

CADERNO DE ENCARGOS¹

ÍNDICE

1ª.	Objeto	2
2ª.	Prazo do contrato	2
3ª.	Obrigações principais do adjudicatário	2
4ª.	Local e condições da prestação de serviços	4
5ª.	Transferência de Propriedade	5
6ª.	Preço contratual	6
7ª.	Condições de pagamento	7
8ª.	Proteção de dados pessoais	8
9ª.	Penalidades contratuais	9
10ª.	Dever de sigilo	10
11ª.	Força maior	11
12ª.	Resolução por parte da entidade adjudicante	12
13ª.	Resolução por parte do adjudicatário	12
14ª.	Foro competente	12
15ª.	Subcontratação e cessão da posição contratual	12
16ª.	Comunicações e notificações	12
17ª.	Critérios ambientais	12
18ª.	Execução do contrato	13
19ª.	Direção e Fiscalização da Execução do Contrato	13
20ª.	Legislação aplicável	13
	Anexo A – Caderno de Requisitos	14
	Anexo B - JobStories	35

¹ Toda a legislação referida neste caderno de encargos considera-se como reportada à redação em vigor à data da mesma.

Cláusulas

1ª. Objeto

1. O presente Caderno de Encargos compreende as cláusulas a incluir no contrato a celebrar na sequência do procedimento pré-contratual que tem por objeto principal a **aquisição de uma Plataforma web e mobile de Registo e Autenticação de Municípios**.
2. O objeto do contrato abrange ainda **serviços de manutenção evolutiva da referida plataforma**.

2ª. Prazo do contrato

1. O contrato mantém-se em vigor pelo **prazo máximo de 3 (três) anos** a contar da data da sua assinatura ou até ser atingido, durante esse prazo, o preço contratual, sem prejuízo das obrigações acessórias que devam perdurar para além da cessação do contrato.
2. A execução das prestações que constituem o objeto do contrato pode ser, total ou parcialmente, suspensa sempre que se verifique a impossibilidade temporária de cumprimento do contrato, designadamente em virtude de mora da entidade adjudicante na entrega ou na disponibilização de meios ou bens necessários à respetiva execução, ou exceção de não cumprimento, nos termos do disposto nos artigos 297.º e 298.º do Código dos Contratos Públicos (CCP).
3. Sem prejuízo das normas legais imperativas, relativas ao reequilíbrio financeiro, findo o prazo referido no n.º 1, e caso não tenha sido atingido o preço contratual, o contrato extingue-se sem que assista ao adjudicatário o direito a qualquer indemnização pelo valor das prestações não executadas.

3ª. Obrigações principais do adjudicatário

1. Sem prejuízo de outras obrigações previstas na legislação aplicável, no presente Caderno de Encargos ou nas cláusulas contratuais, decorrem para o adjudicatário as seguintes obrigações principais:
 - a. Desenvolver e entregar da versão final da plataforma para registo e autenticação de municípios, em cumprimento das especificações constantes do Anexo A – Caderno de Requisitos e Anexo B – Job Stories, ao presente Caderno de Encargos;
 - b. Realizar a manutenção corretiva e evolutiva da plataforma durante o período de vigência;
 - c. Participar em reuniões **quinzenais** de acompanhamento da execução do projeto, as quais serão agendadas, por email, pela entidade adjudicante com a antecedência mínima de 5 (cinco) dias úteis em relação à data pretendida.

