



Anexo I ao Caderno de Encargos

Condições e requisitos funcionais e técnicos

Plataforma Integrada de Gestão de Risco

Índice

1. Introdução.....	5
1.1. Enquadramento	5
1.2. Objetivos do Documento.....	6
1.3. Situação Atual	6
1.3.1. Instituto da Segurança Social (ISS)	6
1.3.2. Instituto de Informática, I.P.	9
1.4. Visão Futura	11
1.4.1. Componente 1 – Estimativa de Índice de risco	15
1.4.2. Componente 2 – Aplicação de Gestão de Risco.....	24
2. Caracterização da Solução	25
2.1. Componente 1 – Estimativa de Índice de Risco.....	25
2.1.1. Visão Geral.....	25
2.1.2. Requisitos gerais	26
2.1.3. Obtenção de dados em várias fontes	27
2.1.4. Tratamento de dados.....	29
2.1.5. Motor de Regras.....	30
2.1.6. Motor de Aprendizagem	31
2.1.7. Motor de Gestão de Risco	33
2.1.8. <i>Dashboard e Reporting</i>	34
2.2. Componente 2 – Aplicação de Gestão de Risco.....	36
2.2.1. Visão Geral.....	36
2.2.2. Requisitos gerais	37
2.2.3. <i>Dashboard e Reporting</i>	38
2.2.4. Análise.....	40
2.2.5. Triagem e distribuição de casos	42
2.2.6. Tratamento de casos	44
2.2.7. Realimentação (para a aprendizagem do <i>Machine Learning</i>)	47
2.3. Interface com o utilizador.....	47
2.4. Integração	49
2.5. Vertentes e requisitos transversais	50
2.5.1. Princípios base	50
2.5.2. <i>Software as a Service (SaaS)</i>	52

2.5.3.	Administração da SOLUÇÃO	54
2.5.4.	Segurança	55
2.5.5.	Cibersegurança	56
2.5.6.	Auditoria	56
2.5.7.	Aplicação do RGPD.....	57
3.	Prestação dos Serviços	59
3.1.	Visão Geral.....	59
3.2.	Requisitos de Implementação.....	62
3.2.1.	Fase I: Conceção	62
3.2.2.	Fase II: Desenvolvimento	64
3.2.3.	Fase III: Exploração.....	74
3.2.4.	Outros requisitos de implementação.....	79
4.	Níveis de desempenho e penalidades	87
4.1.	Níveis de desempenho	87
4.1.1.	Deduções à fatura	88
4.1.2.	Incidentes após as aceitações parcelares	88
4.2.	Penalidades.....	89
5.	Apêndice I – Conceitos e Acrónimos	91
6.	Apêndice II – Dimensionamento	94
7.	Apêndice III – Níveis de Gravidade.....	95
7.1.	Gravidade 1 (emergência)	95
7.2.	Gravidade 2 (problema crítico).....	95
7.3.	Gravidade 3 (problema não crítico).....	95
7.4.	Incidentes de Segurança	Erro! Marcador não definido.

Índice de figuras

Figura 1 – Estrutura do ISS.....	7
Figura 2 – Estrutura organizativa do GAQGR	7
Figura 3 – <i>Outputs</i> gerados pelo modelo	14
Figura 4 – Macro-componentes da Solução.....	15
Figura 5 – Componente 1 – Estimativa de índice de risco	16
Figura 6 – Componente 1 – Estimativa de índice de risco (fluxo inicial)	17
Figura 7 – Componente 1 – Estimativa de índice de risco (fluxo <i>ongoing</i>)	18
Figura 8 – Motor de regras.....	19
Figura 9 – Exemplo do motor de regras	19
Figura 10 – Exemplo de apuramento do valor do fator de risco	20
Figura 11 – Motor de aprendizagem	21
Figura 12 – Motor de gestão de risco.....	22
Figura 13 – Exemplo de cálculo do risco parcial	22
Figura 14 – Exemplo do cálculo do risco global	23
Figura 15 – Exemplo de um <i>dashboard</i> de risco	23
Figura 16 – Componente 2 – Aplicação de Gestão de Risco	24
Figura 17 – Principais componentes da Solução	25
Figura 18 – Diagrama da Componente 1	26
Figura 19 – Diagrama da Componente 2	36
Figura 20 – Âmbito da Solução em modelo <i>On-Prem vs. SaaS</i>	53
Figura 21 - Metodologia da prestação de serviço.....	59
Figura 22 – Abordagem de implementação	61
Figura 23 – Etapas de execução da componente 1	65

Índice de tabelas

Tabela 1 – Descrição dos conceitos	13
Tabela 2 – Manutenção Evolutiva.....	87
Tabela 3 – Níveis de Desempenho.....	87
Tabela 4 – Deduções à fatura.....	88
Tabela 5 – Gestão de incidentes – Tempos de resposta	89
Tabela 6 – Penalidades	90
Tabela 7 – Elementos para dimensionamento	94

1. Introdução

1.1. Enquadramento

O Instituto da Segurança Social (ISS) pretende assegurar direitos básicos dos cidadãos e a igualdade de oportunidades, bem como, promover o bem-estar e a coesão social para todos os cidadãos portugueses ou estrangeiros que exerçam atividade profissional ou residam no território. Sendo os objetivos prioritários do ISS:

- Garantir a concretização do direito à Segurança Social;
- Promover a melhoria sustentada das condições e dos níveis de proteção social e o reforço da respetiva equidade;
- Promover a eficácia do sistema e a eficiência da sua gestão.

A problemática da fraude e os riscos associados ao exercício das diferentes atividades do ISS, tem sido alvo de preocupação nos últimos anos, despoletando projetos e iniciativas para combater estes riscos, com o objetivo específico de identificar as áreas com maior probabilidade de risco de irregularidade e desenvolver instrumentos para o respetivo controlo interno, prevenindo ou detetando a respetiva ocorrência e tornar a ação inspetiva mais eficaz e mais eficiente.

A implementação de mecanismos de avaliação e gestão de riscos permite:

- Aumentar a confiança na prossecução dos objetivos;
- Limitar efetivamente ameaças para níveis aceitáveis;
- Tomar decisões fundamentadas com base na análise de oportunidades.

Numa era de tecnologia digital, existem ferramentas poderosas para combater riscos. A riqueza de dados oferecidos por meio de registos eletrónicos permite que se desenvolvam abordagens mais avançadas para a deteção de inconsistências. O *Machine Learning* e Inteligência Artificial são os métodos mais adequados para este fim devido à quantidade de informações digitais e à facilidade de análise de texto e dados, permitindo que as máquinas processem grandes conjuntos de dados com precisão, algo que de forma manual, além de sujeito a erro, vai demorar muito tempo e exigir muito esforço.

Um sistema de deteção de risco com base em *Machine Learning* baseado em algoritmos com a capacidade de reconhecer padrões e aprender de acordo com o esperado, sugerindo implementar medidas para reduzir o risco, irá garantir que quem comete irregularidades à Segurança Social seja identificado e notificado.

Assim, pretende-se conceber e implementar uma Plataforma Integrada de Gestão de Risco com vista ao combate à evasão e fraude contributiva e prestacional, baseado em tecnologias de *Machine Learning*.

1.2. Objetivos do Documento

O presente anexo, denominado “Condições e requisitos funcionais e técnicos” integra estipulações que regulam a aquisição de serviços para a implementação de uma Plataforma Integrada de Gestão de Risco baseada em *Machine Learning* e Inteligência Artificial (adiante designado por SOLUÇÃO), para suportar a Gestão de Risco da Segurança Social, em linha com as melhores práticas.

A Plataforma Integrada de Gestão de Risco será um elemento fundamental de suporte à gestão, e que tem como objetivo estabelecer um conjunto de práticas de identificação, análise, avaliação, tratamento, revisão, monitorização e reporte dos principais riscos associados às principais linhas de atividade do ISS (nomeadamente no que respeita a contribuições e prestações).

As informações contidas neste documento refletem a situação atual dos sistemas de informação da Segurança Social e os requisitos decorrentes das necessidades de negócio e técnicas.

1.3. Situação Atual

1.3.1. Instituto da Segurança Social (ISS)

O Instituto da Segurança Social (ISS) é um instituto público de regime especial integrado na administração indireta do Estado, dotado de autonomia administrativa e financeira, com personalidade jurídica, património próprio e jurisdição sobre todo o território nacional (sem prejuízo das atribuições e competências das Regiões Autónomas dos Açores e Madeira).

A estrutura orgânica do Instituto compreende os Serviços Centrais, 18 serviços desconcentrados (os Centros Distritais) e o Centro Nacional de Pensões.

Os Serviços Centrais estão organizados em Áreas Operacionais, de Administração Geral e de Apoio Especializado que assumem a natureza de serviços comuns a toda a estrutura do ISS, como apresentado na Figura 1 – Estrutura do ISS.



Figura 1 – Estrutura do ISS

O Setor de Gestão de Risco (SGR) foi criado por Deliberação do Conselho Diretivo n.º 213/2021 de 14.10.2021, no seguimento de uma alteração de organização interna do Gabinete de Auditoria, Qualidade e Gestão de Risco (GAQGR) advinda da necessidade de existir uma equipa dedicada integralmente à Gestão de Risco, reforçando o Sistema de Controlo Interno do ISS.

O GAQGR apresenta a seguinte estrutura organizativa:

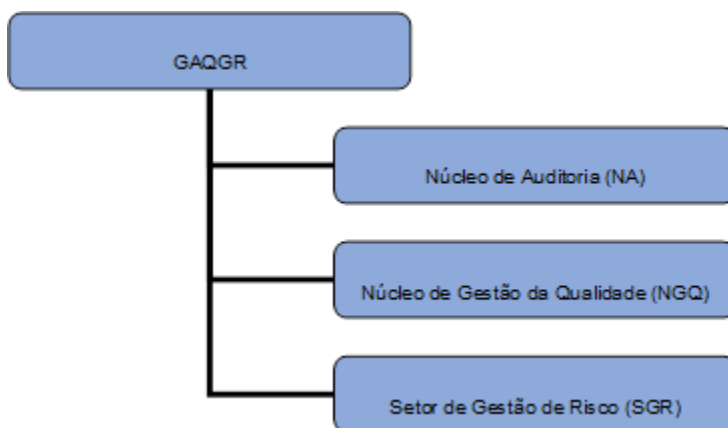


Figura 2 – Estrutura organizativa do GAQGR

O Setor de Gestão de Risco é composto atualmente por 8 elementos, incluindo um Chefe de Setor, e por sete Técnicos Superiores, com habilitações multidisciplinares. Alguns dos elementos da equipa têm igualmente formação e experiência em auditoria.

As funções afetas ao SGR são genericamente:

- a. Acompanhar e controlar os apoios extraordinários de proteção e apoio ao emprego, atribuídos no âmbito da pandemia COVID-19, decorrente da análise de dados e indicadores de risco;
- b. Analisar e avaliar os riscos identificados no Plano de Gestão de Riscos do ISS (PGR);
- c. Analisar, acompanhar e avaliar o risco relativo a universos ou grupos-alvo, no âmbito das competências do ISS;
- d. Analisar, acompanhar e avaliar indicadores de risco no âmbito do controlo interno, em particular no que se refere ao combate à fraude e evasão contributiva e prestacional;
- e. Realizar avaliações de impacto sobre a proteção de dados (AIPD), nos termos do art.º 35.º do RGPD, sempre que se revele necessário em Protocolos a celebrar com o ISS;
- f. Realizar avaliações de impacto de riscos sempre que se revele necessário em Projetos no âmbito das competências do ISS.

Atualmente, as principais atividades realizadas são as seguintes:

- a. Elaboração de estudos de caracterização e avaliação do risco de universos determinados;
- b. Análise e avaliação de risco com base em dados e indicadores;
- c. Construção de suporte para monitorização e acompanhamento de riscos avaliados;
- d. Acompanhamento do Plano de Gestão de Riscos: revisão, monitorização e elaboração de relatórios de acompanhamento;
- e. Consolidação do Processo de Gestão de Risco (Identificação, Análise, Avaliação – matriz de risco aplicada) e Catálogo de Riscos do ISS;
- f. Adequação (sempre que aplicável) e controlo aos normativos aplicáveis em matéria de prevenção de risco no ISS;
- g. Dinamização e preparação das reuniões da Comissão de Gestão de Risco do ISS;
- h. Auditorias (em articulação com o NA/GAQGR);
- i. Avaliações de Impacto na proteção de Dados a Protocolos e Projetos em que o ISS, é responsável pelo tratamento dos dados;
- j. Acompanhamento de Grupos de Trabalhos no ISS (ex.: aplicação do RGPD, Cibersegurança, ...);
- k. Robustecimento do Sistema de Controlo Interno do ISS (SCI).

O SGR desenvolve as suas funções mediante a utilização dos seguintes sistemas de informação e aplicações:

- a. SharePoint – Sistema de Informação da Segurança Social (SISS);
- b. Microsoft Office:
 - a. Word;
 - b. Excel;

- c. PowerPoint;
- d. Power BI.

Atualmente, o GAQGR executa o processo de gestão de risco através de análises manuais, utilizando o Microsoft Excel e Power BI, de modo a produzir relatórios com níveis de risco por NISS para uma amostragem reduzida de casos.

Sempre que existe a necessidade de análises, quer sejam recorrentes ou esporádicas, o GAQGR utiliza dados referentes a diversas áreas de negócio da Segurança Social. Estes dados são solicitados ao Instituto de Informática que realiza extrações através dos sistemas de informação existentes e partilha com o GAQGR.

1.3.2. Instituto de Informática, I.P.

O Instituto de Informática, I. P., doravante abreviadamente designado II, I. P., é um instituto público de regime especial nos termos da lei integrado na administração indireta do Estado, dotado de autonomia administrativa e financeira e património próprio.

O II, I. P., tem por missão definir e propor as políticas e estratégias de tecnologias de informação e comunicação, garantindo o planeamento, conceção, execução e avaliação das iniciativas de informatização e atualização tecnológica do MTSSS.

São atribuições do Instituto de Informática, I.P.:

- a. Elaborar o plano estratégico de sistemas de informação;
- b. Definir e controlar o cumprimento de normas e procedimentos relativos à seleção, aquisição e utilização de infraestruturas tecnológicas e sistemas de informação, enquanto organismo setorial do MTSSS, para as áreas das tecnologias de informação e comunicação;
- c. Assegurar a construção, gestão e operação de sistemas aplicacionais e de infraestruturas tecnológicas nas áreas de tecnologias de informação e comunicação dos serviços e organismos do MTSSS, numa lógica de serviços comuns partilhados;
- d. Promover a unificação e a racionalização de métodos, recursos, processos e infraestruturas tecnológicas nos serviços e organismos do MTSSS, assegurando, designadamente, e nos termos fixados no plano estratégico previsto na alínea a), a aquisição, instalação e funcionamento dos equipamentos informáticos, bem como a sua substituição;
- e. Assegurar a articulação com os organismos com atribuições interministeriais na área das tecnologias de informação e comunicação;
- f. Prestar serviços a departamentos da solidariedade e segurança social, do trabalho e emprego, bem como a outros departamentos da Administração Pública, a empresas públicas ou a entidades privadas, com base em adequados instrumentos contratuais que determinem, designadamente, os níveis de prestação e respetivas contrapartidas.

O II mantém nomeadamente os seguintes sistemas operacionais (com relevância para o projeto em causa):

- a. IDQ – Identificação e Qualificação;
- b. QGEN – Qualificação Genérica;
- c. PS – Pessoa Singular;
- d. PC – Pessoa Coletiva;
- e. GC – Gestão de Contribuições;
- f. GR – Gestão de Remunerações;
- g. SEF – Sistema Execuções Fiscais;
- h. CDF – Consulta de Dados das Finanças;
- i. SAF – Sistema de Apoio à Fiscalização;
- j. CO – Contraordenações;
- k. GIL – Gestão de Ilícitos;
- l. RSI - Rendimento Social de Inserção;
- m. ITPT – Sistema Integrado Conta Corrente;
- n. DES – Desemprego;
- o. ARF – Agregados e Relações Familiares;
- p. Pensões;
- q. COOP – Cooperação;
- r. GUS – Gestão de Utilizadores e Segurança;
- s. Outros a identificar em sede de projeto.

O Departamento de Análise e Gestão de Informação é composto atualmente por 14 elementos, 1 diretor e 13 técnicos.

Atualmente, as principais atividades realizadas pelo departamento são as seguintes:

- a. Desenvolvimento de Sistemas de Disponibilização de Dados e Informação de Apoio à Gestão /Suporte Decisão;
- b. Desenvolvimento e Disponibilização das Estatísticas da SS;
- c. Resposta a pedidos de dados da SS;
- d. Processos de Qualidade de Dados;
- e. Gestão operacional de trocas de dados com sistemas de informação externos à SS.

O Departamento de Análise e Gestão de Informação utiliza no contexto de BI/Suporte à decisão as seguintes ferramentas:

- a. IBM Datastage;
- b. Microstrategy;
- c. Power BI;
- d. SQL/PLSQL;

- e. SGBD Oracle;
- f. VBA.

1.4. Visão Futura

O principal objetivo da aquisição é providenciar o ISS com uma Plataforma Integrada de Gestão do Risco, num modelo de SaaS (Software as a Service), que responda aos requisitos identificados no presente documento e que integre com os sistemas de informação existentes e indispensáveis do universo do ISS.

A Plataforma Integrada de Gestão do Risco será alavancada por uma plataforma tecnológica com a utilização de *Machine Learning* que constituirá uma ferramenta de enorme apoio, contribuindo para uma maior eficiência e eficácia das ações de prevenção, controlo e mitigação do risco, pelas diferentes equipas do ISS.

Pretende-se dar mais um contributo para a sustentabilidade da Segurança Social e consequentemente aumentar a confiança dos cidadãos e empresas. Assim, a Plataforma Integrada de Gestão do Risco da Segurança Social terá por base 3 pilares:

1. **Ação preventiva:** visa a redução da possibilidade de ocorrência de riscos através da implementação de um sistema de gestão e controlo robusto, associado a uma avaliação de risco pró-ativa, estruturada e orientada pelo GAQGR;
2. **Ação educativa:** pretende a simplificação de processos de relacionamento com o cidadão/empresa por forma a clarificar as obrigações e fomentar a comunicação com grupos de risco de modo a forçar o cumprimento das obrigações, através de políticas de sensibilização que promovam o desenvolvimento de uma cultura ética para combater comportamentos indesejados;
3. **Ação reativa:** as equipas de fiscalização através da nova plataforma, que terá a capacidade analítica de deteção de comportamentos fraudulentos através do cruzamento e análise de dados, serão capazes de decidir onde terão de atuar primeiro, garantido o aumento da eficácia das ações de fiscalização.

Neste capítulo apresenta-se a visão futura pretendida para a Plataforma Integrada de Gestão do Risco.

Pretende-se que a nova Plataforma Integrada de Gestão do Risco determine o risco em três áreas de análise distintas:

- **Contribuintes** – pessoa singular ou coletiva sobre a qual recai a obrigação de contribuir para os regimes da Segurança Social, designadamente as pessoas singulares que exercem atividade profissional subordinada, as respetivas entidades empregadoras e os trabalhadores independentes. Esta área, neste projeto, divide-se em:
 - Entidades Empregadoras;

- Trabalhadores Independentes;
- Serviço Doméstico;
- IPSS - Instituições Particulares de Solidariedade Social (Desenvolvimento Social)
- **Beneficiários** – pessoa inscrita como titular do direito a proteção social no âmbito dos Regimes da Segurança Social, contributivos e não contributivo. Esta área, neste projeto, divide-se em:
 - Remunerações;
 - Contribuições;
 - Prestações:
 - Desemprego;
 - RSI;
 - Doença.
 - Pensões:
 - Velhice;
 - Sobrevivência;
 - Invalidez.
- **Fraude interna** – Situação de irregularidade ou fraude realizada por trabalhadores da Segurança Social.

Para entendimento da visão futura do modelo de gestão de risco concetualizado apresenta-se em seguida os conceitos subjacentes (Tabela 1 – Descrição dos conceitos).

Conceito	Descrição	Exemplo
Variáveis	Uma propriedade de um NISS que pode ser quantificada ou enumerada, e podem ser simples ou compostas	NISS; morada; nº trabalhadores; volume de contribuições
Indicadores	Conjunto de variáveis combinados numa forma de cálculo que pretendem representar uma realidade de forma quantitativa	Valor anormal de nº de trabalhadores face ao volume de contribuições; Valor médio de contribuições dos últimos 6 meses
Peso do indicador	Peso do indicador, em percentagem, para o fator de risco	%, sendo que o total para o fator de risco deverá ser de 100%
Fatores de risco	Situação de risco potencial composta por determinadas circunstâncias reais de um NISS	Aumento expressivo da remuneração, temporalmente próximos de afetar a atribuição de pensões ou prestações

Matriz de risco	Ferramenta de gestão de risco que permite classificar o nível de risco, combinando o fator de probabilidade de ocorrência e o impacto de determinada situação / fator de risco	<table><tr><th rowspan="2">Prob Ocorrência</th><th colspan="3">Impacto (Dimensão empresa)</th></tr><tr><th>Pequena</th><th>Media</th><th>Grande</th></tr><tr><td>76-100</td><td>2,5</td><td>3</td><td>4</td></tr><tr><td>51-75</td><td>2</td><td>2,5</td><td>3,5</td></tr><tr><td>26-50</td><td>1,5</td><td>2</td><td>2,5</td></tr><tr><td>0-25</td><td>1</td><td>1,5</td><td>2</td></tr></table>	Prob Ocorrência	Impacto (Dimensão empresa)			Pequena	Media	Grande	76-100	2,5	3	4	51-75	2	2,5	3,5	26-50	1,5	2	2,5	0-25	1	1,5	2
Prob Ocorrência	Impacto (Dimensão empresa)																								
	Pequena	Media	Grande																						
76-100	2,5	3	4																						
51-75	2	2,5	3,5																						
26-50	1,5	2	2,5																						
0-25	1	1,5	2																						
Risco parcial	Nível de risco associado a um fator de risco, obtido através da matriz de risco	Nível de risco parcial de 0 a 4																							
Peso do risco parcial	Peso em que cada risco parcial contribui para o risco global	%, sendo que o total dos riscos parciais deverá ser de 100%																							
Risco global	Risco global de um NISS composto pelos diversos riscos parciais de um NISS	Nível de risco global de 0 a 4 (tendo associado um número em % resultante do cálculo do peso de cada risco parcial)																							
Medidas de mitigação	Intervenções, automáticas ou manuais, com vista a prevenir, reduzir ou controlar a causa dos riscos	Enviar e-mail de alerta																							

Tabela 1 – Descrição dos conceitos

Atualmente existe um documento preliminar, elaborado pelo IIS e pelo II, I.P., que contempla uma extensa lista de indicadores e respetivos fatores de risco (cfr. infra R.C1.2.). Este documento será entregue à EMPRESA PRESTADORA aquando da celebração do auto de consignação.

No entanto, no Anexo II - Dimensionamento estão contemplados os elementos para compreensão em termos de dimensionamento.

Está previsto que a Plataforma Integrada de Gestão de Risco tenha como principal resultado a estimativa do risco por cada NISS em análise. Assim, na Figura 3 – *Outputs* gerados pelo modelo, estão representados os principais outputs resultantes do modelo:

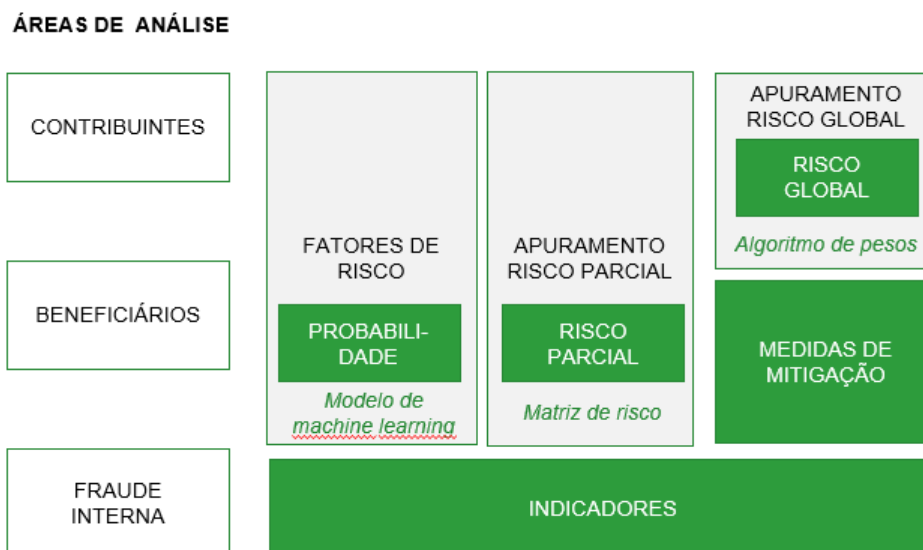


Figura 3 – Outputs gerados pelo modelo

Assim pretende-se que a Plataforma Integrada de Gestão de Risco produza periodicamente:

- Probabilidade de ocorrência de cada fator de risco;
- Risco parcial para cada fator de risco (cruzamento da probabilidade de ocorrência com uma matriz de impacto definida para cada fator de risco);
- Risco global por NISS (calculado consoante o peso definido de cada fator de risco parcial – face ao peso definido para o mesmo);
- Medidas de mitigação para cada risco parcial (definido por cada fator de risco e/ou nível de risco associado);
- Indicadores associados (indicadores pré-definidos que pretendem caracterizar o NISS);
- Outros indicadores considerados relevantes para monitorização da eficácia da Plataforma Integrada de Gestão de Risco.

Em termos conceptuais prevê-se que a Plataforma Integrada de Gestão do Risco (também designada por Solução) seja implementada de forma repartida por duas componentes que se complementam, que serão detalhadas nos capítulos abaixo respetivamente:

- Componente 1 – Permite a estimativa de índice de risco de cada NISS, através de um modelo assente em motores de regras e *Machine Learning*
- Componente 2 – Aplicação de Gestão de Risco - Permite a análise, tratamento e monitorização das situações de risco.

A Figura 4 – Macro-componentes da Solução, apresenta as duas componentes da Solução. A Componente 1 gera os *outputs* que serão utilizados como *input* para a gestão de risco realizada na Componente 2.

