, *67*. https://doi.org/10.5120/11507-7224

Smartsheet. (2019). *The Complete Guide to Gap Analysis*. https://www.smartsheet.com/gap-analysis-method-examples

SuperOffice. (2018). *GDPR: What is It and How Does it Impact My Business?* https://www.superoffice.com/blog/gdpr/

Sweeney, L. (2000). Simple Demographics Often Identify People Uniquely. . . *Pittsburgh*, 34.

SYDLE. (2020). *BPM - Process Automation*. SYDLE. https://www.sydle.com/bpm/?process-automation-platform

Tutorialspoint. (2006). *Eclipse*. https://www.tutorialspoint.com/eclipse/eclipse_overview.htm

Twofish Explained. (1998). http://everything.explained.today/Twofish/

UE. (2016). *Regulamento (UE) 2016/679 Do Parlamento Europeu E Do Conselho*. https://www.cnpd.pt/home/rgpd/CELEX_32016R0679_PT_TXT.html#d1e4683-1-1

Vicente, J. J. (2017). *A segurança da informação*.

Vollmer, N. (2018). Artigo 6 UE Regulamento Geral sobre a Proteção de Dados «- Licitude do tratamento». *PrivazyPlan*. https://www.privacy-regulation.eu/pt/6.htm

W3C. (2008). *Extensible Markup Language (XML)*. https://www.w3.org/TR/xml/

W3C. (2013). *Errata in XSD 1.1*. https://www.w3.org/XML/XMLSchema/v1.1/1e/errata.html

Wang, R. Y., & Strong, D. M. (1996). Beyond Accuracy: What Data Quality Means to Data Consumers. *Journal of Management Information Systems, 12*(4), 5–33.

White, S. A. (2004). *Introduction to BPMN*.