- d. Assegurar um nível de resposta e garantia de serviço (SLA²) de acordo com a criticidade do incidente de:
 - i. Crítico (indisponibilidade dos serviços): até 2 horas após comunicação da entidade adjudicante;
 - ii. Urgente (instabilidade dos serviços): até 8 horas após comunicação da entidade adjudicante;
 - iii. Normal (questões diversas): até 96 horas após comunicação da entidade adjudicante, com acompanhamento em dias úteis.
 - e. Entregar os modelos de *design* da plataforma;
 - f. Entregar o plano de execução do projeto;
 - g. Entregar as versões em desenvolvimento e a versão final;
 - h. Instalar nos servidores da entidade adjudicante;
 - i. Entregar o código fonte e respetiva documentação incluindo os requisitos técnicos de compilação, dependências de frameworks ou de software de terceiros;
 - j. Entregar e atualizar o manual de administração, instalação, suporte e de utilizador da plataforma;
 - k. Dar formação a 4 utilizadores da entidade adjudicante (técnica e utilizador final), pelo período estimado de 1 dia;
 - l. Realizar testes/correções e respetivos relatórios de usabilidade; acessibilidade; segurança; performance/carga.
 - m. Realizar o Licenciamento das plataformas “on premises”, de autenticação de Cartão de Cidadão, reconhecimento facial e prova de vida;
 - n. Garantir a integração da plataforma a desenvolver com os sistemas atuais da entidade adjudicante
2. O adjudicatário obriga-se a respeitar as normas aplicáveis em vigor em matéria social, laboral, ambiental e de igualdade de género, decorrentes do direito internacional, europeu, nacional ou regional.
3. O adjudicatário deverá acautelar a possibilidade de vir a adotar, em sede de execução de contrato, planos de contingência, para fazer face a situações de contenção de epidemias, quer de modo preventivo, quer em situação declarada, quer em fase de reposição da normalidade, sem prejuízo das regras aplicáveis aos casos de força maior constantes do presente caderno de encargos.
4. A título acessório, o adjudicatário fica obrigado, designadamente, a recorrer a todos os meios humanos, materiais e informáticos que sejam necessários e adequados à prestação dos serviços objeto do contrato, bem como ao estabelecimento do sistema de organização necessário à perfeita e completa execução das tarefas a seu cargo.

² Service Level Agreement

5. O adjudicatário deve garantir condições de segurança e saúde do trabalho a todos os seus colaboradores, cumprindo a legislação aplicável nesta matéria, nomeadamente evidenciando a identificação de perigos e avaliação de riscos dos trabalhadores que exercem funções na Autarquia, e as respetivas apólices de seguros de acidentes de trabalho.

4ª. Local e condições da prestação de serviços

1. Sempre que solicitado pela entidade adjudicante, os serviços serão executados no normal horário de funcionamento da mesma, compreendido entre as 9:00 horas e as 17:30 horas (dias úteis), nas instalações afetas ao Departamento Municipal de Sistemas de Informação (DMSI), sitas na Rua Guilherme Costa Carvalho, n.º 38 – 4.º Piso, 4000-274 Porto.
2. O projeto incluirá as seguintes tarefas:
 - a. A- Desenvolvimento e implementação da plataforma que inclui;
 - i. Desenvolvimento da plataforma;
 - ii. Licenciamento das plataformas “on premises”, de autenticação de Cartão de Cidadão, reconhecimento facial e prova de vida;
 - iii. Integração com sistemas existentes da entidade adjudicante;
 - iv. Testes, formação e documentação.
 - b. B- Manutenção corretiva – Após implementação e até final do contrato.
 - c. C- Manutenção evolutiva – Bolsa de horas, sendo previsível um total máximo de 100horas.
3. Os serviços objeto de contrato devem ser executados faseadamente nos seguintes termos e, prazos máximos:
 - a. Fase A1 - Até 15 dias após outorga de contrato – Reunião de Kick off (fecho de especificações).
 - b. Fase A2 - Até 4 meses após outorga - Conclusão de desenvolvimento da plataforma.
 - c. Fase A3 - Até 6 meses após outorga – Testes, formação e entrada em produção da plataforma. Esta fase inclui ainda o licenciamento nas plataformas referidas no n.º 2 desta cláusula, bem como a integração com os sistemas da entidade adjudicante.
 - d. Fase B1 – Manutenção corretiva até final do 1º ano e após implementação da plataforma.
 - e. Fase B2 – Manutenção corretiva do 2º ano.
 - f. Fase B3 – Manutenção corretiva do 3º ano.
 - g. Fase C – Eventual necessidade de manutenção evolutiva após implementação e até ao final do contrato.
4. De forma a garantir o sucesso do projeto, o adjudicatário deve apresentar uma proposta de plano de execução do projeto, nos termos e no prazo que vier a ser acordado na reunião de Kick off, devendo o mesmo seguir as melhores práticas de desenvolvimento, tais como:

- a. Entrega inicial de proposta de *mockups* para análise e validação de design e navegabilidade, por parte da entidade adjudicante.
 - b. Agendamento de pontos de situação regulares (semanais/quinzenais) com a equipa da entidade adjudicante alocada ao projeto;
 - c. Entrega de calendário com a descrição e metodologia para todas as fases de implementação do projeto, indicando os principais marcos (milestones), as dependências de tarefas e respetivos formatos de documentação.
 - d. Indicar qual a metodologia de gestão de projetos que irá utilizar e informar que competências detém nessa metodologia de gestão de projetos.
5. Com a realização das reuniões referidas na alínea c), número 1 da cláusula 3.ª deverá o adjudicatário entregar os relatórios e/ou atas decorrentes dessas mesmas reuniões, até ao 3º dia útil após a reunião.
 6. Todos os relatórios e/ou atas deverão ser **validados pela entidade adjudicante, no prazo máximo de 8 dias úteis após a sua entrega, considerando-se aceites se não houver qualquer pronúncia em contrário** até ao final desse prazo.
 7. Caso existam correções/alterações a efetuar, serão estas da responsabilidade do adjudicatário, bem como todos os encargos que advenham dessa situação.
 8. O adjudicatário dispõe de **um prazo máximo de 2 dias úteis**, a contar da comunicação efetuada pela entidade adjudicante, para efetuar as correções/alterações que esta considere necessárias.
 9. Todos os documentos, nomeadamente os relatórios devem ser entregues, em suporte digital (Excel e Pdf), para o endereço eletrónico do gestor de contrato nomeado pela entidade adjudicante para o efeito.
 10. Excecionalmente, e mediante autorização expressa da entidade adjudicante, os documentos anteriormente referidos poderão ser entregues em suporte físico, devendo para o efeito ser impressos em papel reciclado, privilegiando-se a utilização da opção de impressão frente e verso dos mesmos, no âmbito da Estratégia Nacional para as Compras Públicas Ecológicas e da Resolução do Conselho de Ministros n.º 38/2016, de 29 de julho, que visa assegurar a inclusão de critérios de sustentabilidade em todos os contratos públicos de aquisição de bens e serviços.
 11. Em sede de execução do contrato poderá ser acordado outro prazo ou data de entrega dos relatórios/atas referenciado no número 5 da presente cláusula, mediante acordo entre as partes e desde que não seja prejudicada a execução das fases subsequentes, garantindo que o prazo máximo de vigência do contrato não é ultrapassado.

5ª. Transferência de Propriedade

1. Com a entrega da versão final da plataforma, ocorre a transferência da posse e da propriedade, assim como dos direitos de utilização e do código fonte, para a entidade adjudicante.
2. Pela cessão dos direitos a que alude o número anterior não é devida qualquer contrapartida para além do preço a pagar nos termos do presente Caderno de Encargos