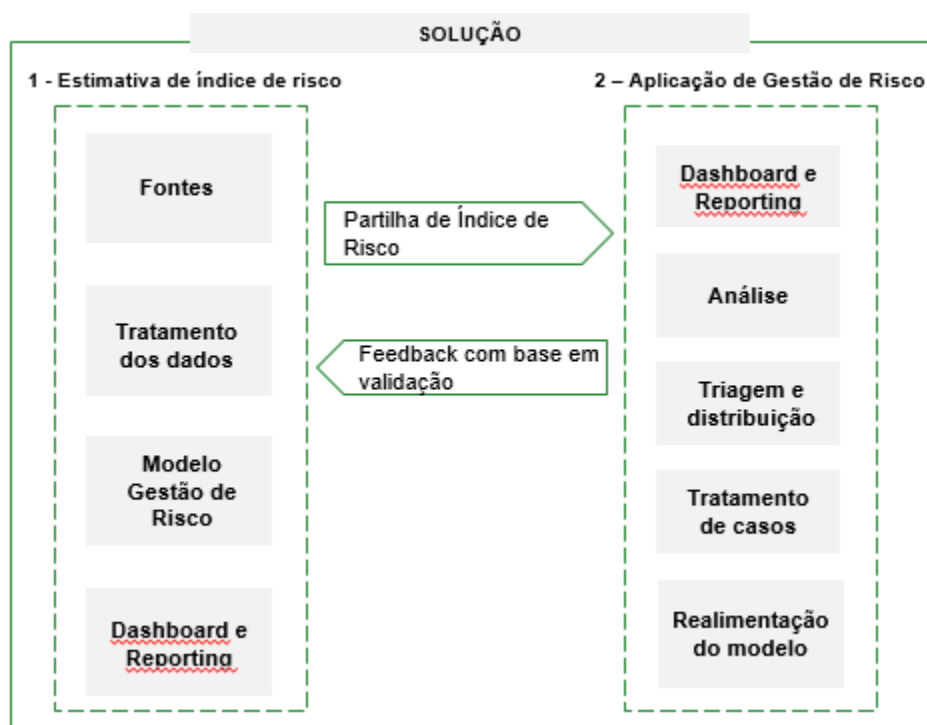


Figura 4 – Macro-componentes da Solução

1.4.1. Componente 1 – Estimativa de índice de risco

A Componente 1 – Estimativa de Índice de Risco é responsável pelo ciclo de vida dos dados desde a extração até à produção de índice de risco, conforme representado na Figura 5 – Componente 1 – Estimativa de índice de risco.

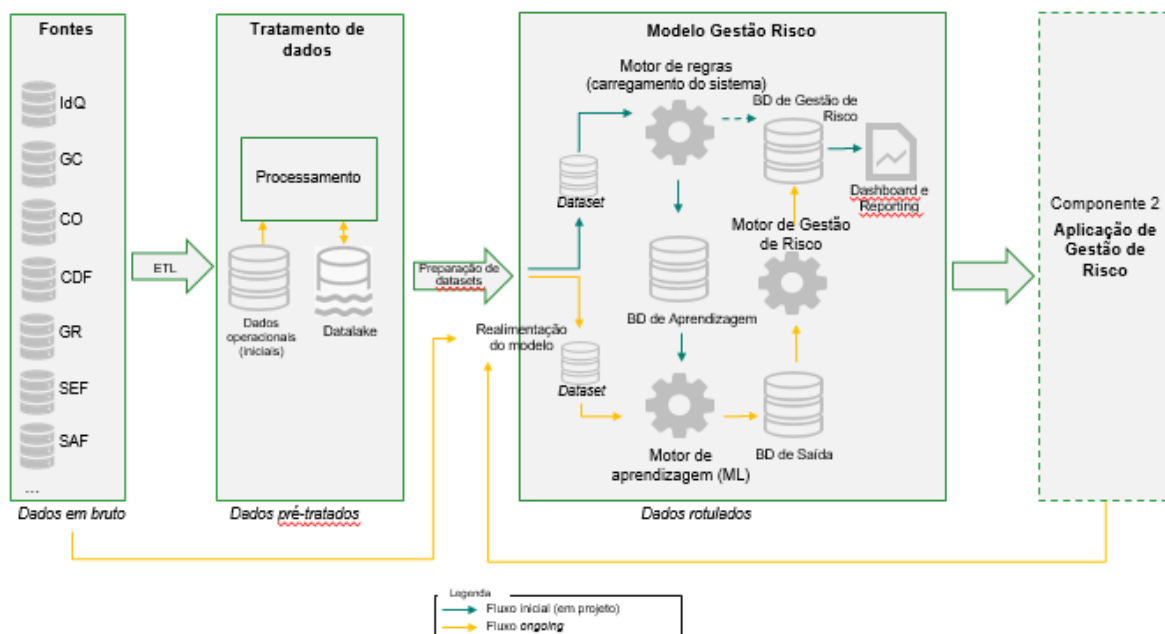


Figura 5 – Componente 1 – Estimativa de índice de risco

A Figura 6 – Componente 1 – Estimativa de índice de risco (fluxo inicial) e a Figura 7 – Componente 1 – Estimativa de índice de risco (fluxo ongoing) apresentam, respetivamente, o fluxo inicial e o fluxo *ongoing* para a Estimativa do índice de risco da Componente 1.

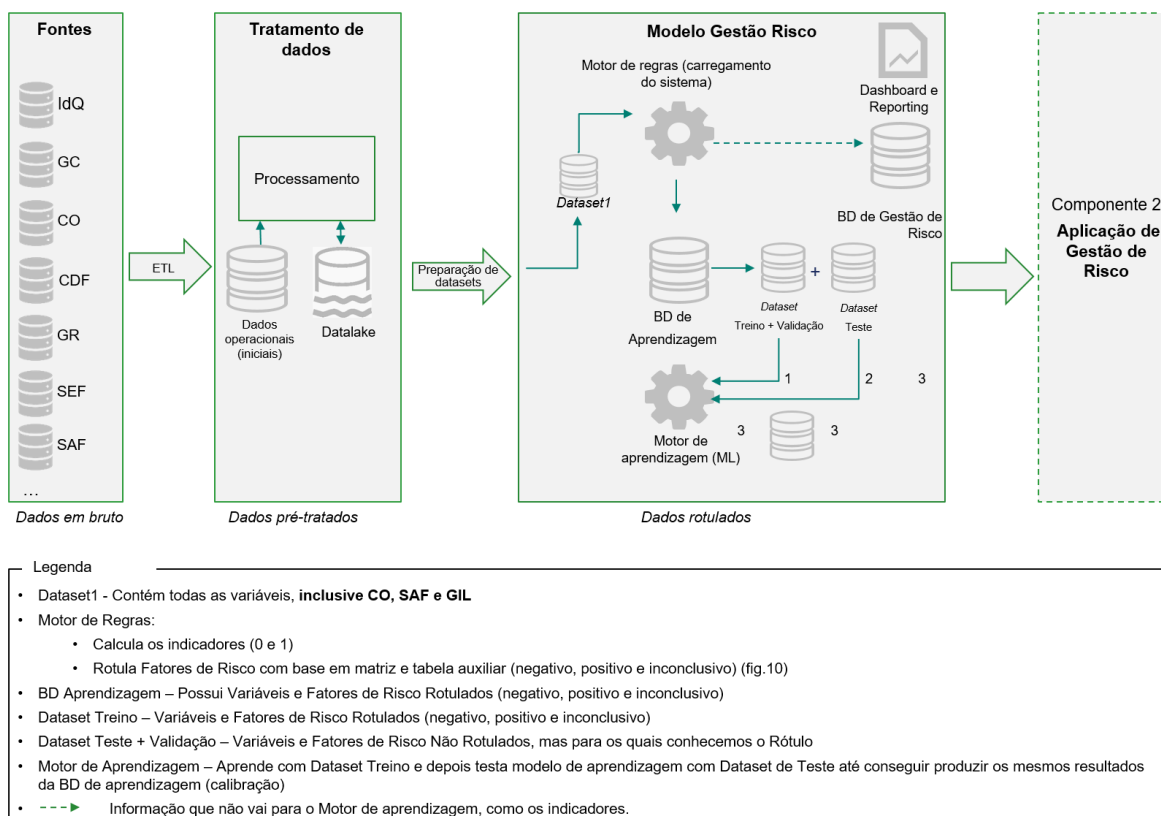
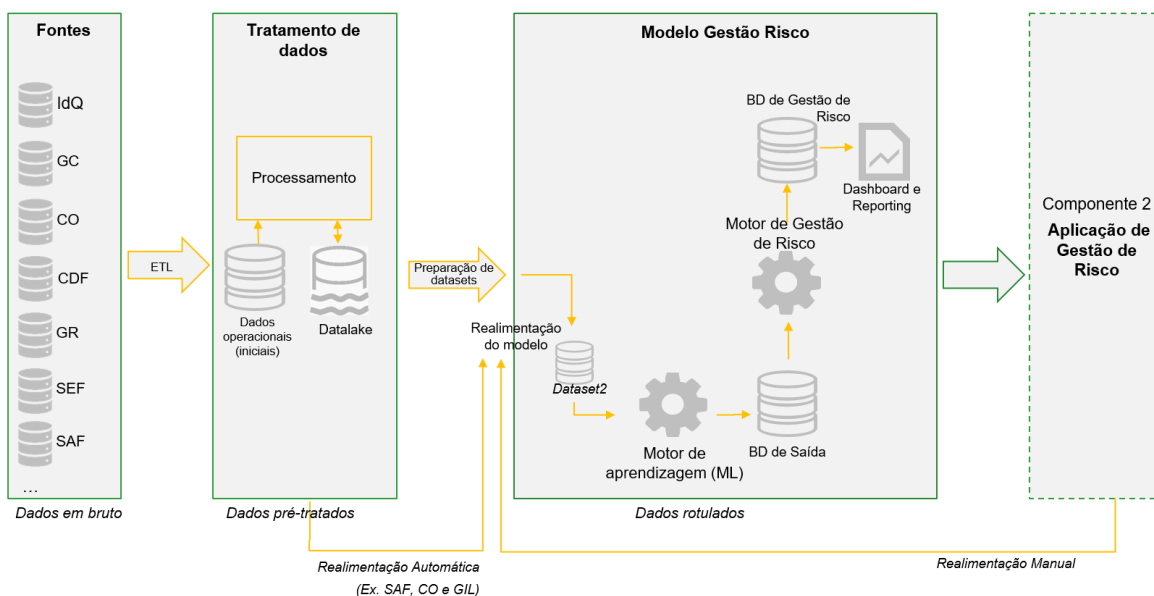
DIAGRAMA COMPONENTE 1 – ATÉ CALIBRAÇÃO DO MODELO DE APRENDIZAGEM**Figura 6 – Componente 1 – Estimativa de índice de risco (fluxo inicial)**

DIAGRAMA COMPONENTE 1 - ONGOING

Dataset2 - Contém todas as variáveis, inclusive CO, SAF e GIL num segundo (ou posterior) momento de execução do processo

Motor de Aprendizagem - recebe periodicamente "novas" variáveis e calcula as probabilidades de ocorrência dos Fatores de Risco

BD de Saída - Possui variáveis e a probabilidade de ocorrência de cada Fatores de Risco, para cada NISS

Motor de Gestão de Risco - Aplica as matrizes de risco (probabilidade/impacto) e os pesos aos dados da BD de saída e calcula, os riscos parciais para cada Fator de Risco e o Risco Global por NISS

BD de Risco - Contém Matrizes de Risco, Pesos, Variáveis, (para efeitos de rastreabilidade, Risco Parcial para cada Fator de Risco e Risco Global por NISS

Figura 7 – Componente 1 – Estimativa de índice de risco (fluxo ongoing)

Esta componente deverá incluir:

- Toda a vertente de captura dos dados fonte, processo de ETL e tratamento dos dados (incluindo o processamento) para carregamento das variáveis que irão alimentar toda a Plataforma Integrada de Gestão do Risco
- Uma vertente do modelo de gestão de risco que inclui três motores:
 1. Motor de regras;
 2. Motor de aprendizagem;
 3. Motor de gestão de risco.

1.4.1.1. Tratamento dos dados

Será necessário, como primeiro momento, de forma à Componente 1 obter dados limpos para o seguimento da implementação dos motores, manter uma réplica de parte dos dados das fontes na base de dados operacional (Dados operacionais), incluindo o tratamento decorrente da aplicação do ETL.

A preparação dos *datasets* será sobre os dados pré tratados, de forma a produzir variáveis e construir os *datasets* adequados aos motores.

1.4.1.2. Motor de Regras

Na Componente 1, propõe-se implementar um motor de regras que irá posteriormente alimentar o motor de aprendizagem. A principal razão de existência deste motor é trabalhar e calcular dados rotulados para posterior aprendizagem do motor de aprendizagem.

O motor de regras é um motor sobretudo de suporte assente em regras e conhecimento recolhido de situações problemáticas que permitirá aferir a informação relevante para aprendizagem (variáveis, indicadores e verificação de um fator de risco).

Este motor irá, com base nas variáveis já carregadas dos sistemas operacionais, processadas e carregadas no *Dataset*, calcular indicadores associados a cada fator de risco (pré-definidos e parametrizados). Os indicadores mostram ocorrência ou a não ocorrência de determinadas situações (tendo como resultados 0 ou 1). Após o cálculo dos indicadores, este motor deverá calcular o valor de cada fator de risco (Negativo, Positivo ou Inconclusivo). Este cálculo será efetuado com base em regras pré-definidas, ver Figura 8 – Motor de regras.



Figura 8 – Motor de regras

A Figura 9 – Exemplo do motor de regras apresenta uma ilustração prática das relações identificadas entre as variáveis, indicadores e fator de risco.

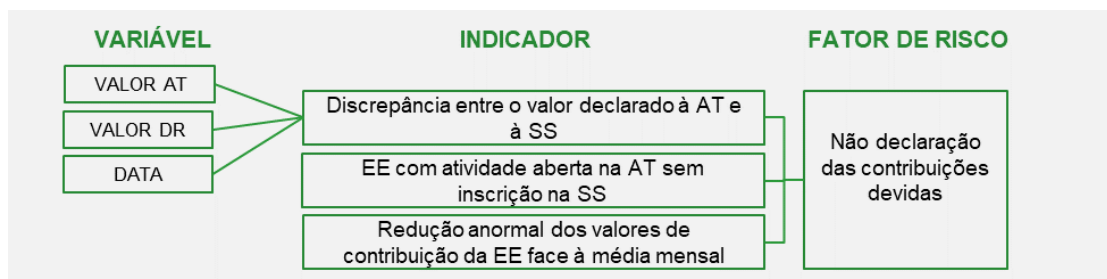


Figura 9 – Exemplo do motor de regras

Considerando o exemplo acima ilustra-se abaixo (Figura 10 – Exemplo de apuramento do valor do fator de risco) o processo de apuramento do valor do fator de risco:

Tabela auxiliar rotulagem de fatores de risco

Indicador	Valor	Peso do Indicador(%)	Valor do fator de risco 1	Rótulo/ <u>Label</u>
Indicador A	1	15%	75%	1
Indicador B	0	30%		
Indicador C	1	30%		
Indicador B	1	30%		

% Fator Risco	Rótulo/ <u>Label</u>
Entre 0% e 30%	0
Entre 31% e 69%	Inconclusivo
Entre 70% e 100%	1

Figura 10 – Exemplo de apuramento do valor do fator de risco

De notar que todo motor de regras deve ser parametrizável, em particular no que refere à associação de indicadores a fatores de risco e a tabela auxiliar de rotulagem de fatores de risco.

1.4.1.3. Motor de Aprendizagem

O motor de aprendizagem (*Machine Learning*) é um motor que irá calcular a probabilidade de ocorrência de um fator de risco por NISS, com base num conjunto de dados com os quais irá realizar a aprendizagem. Esta aprendizagem é feita, num primeiro momento, através do *output* do motor de regras.

O motor de aprendizagem será dividido em dois momentos, conforme apresentado na Figura 11 – Motor de aprendizagem:

1. **Momento de aprendizagem:** o motor de aprendizagem vai aprender com o *output* do motor de regras num primeiro momento e com dados provenientes da realimentação do modelo (definido em 2.2.7 Realimentação (para a aprendizagem do *Machine Learning*)), e também com um conjunto prévio de dados rotulados provenientes de alguns sistemas, nomeadamente, SAF, CO e GIL;
2. **Aplicação do modelo de aprendizagem a dados não rotulados:** para calcular, periodicamente, a probabilidade de ocorrência de cada fator de risco associado a cada NISS.

No primeiro momento, decorrerá a aprendizagem do modelo de *Machine Learning*, e o motor utilizará os seguintes dados:

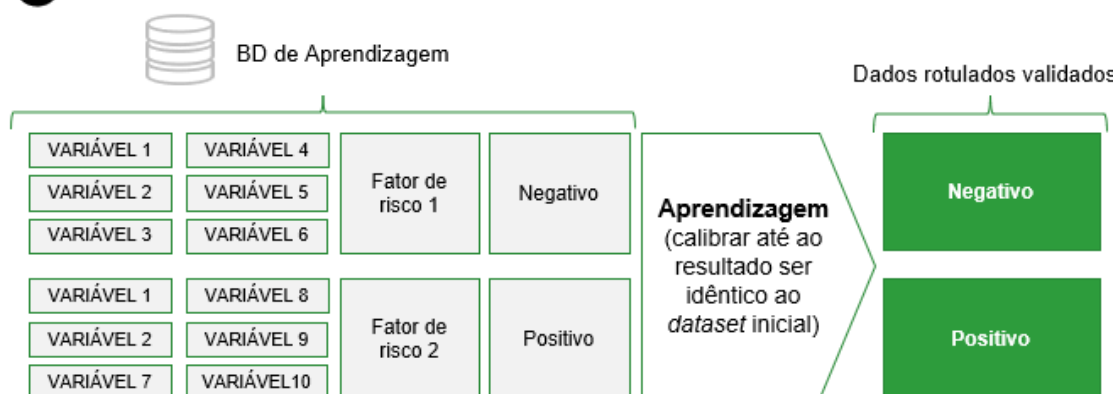
- Variáveis;
- Fatores de risco;
- Rotulagem dos fatores de risco (Positivo; Negativo; Inconclusivo).

O motor de regras rotula a existência de um fator de risco, produzindo o rótulo/*label* do modelo de ML. Nesta fase, o modelo terá de ser testado e calibrado até produzir “os mesmos” resultados do *Dataset* de aprendizagem.

No segundo momento, será aplicado o modelo treinado a um novo *Dataset*, sem dados rotulados, por forma a que produza esses rótulos/*labels*, isto é, a probabilidade de um fator de risco ser negativo ou positivo.

O modelo correrá sobre esse *Dataset* e calculará a probabilidade de ocorrência de cada fator de risco de cada NISS, representado na Figura 11 – Motor de aprendizagem.

1 MOMENTO DE APRENDIZAGEM



2 APLICAR O MOTOR DE APRENDIZAGEM (ML) A DADOS NÃO ROTULADOS

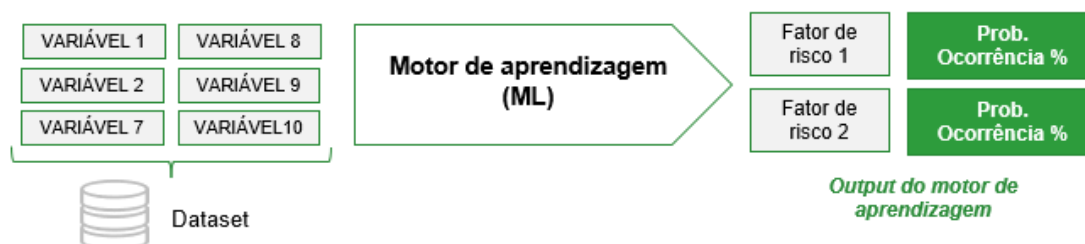


Figura 11 – Motor de aprendizagem

O *output* deste motor, as probabilidades de ocorrência, serão carregados na BD de Saída, tal como as variáveis e os fatores de risco utilizados no motor de aprendizagem. A BD de saída será utilizada no Motor de Gestão de risco.

1.4.1.4. Motor de Gestão de risco

O motor de gestão de risco tem como principal objetivo obter os riscos parciais e global de cada NISS de modo a perceber quais os NISS que necessitam de maior intervenção por parte das equipas do ISS.

Este motor utilizará como *inputs* os vários *outputs* do motor de aprendizagem (variáveis, fatores de risco e probabilidades de ocorrência) e parametrizações necessárias para o seu funcionamento (matrizes de risco e pesos), como se pode observar na Figura 12 – Motor de gestão de risco.

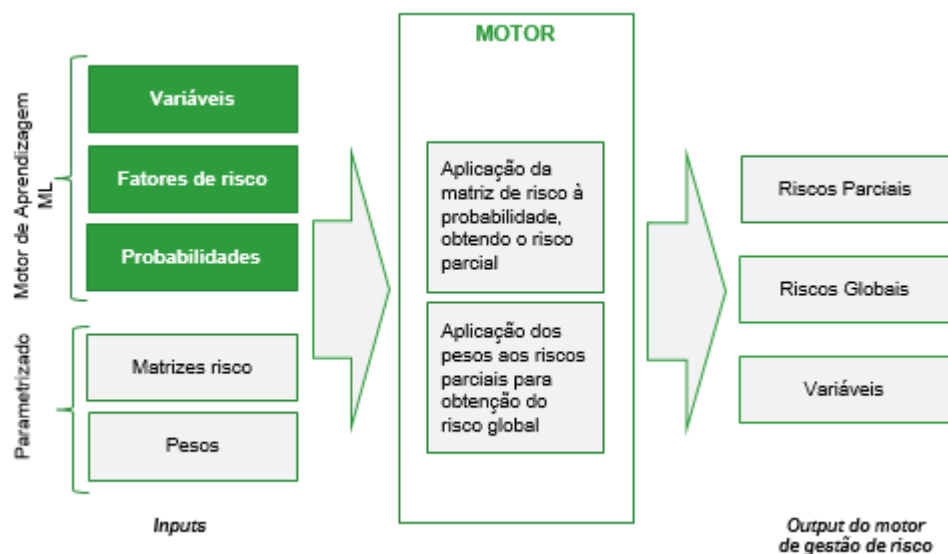


Figura 12 – Motor de gestão de risco

Como *outputs*, o motor de gestão de risco apresentará:

- O risco parcial para cada fator de risco;
- O risco global por NISS;
- As variáveis associadas a cada indicador.

O motor de gestão de risco terá como primeiro passo, a produção do risco parcial, conforme exemplificado na Figura 13 – Exemplo de cálculo do risco parcial, através da aplicação da matriz de risco com duas dimensões, a probabilidade de ocorrência de um fator de risco obtida através do motor de aprendizagem, combinada com o impacto associado.

Importa referir que existirão múltiplas matrizes de risco a serem utilizadas pois o impacto para a SS pode ser calculado de forma distinta consoante a área de análise ou mesmo o fator de risco.

Obtenção do Risco Parcial

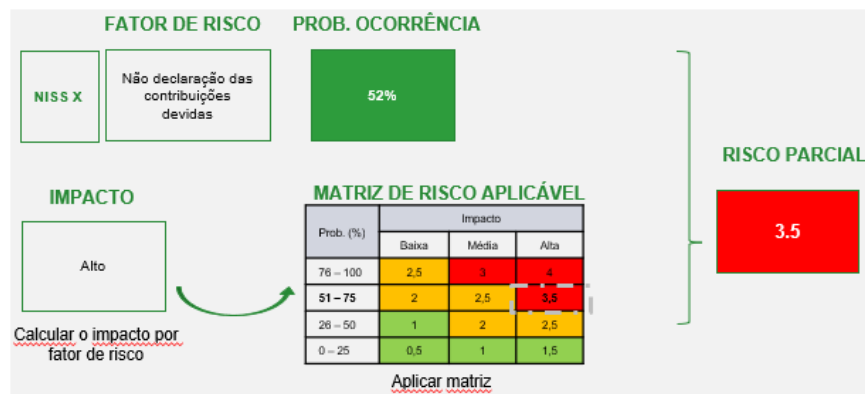


Figura 13 – Exemplo de cálculo do risco parcial

O risco global de cada NISS é calculado tendo em conta os pesos definidos para os riscos parciais dos fatores de risco, como se pode observar na Figura 14 – Exemplo do cálculo do risco global.

	FATORES DE RISCO	Probabilidade	Impacto	Risco Parcial	Peso	Risco global
NISS CONTRIBUINTE	Não declaração das contribuições devidas	52%	alto	3,5	40%	3,05
	Legalização indevida de cidadãos estrangeiros	28%	alto	2,5	15%	
	Não regularização de dívidas	60%	alto	3,5	30%	
	Convivência com trabalhadores para pagamentos indevidos de prestações (ex: pescas, turismo)	10%	alto	1,5	15%	
NISS BENEFICIÁRIO	Obtenção indevida de prestações	10%	medio	1,5	20%	1,5
	Aumento da remuneração para efeitos de pensões ou prestações	50%	medio	2	40%	
	Não contemplar outras pensões CGA	0%	medio	0	20%	
	Não contemplar pensões ou prestações auferidas no estrangeiro	0%	medio	0	20%	

Figura 14 – Exemplo do cálculo do risco global

Os resultados obtidos por este motor deverão ser disponibilizados para *reporting* (ver 2.2- Componente 2) que permite, entre outras visualizações, uma visão agregada de um NISS como se pode ver na Figura 15 – Exemplo de um *dashboard* de risco.

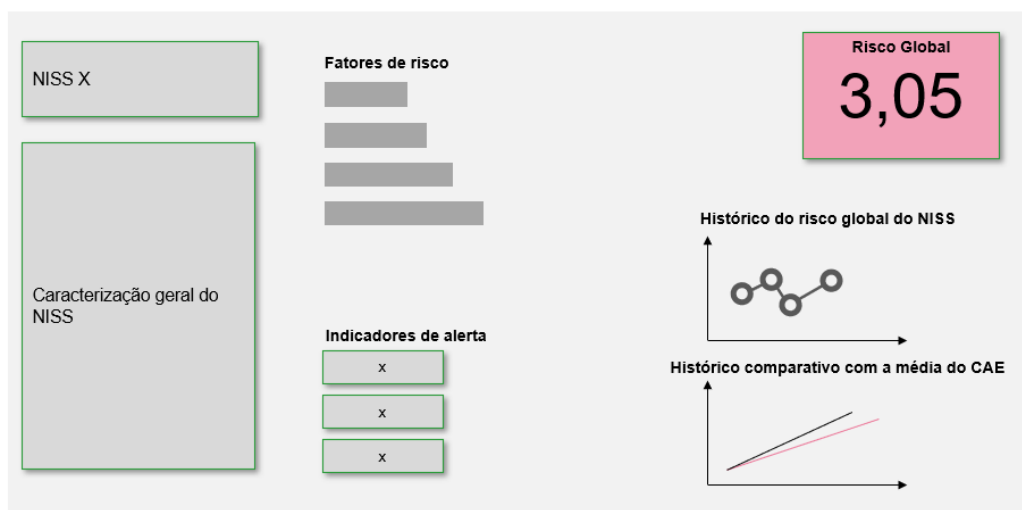


Figura 15 – Exemplo de um *dashboard* de risco

1.4.2. Componente 2 – Aplicação de Gestão de Risco

A componente2, a saber, Aplicação de Gestão de Risco, receberá os índices de risco da Componente 1, que analisará e tratará de forma adequada para cada situação por risco apresentada.

A Aplicação de Gestão de Risco, apresentada na Figura 16 – Componente 2 – Aplicação de Gestão de Risco, deverá incluir o seguinte:

1. Análise / validação inicial dos índices de risco estimados pela Componente 1;
2. Todo o ciclo de tratamento, validação, triagem e distribuição de casos, pelas áreas operacionais das situações de risco;
3. Tratamentos automáticos (com medidas de mitigação) para situações de risco;
4. Gestão das medidas de mitigação;
5. Realimentação do modelo (Componente 1);

A componente, que deverá assentar em ferramentas de *Case Management / Risk Management*, terá ainda de incluir uma vertente de monitorização de resultados de toda a Gestão de Risco.