6ª. Preço contratual

1. Pela execução dos serviços objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente Caderno de Encargos, a entidade adjudicante deve pagar ao adjudicatário **os preços unitários constantes da proposta adjudicada**, acrescidos de IVA à taxa legal em vigor, se este for legalmente devido
2. O somatório dos preços unitários multiplicados pelas quantidades efetivas decorrentes da execução do contrato **não pode, em qualquer caso, ser superior a 74.999,00€**, no prazo máximo de vigência admitido (valores sem IVA) em que se fixam os seguintes máximos:
 - a. Preço para os serviços de desenvolvimento, implementação e manutenção corretiva da plataforma **não pode, em qualquer caso, ser superior a 70.999,00€**,
 - b. O resultado do preço/ hora para os serviços de manutenção evolutiva multiplicado pelo n.º de horas máximo do contrato admitido **não pode, em qualquer caso, ser superior a 4.000,00 €, a que corresponde 40,00€/hora**
3. O preço referido no número 1 inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída à entidade adjudicante, incluindo, nomeadamente as despesas de alojamento, alimentação e deslocação de meios humanos, despesas de aquisição, transporte, armazenamento e manutenção de meios materiais, bem como quaisquer encargos decorrentes da utilização de marcas registadas, patentes ou licenças.
4. O preço a que se refere o n.º 2 é dividido pelas diversas fases de execução do Contrato, nos seguintes termos:
 - a. Com a conclusão da fase A1 definida na alínea a), n.º 3 da cláusula 4ª – 10% do preço contratual da componente de desenvolvimento, implementação e manutenção corretiva da Plataforma;
 - b. Com a conclusão da fase A2 definida na alínea b), n.º 3 da cláusula 4ª - 10% do preço contratual da componente de desenvolvimento, implementação e manutenção corretiva da Plataforma;
 - c. Com a conclusão da fase A3 e início da Fase B1 definida nas alíneas c) e d), n.º 3 da cláusula 4ª – 50% do preço contratual da componente de desenvolvimento, implementação e manutenção corretiva da Plataforma;
 - d. Com o início da fase B2 definida na alínea e), n.º 3 da cláusula 4ª – 15% do preço contratual da componente de desenvolvimento, implementação e manutenção corretiva da Plataforma;
 - e. Com o início da fase B3 definida na alínea f) n.º 3 da cláusula 4ª – 15% do preço contratual da componente de desenvolvimento, implementação e manutenção corretiva da Plataforma;
 - f. Com a prestação de serviços de manutenção evolutiva: o preço hora contratual multiplicado pelo n.º de horas efetivamente consumidas.

7ª. Condições de pagamento

1. As quantias devidas pela entidade adjudicante, nos termos da cláusula anterior, devem ser pagas no prazo de 30 dias após a receção das respetivas faturas, as quais devem cumprir com o disposto no artigo 36.º do CIVA³ e só podem ser emitidas após o vencimento das obrigações respetivas, e após a prestação dos serviços, devendo ainda cumprir com as exigências impostas pelo artigo 9.º, n.º 1, da LCPA⁴, aprovada pela Lei n.º 8/2012, de 21 de fevereiro, na redação atual.
2. Para efeitos do número anterior as obrigações consideram-se vencidas nos termos do número 4 da cláusula 6.ª do presente Caderno de Encargos.
3. Em caso de discordância por parte da entidade adjudicante, quanto aos valores indicados nas faturas, deve esta comunicar ao adjudicatário, por escrito, os respetivos fundamentos, ficando o mesmo obrigado a prestar os esclarecimentos necessários ou proceder à emissão de nova fatura corrigida.
4. As faturas devem ser emitidas em nome do **Município do Porto NIF: 501 306 099**, sito na Praça General Humberto Delgado, 4049-001 PORTO – **Departamento Municipal de Sistemas de Informação**, com referência aos documentos que lhes deram origem, isto é, deve especificar o n.º da encomenda e o respetivo número sequencial de compromisso.
5. Nos termos do n.º 1 do artigo 9.º do Decreto-Lei n.º 111-B/2017, de 31 de agosto, na redação atual, os contraentes públicos são obrigados, a partir de 18 de abril de 2019, a receber e a processar faturas eletrónicas no modelo estabelecido pela norma europeia respetiva aprovada pela Comissão Europeia e publicitada no portal dos contratos públicos, a que se refere o n.º 3 do artigo 299.º-B do CCP.
6. Nos termos do artigo 9.º n.ºs 3 e 4 do mesmo Decreto-Lei n.º 111-B/2017, os cocontratantes podem, até 31 de dezembro de 2020, utilizar mecanismos de faturação diferentes dos previstos no referido artigo 299.º-B do CCP, prazo esse alargado até 30 de junho de 2021 para as pequenas e médias empresas⁵ e até 31 de dezembro de 2021 para as microempresas, definidas nos termos da Diário da República, 1.ª série www.dre.pt N.º 69, de 7 de abril de 2020 Pág. 11-(3) Recomendação 2003/361/CE, da Comissão Europeia, de 6 de maio de 2003, e para as entidades públicas enquanto entidades cocontratantes.

³ Código do Imposto sobre o Valor Acrescentado.

⁴ Lei dos Compromissos e Pagamentos em Atraso.

⁵ De acordo com o artigo 2º da Recomendação nº 2003/361/CE, da Comissão Europeia, de 6 de maio de 2003, a categoria das micro, pequenas e médias empresas (PME) é constituída por empresas que empregam menos de 250 pessoas e cujo volume de negócios anual não excede 50 milhões de euros ou cujo balanço total anual não excede 43 milhões de euros; na categoria das PME, uma pequena empresa é definida como uma empresa que emprega menos de 50 pessoas e cujo volume de negócios anual ou balanço total anual não excede 10 milhões de euros; e na categoria das PME, uma microempresa é definida como uma empresa que emprega menos de 10 pessoas e cujo volume de negócios anual ou balanço total anual não excede 2 milhões de euros.

7. Caso o adjudicatário não tenha ainda aderido à faturação eletrónica⁶, nos termos e prazos definidos no número anterior, as faturas devem ser enviadas digitalmente, para o seguinte endereço de correio eletrónico: mporto@cm-porto.pt
8. Excecionalmente, caso não seja possível a utilização de correio eletrónico, as faturas poderão ser enviadas para o seguinte endereço postal: Apartado 4053, 4000-101 Porto.
9. Sem prejuízo do disposto nos números anteriores poderão, ao longo da execução do contrato, ser indicados outros contactos para o envio das referidas faturas.
10. Desde que devidamente emitidas e observado o disposto nos n.ºs 1, 2 e 4, as faturas são pagas através de transferência bancária.

8ª. Proteção de dados pessoais

1. Constituem obrigações do adjudicatário, no que especificamente diz respeito à proteção de dados pessoais:
 - a. Utilizar os dados pessoais, objeto de tratamento, exclusivamente para as finalidades previstas no contrato, não podendo em caso algum utilizar os dados para fins próprios;
 - b. Dar cumprimento às instruções que possam, no âmbito da execução do contrato, ser emitidas pela entidade adjudicante, enquanto responsável pelo tratamento, para tratamento dos dados pessoais;
 - c. Efetuar uma Avaliação de Impacto sobre a Proteção de Dados que identifique e minimize os riscos em caso de incumprimento das regras de proteção de dados, nas situações expressamente previstas, quer no artigo 35.º do n.º 3 do Regulamento Geral sobre a Proteção de Dados, Reg. (UE) 2016/679 (RGPD) quer no Regulamento n.º 1/2018 da Comissão Nacional de Proteção de Dados, relativo à lista de tratamentos de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados (AIPD);
 - d. Assegurar a realização de auditorias periódicas às medidas técnicas e organizativas para garantir a segurança dos sistemas e dos serviços de tratamento;
 - e. Efetuar um registo de todas as atividades de tratamento de dados pessoais, efetuados no âmbito do contrato, que contenha:
 - i. Uma descrição geral das medidas técnicas e organizativas adequadas para garantir a segurança dos dados pessoais objeto de tratamento, designadamente a capacidade para assegurar a confidencialidade, integridade e resiliência permanentes dos sistemas e dos serviços de tratamento;
 - ii. A capacidade de assegurar a disponibilidade e acesso aos dados pessoais de forma rápida, em caso de incidente;

⁶ Com o objetivo de facilitar a adoção da fatura eletrónica pelos seus fornecedores, o Município do Porto contratualizou um serviço de apoio, que poderá ser solicitado através do seguinte endereço de correio eletrónico: fornecedores.saphety@saphety.com