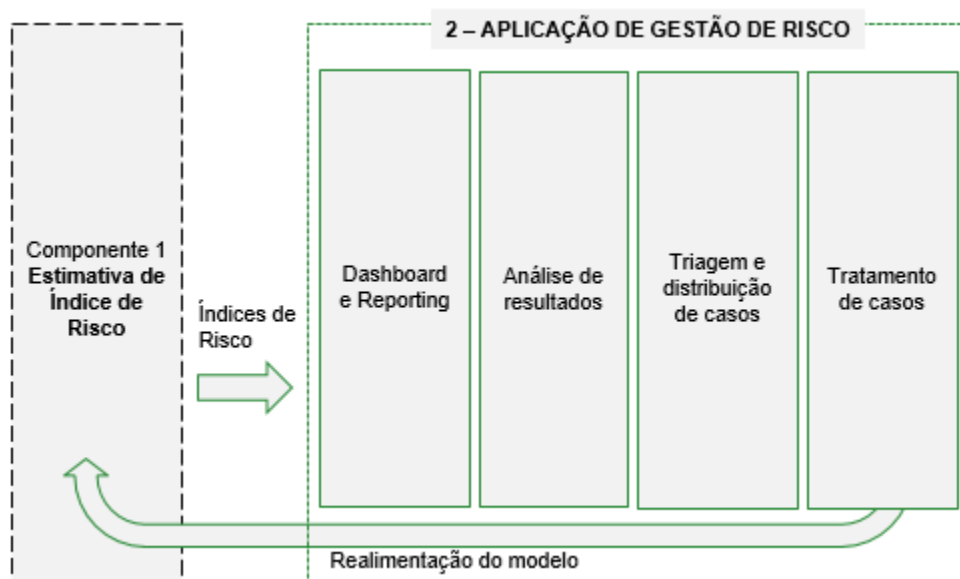


Figura 16 – Componente 2 – Aplicação de Gestão de Risco

2. Caracterização da Solução

A Figura 17 – Principais componentes da Solução apresenta, de forma ilustrativa, a arquitetura de referência (muito alto nível) para a SOLUÇÃO que visa concretizar a “Visão Futura” apresentada anteriormente.

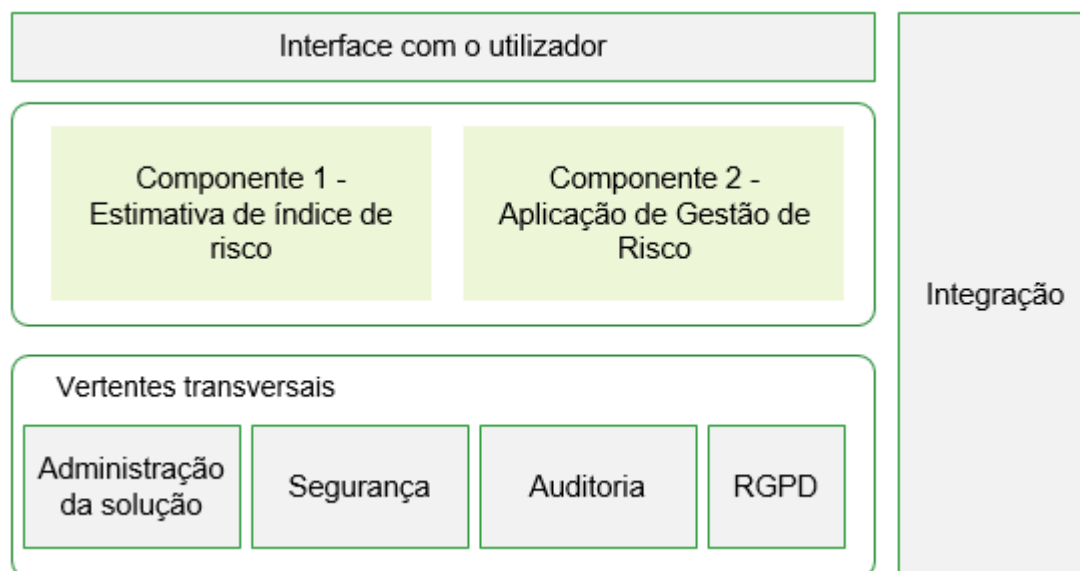


Figura 17 – Principais componentes da Solução

A Solução será disponibilizada em modelo de SaaS (Software as a Service), no âmbito e condições descritas abaixo em “Vertentes e requisitos transversais”.

Tendo em conta esta arquitetura orientadora, neste capítulo apresentam-se os requisitos para a Solução, seguindo cada uma das componentes de referência e iniciando-se desde logo pelas componentes mais relevantes: Componente 1 – Estimativa de índice de Risco e Componente 2 – Aplicação de Gestão de Risco.

2.1. Componente 1 – Estimativa de Índice de Risco

2.1.1. Visão Geral

A Figura 18 – Diagrama da Componente 1 descreve a arquitetura prevista para esta componente.

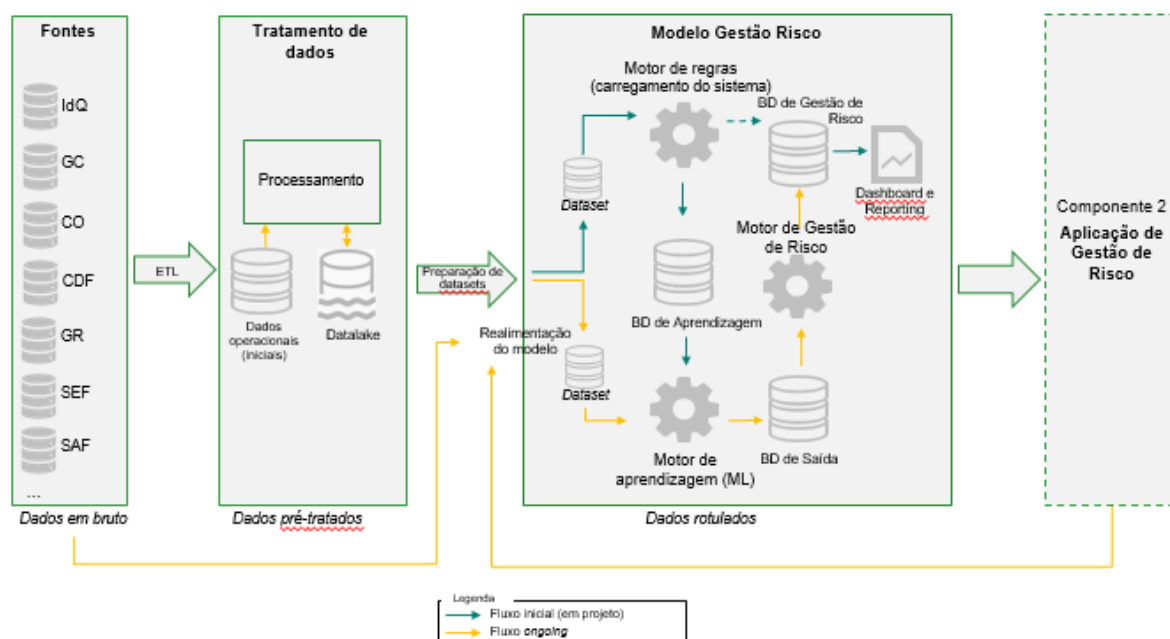


Figura 18 – Diagrama da Componente 1

2.1.2. Requisitos gerais

- R.C1.1. A Componente 1 deverá ser desenhada em detalhe e implementada em sede de projeto pela EMPRESA PRESTADORA, tendo em conta as componentes identificadas na Figura 18 – Diagrama da Componente 1 e os requisitos apresentados de seguida.
- R.C1.2. O CONTRAENTE PÚBLICO elaborou um documento preliminar, que contempla uma extensa lista de:
- Indicadores;
 - Fatores de risco.
- Este documento constituirá uma referência para o desenho e implementação da Solução pela EMPRESA PRESTADORA e será entregue à EMPRESA PRESTADORA aquando da celebração do auto de consignação.
- R.C1.3. O documento poderá sofrer alterações mesmo em sede de implementação, devido a contributos, quer do CONTRAENTE PÚBLICO, quer da EMPRESA PRESTADORA.
- R.C1.4. A Componente 1 deverá ser configurável / parametrizável em diversos aspetos conforme desenho em sede de projeto, e contemplando desde logo o seguinte:
- Configuração do motor de regras;
 - Configuração do motor de aprendizagem;
 - Configuração do motor de gestão de risco;
 - Outros a identificar em sede de projeto.

- R.C1.5. A Componente 1 não deverá ser estática, devendo permitir, para além do que venha a ser definido em sede de projeto, a criação de:
- a. Novas variáveis;
 - b. Novos indicadores;
 - c. Novos fatores de risco;
 - d. Novas regras do motor de regras;
 - e. Outros a identificar em sede de projeto.
- R.C1.6. A Componente 1 deverá utilizar a tecnologia de bases de dados do CONTRAENTE PÚBLICO, a saber, o Oracle SGBD na componente *on-prem* da Solução.

2.1.3. Obtenção de dados em várias fontes

- R.C1.7. Cabe à EMPRESA PRESTADORA, durante a execução do contrato, realizar todas as atividades necessárias para a obtenção dos dados de que a Componente 1 irá necessitar, por forma a alcançar os objetivos definidos no que respeita à estimativa do índice de risco.
- R.C1.8. No contexto do requisito anterior, o CONTRAENTE PÚBLICO fará a passagem de conhecimento e documentação sobre os vários sistemas fontes e sobre os respetivos modelos de dados, por forma a que a EMPRESA PRESTADORA possa ter maior agilidade na prestação dos serviços.
- R.C1.9. A EMPRESA PRESTADORA deverá analisar as diversas fontes de dados, os condicionalismos dos respetivos sistemas de informação (ao nível de desempenho, segurança, entre outros) e identificar os dados a extrair.
- R.C1.10. A EMPRESA PRESTADORA deverá identificar e desenvolver todas as atividades necessárias, incluindo desde logo:
- a. Identificação de dados (fonte) necessários (ou disponíveis);
 - b. Desenho de modelos de dados alvo (quando aplicável);
 - c. Mapeamento de campos / tabelas (quando aplicável);
 - d. Identificação de tratamento inicial aos dados;
 - e. Desenho de processos de extração, transformação e carregamento dos dados;
 - f. Documentação;
 - g. Instalação / configuração de componentes tecnológicas;
 - h. Testes;
 - i. Preparação de ambientes de desenvolvimento, qualidade e produção;
 - j. Quaisquer outros que sejam necessários.
- R.C1.11. A EMPRESA PRESTADORA deverá utilizar a ferramenta de ETL utilizada pelo CONTRAENTE PÚBLICO que é o IBM DataStage, na componente *on-prem* da SOLUÇÃO.

- R.C1.12. A extração de dados tem de ser planeada e acordada entre as partes, para que não haja perturbação do normal funcionamento dos sistemas fonte.
- R.C1.13. A Componente 1 deverá incluir a extração de dados residentes em diversos sistemas de informação internos ao ISS e dados provenientes de protocolos existentes com outras entidades.
- R.C1.14. No contexto do requisito anterior, a Componente 1 deverá incluir a extração de diversas fontes de dados estruturados dos sistemas de informação atuais:
- a. IDQ – Identificação e Qualificação;
 - b. QGEN – Qualificação Genérica;
 - c. PS – Pessoa Singular;
 - d. PC – Pessoa Coletiva;
 - e. GC – Gestão de Contribuições;
 - f. GR – Gestão de Remunerações;
 - g. SEF – Sistema Execuções Fiscais;
 - h. CDF – Consulta de Dados das Finanças;
 - i. SAF – Sistema de Apoio à Fiscalização;
 - j. CO – Contraordenações;
 - k. GIL – Gestão de Ilícitos;
 - l. RSI – Rendimento Social de Inserção;
 - m. ITPT – Sistema Integrado Conta Corrente;
 - n. DES – Desemprego;
 - o. ARF – Agregados e Relações Familiares;
 - p. Pensões;
 - q. COOP – Cooperação;
 - r. GUS – Gestão de Utilizadores e Segurança;
 - s. Outros a identificar em sede de projeto.
- R.C1.15. A Componente 1 deverá permitir a incorporação de novas fontes de dados que possam existir no futuro.
- R.C1.16. A Componente 1 deverá contemplar a configuração da data/hora e a periodicidade de atualização dos dados.
- R.C1.17. A Componente 1 deverá possibilitar o carregamento dos dados fonte para uma base de dados que poderá conter réplicas parciais dos sistemas fonte (Dados operacionais) conforme a Figura 18 – Diagrama da Componente 1. Cabe à EMPRESA PRESTADORA a preparação desta base de dados.

2.1.4. Tratamento de dados

- R.C1.18. Conforme descrito na secção anterior, a Componente 1 deverá manter uma réplica de parte dos dados fonte na base de dados operacional (Dados operacionais), incluindo já algum tratamento decorrente da aplicação do ETL.
- R.C1.19. A Componente 1 deverá permitir que os dados fonte carregados na base de dados operacional sejam tratados por uma componente de processamento conforme previsto na arquitetura da Figura 16 – Componente 2 – Aplicação de Gestão de Risco.
- R.C1.20. O processamento identificado na Figura 18 – Diagrama da Componente 1 deverá preparar os dados operacionais e proceder a cálculos de variáveis necessárias nos motores que constituem a Componente 2. Neste contexto, cabe à EMPRESA PRESTADORA identificar, desenhar, implementar e testar todos os processos / mecanismos técnicos para tratamento de dados, cálculos ou outros necessários.
- R.C1.21. A EMPRESA PRESTADORA em colaboração com o CONTRAENTE PÚBLICO irá identificar as variáveis a produzir que serão utilizadas pelos vários modelos / motores, tendo por base o documento já referido (em R.C1.2).
- R.C1.22. O processamento deverá assim permitir operações sobre os dados através de:
- a. Normalização dos dados;
 - b. Cálculos relativos a históricos;
 - c. Cálculos de variações;
 - d. Cálculos auxiliares / adicionais que facilitem a análise em fases seguintes;
 - e. Cálculo das variáveis que vão suportar os motores.
- R.C1.23. A Componente 1 deverá permitir incluir num *Datalake*, os dados operacionais processados conforme previsto na arquitetura da Figura 18 – Diagrama da Componente 1.
- R.C1.24. A EMPRESA PRESTADORA deverá planear e realizar todas as atividades de preparação do *Datalake*, incluindo nomeadamente:
- a. Identificação de dados (fonte) já existentes na BD com dados operacionais (iniciais);
 - b. Desenho de modelos de dados;
 - c. Mapeamento de campos / tabelas (quando aplicável);
 - d. Articulação com a componente de processamento dos dados;
 - e. Documentação;
 - f. Instalação / configuração de componentes tecnológicas;
 - g. Testes;
 - h. Preparação de ambientes de desenvolvimento, qualidade e produção;
 - i. Quaisquer outros que sejam necessários.
- R.C1.25. A EMPRESA PRESTADORA deverá garantir que o *Datalake* suporta as boas práticas de preparação de dados e que garante modelos/estruturas ágeis.

- R.C1.26. A EMPRESA PRESTADORA deverá adotar uma abordagem que garanta que os dados do repositório possam ter vários níveis de tratamento, devendo estes estar, num último nível, limpos, pré-calculados e estruturados.
- R.C1.27. A Componente 1 deverá manter os dados já com tratamento aprofundado, que vai suportar, mais tarde, tanto a aplicação de análises automáticas (de tendências, preditivas ou outras), como a produção de relatórios pela componente de “*reporting avançado*” (*Power BI* ou *Microstrategy*).
- R.C1.28. A Componente 1 deverá permitir a construção de *datasets* a partir do *Datalake*, nomeadamente para cada tipo de motor e/ou momento do tratamento de ML, conforme se descreve adiante.
- R.C1.29. Cabe à EMPRESA PRESTADORA a apresentação das componentes tecnológicas para permitir a construção de *datasets* a partir do *Datalake*. Poderá utilizar a tecnologia já existente no CONTRAENTE PÚBLICO, nomeadamente SGBD Oracle e IBM DataStage e/ou incluir outras ferramentas tecnológicas no sentido de apresentar a melhor Solução que vá de encontro aos objetivos do CONTRAENTE PÚBLICO.

2.1.5. Motor de Regras

- R.C1.30. Requisito introdutório: O Motor de Regras deverá trabalhar e produzir dados rotulados para posterior aprendizagem do motor de ML.
- R.C1.31. O Motor de Regras deverá produzir dados com uma periodicidade configurável e a definir pelo CONTRAENTE PÚBLICO.
- R.C1.32. A Componente 1 deverá ter a capacidade de incorporar, no motor de regras, os *datasets* obtidos a partir do “tratamento de dados”.
- R.C1.33. O *dataset* deverá ser um conjunto de variáveis, simples ou compostas, calculadas previamente na fase de tratamento de dados (Processamento).
- R.C1.34. O *dataset* deverá contemplar as áreas em âmbito:
 - a. Contribuintes;
 - b. Beneficiários;
 - c. Utilizadores do Sistema de Informação (Fraude Interna).
- R.C1.35. A Componente 1 deverá permitir o cálculo dos indicadores descritos na Visão Futura do Cap. 1, através do Motor de Regras.
- R.C1.36. A EMPRESA PRESTADORA irá, com o apoio do CONTRAENTE PÚBLICO definir/rever e detalhar as fórmulas de cálculo, período temporal de cálculo, regras e exceções aplicáveis, entre outros elementos necessários para o cálculo de cada indicador pelo Motor de Regras.
- R.C1.37. O CONTRAENTE PÚBLICO irá apoiar na definição dos indicadores, disponibilizando um documento que contém:
 - a. Indicadores por área em âmbito;
 - b. Fontes de dados para a construção do indicador;

- c. Variáveis necessárias à construção do indicador;
 - d. Fatores de risco por área em âmbito;
 - e. Indicadores que contribuem para o fator de risco;
 - f. % do peso de cada indicador por fator de risco;
 - g. Tabela auxiliar rotulagem de fatores de risco.
- R.C1.38. A EMPRESA PRESTADORA irá definir de que forma os indicadores são construídos tendo em conta as variáveis a incluir e os respetivos pesos.
- R.C1.39. O Motor de Regras deverá permitir a parametrização de variáveis para o cálculo de indicadores (como por exemplo percentagens de variação; número de dias; número de meses, entre outros).
- R.C1.40. O Motor de Regras deverá permitir o agrupamento de indicadores em fatores de risco.
- R.C1.41. O Motor de Regras deverá ter a capacidade de calcular o valor do fator de risco (positivo, negativo ou inconclusivo), tal como descrito na secção 1.4.1.2 Motor de Regras.
- R.C1.42. O Motor de Regras deverá produzir um resultado fiável, rastreável e preciso.
- R.C1.43. O Motor de Regras deverá carregar os resultados na Base de Dados de Aprendizagem para aprendizagem do motor de aprendizagem, descrito em 2.1.6 Motor de Aprendizagem.
- R.C1.44. O Motor de Regras deverá, de igual forma, carregar os indicadores produzidos na Base de Dados de Gestão de Risco.
- R.C1.45. A Componente 1 deverá garantir a necessária privatização e isolamento dos dados do CONTRAENTE PÚBLICO.

2.1.6. Motor de Aprendizagem

- R.C1.46. Requisito introdutório: O Motor de Aprendizagem deverá calcular a probabilidade de ocorrência de um fator de risco por NISS, com base num conjunto de dados com os quais irá realizar a aprendizagem.
- R.C1.47. A Componente 1 deverá ter a capacidade de incorporar, no Motor de Aprendizagem, o resultado obtido no motor de regras, isto é, se um fator de risco é positivo, negativo ou inconclusivo.
- R.C1.48. A Componente 1 deverá, num primeiro momento, aprender e calibrar o Motor de Aprendizagem até produzir dados rotulados e validados (verificação de um fator de risco), a partir de uma base de dados de aprendizagem.
- R.C1.49. O Motor de Aprendizagem receberá como *input*, no primeiro momento, os dados da Base de dados de Aprendizagem que incluem:
- a. Variáveis;
 - b. Fatores de Risco;
 - c. Rotulagem dos fatores de risco.

- R.C1.50. O Motor de Aprendizagem deverá possibilitar a divisão e construção dos dados em diferentes subconjuntos:
- Dataset* de treino;
 - Dataset* de validação;
 - Dataset* de teste.
- R.C1.51. A tecnologia a fornecer pela EMPRESA PRESTADORA, no que refere ao motor de aprendizagem, deverá permitir a construção de um modelo de aprendizagem supervisionado.
- R.C1.52. A tecnologia a fornecer pela EMPRESA PRESTADORA, no que refere ao motor de aprendizagem, deverá permitir aplicar técnicas de *Machine Learning*, através de algoritmos como:
- Redes neuronais;
 - Árvores de decisão;
 - Regressão linear;
 - Naïve bayes*;
 - Regressão logística;
 - Floresta aleatória;
 - Outros alinhados com as tendências de ML.
- Este requisito respeita à tecnologia / *framework* de ML a fornecer pela EMPRESA PRESTADORA, sendo que caberá à EMPRESA PRESTADORA identificar / definir o(s) algoritmos a aplicar no caso da Solução em âmbito.
- R.C1.53. A EMPRESA PRESTADORA irá propor durante a execução do contrato, e implementar o modelo de aprendizagem mais adequado às necessidades e requisitos da Solução, devendo este modelo ser perceptível e respeitar:
- Sempre que aplicável, as orientações presentes no Guia Responsável para a IA na Administração Pública, desenvolvido pela AMA – “um guia com orientações para o uso responsável da Inteligência Artificial que constitui uma referência para a implementação, pelo setor público, de uma Inteligência Artificial ética, transparente e responsável”, disponível em <https://ia.tic.gov.pt/>;
 - As boas práticas de *Machine Learning*.
- R.C1.54. O Motor de Aprendizagem deverá permitir o treino do modelo de aprendizagem, até à obtenção de um modelo calibrado, possível de ser aplicado a dados não rotulados.
- R.C1.55. Caso necessário, o Motor de Aprendizagem deverá possibilitar a alteração da forma de divisão de dados ou alterar outras características de treino, alterando o modelo de *Machine Learning* de forma a aumentar a performance.
- R.C1.56. O Motor de Aprendizagem, num segundo momento, deverá aplicar o modelo a dados não rotulados, através de um novo *dataset* – *dataset* de teste.
- R.C1.57. O novo *dataset* deverá incluir:

- a. Variáveis;
 - b. Fatores de Risco.
- R.C1.58. O Motor de Aprendizagem deverá possibilitar a avaliação da performance do modelo.
- R.C1.59. A Solução deverá possibilitar a atualização dos *datasets* utilizados pelo Motor de Aprendizagem, com novos dados.
- R.C1.60. O Motor de Aprendizagem deverá possibilitar a afinação do modelo através da atualização dos *datasets*.
- R.C1.61. O Motor de Aprendizagem deverá produzir, como resultado da aplicação do motor de aprendizagem, os fatores de risco e as respectivas probabilidades de ocorrência.
- R.C1.62. O Motor de Aprendizagem deverá produzir um resultado fiável, com qualidade e nível de precisão que não deverá ser inferior a 95%.
- R.C1.63. O Motor de Aprendizagem, assim como a tecnologia a fornecer pela EMPRESA PRESTADORA, deverão garantir a rastreabilidade das variáveis e respetivos valores que estão na origem da estimativa de um determinado nível de risco.
- R.C1.64. A Componente 1 deverá utilizar o resultado do Motor de Aprendizagem, a probabilidade de ocorrência de um fator de risco por NISS como *input* para do Motor de Gestão de Risco, descrito a seguir.
- R.C1.65. Periodicamente a Componente 1, conforme configuração pelo sistema, deverá executar ciclos de reaprendizagem. Para tal, a Solução deverá recorrer a informação:
- a. Proveniente dos sistemas operacionais e que permite confirmar casos positivos ou negativos (Exemplo: Informação proveniente do SAF)
 - b. Proveniente da Componente 2 conforme descrito abaixo no 2.2 Componente 2 – Aplicação de Gestão de Risco.

2.1.7. Motor de Gestão de Risco

- R.C1.66. Requisito introdutório: O Motor de Gestão de Risco visa calcular os níveis de risco parciais e nível de risco global (de cada NISS), aplicando uma matriz que tem em conta o impacto e as probabilidades (provenientes do motor de aprendizagem), conforme descrito no ponto 1.4 Visão Futura.
- R.C1.67. A Componente 1 deverá ter a capacidade de incorporar, no motor de gestão de risco, *inputs*, os *outputs* do motor de aprendizagem:
- a. Variáveis (para efeitos de rastreabilidade);
 - b. Fatores de risco;
 - c. Probabilidades de ocorrência.
- R.C1.68. Para além do referido no requisito anterior, o Motor de Gestão de Risco deverá ter também como *inputs* parametrizáveis:
- a. Matrizes de risco;

- b. Pesos;
- R.C1.69. A Componente 1 deverá permitir a criação e parametrização de Matrizes e pesos conforme requisito anterior. Deverá também permitir a associação de uma dada matriz de risco, por uma dada área (por exemplo, a matriz de risco aplicável às contribuições será distinta daquela aplicada às prestações).
- R.C1.70. O Motor de Gestão de Risco deverá produzir como resultado:
 - a. Risco parcial para cada fator de risco;
 - b. Risco global por NISS;
 - c. Variáveis associadas a cada indicador (sendo estas variáveis já provenientes do Motor de aprendizagem).
- R.C1.71. O Motor de Gestão de Risco deverá produzir um resultado fiável, com qualidade e preciso.
- R.C1.72. Todos os resultados da Componente 1 devem ser rastreáveis e permitir perceber (numa lógica “drill-down”):
 - a. Os fatores de risco que contribuem para cada risco e respetivos pesos;
 - b. As variáveis que contribuem para cada fator de risco e o respetiva peso;
 - c. Indicadores associados a cada risco (estes provenientes do motor de regras).
- R.C1.73. As Bases de Dados que suportam o Modelo de Gestão de Risco (ver Fig18) deverão permitir *Dasboards* e Relatórios.
- R.C1.74. As Bases de Dados que suportam o Modelo de Gestão de Risco deverão ser utilizadas como *input* (e na medida no necessário e adequado) pela Componente 2, descrita em 2.2 Componente 2 – Aplicação de Gestão de Risco.

2.1.8. Dashboard e Reporting

- R.C1.75. A EMPRESA PRESTADORA deverá desenhar de forma detalhada e implementar o ambiente relativo a informação proveniente da Componente 1, relativa a Índices de Risco;
- R.C1.76. O registo de informação proveniente da Componente 1, deverá ser efetuado de forma a manter o histórico de valores dos vários indicadores ao longo de um período parametrizável.
- R.C1.77. Quer os *dashboards*, quer os relatórios serão implementados por forma a permitirem edição por *key-users* (autorizados).
- R.C1.78. No contexto do requisito anterior, quer os *dashboards*, quer os relatórios devem ser facilmente customizáveis.
- R.C1.79. Os *dashboards* serão organizados em quadrantes, sendo, tipicamente, cada quadrante baseado em indicadores chave cuja evolução será apresentada em forma de gráfico.