- iii. O processo de auditoria às medidas técnicas e organizativas para garantir a segurança dos sistemas e dos serviços de tratamento;
 - iv. O nome e contacto do Encarregado de Proteção de Dados, quando for obrigatória a sua designação nos termos do artigo 35.º do RGPD.
 - f. Disponibilizar à entidade adjudicante, periodicamente, todas as informações necessárias para demonstrar o cumprimento das regras de proteção de dados;
 - g. Não partilhar os dados pessoais com terceiros, exceto no caso de autorização expressa da entidade adjudicante, ou decorrente de obrigação legal;
 - h. Manter sigilo referente aos dados pessoais a que tenha acesso no âmbito do contrato;
 - i. Garantir que pessoas autorizadas a tratar os dados pessoais se comprometem, de forma expressa e por escrito, a respeitar a confidencialidade e adotar as medidas de segurança correspondentes;
 - j. Apoiar a entidade adjudicante na resposta aos pedidos dos titulares dos dados tendo em vista o exercício dos direitos de acesso, retificação, limitação, oposição, apagamento e portabilidade.
2. Cada uma das partes obriga-se a notificar a respetiva contraparte de forma imediata, e em qualquer circunstância antes do prazo de 72 horas, por escrito e preferencialmente através de correio eletrónico, das violações de segurança ocorridas no âmbito do contrato.
3. Para o efeito do disposto no número anterior deve anexar-se toda a informação relevante, designadamente a descrição da natureza da violação de segurança, bem como a descrição das possíveis consequências da mesma e ainda das medidas adotadas ou propostas para pôr término à violação de segurança ou mitigar possíveis efeitos negativos. Caso não seja possível enviar a informação simultaneamente, a mesma será expedida gradualmente.
4. Finda a vigência do contrato, o adjudicatário tem a obrigação de eliminar os dados pessoais que tenham sido objeto de tratamento no âmbito do mesmo, bem como eliminar quaisquer outras cópias existentes, devendo para o efeito enviar um comprovativo para a entidade adjudicante.

9ª. Penalidades contratuais

1. Pelo incumprimento de obrigações emergentes do contrato, a entidade adjudicante pode exigir do adjudicatário o pagamento de uma sanção pecuniária, de montante a fixar em função da gravidade do incumprimento, nos seguintes termos:
- a. Pelo incumprimento dos *prazos* de entrega constantes do presente caderno de encargos, até 1% do preço total contratual, por cada dia útil de atraso, desde que este atraso seja única e exclusivamente da responsabilidade do adjudicatário;
 - b. Pelo incumprimento de outras obrigações emergentes do contrato, até 10% do preço total contratual;
 - c. Pelo incumprimento da obrigação de respeitar ao longo da execução do contrato, e apenas no âmbito do referido contrato, as normas aplicáveis em vigor em matéria social, laboral, ambiental

e de igualdade de género, decorrentes do direito internacional, europeu, nacional ou regional, a entidade adjudicante pode exigir do adjudicatário o pagamento de uma sanção pecuniária até 0,5% do preço contratual, sem prejuízo do disposto no n.º 7 da presente cláusula.

2. Em caso de resolução do contrato por incumprimento do adjudicatário, o valor acumulado das sanções pecuniárias não pode exceder 20% do preço contratual, nos termos do n.º 2 do artigo 329.º do CCP, salvo se a entidade adjudicante exercer a prerrogativa prevista no n.º 3, do mesmo artigo, caso em que este limite pode ser elevado para 30%.
3. Ao valor das sanções pecuniárias previstas no número anterior, são deduzidas as importâncias pagas pelo adjudicatário ao abrigo da alínea a) do n.º 1, relativamente aos serviços cujo atraso na respetiva conclusão tenha determinado a respetiva resolução
4. Na determinação da gravidade do incumprimento, a entidade adjudicante tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do adjudicatário e as consequências do incumprimento.
5. A entidade adjudicante pode compensar os pagamentos devidos ao abrigo do contrato com as sanções pecuniárias devidas nos termos da presente cláusula.
6. As sanções pecuniárias previstas na presente cláusula não obstam a que a entidade adjudicante exija uma indemnização pelos danos decorrentes da mora no cumprimento, cumprimento defeituoso e incumprimento definitivo.
7. Em função da gravidade do incumprimento da obrigação prevista na alínea c) do n.º 1 da presente cláusula, ou da sua reiteração após instruções transmitidas no exercício do poder de direção por parte da entidade adjudicante tendente à respetiva observância, e apenas no âmbito do referido contrato, pode este ser resolvido a título sancionatório, nos termos da alínea b) do n.º 1 do artigo 333.º do CCP, sem prejuízo do disposto no n.º 3 desta mesma disposição legal.