- R.C1.80. Os relatórios podem ser “reutilizados” em um ou vários *dashboards*. Neste contexto, um *dashboard* pode “embeber” elementos, desde:
- Relatórios;
 - Widgets*;
 - Outros, de acordo com as potencialidades das tecnologias utilizadas.
- R.C1.81. Os relatórios devem, em geral, constituir componentes interativas, permitindo nomeadamente:
- Fazer pesquisas;
 - Aplicar filtros ricos (atributos, intervalos de datas, ...);
 - Aplicar filtros dinâmicos, que permitam filtrações automáticas, face às características de um dado utilizador;
 - Fazer ordenações;
 - Retirar ou adicionar atributos ao relatório;
 - Navegação do tipo *drill-down*;
 - Outros, de acordo com as potencialidades das tecnologias utilizadas.
- R.C1.82. Os relatórios, de acordo com os seus objetivos, devem permitir:
- Adotar diversos tipos de gráficos;
 - Apresentar dados tabulares;
 - Apresentar mapas e dados geográficos;
 - Outros, de acordo com as potencialidades das tecnologias utilizadas.

2.1.8.1. Ambiente relativo a Índices de Risco

- R.C1.83. O ambiente relativo a Índices de Risco, irá disponibilizar *dashboards* e relatórios implementados sobre dados disponíveis pela Componente 1, nomeadamente da base de dados de Gestão de Risco.
- R.C1.84. Este ambiente vai apresentar *dashboards* que serão desenhados e implementados pela EMPRESA PRESTADORA em sede de projeto, considerando desde logo os seguintes exemplos:
- Número e percentagem de entidades (Entidade Empregadora, Trabalhador Independente, Beneficiário, ...) por cada nível de risco (ou pelos níveis de risco mais elevados);
 - Variação de número e percentagem de entidades face ao processamento anterior (total e por tipo de entidade);
 - Número de fatores de risco que mais contribuíram para o risco global (contribuíram para x% do risco global);
 - Lista de fatores de risco da alínea anterior;
 - Distribuição geográfica (sobre mapa simples) das entidades com nível de risco mais elevado;

- f. Outros a identificar em sede de projeto.
- R.C1.85. Este ambiente vai apresentar relatórios que serão desenhados e implementados pela EMPRESA PRESTADORA em sede de projeto, considerando desde logo os seguintes exemplos:
- a. Entidades por cada nível de risco, agregando por tipo de entidade, por nível de risco ou por combinação de tipo de entidade e nível de risco;
 - b. Variação de número e percentagens de entidades em cada nível de risco, face aos N últimos processamentos;
 - c. *Drill-down* de fatores de risco face ao relatório da alínea a), assim como *drill-down* até ao nível dos indicadores que contribuíram para o risco;
 - d. Possibilidade de visualização em mapa das entidades por nível de risco;
 - e. Lista de fatores de risco e respetivo nível de risco médio;
 - f. Lista de indicadores e respetivos resultados (com respetiva contribuição ou não contribuição para o risco);
 - g. Outros a identificar em sede de projeto.

2.2. Componente 2 – Aplicação de Gestão de Risco

2.2.1. Visão Geral

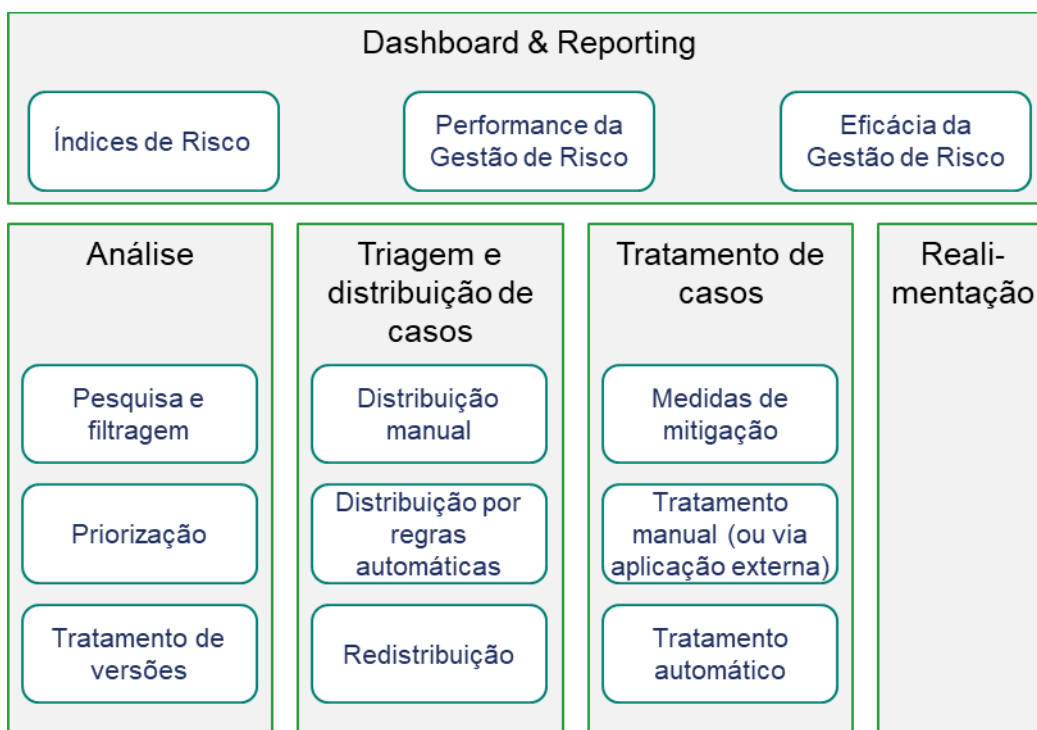


Figura 19 – Diagrama da Componente 2

A Componente 2, enquadra-se na arquitetura mais ampla já descrita anteriormente e constitui uma aplicação cujo objetivo é o de dar suporte às equipas do ISS que irão tratar os resultados dos índices de risco estimados na Componente 1.

Esta aplicação, assente em ferramentas de *Risk Management / Case Management* e ferramentas de *reporting*, será desenhada em detalhe e personalizada em sede de projeto.

Esta aplicação deverá incluir os seguintes componentes, conforme figura acima (cujos requisitos se apresentam abaixo):

- **Dashboard & Reporting** – Trata-se de uma vertente com informação para suporte à gestão, no que respeita aos índices de Risco obtidos na Componente 1, ao desempenho do Sistema de Gestão de Risco e, finalmente, sobre a eficácia do Sistema de Gestão de Risco.
- **Análise** – Componente que permite efetuar a análise em detalhe dos índices de risco obtidos e fazer a preparação de casos que necessitem de tratamento.
- **Triagem e distribuição de casos** – Vertente que vai suportar a seleção e distribuição de casos para tratamento por equipas e/ou por automatismos.
- **Tratamento de casos** (de forma manual ou automática) – Vertente que vai permitir a gestão das medidas de mitigação, e também permitir às equipas registarem o resultado do tratamento e definir e gerir tratamentos automáticos.
- **Realimentação** – Vertente que vai permitir recolher informação que irá realimentar o motor de ML, permitindo melhorar o nível de aprendizagem.

2.2.2. Requisitos gerais

- R.C2.2. A Componente Aplicação de Gestão de Risco deverá ser desenhada em detalhe e personalizada durante a execução do contrato, pela EMPRESA PRESTADORA, tendo em conta os blocos identificados na Figura 19 – Diagrama da Componente 2 e os requisitos apresentados de seguida.
- R.C2.3. A Aplicação proposta deverá ter como base soluções de *Case Management* e/ou *Risk Management*, tirando assim proveito das funcionalidades e tecnologias destas soluções e potenciando uma implementação mais rápida (face a um desenvolvimento à medida).
- R.C2.4. Os vários blocos identificados devem, em geral, contemplar visualização de informação para o Setor de Gestão de Risco, para as várias unidades que participem nos processos de Gestão de Risco, e para a Gestão de Topo (nomeadamente ao nível do ISS). Neste contexto, a Aplicação deverá permitir configurar os acessos de cada equipa ou área.
- R.C2.5. Estes blocos terão mecanismos de controlo de acesso, permitindo que determinados perfis / utilizadores tenham acesso a um ou vários dos blocos. Utilizadores sem acesso não poderão visualizar qualquer informação.
- R.C2.6. Para além do referido do requisito anterior, a plataforma deverá ser configurável em diversos aspetos conforme desenho em sede de projeto, e contemplando desde logo o seguinte:

- a. Configuração das equipas para as quais podem ser encaminhados casos para tratamento;
 - b. Configuração de medidas de mitigação, de forma associada a fatores de risco;
 - c. Configuração de regras para encaminhamento (ver bloco de triagem e distribuição de casos);
 - d. Configuração do ambiente de cada utilizador, por exemplo no que refere às colunas que poderá ver em determinados relatórios;
 - e. Configuração do número de versões decorrentes de processamentos dos índices de risco que devem estar visíveis na plataforma;
 - f. Configuração de datas e periodicidade de processamentos (no que respeita a realimentação ou outros);
 - g. Outros a definir em sede de projeto.
- R.C2.7. A informação a mostrar ao nível dos *dashboards* e relatórios deverá permitir, sempre que aplicável, selecionar a versão fonte da estimativa dos índices de risco. Ou seja, espera-se que, periodicamente, o motor de aprendizagem faça um processamento, “recalculando” as estimativas de índices de risco (para cada entidade com NISS). De cada vez que existe um novo processamento, será gerada uma versão de índices de risco, versão essa que a plataforma permitirá analisar individualmente.
- R.C2.8. Sem prejuízo do requisito anterior, a Aplicação vai, em diversas situações, apresentar *dashboards* e/ou relatórios (incluindo relatórios dinâmicos) que cruzam a informação resultante de vários processamentos (por exemplo, quando apresenta a evolução de um dado indicador). Veja-se os requisitos em cada um dos blocos previstos para a plataforma.
- R.C2.9. Os relatórios ou listagens obtidas na Aplicação devem possibilitar a exportação de dados, nomeadamente nos seguintes formatos:
- a. MS Excel;
 - b. PDF;
 - c. HTML/XML.

2.2.3. Dashboard e Reporting

- R.C2.10. A EMPRESA PRESTADORA deverá desenhar de forma detalhada e implementar dois ambientes com informação de gestão, para além do ambiente referido na Componente 1, incluindo *dashboards* e *reporting* (no contexto da Gestão de Risco) referentes a:
- a. Informação relativa à atividade e desempenho de Gestão de Risco (numa perspetiva transversal que inclui pessoas, processos e ferramentas, englobando a área diretamente responsável pela gestão de risco, assim como as diversas áreas que participam nos processos, para além do desempenho da própria Solução);

- b. Informação relativa à eficácia da Gestão da Risco (incluindo indicadores que capturem a evolução do nível de risco, que resultem da atuação pelas pessoas processos e sistema tecnológico).
- R.C2.11. O registo de informação proveniente da Aplicação (Componente 2), deverá ser efetuado de forma a manter o histórico de valores dos vários indicadores ao longo de um período parametrizável.
- R.C2.12. Os requisitos da Componente 1, referidos em 2.1.8 *Dashboard e Reporting* deverão ser cumpridos para a Componente 2.

2.2.3.1. Módulo relativo a desempenho da Gestão de Risco

- R.C2.13. No respeitante à Gestão de Risco, nomeadamente, no que refere à atividade pela utilização da Componente 2, este módulo de desempenho deverá disponibilizar a informação / relatórios adequados para suporte às atividades de gestão e também das atividades mais operacionais, com o nível de detalhe adequado à tomada de decisão.
- R.C2.14. Os dados de suporte à informação deste ambiente, assim como o cálculo de indicadores necessários, processamento dos dados e outros, constituem âmbito da implementação da própria Aplicação de Gestão de Risco.
- R.C2.15. Este módulo vai apresentar *dashboards* que serão desenhados e implementados pela EMPRESA PRESTADORA em sede de projeto, considerando desde logo os seguintes exemplos:
 - a. Número e percentagem de casos (correspondentes a entidades) assinalados para tratamento, por nível de risco;
 - b. Número e percentagem de casos assignados a áreas para tratamento (incluindo aqueles no âmbito da própria área da Gestão de Risco);
 - c. Número e percentagem de casos tratados (no período);
 - d. Número e percentagem de casos por tratar (no período);
 - e. Número e percentagem de casos com ações de mitigação automáticas;
 - f. Outros a identificar em sede de projeto.
- R.C2.16. Este módulo vai apresentar relatórios que serão desenhados e implementados pela EMPRESA PRESTADORA em sede de projeto, considerando desde logo os seguintes exemplos:
 - a. Número total de casos, número de casos num dado período e/ou percentagem, por entidade, por valor das contribuições / prestações, por estados de tratamento e por tipo de tratamento (automático, manual ou ambos);
 - b. Possibilidade de *drill-down* dos relatórios anteriores, por diversas perspetivas (nível de risco, fatores de risco, entidades e outros);
 - c. Número e percentagem de casos com tratamento automático, por medidas de mitigação e possibilidade de *drill-down* por diversas perspetivas;

- d. Outros a identificar em sede de projeto.

2.2.3.2. Módulo relativo à eficácia da Gestão de Risco

- R.C2.17. Este módulo deverá focar-se em informação de gestão e indicadores adequados para a análise e avaliação da eficácia de toda a Gestão de Risco (incluindo a Componente 1 e a Componente 2, pessoas, processos, ...), com o nível de detalhe adequado à tomada de decisão.
- R.C2.18. Os dados de suporte à informação deste módulo, assim como o cálculo de indicadores necessários, processamento dos dados e outros, provêm da Componente 1 (índices de risco) de forma conjugada com dados da própria Aplicação de Gestão de Risco.
- R.C2.19. Este módulo vai apresentar *dashboards* que serão desenhados e implementados pela EMPRESA PRESTADORA em sede de projeto, considerando desde logo os seguintes exemplos:
 - a. Variação geral do número de entidades com os dois níveis de risco mais elevados;
 - b. Para as entidades com casos tratados / intervencionados, apresentar variação média do nível de risco, por número de casos totais, por situações com tratamento automático e por tratamento manual;
 - c. Para entidades com casos tratados / intervencionados, apresentar a evolução do valor médio das remunerações e das prestações (conforme aplicável);
 - d. Outros a identificar em sede de projeto.
- R.C2.20. Este módulo vai apresentar relatórios que serão desenhados e implementados pela EMPRESA PRESTADORA em sede de projeto, considerando desde logo os seguintes exemplos:
 - a. Variação do número e percentagem de entidades por cada nível de risco;
 - b. Lista dos casos tratados, com evolução no nível médio de risco, por tipo de tratamento (manual, automático ou misto);
 - c. Lista dos casos tratados, com evolução no nível médio de contribuições e/ou prestações, por tipo de tratamento (manual, automático ou misto);
 - d. *Drill down* da lista das duas alíneas anteriores, por entidades, fatores de risco, região geográfica e outros;
 - e. Outros a identificar em sede de projeto.

2.2.4. Análise

- R.C2.21. A Aplicação de Gestão de Risco deverá suportar a análise dos Índices de Risco, apresentando para tal um ambiente rico e flexível que permita, de forma ágil, que a área de Gestão de Risco identifique os casos que carecem de tratamento prioritário (e que possam assim ser identificados para tratamento posterior). A

Aplicação deve, a este nível, incluir a configuração de automatismos que permitam identificar determinados casos que podem depois se encaminhados para equipas e/ou para tratamentos automáticos, face às medidas de mitigação.

2.2.4.1. Módulo para pesquisa e filtragem

- R.C2.22. A componente de análise deve ser constituída por um módulo de pesquisa e filtragem por seleção simples (com fachada de vários filtros des/ativáveis que por seleção, por introdução de intervalos de limites ou outros mecanismos) facilitem a identificação de casos específicos.
- R.C2.23. No contexto do requisito anterior, a Aplicação deverá permitir guardar uma dada combinação de filtros / critérios de pesquisa, permitido que esta seja reaplicada posteriormente.
- R.C2.24. A Aplicação deverá suportar diversos filtros, incluindo a possibilidade de adicionar novos filtros de forma rápida, tendo desde logo em conta os seguintes:
- a. Entidade (EE, TI, TCO, ...);
 - b. Nível de Risco;
 - c. Fator de Risco;
 - d. Indicador;
 - e. Nível de prioridade;
 - f. Número ou intervalo de número de funcionários (para as entidades aplicáveis);
 - g. Intervalo de valor das contribuições (para as entidades aplicáveis);
 - h. Intervalo de valor das prestações (para as entidades aplicáveis);
 - i. Distrito e/ou Concelho;
 - j. CAE;
 - k. Outros a identificar em sede de projeto.
- R.C2.25. Os resultados da pesquisa / filtragem podem ainda ser gravados e/ou exportados. Isto, é, o conjunto específico de casos identificados, poderão ficar guardados e assim ser consultados posteriormente (ou em ferramentas externas).
- R.C2.26. Os resultados da pesquisa / filtragem poderão adicionalmente ser identificados (marcados) para posterior triagem adicional e distribuição. Esta identificação deverá ser distintiva, de acordo com o tipo de tratamento pretendido:
- a. Reavaliação do cálculo do índice de risco (significa que áreas técnicas deverão verificar se os mecanismos que determinaram o nível de risco funcionaram de forma adequada);
 - b. Tratamento por mecanismos automáticos;
 - c. Tratamento por equipas com intervenção manual;
 - d. Outros que sejam identificados em sede de projeto.

- R.C2.27. As listagens obtidas neste módulo devem poder ser visualizadas em formato tabela e, quando aplicável, em gráficos e/ou mapas (para dados com informação geográfica).

2.2.4.2. Priorização

- R.C2.28. A Aplicação deverá fazer uma priorização automática dos casos, face a critérios (algoritmo) a definir em sede de projeto, tendo desde logo em conta o seguinte:
- a. Nível de índice de risco;
 - b. Valor do índice de risco (valor base antes de ser convertido num nível);
 - c. Tipo de entidade;
 - d. Número de funcionários, se aplicável;
 - e. Valor médio das contribuições, se aplicável;
 - f. Valor médio das prestações, se aplicável;
 - g. Localização geográfica;
 - h. Outros que sejam identificados.
- R.C2.29. A priorização é aplicada para todos os casos / entidades com índice de risco estimado, e é recalculado sempre que ocorra um novo processamento pelo *Machine Learning*.

2.2.4.3. Tratamento de versões (histórico)

- R.C2.30. A Solução deverá atualizar a informação associada a cada entidade (baseada num NISS), sempre que ocorra num novo processamento pelo motor de aprendizagem (conforme Componente 1), tendo em conta o seguinte:
- a. O índice de risco de uma entidade ou caso em tratamento, deverá ser atualizado com a informação do processamento mais recente;
 - b. A informação dos índices de risco dos tratamentos anteriores deve manter-se visível e devidamente identificada com a data do processamento associado;
 - c. O *drill-down* do nível de risco deverá ser possível pelo índice de risco mais recente, assim como pelos índices de risco de processamentos anteriores;
 - d. Quando os dados de entidades e/ou casos são mostrados em tabela, por defeito é mostrado o índice de risco mais recente, podendo os índices de risco de processamentos anteriores ser visualizados por consulta ao caso.

2.2.5. Triagem e distribuição de casos

- R.C2.31. A componente de triagem e distribuição de casos deverá funcionar de forma muito articulada com a componente de análise, e vai permitir distribuir casos pelas várias equipas e/ou para tratamento automático e vai também permitir reapreciar casos que estejam em tratamento (por exemplo, mediante

informação mais atualizada dos índices de risco), permitindo a sua redistribuição.

2.2.5.1. Distribuição manual

- R.C2.32. A distribuição manual, tipicamente a realizar pela área de Gestão de Risco (ou outra equipa conforme configuração da Aplicação), deverá ocorrer da seguinte forma:
- a. Identificação de casos a distribuir (para um dado destino, quer seja equipa, quer seja para um sistema externo, quer seja para tratamento automático). Esta identificação decorre do ambiente de filtragem da análise, mas mostrando apenas os casos que não estejam distribuídos;
 - b. Seleção dos casos a distribuir. A seleção poderá ser realizada para todos os casos identificados (em conjunto), ou por (des)seleção de casos um a um;
 - c. Identificação do destino da distribuição;
 - d. Confirmação.
- R.C2.33. Os casos distribuídos vão desaparecer da lista de casos ainda a distribuir e irão aparecer nas áreas das equipas ou ambientes destino.
- R.C2.34. A equipa que faz a distribuição poderá consultar os processos distribuídos, por opção a disponibilizar explicitamente pela plataforma. Neste caso, a equipa poderá visualizar os casos distribuídos em cada destino, assim como o respetivo estado.

2.2.5.2. Distribuição por regras automáticas

- R.C2.35. Para além da distribuição de forma manual, a Aplicação deverá permitir a distribuição por regras automáticas.
- R.C2.36. A Aplicação deverá suportar a configuração de regras de encaminhamento, a desenhar de forma detalhada em sede de projeto, considerando desde logo o seguinte:
- a. Os critérios de seleção de casos a que se aplicam as regras, poderão ser implementados com mecanismos semelhantes à pesquisa / filtragem descritos para o ambiente de análise;
 - b. A seleção do destino, faz-se tendo por base os destinos configurados (equipas de tratamento manual, mecanismos de tratamento automático, ...);
 - c. Definição de data / hora em que são aplicadas;
 - d. Definição de um nome para cada regra;
 - e. Definição de prioridade na execução da regra (face a outras regras).
- R.C2.37. A Aplicação deve permitir definir as regras com interface simples e ágil.

- R.C2.38. Deve permitir validar as regras (correr sem impactar os dados reais, mas informando sobre o que seria o resultado).
- R.C2.39. Deve permitir que as regras sejam ativadas ou desativadas.
- R.C2.40. Deve permitir que as regras sejam editadas / alteradas.

2.2.5.3. Redistribuição de casos

- R.C2.41. A Aplicação deverá permitir reavaliar os casos já distribuídos e, por opção do utilizador, permitir a sua redistribuição. Entende-se aqui a redistribuição como possibilidade de:
 - a. Alocar os casos a diferentes equipas;
 - b. Desalocar os casos de determinadas equipas e marcar como casos que não necessitem de tratamento.
- R.C2.42. A redistribuição pode ser feita de forma manual ou por regras automáticas, seguindo uma mecânica similar à descrita acima.
- R.C2.43. No caso particular das regras para redistribuição automática, estas regras têm de, em particular, permitir definir critério que contempla situações de alteração de nível de risco e/ou prioridade em baixa (permitindo assim desalocar casos que tenham perdido pertinência).

2.2.6. Tratamento de casos

- R.C2.44. A Aplicação deverá apresentar um módulo para acesso aos casos e deverá ter funcionalidades que permitam registar o seu tratamento. Adicionalmente deve ter mecanismos para tratamento automático (tipicamente baseado em medidas de mitigação).
- R.C2.45. O módulo de tratamento de casos deve incluir o conceito de equipa / grupo e ainda utilizador. Um utilizador deve pertencer a um grupo. A cada utilizador, a plataforma deve mostrar os casos do grupo a que o utilizador pertence, assim como os casos alocados diretamente ao utilizador.
- R.C2.46. A Aplicação deverá permitir configurar um utilizador responsável por um grupo que terá permissões especiais, nomeadamente:
 - a. Designação de casos a utilizadores da equipa;
 - b. Possibilidade de adicionar ou remover utilizadores ao grupo;
 - c. Outros que venham a ser identificados.
- R.C2.47. A Aplicação deve permitir o tratamento de casos de forma individual ou em conjunto, sendo que, nesta última situação a informação registada na sequência do tratamento será idêntica para todos os casos.

2.2.6.1. Medidas de mitigação

- R.C2.48. A Aplicação deverá suportar a configuração de medidas de mitigação de forma associada aos fatores de risco. Isto, é por cada tipo de fator de risco, será possível associar uma ou mais medidas de mitigação.
- R.C2.49. As medidas de mitigação poderão constituir:
- a. Textos, scripts de atuação ou FAQs;
 - b. Automatismos que sejam suportados pela plataforma.
- R.C2.50. As medidas de mitigação poderão ser:
- a. Suficientes, no sentido em que não são requeridas mais medidas;
 - b. Parciais, na medida em que os casos carecem ainda de intervenção manual.
- R.C2.51. Os automatismos previstos serão (entre outros que possam ser identificados):
- a. Envio de e-mail a uma entidade, de acordo com *template*;
 - b. Envio de SMS a uma entidade, também baseado em *template*;
 - c. Envio de carta (correio tradicional), da mesma forma baseado em *template*.
- R.C2.52. Os automatismos do requisito anterior funcionarão por chamada a serviços (*web services* ou outros) já implementados pelo II e que serão disponibilizados à EMPRESA PRESTADORA em sede de projeto.

2.2.6.2. Tratamento manual na Aplicação

- R.C2.53. A Aplicação irá disponibilizar um módulo em que um utilizador vai poder selecionar um caso ou um conjunto de casos (em aberto), na sua lista pessoal, ou na lista do Grupo/Equipa a que pertença, e proceder ao seu tratamento.
- R.C2.54. A Aplicação vai permitir ao utilizador registar o resultado do tratamento. O utilizador pode dar o caso como concluído ou pode atualizar o caso para conclusão posterior.
- R.C2.55. O resultado do tratamento deve incluir o registo de tratamento feito, incluindo o registo da eventual descrição e eventual associação de documentos.
- R.C2.56. A Aplicação vai também permitir que o utilizador registe informação sobre o nível de risco do caso:
- a. Podendo confirmar que o nível de risco proveniente do *Machine Learning* está ajustado à situação;
 - b. Ou indicando que o nível de risco não está ajustado à situação, devendo ser superior ou inferior.

2.2.6.3. Tratamento por integração com aplicação externa

- R.C2.57. Determinados casos poderão ser tratados pelas equipas em aplicações externas, conforme decisão de distribuição (por via manual ou por regras automáticas).

- R.C2.58. Por forma a tratar estes casos, a Aplicação incluirá interface com sistema externo por forma a:
- Enviar informação chave sobre os casos a tratar;
 - Receber informação chave sobre o resultado do tratamento.
- R.C2.59. No que respeita a informação enviar, esta será identificada em detalhe em sede de projeto, contemplando desde logo o seguinte:
- Tipo da entidade e dados da entidade;
 - Nível de risco;
 - Riscos parciais e fatores de risco;
 - Medidas de mitigação.
- R.C2.60. No que respeita a informação a receber, esta será também identificada em detalhe em sede de projeto, contemplando desde logo o seguinte:
- Entidade (NISS);
 - Estado do tratamento;
 - Resultado do tratamento;
 - Informação sobre reavaliação do nível de risco (confirmação ou não, correção para cima ou para baixo).

2.2.6.4. Tratamento automático

- R.C2.61. A Aplicação deverá suportar a execução de medidas de mitigação de forma automática, de acordo com o seguinte:
- Para o caso em tratamento, verificou-se um fator de risco para o qual existe medida de mitigação automática;
 - Sendo a medida de mitigação única, a plataforma avança com a sua execução;
 - Se para um dado caso, vários fatores de risco forem verificados e, também assim, forem identificadas várias medidas de mitigação automáticas, o caso ficará sujeito a intervenção manual (para identificação das medidas a aplicar, garantindo a coerência das medidas de mitigação).
- R.C2.62. A Aplicação irá permitir configurar se os automatismos podem ser executados de forma automática, sem validação e confirmação pelo utilizador ou se, pelo contrário, ficarão sempre dependentes dessa validação.
- R.C2.63. Em qualquer dos casos, todos os tratamentos automáticos ficarão devidamente registados, com informação da sua execução, se houve falhas que careçam de intervenção, entre outros conforme desenho em sede de projeto.

2.2.7. Realimentação (para a aprendizagem do *Machine Learning*)

- R.C2.64. A Aplicação irá, periodicamente (de acordo com parametrização), preparar informação para realimentar a *Solução*. A informação de realimentação irá incluir:
- Confirmação ou não do nível de risco;
 - Correção do nível de risco (com subida ou descida).
- R.C2.65. A informação referida no requisito anterior será obtida pelos resultados dos casos com tratamento (quer o tratamento tenha sido registado na própria Aplicação, quer tenha sido efetuado em sistema externo, mas cujos resultados tenham sido recebidos).
- R.C2.66. A informação de realimentação, conforme descrito nos capítulos anteriores, será processada e irá envolver atualizações na Componente 1, em *datasets* para aprendizagem devidamente identificados para o efeito.

2.3. Interface com o utilizador

- R.INTER.1 Requisito introdutório: A Solução deve permitir um ambiente gráfico / interface com o utilizador *user friendly*, com organização das funcionalidades / menus e navegação intuitiva e seguindo modelos familiares aos utilizadores (nomeadamente com navegação tipo web), capaz de garantir os padrões e regras das melhores práticas existentes, nomeadamente:
- Princípio de estrutura:** o design da Solução deve estruturar a interface do utilizador de forma organizada e facilmente utilizável, com base em modelos claros e consistentes que sejam facilmente reconhecidos e entendidos pelos utilizadores, juntando o que é relacionado e separando o que não o é, diferenciando visualmente o que é fundamentalmente diferente e tornando o que é semelhante visualmente reconhecível;
 - Princípio de simplicidade:** o design da Solução deve simplificar a execução de tarefas simples e frequentes, comunicando de forma clara e simples na linguagem do utilizador, e oferecendo bons atalhos relativamente a procedimentos mais longos;
 - Princípio de visibilidade:** o design da Solução deve dar visibilidade sobre todas as opções e materiais necessários para cada tarefa sem distrair o utilizador com informação redundante ou irrelevante;
 - Princípio de feedback:** o design da Solução deve manter o utilizador informado sobre ações ou interpretações, mudanças de estado, erros ou exceções que sejam relevantes e do interesse do utilizador através de linguagem clara, concisa e familiar ao utilizador;
 - Princípio de tolerância:** o design da Solução deve ser flexível e tolerante, reduzindo o custo de erros e má utilização, permitindo reverter ou refazer

ações, prevenindo ainda erros onde possível, tolerando diversos inputs e sequências de ações razoáveis;

- f. **Princípio de reutilização:** o design da Solução deve reutilizar componentes e comportamentos internos e externos, mantendo a consistência com o seu propósito de forma não arbitrária, reduzindo a exigência cognitiva e de memória do utilizador.

R.INTER.2 A Solução deverá ter a capacidade de parametrizar os elementos que constituem a imagem gráfica a definir pelo CONTRAENTE PÚBLICO (por exemplo, fontes, cores e logotipos).

R.INTER.3 A Solução deverá ajudar os utilizadores a evitar e a corrigir os erros e, se surgirem, deve ser possível identificá-los e corrigi-los de forma expedita.

R.INTER.4 A interface da Solução deve garantir que:

- a. O número de *clicks* / toques no ecrã para atingir qualquer objetivo é o mínimo possível e que, em geral, toda a interação está otimizada para facilitar e simplificar as funções do utilizador;
- b. O número de campos necessários para atingir qualquer objetivo é o mínimo possível;
- c. A utilização de páginas *pop-up* ou sub-páginas para a introdução de dados em listas é minimizada, utilizando mecanismos de preenchimento na lista;
- d. Todas as interfaces que contenham formulários eletrónicos de recolha de dados deverão permitir a apresentação de listas de valores admissíveis, validação do formato e tipo dos dados inseridos;
- e. O utilizador tem à sua disposição atalhos a partir do teclado para navegar ao longo dos mesmos e para aceder às ações disponíveis;
- f. Os formulários eletrónicos alertam para valores obrigatórios em falta e para valores incongruentes ou errados; neste contexto, eventuais erros são imediatamente identificados através de mensagens de erro ou explicativas relevantes;
- g. Os campos dos ecrãs e formulários eletrónicos permitem inserir / ler valores pertencentes ao conjunto de caracteres ISO 8859 (Latin 1, Latin 2 e Latin 3) em todos os campos de texto.

R.INTER.5 A reação da Solução aos pedidos do utilizador deverá ser tal que:

- a. Garanta a perceção pelo utilizador do processamento do pedido;
- b. Não comprometa o alcance dos requisitos exigidos pela Solução;
- c. Facilite e assegure a eficiência das sequências de trabalho do utilizador necessárias à sua função, incluindo a simultaneidade e encadeamento de pedidos e seus resultados;
- d. A eficiência e rapidez de execução das interfaces devem resultar de uma minimização do número de *clicks* / toques necessários para navegar, do número de páginas carregadas, do tempo de carregamento médio das páginas e do tempo necessário para ler e/ou introduzir informação;

- e. A interação e a qualidade da apresentação ao utilizador da informação processada pela Solução deverá ser tal que não prejudique, de forma imediata ou a longo prazo, a saúde do utilizador;
- f. Está imediatamente disponível informação de ajuda (*help*) para o utilizador, contextualizada à função que este estiver a executar.

R.INTER.6 A Solução deverá ser disponibilizada na língua portuguesa.

R.INTER.7 A Solução deverá garantir que todas as mensagens de erro são claras, a fim de que os utilizadores possam atuar de forma apropriada. Cada mensagem de erro deve conter um texto explanatório e a indicação da ou das ações que o utilizador poderá empreender em resposta ao erro.

R.INTER.8 A Solução deverá conter múltiplas opções de seleção para impressão ou exportação: documento, partes de um mesmo documento (página, conjunto de páginas, texto selecionado, imagem, parte de imagem, grupos de imagens) ou todas as imagens ou ficheiros contidos numa estrutura de ficheiros/pasta.

2.4. Integração

R.INTEG.1 Requisito Introdutório: A Solução deverá disponibilizar interfaces para integração aplicacional com sistemas externos. Nesse sentido, a SOLUÇÃO deverá ser aberta e facilmente integrada através de boas práticas de mercado, nomeadamente *web-services*. Isto para além de todos os aspetos de “integração” contemplada ao nível de dados para os sistemas que irão disponibilizar dados fonte.

R.INTEG.2 Para efeitos de envio e receção de emails e/ou SMS pela Solução, a mesma deverá ter condições para integrar-se com o sistema do II, I.P. existente para o efeito, e de acordo com o desenho da Solução a acontecer em sede de projeto.

R.INTEG.3 A Solução deverá incluir interfaces de integração com sistemas operacionais (como exemplo o Sistema de Apoio à Fiscalização – SAF), a desenhar e implementar em sede de projeto, por forma a:

- a. comunicar níveis de risco (de uma entidade), fatores de risco associados (respetivos pesos) e informação relacionada;
- b. receber dados de validação / correção desse nível de risco;
- c. Outra informação a definir em sede de projeto.

R.INTEG.4 A Solução deverá ter a capacidade de exportar a informação nas suas bases de dados de modo a facilitar a importação completa para outros sistemas, nomeadamente informação sobre a classificação de risco das entidades e beneficiários (NISS).

R.INTEG.5 Sem prejuízo de outras integrações, em particular no que respeita a recolha de dados fonte conforme descrito na secção 2.1, a Solução deverá apresentar mecanismos de integração com sistemas do II, baseado em boas práticas e em

particular em *webservices*. Para tal, deverá ser contemplada a integração da Solução com as aplicações existentes no II para o efeito de:

- a. Autenticação de Utilizadores, tirando partido de plataforma Microsoft Active Directory existente e/ou por integração via protocolos standard com outras soluções existentes;
- b. Gestão de Utilizadores/Perfis e Segurança, tirando também partido de plataforma de gestão de utilizadores no contexto de MS Active Directory
- c. Envio de Mensagens / Envio de Correio Tradicional, face às opções a serem definidas em sede de implementação.

2.5. Vertentes e requisitos transversais

2.5.1. Princípios base

R.TRSV.1 Requisito introdutório: A Solução deverá estar concebida e implementada de modo a respeitar os seguintes princípios:

- a. **Adequabilidade** (completude e correção) – A Solução assegura todos os requisitos numa lógica de resultados a alcançar, sem falhas (sem efeitos colaterais indesejados).
- b. **Privacidade e segurança** – A Solução deverá suportar e garantir a operacionalização de procedimentos de segurança e privacidade condizentes com a exigência do tipo de informação e serviços assegurados. Em particular, deve garantir a segurança das componentes aplicacionais e dos dados, recorrendo às melhores práticas, nomeadamente por utilização de controlo de acessos, encriptação, assinatura digital, etc.
- c. **Proteção** – A Solução deverá garantir a recuperação, legibilidade e não distorção da informação nela armazenada e processada.
- d. **Estruturação por camadas / perímetros de segurança** – A arquitetura da Solução deve estar estruturada em camadas, de acordo com as melhores práticas, sendo que cada camada deve estar protegida por um perímetro de segurança próprio.
- e. **Elevada disponibilidade** – A Solução, no que respeita ao ambiente de produção, deverá cumprir elevados níveis de fiabilidade e disponibilidade, com capacidades de recuperação de falhas, entre outros, através da redundância nos vários componentes tecnológicos. Neste contexto, deverão ser também implementados mecanismos de monitorização.
- f. **Performance e distribuição de carga** – A Solução deve estar adaptada a funcionar adequadamente com mecanismos de distribuição de carga.
- g. **Mínima dependência da Empresa Prestadora e de tecnologias específicas** – a dependência da Empresa Prestadora com

tecnologias/*frameworks* não genericamente utilizadas pelo mercado deve ser minimizada, recorrendo-se a estas apenas em casos onde alguma funcionalidade específica não se encontre em produtos de mercado.

- h. **Capacidade de integração com sistemas terceiros** – a Solução deverá ser facilmente integrável com sistemas externos, estando em conformidade com as normas técnicas e melhores práticas utilizadas para integração.
- i. **Modularidade e Capacidade de crescimento** – a Solução deverá ser modular e baseada numa arquitetura orientada a serviços que permita a sua evolução de forma simples e com esforço de integração reduzido, seguindo as melhores práticas de mercado. Adicionalmente, a Solução deverá ser capaz de suportar de forma incremental novas funcionalidades e o acréscimo de volumes de trabalho, através da reconfiguração e reparametrização das componentes fornecidas.
- j. **Responsive** – De modo a permitir uma utilização fluída por parte dos utilizadores e a poder ser utilizado por dispositivos com ecrãs de diversos tamanhos.
- k. **Conformidade com Normas** – Sempre que aplicável, a Solução tem de apresentar um nível de conformidade AA de acordo com o WCAG 2.0 (com especial importância no que respeita às regras de acessibilidade para pessoas com necessidades especiais).
- l. **Auditabilidade** – a Solução deve manter em histórico quem, quando e que adições/alterações/remoções são efetuadas sobre a informação e parametrização da Solução.
- m. **Boas práticas da AMA** – a Solução deve respeitar, sempre que aplicável, o Guia Responsável para a IA na Administração Pública.
- n. **Princípios de uma IA Responsável** – A Solução deverá assegurar as seguintes dimensões:
 - **Responsabilização** (responsabilidade e possibilidade de auditoria/inspeção);
 - **Transparência** (acesso às componentes e procedimentos);
 - **Explicabilidade** (explicação da escolha do algoritmo e do seu funcionamento);
 - **Justiça** (proteção e garantias para os utilizadores e beneficiários);
 - **Ética** (mecanismos efetivos de mitigação de vieses inesperados).

R.TRSV.2 A Solução deverá cumprir os requisitos e normativas legais.

R.TRSV.3 No contexto dos requisitos anteriores, faz parte do âmbito do projeto uma análise entre a EMPRESA PRESTADORA e o CONTRAENTE PÚBLICO, no sentido

de desenhar e detalhar as opções técnicas a implementar no contexto do projeto.

R.TRSV.4 A Solução deverá disponibilizar os meios para permitir a sua expansão, ou seja, a adição de novas funcionalidades ou a adaptação de funcionalidades existentes.

R.TRSV.5 A Solução deverá permitir a extensão funcional e/ou customização dos seus módulos.

2.5.2. Software as a Service (SaaS)

R.TRSV.6 Requisito introdutório – Os Sistemas de Informação do ISS e do II encontram-se alojados em ambiente on-premises. Neste contexto, no que refere à Solução em âmbito, desde logo no respeitante às fontes de dados, estas estão também localizadas *on-prem*. Todavia, a Solução deverá ser fornecida num modelo Software as a Service (SaaS) suportado em cloud, no que respeita à maior parte da Componente 1 (ver abaixo) e no que respeita a toda a Componente 2.

R.TRSV.7 No contexto do requisito anterior, entende-se que toda a preparação e implementação da Solução, são executadas em sede de projeto conforme descrito no Capítulo 3 adiante. Após a implementação da Solução (o que acontece de forma gradual conforme descrito do Capítulo 3), a EMPRESA PRESTADORA passa a disponibilizá-la num modelo SaaS (também de forma gradual).

R.TRSV.8 Ainda no contexto dos requisitos anteriores, entende-se que no modelo SaaS a EMPRESA PRESTADORA é responsável por todas as componentes / infraestruturas, software e serviços necessários para que a Solução funcione devidamente. Tal inclui, ao nível dos serviços, as vertentes de suporte e manutenção corretiva, administração e configuração da Solução, *on-going*.

R.TRSV.9 No que respeita à Componente 1:

- a. A subcomponente de importação e tratamento de dados, em particular o *Datalake*, deverá ser implementada em ambiente *on-prem*, sendo, todavia, esta componente da SOLUÇÃO também incluída nos serviços de administração e configuração, manutenção a prestar pela EMPRESA PRESTADORA.
- b. As restantes subcomponentes da Componente 1 serão disponibilizadas integralmente em modelo SaaS.

R.TRSV.10A figura seguinte reflete o âmbito da Solução em modelo *on-prem* vs SaaS.

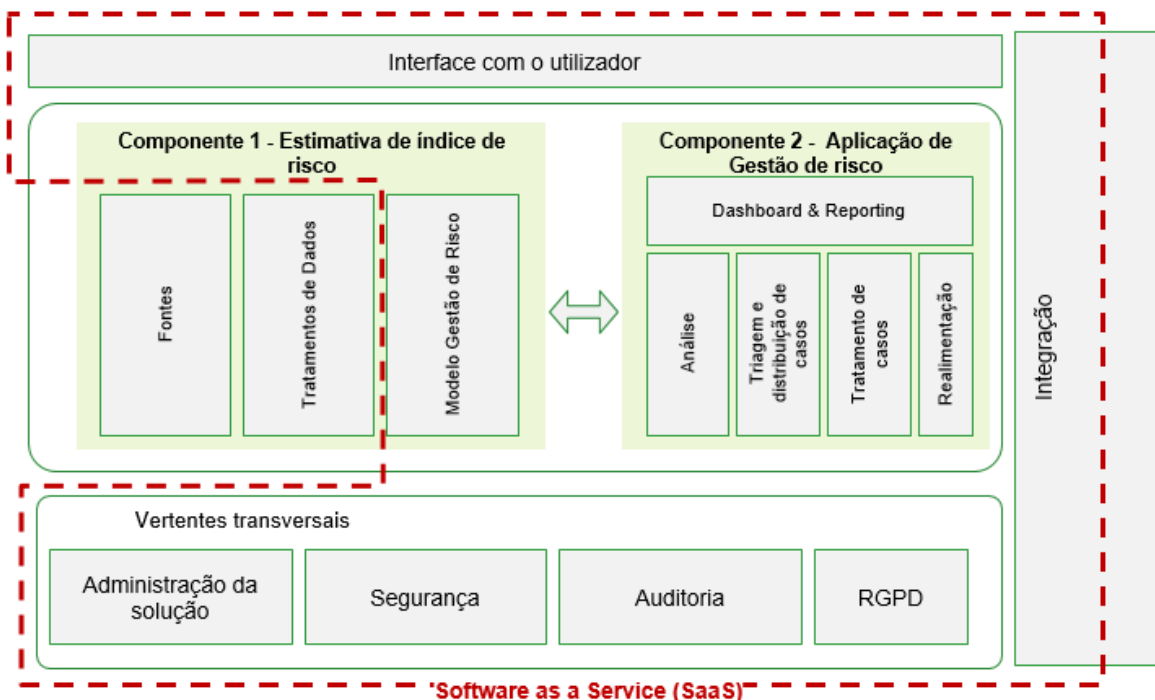


Figura 20 – Âmbito da Solução em modelo *On-Prem* vs. *SaaS*

R.TRSV.11 Para operacionalizar e oferecer o serviço SaaS, a EMPRESA PRESTADORA deverá incluir os componentes necessários para o efeito, desde infraestruturas e/ou componentes *cloud*, software e produtos base, Solução implementada no projeto, serviços de suporte e manutenção e administração e configuração necessários.

R.TRSV.12 No que respeita à forma como a integração será implementada, particularmente no caso de integração entre componentes SaaS (em *cloud*) com componentes *on-prem*, tal será definido em sede de execução do contrato tendo em conta os requisitos constantes da seção 2.4 Integração do presente Anexo e a descrição da Solução constante da proposta, respeitando as melhores práticas de segurança.

R.TRSV.13 A Solução no que respeita à sua vertente SaaS, deverá incluir:

- Componentes / consola para monitorização ou consulta do estado do serviço por parte do CONTRAENTE PÚBLICO;
- Estas componentes devem incluir a disponibilização de indicadores e informação sobre o serviço, quer através de *dashboards*, quer através de relatórios.

R.TRSV.14 No caso dos subcomponentes *on-cloud*, os dados:

- Devem ser encriptados (para os atributos que se considerem aplicáveis) antes do envio para *cloud*

- b. A descriptação deverá depois fazer-se no caso do regresso dos dados ao ambiente *on-prem*

R.TRSV.15 Ainda no caso de subcomponentes on-cloud:

- c. A arquitetura deverá corresponder a uma gestão multi-tenant. A infraestrutura não deverá ser partilhada entre diferentes tenants. Ou seja, no caso de existir mais do que uma organização/cliente a utilizar serviços no âmbito do contrato, cada organização deverá ter infraestrutura segregada, garantindo assim que não poderá ser afetada por qualquer outra organização que utilize a mesma Solução.
- d. Toda a infraestrutura que for criada para a organização deve ter IPs públicos dedicados que não sejam utilizados por qualquer outro eventual cliente da Solução. Desta forma pretende-se que os IPs utilizados pela organização nunca possam ser colocados em blacklists devido a comportamentos incorretos de outros clientes.

R.TRSV.16 Atendendo à natureza dos dados tratados pela Solução, o tratamento de dados tem de ser realizado integralmente dentro do espaço geográfico da União Europeia. Os serviços deverão ser prestados a partir de, pelo menos, dois centros de dados distintos situados na União Europeia, que ofereçam proteção elevada quanto ao risco sísmico e suficientemente afastados para oferecerem redundância.

2.5.3. Administração da SOLUÇÃO

R.TRSV.17 Requisito introdutório: Não obstante o modelo SaaS, a Solução deverá suportar processos de operação, administração e manutenção da Solução baseados nas melhores práticas do mercado. A Solução deve ainda ter um ambiente específico para a sua administração, à qual apenas utilizadores especialmente definidos poderão ter acesso. A Solução deve ainda disponibilizar uma consola para monitorização pelo CONTRAENTE PÚBLICO que permita a monitorização dos serviços, o seguimento de indicadores relativos aos níveis de desempenho e outros indicadores que sejam adequados.

R.TRSV.18 A Solução deverá permitir proceder a ações de manutenção regulares sem indisponibilidade da mesma, tirando partido das redundâncias existentes.

R.TRSV.19 A Solução deverá incluir mecanismos para a monitorização global do seu funcionamento.

R.TRSV.20 A Solução deverá usufruir de componentes de gestão / administração cloud, no contexto da plataforma de SaaS com descrita anteriormente.

R.TRSV.21A Solução deverá ter uma gestão de utilizadores e de acessos com possibilidade de articular com a Active Directory.

R.TRSV.22A Solução deverá incluir as diversas parametrizações conforme descrito nas secções 2.1 e 2.2 anteriores.

R.TRSV.23As diferentes parametrizações da Solução deverão poder ser administradas de forma centralizada.

2.5.4. Segurança

R.TRSV.24Requisito introdutório: A Solução deverá dispor de meios e mecanismos que garantam os princípios base da segurança:

- a. **Confidencialidade** – garantir que a informação só poderá ser acedida ou tratada por utilizadores com permissão para tal e de acordo com as necessidades específicas para a realização das respetivas funções;
- b. **Integridade da informação** – garantir que a informação tratada e gerada por qualquer dos utilizadores não é alterada ou corrompida, intencional ou acidentalmente, desde a sua criação até à respetiva eliminação, mantendo-a completa, sem supressões ou acréscimos, com particular atenção durante a sua circulação;
- c. **Disponibilidade** – desde que estejam reunidas as condições necessárias para acesso e tratamento da informação, nomeadamente a autenticação e autorização do utilizador, garantir que esta está atempadamente disponível.

R.TRSV.25O acesso de um utilizador a qualquer uma das componentes da Solução deverá implicar apenas um único procedimento de autenticação (*login*), mas sempre condicionado ao respetivo perfil de acesso e autorizações definidas.

R.TRSV.26As permissões têm de poder ser configuradas de modo a refletir as necessidades do modelo operacional e processos de negócio suportados.

R.TRSV.27A Solução terá de permitir a exportação integral dos dados que gere, de modo que o CONTRAENTE PÚBLICO possa efetuar a sua cópia para armazenamento remoto. Os dados assim exportados deverão ser suficientes para repor a situação à data da exportação.

R.TRSV.28Tendo em conta o modelo SaaS preconizado, a Solução irá contemplar medidas de forma a não colocar em causa a segurança dos dados e o cumprimento de normas, como seja o RGPD.

R.TRSV.29A EMPRESA PRESTADORA obriga-se ainda a adotar mecanismos de segurança pró-ativos, com recomendações de melhorias de segurança específicas.

2.5.5. Cibersegurança

R.TRSV.30A EMPRESA PRESTADORA obriga-se a cumprir o Quadro Nacional de Referência para a Cibersegurança do Centro Nacional para a Cibersegurança de Portugal.

R.TRSV.31 A ocorrência de incidentes de segurança determina o cumprimento pela EMPRESA PRESTADORA das seguintes obrigações específicas:

- a. Notificar o CONTRAENTE PÚBLICO no prazo de 1 hora a contar da deteção;
- b. Assim que possível, notificar o CONTRAENTE PÚBLICO dos procedimentos destinados a mitigar e eliminar as consequências do incidente;
- c. Notificar, assim que possível, o CONTRAENTE PÚBLICO da cessação do incidente, acompanhado do relatório com a informação relevante, designadamente, quanto aos danos provocados na informação deste.

2.5.6. Auditoria

R.TRSV.32 Requisito introdutório: A Solução deverá incluir mecanismos de registo, para efeitos de auditoria, de todas as ações realizadas, nomeadamente que impliquem manipulação de dados, bem como mecanismos específicos de pesquisa nos *logs* de fácil utilização (possibilitando a utilização de filtros por utilizador, por documentos), consulta e análise desses registos.

R.TRSV.33A Solução deverá manter registos de auditoria inalteráveis que capturem e armazenem automaticamente informações sobre:

- a. Ações desencadeadas direta ou indiretamente por um utilizador que incida sobre a Solução ou objeto de informação aí existente;
- b. Infrações (isto é, as tentativas de um utilizador para aceder a informação para a qual não tem acesso);
- c. Tentativas de infração cometidas contra mecanismos de controlo de acesso.

R.TRSV.34 Para efeitos do requisito anterior, consideram-se ações todas as operações realizadas sobre a Solução, sejam de consulta, inserção, alteração ou remoção.

R.TRSV.35 Para cada operação deverá ser registado: o tipo de operação, a informação acedida ou manipulada, valor inicial e final (se alterado), o momento em que foi efetuada, o utilizador que a desencadeou e a estação de trabalho utilizada.

R.TRSV.36A Solução deverá assegurar o registo de eventos de segurança, assim como o envio de alertas e notificações de segurança. Quer o registo de eventos de segurança quer o envio de alertas e notificações de segurança devem possuir um mecanismo de parametrização do nível de informação pretendido (ex.: todos

os eventos; só eventos relacionados com tentativas de violação de acesso, etc.).

R.TRSV.37A Solução deverá garantir que os registos de auditoria não podem ser modificados, seja de que forma for, nem eliminados por nenhum utilizador e devem poder ser reorganizados e copiados por administradores para suportes amovíveis sempre que necessário.

R.TRSV.38A Solução deverá garantir que, uma vez em operação e com os mecanismos de auditoria parametrizados, terá de acompanhar os acontecimentos sem intervenção manual, armazenando de forma automática os registos de auditoria de acordo com essa configuração.

R.TRSV.39A informação de auditoria deverá ser mantida por um período de tempo parametrizável.

R.TRSV.40A Solução deverá garantir que a criação e alteração da configuração dos registos de auditoria sejam, elas próprias, registadas para efeitos de auditoria.

R.TRSV.41A Solução deverá disponibilizar o acesso aos registos de auditoria a utilizadores com a permissão adequada, permitindo a análise da sequência de atividades efetuadas por qualquer utilizador, dentro do período de retenção da informação de auditoria.

R.TRSV.42A informação de auditoria deverá ser considerada informação confidencial pelo que deverá ser protegida contra alterações ou outros acessos indevidos.

R.TRSV.43 A Solução deverá possuir a capacidade de exportar uma seleção de registos de auditoria, sem afetar os registos de auditoria armazenados.

R.TRSV.44A Solução deverá, no mínimo, poder fornecer relatórios contemplando os registos de auditoria, permitindo especificar critérios de seleção apropriados.

2.5.7. Aplicação do RGPD

R.TRSV.45 Requisito introdutório: A Solução deverá estar concebida e implementada de modo a respeitar os seguintes princípios:

- a. **Privacy by Design** – a Solução tem de assegurar a conformidade com o RGPD no tratamento de dados pessoais ao longo do ciclo de vida de cada processo (para componentes a serem desenhadas de novo), ou
- b. **Privacy by Default** – a Solução tem de assegurar a conformidade com o RGPD no que diz respeito ao limite máximo de tempo de manutenção ou acesso dos dados para prossecução do objetivo.

R.TRSV.46A Solução terá de garantir, entre outros, a estrita aplicação de perfis não só ao acesso a funcionalidades, mas também no acesso a dados pessoais, a segurança no manuseamento de dados pessoais internamente, nas interfaces humanas e com outros sistemas, no armazenamento de dados pessoais e nas funcionalidades da auditoria do acesso a dados pessoais.

- R.TRSV.47A Solução deverá estar preparada para o respeito integral do RGPD no que respeita à segurança dos dados, à manutenção de dados, entre outros.
- R.TRSV.48A Solução deverá apresentar uma análise de impacto e medidas para o cumprimento do RGPD. A EMPRESA PRESTADORA deverá apresentar um documento de AIPD (Análise de Impacto de Proteção de Dados), elaborado na etapa de Conceção e concretização da arquitetura e na etapa de especificação funcional de cada ciclo de implementação. O documento deverá ser atualizado antes de cada entrada em produção. A EMPRESA PRESTADORA poderá propor a utilização de um *template* próprio ou utilizar o *template* disponibilizado pelo CONTRAENTE PÚBLICO.
- R.TRSV.49A Solução deverá ainda permitir conservar todos os documentos relativos ao tratamento de dados por forma a demonstrar o cumprimento com o Regulamento, por exemplo, resultados de avaliação de impacto de risco, políticas de privacidade, procedimentos que permitem o exercício dos direitos dos titulares dos dados, contratos com subcontratantes e evidências de consentimentos.
- R.TRSV.50Os dados pessoais deverão ser encriptados e/ou anonimizados em todas as situações em que estejam acessíveis às equipas técnicas de desenvolvimento, manutenção e administração da Solução.

3. Prestação dos Serviços

Os serviços a prestar para desenvolver, instalar, operacionalizar, disponibilizar e manter a Solução terão de cumprir os requisitos constantes deste capítulo.

3.1. Visão Geral

- R.IMP.1 Requisito introdutório: Tendo em conta o cumprimento dos objetivos no quadro de um calendário bem estabelecido e com o menor impacto possível nas operações normais, a prestação do SERVIÇO deverá seguir uma abordagem híbrida, apresentando resultados de uma forma faseada, utilizando uma metodologia Agile. O objetivo deste faseamento é assegurar, por um lado, que as equipas operacionais comecem a testar e a trabalhar na Solução e por outro permitir a incorporação do feedback da equipa de gestão de risco e equipas operacionais, como forma de melhoria nas entregas seguintes. É objetivo também que, para além do faseamento por áreas, existam entregas parciais das diversas componentes (principalmente dos motores) o que permitirá uma validação e calibração mais eficiente.
- R.IMP.2 A EMPRESA PRESTADORA deverá cumprir a abordagem da prestação do SERVIÇO, constante da proposta, tendo em conta as orientações apresentadas nos requisitos seguintes.
- R.IMP.3 A EMPRESA PRESTADORA deverá cumprir com a duração de cada fase constante da proposta tendo em conta os prazos mencionados no artigo 6º do caderno de encargos
- R.IMP.4 A prestação do SERVIÇO deve ser realizada de acordo com o seguinte encadeamento:

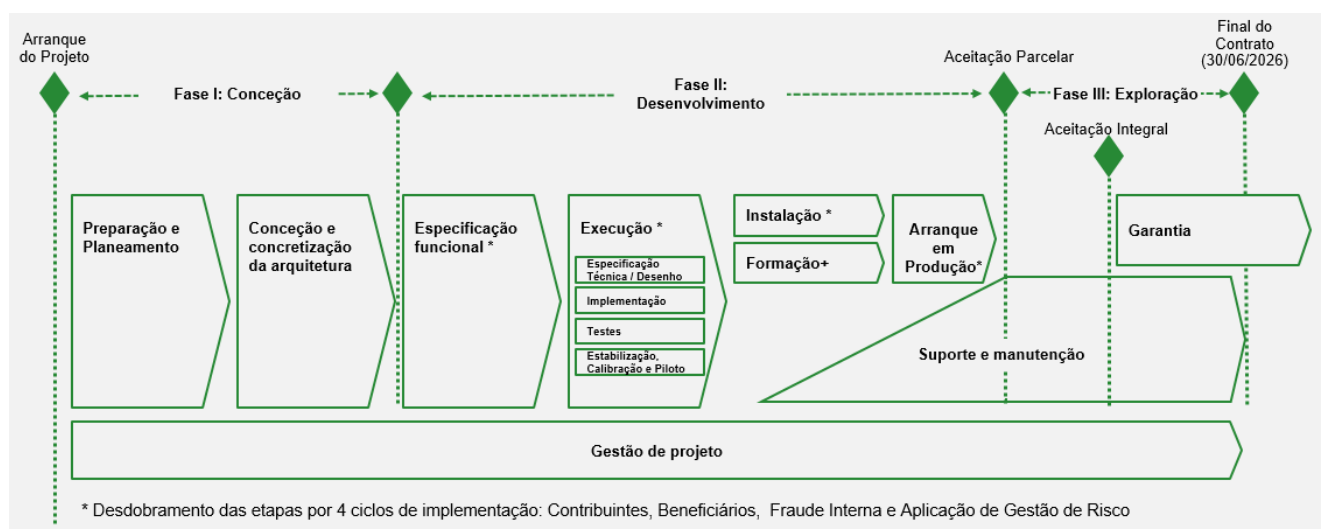


Figura 21 - Metodologia da prestação de serviço

- R.IMP.5 A fase de Conceção compreende as etapas:
- a. Preparação e Planeamento;
 - b. Conceção e concretização da arquitetura.
- R.IMP.6 A fase de Desenvolvimento compreende as etapas e subetapas:
- a. Especificação funcional;
 - b. Execução:
 - i. Especificação técnica / Desenho;
 - ii. Implementação;
 - iii. Testes;
 - iv. Estabilização, Calibração e Piloto.
 - c. Instalação;
 - d. Formação;
 - e. Arranque em produção (rollout);
 - f. Suporte e Manutenção para componentes que entrem em funcionamento gradual.
- R.IMP.7 A fase de Exploração compreende as etapas:
- a. Suporte e Manutenção
 - b. Garantia
 - c. Cessação
- R.IMP.8 Estas fases, etapas e subetapas, detalhadas de seguida, constituem blocos de trabalho obrigatórios da prestação do SERVIÇO.
- R.IMP.9 As fases do projeto apresentadas anteriormente deverão seguir uma abordagem de implementação faseada no tempo e dividida por 4 ciclos de implementação consoante as componentes e áreas desenvolvidas, que serão:
- Componente 1 – Contribuintes;
 - Componente 1 – Beneficiários;
 - Componente 2 - Aplicação de Gestão de Risco e
 - Componente 1 - Fraude Interna,
 - conforme o descrito na Figura 22 – Abordagem de implementação.

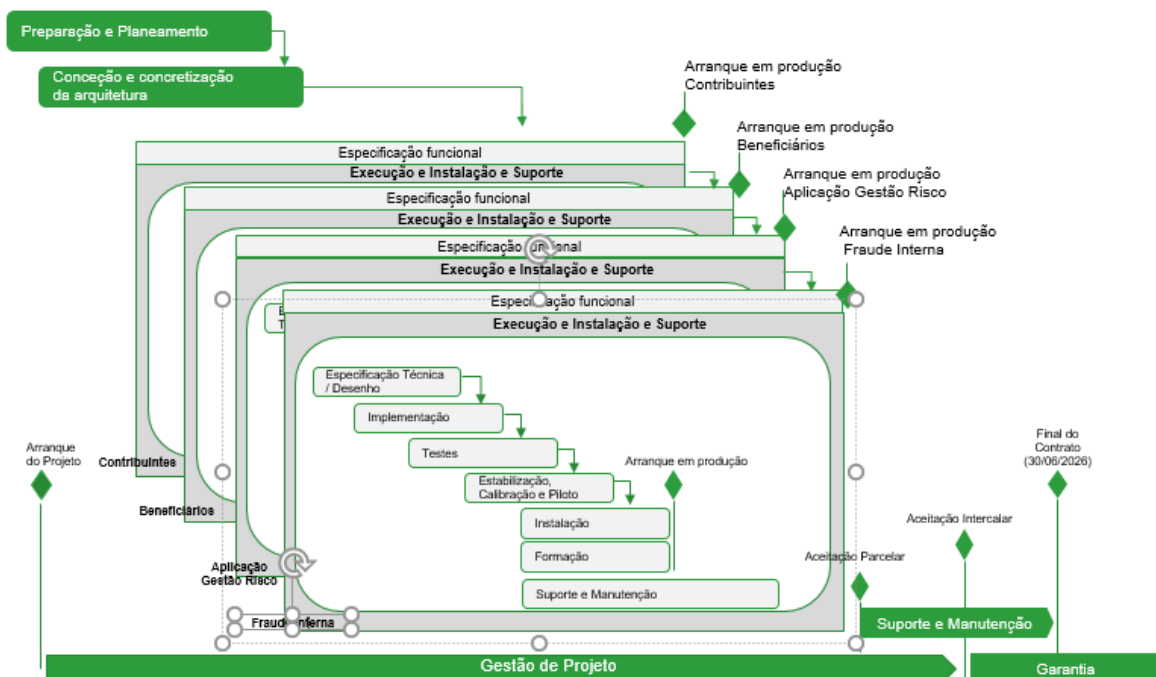


Figura 22 – Abordagem de implementação

- R.IMP.10 Pretende-se que a fase de desenvolvimento seja efetuada por ciclos de implementação que acontecem depois de forma encadeada, por cada uma das componentes/áreas de negócio referidas no ponto anterior.
- R.IMP.11 A Componente 1 - Contribuintes deverá constituir o primeiro ciclo de implementação, devendo considerar as vertentes em âmbito (Entidades Empregadoras; Trabalhadores Independentes; Serviço Doméstico e Desenvolvimento Social (este último a avaliar planeamento em sede de projeto)).
- R.IMP.12 A Componente 1- Beneficiários deverá constituir o segundo ciclo de implementação, devendo considerar também o âmbito definido anteriormente nomeadamente:
- Prestação de Desemprego;
 - Prestação de RSI;
 - Prestação de Doença;
 - Pensão de Velhice;
 - Pensão de Sobrevivência;
 - Pensão de Invalidez.
- R.IMP.13 A Componente 2 - Aplicação de Gestão de Risco deverá constituir o terceiro ciclo de implementação. A ordem dos ciclos de implementação poderá ser avaliada em sede de gestão de projeto.

- R.IMP.14 A Componente 1 - Fraude Interna deverá ser o último ciclo de implementação.
- R.IMP.15 Todos os ciclos de implementação deverão contemplar as subetapas de Especificação funcional, Execução, Instalação e Formação.
- R.IMP.16 No final de cada ciclo de implementação, a vertente implementada nesse ciclo entrará ARRANQUE EM PRODUÇÃO (ou piloto com dados reais, conforme decisão em sede de gestão de projeto).
- R.IMP.17 Após o ARRANQUE EM PRODUÇÃO de cada ciclo de implementação, será o momento de ACEITAÇÃO PARCELAR para o respetivo ciclo. A ACEITAÇÃO PARCELAR será efetuada nos termos do artigo 9º do caderno de encargos.
- R.IMP.18 A ACEITAÇÃO INTEGRAL, será efetuada, nos termos do artigo 10º do caderno de encargos e conforme descrito no capítulo 3.2.3 Fase III: Exploração.
- R.IMP.19 A etapa de Suporte e Manutenção Corretiva tem início com a primeira ACEITAÇÃO PARCELAR.
- R.IMP.20 A fase de Garantia inicia-se com a ACEITAÇÃO INTEGRAL.

3.2. Requisitos de Implementação

3.2.1. Fase I: Conceção

- R.IMP.21 Requisito introdutório: A fase de conceção tem por objetivo definir as medidas, a organização e as ferramentas necessárias à implementação da SOLUÇÃO, bem como a conceção e a concretização da arquitetura de toda a Solução.
- R.IMP.22 Esta fase só se considera concluída com a aceitação nos termos do artigo 8º do caderno de encargos.

3.2.1.1. Etapa de Preparação e Planeamento

- R.IMP.23 Requisito introdutório: A EMPRESA PRESTADORA deverá, durante esta etapa, estabelecer as várias ferramentas de gestão da prestação do SERVIÇO, como por exemplo a calendarização detalhada das atividades, a definição de papéis e responsabilidades, que irão reger as atividades subsequentes.
- R.IMP.24 Esta etapa inicia-se com o ARRANQUE DO PROJETO (AUTO DE CONSIGNAÇÃO) e termina com a validação da metodologia e ferramentas propostas para a gestão da prestação do SERVIÇO e aceitação do plano detalhado do projeto.
- R.IMP.25 A EMPRESA PRESTADORA deverá apresentar um plano detalhado do projeto com respeito pelo estipulado no artigo 6º do caderno de encargos, para aprovação pelo CONTRAENTE PÚBLICO, no prazo de 30 dias após o ARRANQUE DO PROJETO (AUTO DE CONSIGNAÇÃO). Considera-se conforme o plano detalhado se o CONTRAENTE PÚBLICO nada disser no prazo de 4 dias.

R.IMP.26 O plano de projeto deverá endereçar, no mínimo, as fases e etapas definidas na secção 3.1 Visão Geral e deverá especificar detalhadamente as atividades e *milestones* da prestação do SERVIÇO, como sejam as entregas de componentes de software ou documentação, bem como, a realização das ações de formação e de testes.

R.IMP.27 A EMPRESA PRESTADORA deverá realizar uma reunião de *kickoff* oficial de projeto no prazo de 20 dias a contar da assinatura do auto de consignação, em data a acordar pelas partes.

O CONTRAENTE PÚBLICO terá de dar resposta no máximo com 2 dias.

R.IMP.28 Nas reuniões de acompanhamento realizadas durante a execução do contrato e mencionadas no ponto 3.2.4.2. Anexo I, a EMPRESA PRESTADORA deverá apresentar a demonstração de desenvolvimento da SOLUÇÃO para cada entrega faseada.

3.2.1.2. Etapa de Conceção e concretização da arquitetura

R.IMP.29 Requisito introdutório: A EMPRESA PRESTADORA deverá, durante esta etapa, conceber e concretizar detalhadamente toda a arquitetura da SOLUÇÃO.

R.IMP.30 A EMPRESA PRESTADORA deverá desenhar a arquitetura da SOLUÇÃO, tendo como modelo orientativo a arquitetura apresentada, neste Caderno de Encargos, para a Componente 1 e Componente 2.

R.IMP.31 A EMPRESA PRESTADORA deverá detalhar a arquitetura da Componente 1 dividindo-a nos seguintes blocos e pela seguinte ordem:

- a. Preparação de dados;
- b. Motor de regras;
- c. Motor de aprendizagem;
- d. Motor de gestão de risco;
- e. Dashboard & Reporting;

R.IMP.32 A EMPRESA PRESTADORA deverá detalhar a arquitetura da Aplicação de Gestão de Risco, Componente 2, dividindo-a da seguinte forma e pela seguinte ordem:

- a. Análise;
- b. Triagem e distribuição de casos;
- c. Tratamento de casos de forma manual;
- d. Tratamento automático;
- e. Realimentação;
- f. Dashboard & Reporting.

R.IMP.33 A EMPRESA PRESTADORA deverá detalhar todos os componentes incluídos na arquitetura da Solução.

- R.IMP.34 A EMPRESA PRESTADORA deverá detalhar o modelo de dados da arquitetura da Solução.
- R.IMP.35 A EMPRESA PRESTADORA deverá incluir na arquitetura da Solução, as integrações necessárias, explicando-as em detalhe.
- R.IMP.36 A Fase de Conceção só se considera concluída com a aceitação nos termos do artigo 8º do caderno de encargos, dos seguintes documentos:
- Plano do Projeto, com especificação das atividades e milestones da prestação do serviço, como sejam as entregas de componentes de software ou documentação, bem como, a realização das ações de formação e de testes.
 - Documento de Visão (Conceção da Solução global, as suas componentes e subcomponentes);
 - Documento com a Arquitetura Global da Solução Global, referindo as duas componentes e respetivas subcomponentes;
 - Documentação a utilizar na Gestão de Projeto, designadamente, Relatório de Progresso, Plano de Comunicação, Gestão de Riscos, Lições aprendidas.
 - Documento com avaliação de impacto na proteção de dados (AIPD);

3.2.2. Fase II: Desenvolvimento

- R.IMP.37 Requisito introdutório: A EMPRESA PRESTADORA deverá, durante esta fase de Desenvolvimento, seguir a lógica de abordagem faseada conforme definido em 3.1 Visão Geral. Cada uma das etapas apresentadas de seguida será realizada para os 4 ciclos de implementação (Componente 1 - Contribuintes, Componente 1 - Beneficiários, Componente 2 - Aplicação de Gestão de Risco e Componente 1 - Fraude Interna).
- R.IMP.38 O CONTRAENTE PÚBLICO dispõe de 10 dias para realizar a validação preliminar dos entregáveis mencionados no número 1 do artigo 7º do caderno de encargos.

3.2.2.1. Etapa de Especificação funcional

- R.IMP.39 Requisito introdutório: A EMPRESA PRESTADORA deverá, durante esta etapa, proceder ao levantamento e caracterização de todos os requisitos funcionais, culminando numa especificação funcional da SOLUÇÃO, pelos ciclos de implementação conforme Figura 22 – Abordagem de implementação.
- R.IMP.40 Após uma atividade inicial para levantamento, análise e revisão de todos os requisitos funcionais junto dos elementos indicados pelo CONTRAENTE PÚBLICO (equipas de negócio), a EMPRESA PRESTADORA deverá elaborar a especificação funcional da SOLUÇÃO que submete à validação

preliminar pelo CONTRAENTE PÚBLICO nos termos do nº 1 do artigo 7º do caderno de encargos.

- R.IMP.41 A especificação funcional deverá contemplar a descrição detalhada das capacidades funcionais da SOLUÇÃO por ciclo.
- R.IMP.42 Para a especificação funcional, a EMPRESA PRESTADORA deverá realizar um mapeamento entre as capacidades funcionais e os requisitos, mencionados no presente Caderno de Encargos, numa matriz de rastreabilidade.
- R.IMP.43 Esta etapa só se considera concluída após validação preliminar nos termos do nº 1 do artigo 7º do caderno de encargos, do Documento de especificação funcional detalhado e da matriz de rastreabilidade e do documento de AIPD (Análise de Impacto de Proteção de Dados), elaborado na fase de especificação funcional de cada ciclo de implementação e atualizado na etapa de arranque em produção, se necessário.

3.2.2.2. Etapa de Execução

- R.IMP.44 Requisito introdutório: A etapa de execução tem por objetivo executar as medidas necessárias à implementação da SOLUÇÃO.
- R.IMP.45 A etapa de execução está dividida nas seguintes subetapas:
- Especificação técnica / Desenho;
 - Implementação;
 - Testes;
 - Estabilização, Calibração e Piloto.
- R.IMP.46 A etapa de execução dos ciclos de implementação da Componente 1, para além de faseada por área (Contribuintes, Beneficiários e Fraude Interna), terá de ser faseada por módulos conforme apresentado na Figura 23 - Etapas de execução da componente 1.

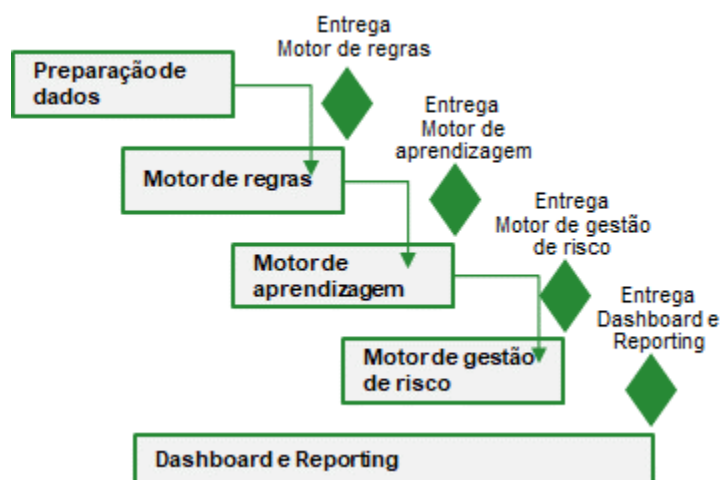


Figura 23 – Etapas de execução da componente 1

- R.IMP.47 Pretende-se que a etapa de execução, comece com a preparação dos dados, de seguida o motor de regras, o motor de aprendizagem, o motor de gestão de risco e por fim o módulo de *Dashboard e Reporting*.
- R.IMP.48 Para cada uma das componentes apresentadas, terão de ser realizadas todas as subetapas da etapa de execução (Especificação técnica / Desenho, Implementação, Testes, Estabilização, Calibração e Piloto).
- R.IMP.49 Só após a execução de cada uma destas subetapas para cada componente serão entregues:
- a. O Motor de regras;
 - b. O Motor de aprendizagem;
 - c. O Motor de gestão do risco;
 - d. A Aplicação de gestão do risco.
- R.IMP.50 Para a Aplicação de Gestão de Risco da Componente 2, terão de ser realizadas todas as subetapas da etapa de execução (Especificação técnica / Desenho, Implementação, Testes, Estabilização, Calibração e Piloto).
- R.IMP.51 Para efeitos de determinação da duração, esta etapa só se considera concluída, para cada ciclo de implementação, após validação preliminar, nos termos do nº 1 do artigo 7º do caderno de encargos, dos seguintes produtos/documentos descritos neste capítulo:
- a. Modelo de Dados e respetiva explicação em documento;
 - b. Documento com o desenho e especificação dos processos de extração, transformação e carregamento dos dados;
 - c. Documento com as indicações necessárias à instalação e configuração de componentes tecnológicas,
 - d. Documento de especificação técnica detalhada (cfr. R. IMP 56);
 - e. Documentos de “Relatório de progresso do projeto”;
 - f. Componentes tecnológicas referente ao ciclo de implementação:
 - i. O Motor de regras;
 - ii. O Motor de aprendizagem;
 - iii. O Motor de gestão do risco;
 - iv. A Aplicação de gestão do risco.
 - g. Documento “Manual de administração da Solução” (podendo o manual ser para utilização pelo próprio fornecedor no contexto do serviço SaaS que irá prestar);
 - h. Documento “Manual de utilização da Solução”;
 - i. Documento “Plano de testes”;

- j. Documento “Plano de formação”;
- k. Documentação de formação referente a cada ciclo de implementação, à medida que vão sendo desenvolvidas e entregues;
- l. Documento “Plano de Arranque em Produção”;
- m. Documento “FAQ de suporte”;
- n. Testes de Aceitação realizados;
- o. Documento “Plano de manutenção preventiva”;
- p. Documento “Relatório dos testes de aceitação”, incluindo relatórios de testes de segurança;
- q. Estabilização da Solução;
- r. Pilotos;
- s. Instalação em produção;
- t. ACEITAÇÃO PARCELAR.

3.2.2.2.1. Especificação técnica / Desenho

- R.IMP.52 Requisito introdutório: A EMPRESA PRESTADORA deverá, durante esta subetapa, proceder ao levantamento e caracterização de todos os requisitos técnicos / de desenho, culminando numa especificação técnica da Solução, por cada ciclo de implementação (referidas em 3.1 Visão Geral) e por componentes como referido em 3.2.2.2 Etapa de Execução.
- R.IMP.53 Após uma atividade inicial para levantamento, análise e revisão de todos os requisitos técnicos junto das equipas do CONTRAENTE PÚBLICO, a EMPRESA PRESTADORA deverá elaborar uma especificação técnica da Solução (para cada ciclo de implementação) que irá submeter à validação pelo CONTRAENTE PÚBLICO nos termos do nº 1 do artigo 7º do caderno de encargos
- R.IMP.54 A especificação técnica deverá contemplar a descrição detalhada da SOLUÇÃO, assim como das suas características e funcionalidades, por área ou subárea e componente.
- R.IMP.55 Para a especificação técnica, a EMPRESA PRESTADORA deverá realizar um mapeamento entre as características / funcionalidades da Solução e os requisitos, mencionados no presente Caderno de Encargos, numa matriz de rastreabilidade.
- R.IMP.56 A especificação referida no ponto anterior deverá contemplar, nomeadamente:
- a. Mapeamento entre características / funcionalidades da Solução e os requisitos contratados numa Matriz de Rastreabilidade;
 - b. Relatórios para extração e visualização da informação;
 - c. Documento de interface;

- d. Elementos de integração tecnológica com os SI/TI tal como determinado pelos requisitos de integração;
 - e. Estrutura de perfis e permissões;
 - f. Necessidades ao nível de infraestrutura, rede de comunicações e demais componentes a disponibilizar pelo CONTRAENTE PÚBLICO no que respeite a componentes on-prem e/ou elementos de interligação com *cloud*
 - g. Análise dos processamentos que abranjam dados pessoais.
- R.IMP.57 A EMPRESA PRESTADORA tem flexibilidade para definir a sua própria metodologia de desenho e construção da Solução, sem prejuízo do alinhamento com as atividades descritas, com as melhores práticas do mercado e com condições para se adaptar às práticas e realidade do CONTRAENTE PÚBLICO.
- R.IMP.58 A EMPRESA PRESTADORA apresentará a documentação do desenho e especificações técnicas, para validação pelo CONTRAENTE PÚBLICO, nos termos do nº 1 do artigo 7º do caderno de encargos

3.2.2.2.2. Implementação

- R.IMP.59 Requisito introdutório: A EMPRESA PRESTADORA deverá, durante esta subetapa, proceder à implementação da Solução considerando as especificações validadas como referido em 3.2.2.2 Etapa de Execução.
- R.IMP.60 O desenvolvimento da SOLUÇÃO deverá ser realizado sobre os ambientes preparados pela EMPRESA PRESTADORA no âmbito do contrato e para este efeito.
- R.IMP.61 Durante a implementação, terão de ser implementados os ciclos de entrega com os prazos definidos. Devem ser planeadas as versões da Solução tendo em conta o âmbito de cada entrega. O âmbito deve ser definido com base nas estimativas de entrega, risco e prioridades definidas pelo CONTRAENTE PÚBLICO. Esse facto implica entregar ao CONTRAENTE PÚBLICO as funcionalidades de maior valor primeiro e de carácter mais urgente, decididas por este nas reuniões de acompanhamento, em ordem à diminuição do risco do desenvolvimento da Solução.
- R.IMP.62 Durante esta subetapa, deverá existir uma comunicação constante entre as equipas de todas as partes envolvidas no projeto, devendo esta ocorrer de forma planeada, com periodicidade a definir entre o CONTRAENTE PÚBLICO e a EMPRESA PRESTADORA.
- R.IMP.63 O processo de implementação da Solução deve ser documentado, exposto e difundido entre o CONTRAENTE PÚBLICO e a EMPRESA PRESTADORA., para que quando um novo membro se junte à equipa, possa ter uma base de como o mesmo processo de implementação funciona;
- R.IMP.64 No decorrer desta etapa, a EMPRESA PRESTADORA deverá também elaborar a documentação relativa à SOLUÇÃO, incluindo o manual de

administração da Solução, mesmo que para utilização pela própria EMPRESA PRESTADORA no contexto do serviço SaaS (incluindo vertentes como instalação, parametrização, operação e administração), o manual de utilização da Solução, o plano de testes, o plano de formação, o plano de Arranque em Produção e a FAQ de suporte.

- R.IMP.65 Sempre que possível, deverá a EMPRESA PRESTADORA promover a realização de demonstrações e testes de funcionalidades à medida que sejam desenvolvidas, por forma a minimizar o risco de desajuste de expectativas.
- R.IMP.66 O plano de testes, para aprovação pelo CONTRAENTE PÚBLICO, deverá contemplar todos os casos de teste.
- R.IMP.67 É parte integrante do Plano de Testes, o cruzamento entre cada caso de teste e a Matriz de Rastreabilidade produzida nas especificações funcionais e técnicas da SOLUÇÃO.
- R.IMP.68 O plano de formação deverá incluir a identificação dos formadores, incluindo o nome, qualificações, experiência no desenvolvimento da Solução e envolvimento na prestação do SERVIÇO.
- R.IMP.69 O plano de Arranque em produção da SOLUÇÃO, para aprovação pelo CONTRAENTE PÚBLICO, deverá considerar as vertentes *on cloud* e *on-prem*, devendo contemplar necessidades de suporte das equipas informáticas e dos utilizadores do CONTRAENTE PÚBLICO e demais informações necessárias a um Arranque em produção.
- R.IMP.70 A FAQ de suporte deverá constituir um guião que permita o correto despiste, encaminhamento e resolução dos pedidos de suporte, podendo a mesma ser para utilização pela própria EMPRESA PRESTADORA no contexto do serviço SaaS.

3.2.2.2.3. Testes

- R.IMP.71 Requisito introdutório: A EMPRESA PRESTADORA deverá, durante esta etapa, executar e acompanhar a realização dos testes que irão comprovar o correto desenvolvimento da SOLUÇÃO e executar as necessárias ações de formação considerando as especificações validadas para a área, subárea por componentes como referido em 3.2.2.2 Etapa de Execução.

A participação do CONTRAENTE PÚBLICO nos testes poderá envolver, caso seja necessário, a execução dos seus próprios testes.

- R.IMP.72 A validação pelo CONTRAENTE PÚBLICO do plano de testes nos termos do nº 1 do artigo 7º do caderno de encargos, é condição prévia para o início dos testes.
- R.IMP.73 A EMPRESA PRESTADORA deverá contemplar, planear e realizar diversos tipos de testes. A metodologia de testes terá de ser adaptada à natureza das componentes da Solução. No mínimo deverão ser realizados os seguintes tipos de testes:

- a. Testes de componentes: testes sob inteira responsabilidade da EMPRESA PRESTADORA durante os quais as suas equipas verificam a qualidade dos componentes que irão constituir a SOLUÇÃO, individualmente e entre si. O CONTRAENTE PÚBLICO não participa nestes testes;
- b. Testes de sistema: testes à SOLUÇÃO e integrações com sistemas externos, visando aferir a qualidade, segurança e cumprimento de todos os requisitos pela SOLUÇÃO (incluindo a capacidade para suportar o seu dimensionamento máximo). Estes testes estão naturalmente limitados às funcionalidades e capacidades não dependentes da operacionalização da SOLUÇÃO. O CONTRAENTE PÚBLICO participa nestes testes.

Estes testes de sistema englobam testes funcionais, nomeadamente:

- Testes às funcionalidades das diferentes componentes da Solução
- Testes à interface do utilizador
- Testes de integridade dos serviços e dados.

E englobam testes não funcionais, que deverão ser realizados sempre que aplicável, nomeadamente:

- Testes de estabilidade (Fiabilidade da aplicação)
- Testes de usabilidade;
- Testes de failover / recuperação;
- Testes de autenticação e testes de controle de acessos;
- Testes de configuração;
- Testes de instalação e compatibilidade;
- Testes batch;
- Testes de concorrência;
- Testes de acessibilidade;
- Testes de segurança (Análise de Vulnerabilidades/Testes de Penetração);
- Testes de volume;
- Testes de carga/stress (Performance);
- Testes de alta disponibilidade.

- c. Testes específicos prévios à aceitação: testes que visam aferir a qualidade e cumprimento de todos os requisitos da SOLUÇÃO, de acordo com a especificação detalhada. O CONTRAENTE PÚBLICO participa nestes testes.

Incluem, entre outros e sempre que aplicável:

- Testes às funcionalidades que satisfazem os requisitos e necessidades do contraente público;
- Testes à Interface do Utilizador e facilidade de utilização;
- Testes à estabilidade do sistema (o sistema não deverá ter erros críticos);
- Testes de Regressão, sempre que aplicável;
- Testes de Configuração;

- d. Testes de Manutenção evolutiva e corretiva: testes que se realizam a cada nova entrega realizada quando ocorra a correção de erros ou alterações e/ou novas funcionalidades. Visam garantir que o software foi alterado corretamente antes de ser colocado em produção. Inclui testes de unidade, integração, sistema e, se necessário, de aceitação. Devem-se efetuar testes de regressão (repetição de testes realizados anteriormente) para garantir que as alterações não causaram defeitos em funcionalidades que anteriormente estavam corretas. O CONTRAENTE PÚBLICO participa nestes testes.

As alterações podem ser:

- Correções de erros detetados;
- Melhorias (algoritmos mais eficientes);
- Adaptações;
- Introdução, modificação ou remoção de certas funcionalidades;
- Adaptação do sistema a novas plataformas;

Dada a sua natureza, sempre que possível, devem-se automatizar os testes de regressão para facilitar a sua repetição, considerando o uso de ferramentas existentes para este efeito.

- R.IMP.74 A EMPRESA PRESTADORA é responsável pela preparação (incluindo a geração de casos e dados de teste) e execução dos testes. Os scripts de teste, sempre que aplicável, deverão ser validados pelo CONTRAENTE PÚBLICO, nos termos do nº 1 do artigo 7º do caderno de encargos.
- R.IMP.75 Para efeitos de cumprimento desta etapa, a EMPRESA PRESTADORA em colaboração com o CONTRAENTE PÚBLICO deverá:
- a. Testar autonomamente, todos os módulos da SOLUÇÃO;
 - b. Instalar e configurar a SOLUÇÃO (em ambiente de qualidade) seguindo os passos descritos no manual de administração da SOLUÇÃO;
 - c. Iniciar as ações de formação que permitam suportar a realização de testes da SOLUÇÃO;
 - d. Executar o carregamento de dados que suportem os testes (em ambiente de qualidade e/ou conforme a Solução definida, nomeadamente no que respeita a *machine learning*).
- R.IMP.76 Durante os testes, a EMPRESA PRESTADORA deverá manter um registo detalhado do progresso dos testes, assim como das não conformidades detetadas, das dúvidas que possam surgir, a sua análise e data prevista de resolução. As não conformidades não se limitam estritamente aos casos de teste e resultados esperados – a verificação do cumprimento de alguns requisitos poderá não se coadunar, na prática, com a criação de casos de teste específicos, materializando-se em observações ao longo dos testes e na utilização livre da Solução – ainda assim, as não conformidades terão sempre por base os requisitos.

- R.IMP.77 A EMPRESA PRESTADORA é responsável pela realização de um documento sumário, por cada atividade de teste, em que detalha os resultados obtidos, incluindo não conformidades resolvidas e por resolver.
- R.IMP.78 A EMPRESA PRESTADORA documentará num relatório dos testes de aceitação, para cada caso de teste, (i) o seu resultado, (ii) em caso de insucesso, ações de mitigação e corretivas, (iii) criticidade das falhas, (iv) eventuais datas da realização de novos testes e (v) o plano de resolução das não conformidades detetadas.
- R.IMP.79 Os testes deverão demonstrar o correto e completo funcionamento da SOLUÇÃO, considerando todas as suas componentes e a integração com sistemas externos.

3.2.2.2.4. Estabilização, Calibração e Piloto

- R.IMP.80 Requisito introdutório: A validação dos entregáveis concluídos deverá obedecer a um processo envolvendo a EMPRESA PRESTADORA e o CONTRAENTE PÚBLICO. No caso do software, esta validação envolve a estabilização da SOLUÇÃO após aceitação dos testes.
- R.IMP.81 A EMPRESA PRESTADORA deverá disponibilizar pilotos por âmbito conforme referido em 3.2.2.2 Etapa de Execução.
- R.IMP.82 A EMPRESA PRESTADORA deverá, por cada piloto, proceder à estabilização, através das correções necessárias dos problemas identificados pela equipa de testes durante a execução dos testes. Esta etapa pode ocorrer em paralelo com a conclusão dos testes.

3.2.2.3. Etapa de Instalação e Arranque em Produção

- R.IMP.83 Requisito introdutório: A EMPRESA PRESTADORA deverá, durante esta etapa, realizar a entrega da SOLUÇÃO aceite com a documentação de formação, documento de Arranque de produção, documento de utilização da SOLUÇÃO e guia de manutenção, por áreas e subáreas em análise (referidas em 3.1 Visão Geral).
- R.IMP.84 Quando a SOLUÇÃO estiver validada pelo CONTRAENTE PÚBLICO ocorre a etapa de entrega, passando a SOLUÇÃO a produção e arrancando assim o serviço SaaS a cargo da EMPRESA PRESTADORA.
- R.IMP.85 Esta etapa tem início com o fim da etapa Estabilização, Calibração e Piloto.
- R.IMP.86 Para efeitos de cumprimento desta etapa, a EMPRESA PRESTADORA em colaboração com o CONTRAENTE PÚBLICO deverá:
- Completar as ações de formação previstas;
 - Na Solução, executar a importação e carregamento de dados operacionais e dados mestre no ambiente de produção, com o acompanhamento do CONTRAENTE PÚBLICO, tendo por base o manual de administração da SOLUÇÃO a fornecer pela EMPRESA PRESTADORA;

- c. Realizar a instalação e configuração da Solução no ambiente de produção – Arranque em Produção.
 - d. Entrega do documento AIPD (Análise de Impacto de Proteção de Dados) atualizado, se necessário.
- R.IMP.87 Para a realização desta etapa, a EMPRESA PRESTADORA deverá contemplar a adoção de uma abordagem de transferência de conhecimento que maximize a apropriação de conhecimentos sobre a SOLUÇÃO pelo CONTRAENTE PÚBLICO de modo a garantir que este tenha condições para desenvolver as atividades da sua responsabilidade, como sejam monitorização do serviço SaaS a prestar pela EMPRESA PRESTADORA, controlar o cumprimento dos níveis de desempenho e reportar *issues* ou pedidos à EMPRESA PRESTADORA.
- R.IMP.88 A ACEITAÇÃO PARCELAR será no final da etapa de Arranque de Produção, para cada ciclo de implementação, nos termos do artigo 9º do caderno de encargos.

3.2.2.4. Etapa de Formação

- R.IMP.89 Esta etapa poderá ser em simultâneo com a de Instalação.
- R.IMP.90 A EMPRESA PRESTADORA deverá assegurar, por meios próprios, a formação necessária ao uso e monitorização da Solução. Deve também incluir formação para as suas próprias equipas e formação que seja de alguma forma aplicável ao CONTRAENTE PÚBLICO, não obstante o modelo SaaS, isto no que refere a operação, administração e manutenção da Solução.
- R.IMP.91 As ações de formação dirigidas ao CONTRAENTE PÚBLICO deverão ser realizadas nas instalações do mesmo, sendo garantidos pela EMPRESA PRESTADORA os seguintes meios:
- a. Comunicações de dados para a Solução;
 - b. Meios audiovisuais de apoio à formação.
- R.IMP.92 As ações de formação poderão ser realizadas de forma remota desde que solicitado e aprovado pelo CONTRAENTE PÚBLICO, cabendo à EMPRESA PRESTADORA a necessária adaptação de meios e métodos para a sua realização.
- R.IMP.93 As ações de formação a ministrar pela EMPRESA PRESTADORA, serão dirigidas ao conjunto de utilizadores indicados pelo CONTRAENTE PÚBLICO
- R.IMP.94 A efetividade da formação deverá ser avaliada, procedendo-se a novas sessões (eventualmente em moldes mais simples) em caso de necessidade.

3.2.3. Fase III: Exploração

- R.IMP.95 Para efeitos de determinação da duração, esta fase só se considera concluída após validação preliminar, nos termos do nº 1 do artigo 7º do caderno de encargos, dos seguintes produtos/documentos descritos neste subcapítulo:
- a. Documentos “Manuais de formação”, tendo em conta os vários perfis;
 - b. Execução das ações de formação que ainda possam ser necessárias de acordo com o respetivo plano;
 - c. Suporte à SOLUÇÃO em produção durante a etapa de Suporte e Manutenção;
 - d. Resolução de todos os problemas técnicos identificados no Relatório dos Testes de Aceitação, assim como daqueles identificados antes da ACEITAÇÃO INTEGRAL;
 - e. Documento “FAQ de suporte” atualizado;
 - f. ACEITAÇÕES PARCELARES e ACEITAÇÃO INTEGRAL.
 - g. Relatório final

3.2.3.1. Etapa de Suporte e Manutenção

- R.IMP.96 Requisito Introdutório: Esta etapa engloba atividades de suporte à exploração, manutenção preventiva e corretiva e evolutiva da SOLUÇÃO e serviços de administração/configuração da Solução on-going. A etapa tem início com a entrada em exploração do 1º ciclo.
- R.IMP.97 A EMPRESA PRESTADORA deverá, durante esta etapa, disponibilizar apoio técnico de manutenção com acompanhamento permanente para monitorizar a estabilidade e desempenho da Solução, devendo ainda possuir capacidade de intervenção rápida, de modo a maximizar a operacionalidade da Solução e evitar a disrupção do serviço no período após o Arranque em Produção, pelos ciclos de implementação (referidas em 3.1 Visão Geral).
- R.IMP.98 A Manutenção evolutiva desenvolve-se até ao termo do SaaS.
- R.IMP.99 Para efeitos de cumprimento desta etapa, a EMPRESA PRESTADORA deverá, no que se refere ao Suporte à Exploração:
- a. Prestar suporte e monitorizar à SOLUÇÃO em produção, incluindo a monitorização da plataforma que suporta toda a vertente disponibilizada em modelo SaaS;
 - b. Prestar apoio técnico para análise de incidentes que possam ocorrer durante a operação da SOLUÇÃO;
 - c. Resolver os problemas técnicos identificados no Relatório dos Testes de Aceitação;
 - d. Resolver qualquer tipo de problema técnico que ocorra com a SOLUÇÃO;

- e. Disponibilizar e, de acordo com as boas práticas, instalar *patches* e *hotfixes* à SOLUÇÃO;
- f. Avaliar o estado e desempenho das bases de dados e sistemas de suporte à SOLUÇÃO e proceder à sua otimização;
- g. Prestar apoio técnico de aconselhamento em aspetos relacionados com a utilização da SOLUÇÃO;
- h. Cumprir os níveis de serviço descritos no Capítulo 4 – Níveis de desempenho e penalidades (Considerados apenas após a ACEITAÇÃO PARCELAR).
- i. Manter atualizada a FAQ de suporte e demais documentação técnica.

R.IMP.100 No contexto desta etapa, a EMPRESA PRESTADORA obriga-se ainda a prestar a seguinte informação ao CONTRAENTE PÚBLICO:

- a. Informação sobre cumprimento de standards relevantes do serviço;
- b. Relatórios de auditoria efetuados por entidades reconhecidamente independentes;
- c. Informação online do estado dos diferentes serviços da Solução (disponibilidade e desempenho) e histórico de incidentes, com periodicidade mensal;
- d. Comunicação proactiva das falhas do serviço

R.IMP.101 No âmbito da Manutenção Preventiva e Corretiva e dos Serviços de Administração / configuração da Solução on-going, a EMPRESA PRESTADORA deverá assegurar o seguinte:

- a. Cumprir o plano de manutenção preventiva validado pelo CONTRAENTE PÚBLICO, nos termos do nº 1 do artigo 7º do caderno de encargos;
- b. Analisar eventuais incidentes que prejudiquem a operação da SOLUÇÃO;
- c. Realizar as ações tendentes a manter em boas condições de funcionamento os componentes (de HARDWARE, *software* ou documentos) da sua responsabilidade no âmbito do CONTRATO;
- d. Corrigir todos e quaisquer problemas técnicos nos serviços ou produtos entregues. Os defeitos compreendem, mas não se limitam a esses casos, as falhas, avarias e imperfeições detetadas nos serviços ou produtos entregues, a ausência de objeto ou de documentação obrigatórios e qualquer outra ocorrência que impeça o funcionamento normal do SERVIÇO contratado ou que não se apresente dentro dos padrões e níveis de qualidade predefinidos (exemplo de possível situação de defeito: avarias de hardware, código que contenha erros, vulnerabilidades, assim como falta de enquadramento na arquitetura tecnológica do CONTRAENTE PÚBLICO) incluindo a reparação ou substituição dos componentes que apresentem defeitos ou anomalias;

- e. Disponibilizar e, de acordo com as boas práticas, instalar *patches* e *hotfixes* à SOLUÇÃO, entre outros, as correções de erros identificados pelos fabricantes, bem como as *minor releases*, correspondentes à versão instalada na SOLUÇÃO, sem provocar falhas de serviço;
- f. Prestar apoio técnico de aconselhamento em aspetos relacionados com a utilização da SOLUÇÃO;
- g. Avaliar o estado e desempenho das bases de dados e demais componentes de software da Solução e sua otimização;
- h. Apoiar o Contraente público no processo de gestão de alterações relacionadas com a SOLUÇÃO;
- i. Realizar os testes necessários após qualquer alteração com potencial impacto na SOLUÇÃO;
- j. Reinstalar e recolocar as definições em condições normais de uso, quando aplicável;
- k. Prestar apoio técnico de aconselhamento aos vários tipos de utilizadores e administradores em aspetos relacionados com a utilização e gestão da SOLUÇÃO;
- l. Manter atualizada toda a documentação de suporte e o código fonte.

R.IMP.102 As ações referidas nos requisitos anteriores serão realizadas sem qualquer encargo adicional para o CONTRAENTE PÚBLICO.

R.IMP.103 Para efeitos de Manutenção Evolutiva, a EMPRESA PRESTADORA deverá, a pedido do CONTRAENTE PÚBLICO acompanhado da indicação dos trabalhos, apresentar um orçamento com o número de horas e o prazo de execução, no prazo de 5 dias. A EMPRESA PRESTADORA obriga-se a iniciar os trabalhos no prazo de 10 dias a contar da aceitação do orçamento pelo CONTRAENTE PÚBLICO.

R.IMP.104 No âmbito da Manutenção Evolutiva, a EMPRESA PRESTADORA deverá assegurar:

- a. Desenvolvimento de novas funcionalidades ou alteração de funcionalidades existentes, após análise e especificação pelo CONTRAENTE PÚBLICO;
- b. Estes desenvolvimentos serão prestados segundo a mesma metodologia empregue no desenvolvimento da SOLUÇÃO, nomeadamente no que respeita ao desenho, implementação, testes, formação, elaboração de documentação, instalação e manutenção.

R.IMP.105 A EMPRESA PRESTADORA deverá garantir o bom funcionamento do modelo e das equipas de suporte, medindo os resultados do trabalho de suporte e afinando o modelo de forma a melhorar o SERVIÇO.

R.IMP.106 A EMPRESA PRESTADORA deverá destacar técnicos seus com as competências necessárias para apoiar eficazmente o CONTRAENTE PÚBLICO (local ou remotamente) durante toda a duração desta etapa. Estes técnicos

deverão ter uma alocação próxima de 100%, apresentando disponibilidade para intervenção imediata na realização das atividades descritas nesta etapa.

R.IMP.107 A EMPRESA PRESTADORA deverá disponibilizar um número de contacto telefónico para reporte de incidentes, criando o registo dos mesmos num sistema auditável que permita aferir o cumprimento dos níveis de serviços contratados.

R.IMP.108 A ACEITAÇÃO INTEGRAL ocorrerá nos termos do artigo 10º do caderno de encargos.

3.2.3.2. Etapa de Garantia

R.IMP.109 À garantia aplica-se o artigo 14º do caderno de encargos e as disposições seguintes

R.IMP.110 Ao abrigo da GARANTIA, a EMPRESA PRESTADORA garante:

- a. Analisar eventuais incidentes que prejudiquem a operação da SOLUÇÃO;
- b. Realizar as ações tendentes a manter em boas condições de funcionamento os componentes (de hardware, software ou documentos) da sua responsabilidade no âmbito do CONTRATO;
- c. Corrigir todos e quaisquer defeitos nos serviços ou produtos entregues. Os defeitos compreendem, mas não se limitam a esses casos, as imperfeições detetadas nos serviços ou produtos entregues, a ausência de objeto ou de documentação obrigatórios e qualquer outra ocorrência que impeça o funcionamento normal do serviço contratado ou que não se apresente dentro dos padrões e níveis de qualidade predefinidos (Exemplo de possível situação de defeito: código que contenha erros, vulnerabilidades ou de difícil manutenção, assim como não se enquadrarem na arquitetura tecnológica do CONTRAENTE PÚBLICO) incluindo a reparação ou substituição dos componentes que apresentem defeitos ou anomalias;
- d. Disponibilizar *patches* e *hotfixes* à SOLUÇÃO;
- e. Prestar apoio técnico de aconselhamento em aspetos relacionados com a utilização da SOLUÇÃO.

R.IMP.111 Sem prejuízo do momento de início desta etapa, qualquer defeito ou anomalia detetado durante qualquer etapa da prestação do SERVIÇO, com potencial impacto no bom desenrolar do SERVIÇO, deverá ser reparado ou substituído de modo a minimizar tal impacto.

R.IMP.112 A aceitação do serviço pelo CONTRAENTE PÚBLICO não suprime a responsabilidade da EMPRESA PRESTADORA pela correção de todos os defeitos identificados no quadro de duração desta etapa.

R.IMP.113 O facto de a EMPRESA PRESTADORA proceder a uma intervenção com vista a realizar uma correção, não a dispensa de penalidades e de outras

sanções previstas no contrato, assim como dos prazos definidos para a sua execução.

R.IMP.114 Em nenhuma hipótese serão pagas as intervenções da EMPRESA PRESTADORA por motivos de ativação da garantia.

R.IMP.115 O CONTRAENTE PÚBLICO poderá realizar avaliações, auditorias, validações e verificações adicionais aos serviços e produtos entregues, por meios próprios ou recorrendo a entidades terceiras, recusando-os caso seja encontrado algum defeito face aos requisitos apresentados, solicitando a ativação dos serviços de garantia. Os custos a incorrer pelo CONTRAENTE PÚBLICO neste contexto são da sua responsabilidade.

3.2.3.3. Etapa da Cessação

R.IMP.116 A EMPRESA PRESTADORA deve apresentar, em sede de proposta, a estratégia de saída que propõe adotar para a passagem de *know-how* para as equipas a designar pelo CONTRAENTE PÚBLICO e a transferência da plataforma, contemplando os seguintes cenários:

- a. Saída para infraestrutura *on-prem* do CONTRAENTE PÚBLICO
- b. Saída para outra *Cloud* (de tecnologia distinta);

R.IMP.117 Por forma a garantir a cessação e transferência da SOLUÇÃO para o CONTRAENTE PÚBLICO, a EMPRESA PRESTADORA terá de apresentar uma lista detalhada de todo o software base e/ou de suporte à SOLUÇÃO.

R.IMP.118 A lista de software referida no requisito anterior deverá ser apresentada, desde logo em sede de proposta, sendo depois sujeita a atualização no final da etapa de “Especificação técnica / desenho”. Nessa altura, a EMPRESA PRESTADORA irá apresentar uma lista detalhada desse software.

R.IMP.119 A EMPRESA PRESTADORA vai apresentar, desde logo em sede de proposta e também no final da etapa de “Especificação técnica / desenho”, as formas que o CONTRAENTE PÚBLICO tem ao seu dispor para ter acesso / utilizar o software referido nos dois requisitos anteriores, mesmo após a cessação do serviço com a EMPRESA PRESTADORA. O CONTRAENTE PÚBLICO tem de ter ao seu dispor opções / serviços de mercado para continuar a utilizar o software referido.

R.IMP.120 No que refere a componentes de software implementadas e/ou adaptadas especificamente no âmbito do projeto, assim como configurações específicas no âmbito do projeto, a EMPRESA PRESTADORA obriga-se a apresentar os elementos da Solução em formatos que permitam a sua importação, adaptação, carregamento ou instalação noutra *Cloud ou on-prem*. Tal incluirá código fonte, código compilado, ficheiros de configuração, modelos de dados, bases de dados e todos os elementos necessários ao funcionamento da SOLUÇÃO.

- R.IMP.121 A estratégia de saída será depois detalhada em sede de implementação de projeto, devendo então incluir a elaboração de um plano de transferência de *know-how* que inclua:
- a. Formação à equipa a identificar pelo CONTRAENTE PÚBLICO
 - b. Transferência de todos os manuais técnicos dos equipamentos e/ou componentes da SOLUÇÃO e formas de acesso remoto aos mesmos, as configurações atuais existentes, o registo de incidentes e de *backlogs* e o inventário atualizado.
 - c. Toda a documentação de suporte deverá ser fornecida em suporte digital, incluindo os manuais de instalação, configuração e operação.
- R.IMP.122 O plano de implementação da estratégia de saída, elaborado com base na estratégia de saída mencionada na proposta, deve ser apresentado ao CONTRAENTE PÚBLICO no prazo de 270 dias a contar da assinatura do auto de consignação.
- R.IMP.123 Ocorrendo mudança de fornecedor, a transferência da Solução e a transferência do conhecimento deverá iniciar-se no prazo de 15 dias a contar da notificação do CONTRAENTE PÚBLICO.
- R.IMP.124 Toda a informação deve ser fornecida em formatos neutros e padronizados que possibilitem a sua portabilidade. Os dados do CONTRAENTE PÚBLICO devem permanecer acessíveis para qualquer função de migração durante pelo menos 120 dias após término da prestação do serviço, período este passível de ser ajustado mediante acordo entre as partes.
- R.IMP.125 Aquando da cessação do contrato, qualquer que seja o motivo, ou a simples pedido do Contraente Público, a EMPRESA PRESTADORA restituir-lhe-á, no prazo de 10 dias, uma cópia de todos os dados tratados no mesmo formato usado aquando da transmissão ou, não sendo possível, num formato estruturado e de uso comum.
- R.IMP.126 Os dados do CONTRAENTE PÚBLICO devem ser eliminados pela EMPRESA PRESTADORA, no prazo de 20 dias a contar do pedido do CONTRAENTE PÚBLICO. Deverão ser apresentadas evidências desta ação no prazo de 30 dias após a eliminação.

3.2.4. Outros requisitos de implementação

3.2.4.1. Equipa de trabalho

- R.IMP.127 A EMPRESA PRESTADORA terá de assegurar uma equipa com a dimensão, organização, competências e certificações necessárias para que possa planear e realizar as atividades previstas e efetuar a necessária articulação com o CONTRAENTE PÚBLICO.

A substituição dos recursos humanos propostos pela empresa prestadora ocorre nos termos do nº6 do artigo 75º do CCP.

R.IMP.128 Deverá estar sempre nomeado por parte da EMPRESA PRESTADORA um encarregado de proteção de dados – função da EMPRESA PRESTADORA que assegura as responsabilidades de proteção dos dados e conformidade do RGPD no contexto do CONTRATO.

R.IMP.129 A equipa de projeto deve conter, no mínimo, os seguintes elementos e perfis, sendo que todos os elementos têm de cumprir todas as alíneas do respetivo perfil:

- a. Gestor de projeto (1 elemento)
 - i. Licenciatura ou grau académico superior na área das Tecnologias de Informação e Comunicação ou similar;
 - ii. Certificação válida em PMP (*Project Management Professional*) pelo *Program Management Institute* ou similar;
 - iii. Experiência profissional mínima de 10 (dez) anos em gestão de projetos;
 - iv. Experiência profissional mínima de 2 (dois) anos em gestão de projetos de *Machine Learning* ou Inteligência Artificial.
- b. Arquiteto de *Software* (mínimo 1 elemento)
 - i. Licenciatura ou grau académico superior na área das Tecnologias de Informação e Comunicação ou similar;
 - ii. Experiência profissional mínima de 5 (cinco) anos em projetos como arquiteto de *software*;
 - iii. Experiência profissional em pelo menos 2 projetos de integração, desenvolvimento e implementação de sistemas de informação que incluam componentes da SOLUÇÃO.
- c. *Data Scientist* (mínimo 1 elemento)
 - i. Licenciatura ou Mestrado nas áreas de Engenharia, Informática, Ciências Empresariais, Matemática, Estatística ou similar;
 - ii. Experiência profissional mínima de 3 (três) anos em implementação de sistemas de informação com *Machine Learning* ou Inteligência Artificial.
- d. *Consultor Tecnológico* (mínimo 2 elementos sénior e mínimo 3 elementos júnior)
 - i. Licenciatura ou grau académico superior na área das Tecnologias de Informação e Comunicação ou similar;
 - ii. Experiência profissional mínima de 5 (cinco) anos em projetos de desenvolvimento de sistemas de informação que incluam componentes da Solução, para o perfil *Consultor Tecnológico* sénior;

- iii. Experiência profissional, da equipa, no desenvolvimento de projetos de sistemas de informação utilizando as tecnologias necessárias referidas no presente Caderno de Encargos (*DataStage*, *MicroStrategy* e *PowerBI*) e na SOLUÇÃO proposta;
 - iv. Experiência profissional mínima de 1 (um) ano em projetos de desenvolvimento de sistemas de informação, para o perfil *Consultor Tecnológico* júnior.
- e. *Business Analyst*. (mínimo 2 elementos sénior e 3 elementos júnior)
- i. Licenciatura ou Mestrado nas áreas de Ciências Empresariais Engenharia ou similar;
 - ii. Experiência profissional mínima de 5 (cinco) anos de experiência em consultoria no âmbito da análise funcional de implementação de modelos de gestão de risco, gestão de fraude, *business intelligence* e/ou *big data analytics* para o perfil *business analyst* sénior;
 - iii. Experiência profissional mínima de 1 (um) ano de experiência em consultoria no âmbito da análise funcional de implementação de modelos de gestão de risco, gestão de fraude, *business intelligence*, *big data analytics* e/ou *reporting* operacional, para o perfil *business analyst* júnior.

R.IMP.130 Em complemento aos elementos referidos no requisito anterior, é da responsabilidade da EMPRESA PRESTADORA alocar a quantidade de elementos com as competências e certificações necessárias para apoiar eficazmente o CONTRAENTE PÚBLICO (local ou remotamente) durante toda esta fase e cumprindo os requisitos aplicáveis.

R.IMP.131 Os recursos desempenharão a sua atividade sob ordens e orientação da **Empresa Prestadora**, obrigando-se esta a garantir que os agentes por si designados coloquem toda a sua perícia, cuidado e diligência na realização dos serviços que lhes sejam cometidos.

3.2.4.2. Gestão do projeto

R.IMP.132 Requisito introdutório: Por forma a melhor atingir os objetivos da prestação do SERVIÇO em termos de qualidade, preço e tempo de execução, a EMPRESA PRESTADORA deverá empregar uma abordagem e metodologia de gestão de projetos, suportada nas melhores práticas da indústria, endereçando nomeadamente áreas como a gestão de risco e a gestão da mudança.

R.IMP.133 Esta etapa inicia-se com o AUTO DE CONSIGNAÇÃO e deverá durar até ao termo do contrato acompanhando as fases de Conceção, Desenvolvimento e Exploração.

- R.IMP.134 Deverá ser empregue uma abordagem e metodologia de gestão de projetos que permita atingir os objetivos expressos no Caderno de Encargos, em sintonia com o CONTRAENTE PÚBLICO, em termos de qualidade, preço e tempo de execução das atividades. Em particular, a metodologia de gestão de projetos a empregar deverá estar suportada nas melhores práticas do mercado, endereçando temas como planeamento, controlo de progresso, *reporting*, gestão de recursos, gestão de risco, controlo da qualidade e gestão de âmbito.
- R.IMP.135 Em todas as fases, a EMPRESA PRESTADORA deverá estimar e comunicar as necessidades específicas de colaboração do CONTRAENTE PÚBLICO, nomeadamente com uma estimativa das reuniões ou outras atividades que envolvam elementos para além da equipa da EMPRESA PRESTADORA.
- R.IMP.136 Em complemento à abordagem e metodologia atrás referidas, a EMPRESA PRESTADORA deverá desenvolver atividades de gestão da mudança tendentes a antecipar dificuldades que a prestação do SERVIÇO possa enfrentar, a assegurar a articulação entre todos os elementos envolvidos nas atividades, a divulgar os resultados e a preparar a organização para a SOLUÇÃO.
- R.IMP.137 É da responsabilidade da EMPRESA PRESTADORA a proposta de um modelo de governo da prestação do SERVIÇO para controlar e acompanhar a execução das respetivas atividades em contínuo. Esta proposta será validada pelo CONTRAENTE PÚBLICO.
- R.IMP.138 Deverá estar sempre nomeado por parte da EMPRESA PRESTADORA:
- Um diretor de projeto responsável pelo controlo de qualidade da prestação do SERVIÇO e pelo diálogo a alto nível com o CONTRAENTE PÚBLICO;
 - Um Gestor de projeto encarregue da implementação global da SOLUÇÃO, assegurando a coordenação de todas as atividades, assim como a interlocução com a equipa de trabalho e de eventuais outros parceiros envolvidos na prestação do SERVIÇO;
 - Equipa de recursos humanos técnicos (distintos do Gestor de projeto) alocados às atividades de desenvolvimento e atividades conexas da SOLUÇÃO.
- R.IMP.139 Deverão ser realizadas reuniões ordinárias de acompanhamento da prestação do SERVIÇO, quinzenalmente, ou sempre que necessário de forma extraordinária;
- R.IMP.140 No âmbito das reuniões de acompanhamento, a EMPRESA PRESTADORA deverá elaborar Relatórios de Progresso que resumam as atividades realizadas, num determinado período, as próximas atividades, a análise dos riscos, a análise de qualidade, necessidades de intervenção de outras entidades para além da EMPRESA PRESTADORA e previsões para

a conclusão de atividades. Na etapa de suporte, inclui ainda a lista de incidentes reportados e o apuramento dos níveis de desempenho.

R.IMP.141 As reuniões previstas nos números anteriores devem ser convocadas, por escrito, pela EMPRESA PRESTADORA OU PELO CONTRAENTE PÚBLICO no caso das extraordinárias, com uma antecedência mínima de 4 dias, e ser acompanhadas da agenda prévia para cada reunião.

R.IMP.142 Os relatórios de progresso deverão ser apresentados pela EMPRESA PRESTADORA em periodicidade mensal devendo ser entregues no prazo de 5 dias a contar do último dia de cada mês de calendário.

R.IMP.143 Durante a primeira semana de cada fase, a EMPRESA PRESTADORA deverá entregar ao CONTRAENTE PÚBLICO um plano detalhado dessa fase e um macro plano das restantes atividades. Considera-se conforme o plano, se o CONTRAENTE PÚBLICO nada disser no prazo de 4 dias a contar da entrega.

R.IMP.144 Para além das fases e etapas da prestação do SERVIÇO, o plano de projeto deverá evidenciar a divisão de todos os ciclos de implementação e endereçar, no mínimo, as seguintes atividades indicando a data de início, duração, data de fim e pontos de intervenção ou de suporte por outras entidades para além da equipa da EMPRESA PRESTADORA:

- a. Especificação Detalhada da SOLUÇÃO;
- b. Construção/Customização e Desenvolvimentos;
- c. Instalação da SOLUÇÃO;
- d. Testes e momentos de Aceitação;
- e. Pilotos;
- f. Formação e sessões de refrescamento periódicas;
- g. Operacionalização da SOLUÇÃO;
- h. Elaboração da documentação;
- i. ACEITAÇÕES PARCELARES E ACEITAÇÃO INTEGRAL.

R.IMP.145 O detalhe do plano de projeto para cada etapa deverá endereçar, entre outros, os momentos de envolvimento de elementos que não pertençam à equipa da EMPRESA PRESTADORA, os momentos de entrega de produtos e documentação e os momentos de aceitação, sendo que estes deverão ser entregues para aprovação do CONTRAENTE PÚBLICO até 20 dias antes do início da etapa seguinte. Considera-se conforme o detalhe do plano se o CONTRAENTE PÚBLICO nada disser no prazo de 4 dias a contar da entrega.

R.IMP.146 Os resultados de todas as reuniões (reuniões de acompanhamento da prestação do SERVIÇO ou outras de trabalho que envolvam o CONTRAENTE PÚBLICO e/ou terceiros) deverão ser sistematizados em documentos a preparar pela EMPRESA PRESTADORA E A ENTREGAR NO

PRAZO DE 4 DIAS. Caso a caso, o CONTRAENTE PÚBLICO determinará se (i) estes documentos deverão assumir a forma de atas com a síntese da informação recolhida e/ou das decisões tomadas, lista de atividades de seguimento e respetivas responsabilidades e prazos ou (ii) se será suficiente que aqueles resultados sejam incorporados na documentação já prevista no âmbito da prestação do SERVIÇO.

R.IMP.147 No termo da vigência do CONTRATO, a EMPRESA PRESTADORA deve ainda elaborar um relatório final, discriminando os principais acontecimentos e atividades ocorridos em cada fase de execução do CONTRATO.

3.2.4.3. Metodologia AGILE

R.IMP.148 Requisito introdutório: Por forma a melhor atingir os objetivos da prestação do SERVIÇO em termos de entrega de valor iterativo, validação periódica pelo CONTRAENTE PÚBLICO, a EMPRESA PRESTADORA deverá empregar uma abordagem e metodologia de gestão de projetos, suportada nas melhores práticas de *Agile*, através da execução de vários sprints com a entrega de pilotos, tendo como objetivo melhorar a qualidade do produto e aumentar valor de entrega.

R.IMP.149 A gestão desta metodologia *Agile* deve contemplar, nomeadamente:

- a. Interação e colaboração com o CONTRAENTE PÚBLICO mais que utilização de ferramentas e negociação de contratos;
- b. Quando existe uma necessidade de mudança, esta prevalece em vez do seguimento do plano diário;
- c. Entregas contínuas;
- d. Aceitar mudanças de requisitos, mesmo no fim do desenvolvimento;
- e. A equipa de Projeto/Negócio deve trabalhar em conjunto com a EMPRESA PRESTADORA durante todo o curso do projeto;
- f. Um plano de comunicação semanal com o CONTRAENTE PÚBLICO;
- g. A equipa de desenvolvimento deve ter a capacidade de se auto-organizar, isto é, todos os elementos devem ter a capacidade de entrega e conhecimento transversal do desenvolvimento a implementar.

3.2.4.4. Ambientes de trabalho

R.IMP.150 A SOLUÇÃO deverá contemplar pelo menos os seguintes ambientes para respetiva exploração:

- a. Desenvolvimento;
- b. Qualidade;
- c. Produção.

3.2.4.5. Documentação

- R.IMP.151 Requisito introdutório: Aquando da conclusão de cada ciclo de implementação, a EMPRESA PRESTADORA deverá fornecer documentação completa sobre todos os componentes da SOLUÇÃO, incluindo descrição detalhada de cada componente, seja este software ou hardware.
- R.IMP.152 Deverão ser elaborados e fornecidos os manuais relevantes da SOLUÇÃO, que permitam ao CONTRAENTE PÚBLICO, de forma autónoma, realizar a exploração da SOLUÇÃO. Nestes manuais devem incluir-se, pelo menos, os seguintes:
- a. Manual de administração da SOLUÇÃO;
 - b. Manual de utilização da SOLUÇÃO;
 - c. Manuais de formação.
- R.IMP.153 Sem prejuízo do fornecimento de manuais em papel, toda a documentação deverá ser fornecida em formato eletrónico normalizado, editável e pesquisável (com a exceção de catálogos de produtos de hardware ou software, que pode ser fornecida em formato eletrónico não editável, mas pesquisável).
- R.IMP.154 O prazo limite de entrega da documentação corresponde, salvo indicação em contrário, ao momento de aprovação ou aceitação do marco da prestação do SERVIÇO associado a essa documentação.
- R.IMP.155 A documentação deverá ser preferencialmente escrita em português, mas considera-se aceitável a entrega de manuais técnicos em inglês nos casos de componentes de hardware e software que sejam referentes a produtos incorporados na SOLUÇÃO fornecida, com exceção do software que seja considerado central no contexto da SOLUÇÃO, sendo que neste caso deverá pelo menos existir uma versão em português.

3.2.4.6. Propriedade

- R.IMP.156 As componentes e/ou partes da SOLUÇÃO implementadas e/ou configuradas no contexto do projeto, serão propriedade do CONTRAENTE PÚBLICO. Tal incluiu todos os elementos que permitam que a Solução funcione devidamente sobre o software base em que assenta, e inclui, além de software, configurações, parâmetros de modelos de machine learning, modelos de dados, bases de dados e dados preparados especificamente no âmbito do projeto.
- R.IMP.157 No contexto do requisito anterior, a EMPRESA PRESTADORA, construirá, no prazo de 270 dias a contar do auto de consignação, um repositório de controlo de versões onde irá colocar todos os elementos resultantes do projeto de implementação, desde software construído e respetivo código fonte, configurações, modelos de machine learning, modelos de dados e outros. Este repositório será propriedade e estará sempre acessível ao

CONTRAENTE PÚBLICO. A EMPRESA PRESTADORA manterá este repositório sempre atualizado – com mecanismos de sincronização automática.

R.IMP.158 No caso de software base utilizado e sobre o qual é implementada a SOLUÇÃO, embora não sendo este, propriedade do CONTRAENTE PÚBLICO, a EMPRESA PRESTADORA terá de apresentar ao CONTRAENTE PÚBLICO garantias de acesso e utilização do mesmo, conforme estabelecido nas condições de cessação.

R.IMP.159 Toda a documentação, de natureza funcional ou técnica, que seja desenvolvida no âmbito da prestação do SERVIÇO, ficará propriedade originária do CONTRAENTE PÚBLICO, para seu uso e para uso pela EMPRESA PRESTADORA no contexto da prestação do serviço.

4. Níveis de desempenho e penalidades

Este capítulo apresenta os Níveis de Desempenho a assegurar pela EMPRESA PRESTADORA, bem como as regras sobre penalidades.

As penalidades em sede de projeto e em sede da manutenção evolutiva constam da alínea a) do nº 1 do artigo 22º do caderno de encargos.

No que se refere à MANUTENÇÃO EVOLUTIVA, a EMPRESA PRESTADORA deverá assegurar os tempos indicados na tabela abaixo:

Tipo	Descrição	Tempo de Resposta	Tempo de Preparação
Pedidos	Resposta a pedidos de MANUTENÇÃO EVOLUTIVA	5 dias para apresentar o orçamento para consumo da Bolsa de Horas	10 dias para iniciar a realização dos trabalhos após aprovação pelo CONTRAENTE PÚBLICO

Tabela 2 – Manutenção Evolutiva

4.1. Níveis de desempenho

Após a ACEITAÇÃO PARCELAR, a EMPRESA PRESTADORA deverá assegurar a disponibilidade do serviço da seguinte forma:

Descrição	Nível de Desempenho
Indisponibilidade do serviço (tempo máximo de indisponibilidade num único evento, a medir anualmente) – RTO (Recovery Time Objective)	120 minutos
Tempo mínimo de disponibilidade mensal (base 24x7) = (N.º máximo de minutos disponibilidade – Indisponibilidade) / (N.º máximo de minutos disponibilidade x 100)	99,90%

Tabela 3 – Níveis de Desempenho

4.1.1. Deduções à fatura

Nas situações em que o serviço é prestado de forma degradada, aplicam-se as seguintes deduções:

Descrição	Dedução à fatura
Tempo mínimo de disponibilidade mensal (base 24x7) = (N.º máximo de minutos disponibilidade – Indisponibilidade) / (N.º máximo de minutos disponibilidade x 100)	Por cada décima percentual abaixo do nível de serviço – 1 ponto, para efeitos de dedução na fatura mensal referente ao SaaS

Tabela 4 – Deduções à fatura

Exemplo:

Num mês de 30 dias, temos disponibilidade máxima de 43.200 minutos.

A indisponibilidade “tolerada” pelo nível de serviço é de 43,2 minutos nesse mês:

- $((100\% - 99,90\%) * 43.200 / 100) = 43,2$ minutos

Supondo que a indisponibilidade medida no mês foi de 2 horas (120 minutos). Significa uma disponibilidade de 99,72%:

- $(N.º \text{ máximo de minutos disponibilidade} - \text{Indisponibilidade}) / (N.º \text{ máximo de minutos disponibilidade} \times 100) = (43.200 - 120) / 43.200 \times 100 = 99,72\%$

Temos uma variação de 1,8 décimas percentuais ($99,90 - 99,72 = 0,18$) face ao “tolerado”, logo aplica-se 1,8 pontos de dedução à fatura mensal.

4.1.2. Incidentes após as aceitações parcelares

Na etapa de Suporte e Manutenção corretiva bem como na etapa de Garantia deverá ser assegurado o suporte ao tratamento de incidentes no período das 9h às 18h (dias úteis), exceto os incidentes de segurança cuja contagem é ininterrupta (24x7).

A EMPRESA PRESTADORA deverá assegurar tempos de resposta e de resolução inferiores aos máximos indicados na seguinte tabela:

Compete ao CONTRAENTE PÚBLICO qualificar os níveis de gravidade em função do interesse público envolvido.

Aos tempos de resolução aplica-se o número 4 do artigo 14º do caderno de encargos.

Gravidade ¹	Descrição	Tempo de Resposta
Gravidade 1 (emergência)	Impossibilidade de efetuar operações críticas	2 horas úteis
Gravidade 2 (crítico)	Impossibilidade de efetuar operações não críticas	8 horas úteis
Gravidade 3 (não crítico)	Impossibilidade de efetuar operações com um impacto reduzido na utilização da SOLUÇÃO	16 horas úteis
Incidente de Segurança	Notificação enviada ao Contraente Público	1 hora

Tabela 5 – Gestão de incidentes – Tempos de resposta

4.2. Penalidades

As penalidades, aplicadas a incumprimentos nas situações previstas em 4.1.2., obedecem às seguintes regras:

1. O Tempo de Resposta e o Tempo de Resolução serão contados a partir da data/hora de envio da notificação do incidente/problema à EMPRESA PRESTADORA pelo Contraente público;
2. A resposta da EMPRESA PRESTADORA consiste na comunicação da evidência de que um técnico de perfil adequado se encontra a resolver o incidente/problema.
3. A reparação ocorre com a comunicação da EMPRESA PRESTADORA de que o incidente/problema se encontra resolvido;
4. A contagem de tempos suspende-se fora do horário da gestão de incidentes (no período das 18h às 9h (dias úteis), feriados e fins de semana), exceto os incidentes de segurança cuja contagem é ininterrupta (24x7).

¹ Ver Apêndice III – Níveis de Gravidade

5. As penalidades são contabilizadas em pontos convertíveis em euros nos termos da alínea c) do nº 1 do artigo 22º do caderno de encargos.
6. Abaixo encontra-se a tabela que indica o número de pontos definidos pelo incumprimento de cada nível de serviço:

Tipo de Penalidade	Descrição da Penalidade	Pontos (Tempo de Resposta)
Níveis de serviço em sede de Manutenção e Garantia	Atraso na resposta a um incidente	Por cada duas horas úteis de atraso: <ul style="list-style-type: none">• 0,5 pontos (Gravidade 1)• 0,25 pontos (Gravidade 2)
	Atraso na reparação de um incidente	Por cada dia de atraso: <ul style="list-style-type: none">• 0,5 pontos (Gravidade 1)• 0,25 pontos (Gravidade 2)
Incidente de Segurança	Notificação enviada ao Contraente Público	<ul style="list-style-type: none">• 0,5 pontos por cada hora de atraso

Tabela 6 – Penalidades

5. Apêndice I – Conceitos e Acrónimos

Para efeitos do presente CADERNO DE ENCARGOS, adotam-se as definições e acrónimos seguintes:

Definições

- *ACEITAÇÃO INTEGRAL* – A sequência mencionada no artigo 10º do caderno de encargos
- *ACEITAÇÃO PARCELAR* – A sequência mencionada no artigo 9º do caderno de encargos
- *ARRANQUE DO PROJETO* – Momento em que se procede à assinatura do auto de consignação;
- *ARRANQUE EM PRODUÇÃO* – Momento em que a EMPRESA PRESTADORA disponibiliza, em conformidade com as condições especificadas na ACEITAÇÃO PARCELAR, o resultado de um ciclo de implementação, em produção.
- *AUTO DE CONSIGNAÇÃO* – A declaração mencionada no anexo IV do caderno de encargos;
- *EMPRESA PRESTADORA* – O operador económico cuja proposta foi objeto de adjudicação no âmbito do Concurso;
- *CONTRATO* – O *CONTRATO* de aquisição dos serviços a celebrar de acordo com as cláusulas jurídicas e técnicas constantes do CADERNO DE ENCARGOS e das demais peças do procedimento;
- *CONTRAENTE PÚBLICO* – O Instituto de Informática, I.P.;
- *EMPRESA PRESTADORA* – A adjudicatária
- *INCIDENTE* - É uma interrupção ou degradação da qualidade na prestação de um serviço de IT. Interrupção não planeada de um serviço, uma redução na qualidade de um serviço ou um evento que ainda não teve impacto no serviço para o cliente.
- *INCIDENTE DE SEGURANÇA DE INFORMAÇÃO* - Evento isolado ou uma série de eventos de segurança da informação indesejados ou inesperados, com uma probabilidade significativa de comprometer os ativos e/ou as operações do Instituto de Informática e de ameaçar a segurança da informação. Um evento com um efeito adverso real na segurança das redes e dos sistemas de informação.
Ações tomadas através da utilização de uma rede de computadores que resultam num efeito atual ou potencialmente adverso sobre um sistema de informação e/ou a informação aí armazenada. Exemplos:
 - Situações de ataque direcionado à Solução
 - Situações de indícios e/ou de intrusão

- Outras situações de quebras de segurança que ponham em risco os dados/informação
- *MANUTENÇÃO CORRETIVA* – Serviço a prestar pela EMPRESA PRESTADORA visando o correto funcionamento da *SOLUÇÃO*. A MANUTENÇÃO CORRETIVA visa a correção de eventuais defeitos. Os defeitos compreendem, mas não se limitam a esses casos, as imperfeições detetadas nos serviços ou produtos entregues, a ausência de objeto ou de documentação obrigatórios e qualquer outra ocorrência que impeça o funcionamento normal do SERVIÇO ou que não se apresente dentro dos padrões e níveis de qualidade predefinidos (Exemplo de possível situação de defeito: código que contenha erros, vulnerabilidades ou de difícil manutenção, assim como não se enquadrarem na arquitetura tecnológica do CONTRAENTE PÚBLICO);
- *MANUTENÇÃO EVOLUTIVA* – Serviço a prestar pela EMPRESA PRESTADORA visando a evolução da *SOLUÇÃO*, a pedido ou mediante aprovação do CONTRAENTE PÚBLICO, num modelo de consumo de Bolsa de Horas, conforme definido;
- *MANUTENÇÃO PREVENTIVA* – Serviço a prestar pela EMPRESA PRESTADORA visando intervenções que previnem avarias e diminuem a probabilidade de falha da *SOLUÇÃO*.
- *NÍVEIS DE DESEMPENHO* – Conjunto de metas a cumprir na prestação do SERVIÇO, face a vários parâmetros / indicadores estabelecidos no CADERNO DE ENCARGOS;
- *PROPOSTA* – A *PROPOSTA* adjudicada;
- *SERVIÇO* – Designação genérica do conjunto de serviços a prestar pela EMPRESA PRESTADORA expressamente identificados no CADERNO DE ENCARGOS ou necessários para o cumprimento das suas obrigações ao abrigo do CONTRATO;
- *SOLUÇÃO* – Nova Plataforma Integrada de Gestão do Risco que abrange a Componente 1 e a Componente 2, que implementa as funcionalidades descritas neste documento, e que se pretende contratar no âmbito desta consulta.
- *COMPONENTE* – Bloco funcional da *SOLUÇÃO* (Componente 1- Estimativa de índice de risco e Componente 2 – Aplicação de Gestão de Risco)
- *CICLOS DE IMPLEMENTAÇÃO* – Faseamento de entregas/ disponibilização de Componentes e áreas (Componente 1 - Contribuintes, Componente 1 - Beneficiários, Componente 2 - Aplicação de Gestão de Risco, Componente 1 - Fraude Interna)

Acrónimos

- AIPD – Avaliação de Impacto sobre a Proteção de Dados;
- BD – Base de Dados
- ETL – Extração, Tratamento e *Loading*
- GAQGR – Gabinete de Auditoria, Qualidade e Gestão de Risco;
- II – Instituto de Informática, I.P.;

- ISS – Instituto de Segurança Social, I.P.;
- MTSSS – Ministério do Trabalho, Solidariedade e Segurança Social;
- RGPD – Regulamento Geral de Proteção de Dados;
- SGBD – Sistema de Gestão de Base de Dados
- SGR – Setor de Gestão de Risco.

6. Apêndice II – Dimensionamento

O CONTRAENTE PÚBLICO elaborou um documento preliminar que será partilhado com a EMPRESA PRESTADORA (cfr. infra R.C1.2.). No entanto, a tabela seguinte apresenta um número aproximado de indicadores e fatores de risco por área em análise:

Área	Nº NISS registados	Intervalo de Nº de variáveis	Intervalo de Nº de indicadores	Intervalo de Nº de fatores de risco	Intervalo de Nº de Sistemas Fonte
Entidades Empregadoras (EE) com qualificação EE aberta	1.4M	440-520	110-130	15 - 25	15-25
Pessoas Singulares (PS) com enquadramento ativo	8M	360-480	90-120		
Fraude Interna (Nº de utilizadores registados na rede da Segurança Social)	14K	60-100	15-25		

Tabela 7 – Elementos para dimensionamento

Para efeitos de dimensionamento da SOLUÇÃO, apresentam-se as quantidades mínimas de utilizadores e volumetria de dados a respeitar, dividido por componente:

Estima-se que em termos de utilizadores:

- A Componente 1 seja operada por cerca de 30 utilizadores;
- A Componente 2 seja operada por cerca de 100 utilizadores em simultâneo escalável até 200.

Estima-se que em termos de volume de dados a SOLUÇÃO tenha a capacidade mínima de 25 TB, escalável caso necessário.

7. Apêndice III – Níveis de Gravidade

Compete ao Contraente Público qualificar a gravidade dos incidentes ou problemas em função dos seguintes níveis:

7.1. Gravidade 1 (emergência)

- Paragem total ou parcial da SOLUÇÃO;
- Impossibilidade de operação da SOLUÇÃO ou indisponibilidade das suas interfaces de comunicação com o exterior;
- Falhas de serviço, intermitentes ou não, que afetem a utilização da SOLUÇÃO;
- Falhas ou situações que elevem significativamente a probabilidade de ocorrência de uma quebra de serviço;
- Problemas que originem a utilização fraudulenta do serviço;
- Falhas graves de alarmística/monitorização de serviço;

7.2. Gravidade 2 (problema crítico)

- Falha de redundância;
- Falhas não graves de alarmística/monitorização de serviço;
- Falhas em funcionalidades da SOLUÇÃO sem impacto nos clientes
- Falhas de serviço que sejam considerados como casos de utilizadores isolados, sem afetação geral.

7.3. Gravidade 3 (problema não crítico)

- Situações de falha que não afetam o serviço;
- Falhas de documentação;
- Falhas/demora em esclarecimentos técnicos.