10ª. Dever de sigilo

1. O adjudicatário deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, relativa a entidade adjudicante de que possa ter conhecimento ao abrigo ou em relação com a execução do contrato.
2. A informação e a documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros, nem objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do contrato.
3. Exclui-se do dever de sigilo previsto a informação e a documentação que fossem comprovadamente do domínio público à data da respetiva obtenção pelo adjudicatário ou que este seja legalmente obrigado a revelar, por força da lei, de processo judicial ou a pedido de autoridades reguladoras ou outras entidades administrativas competentes.

4. O adjudicatário deverá guardar sigilo quanto a informações que possa obter no âmbito da execução do presente contrato, por qualquer causa, sem prejuízo da sujeição subsequente a quaisquer deveres legais relativos, designadamente, à proteção de segredos comerciais ou da credibilidade, do prestígio ou da confiança devidos às pessoas coletivas.

11ª. Força maior

1. Não podem ser impostas penalidades ao adjudicatário, nem é havida como incumprimento, a não realização pontual das prestações contratuais a cargo de qualquer das partes que resulte de caso de força maior, entendendo-se como tal as circunstâncias que impossibilitem a respetiva realização, alheias à vontade da parte afetada, que ela não pudesse conhecer ou prever à data da celebração do contrato e cujos efeitos não lhe fosse razoavelmente exigível contornar ou evitar.
2. Podem constituir força maior, se se verificarem os requisitos do número anterior, designadamente, tremores de terra, inundações, incêndios, epidemias, sabotagens, greves, embargos ou bloqueios internacionais, atos de guerra ou terrorismo, motins e determinações governamentais ou administrativas injuntivas.
3. Não constituem força maior, designadamente:
 - a. Circunstâncias que não constituam força maior para os subcontratados do adjudicatário, na parte em que intervenham;
 - b. Greves ou conflitos laborais limitados às sociedades do adjudicatário ou a grupos de sociedades em que este se integre, bem como a sociedades ou grupos de sociedades dos seus subcontratados;
 - c. Determinações governamentais, administrativas, ou judiciais de natureza sancionatória ou de outra forma resultantes do incumprimento pelo adjudicatário de deveres ou ónus que sobre ele recaiam;
 - d. Manifestações populares devidas ao incumprimento pelo adjudicatário de normas legais;
 - e. Incêndios ou inundações com origem nas instalações do adjudicatário cuja causa, propagação ou proporções se devam a culpa ou negligência sua ou ao incumprimento de normas de segurança;
 - f. Avarias nos sistemas informáticos ou mecânicos do adjudicatário não devidas a sabotagem;
 - g. Eventos que estejam ou devam estar cobertos por seguros.
4. A ocorrência de circunstâncias que possam consubstanciar casos de força maior deve ser imediatamente comunicada à outra parte.
5. A força maior determina a prorrogação dos prazos de cumprimento das obrigações contratuais afetadas pelo período de tempo comprovadamente correspondente ao impedimento resultante da força maior.

12ª. Resolução por parte da entidade adjudicante

Sem prejuízo de outros fundamentos de resolução do contrato previstos na lei e no contrato, nomeadamente os constantes na cláusula referente às penalidades contratuais, a entidade adjudicante pode resolver o contrato, a título sancionatório, no caso de o adjudicatário violar de forma grave ou reiterada qualquer das obrigações que lhe incumbem.

13ª. Resolução por parte do adjudicatário

O adjudicatário pode resolver o contrato nos casos previstos no artigo 332.º do CCP.

14ª. Foro competente

Para resolução de todos os litígios decorrentes do contrato fica estipulada a competência do Tribunal Administrativo e Fiscal do Porto, com expressa renúncia a qualquer outro.

15ª. Subcontratação e cessão da posição contratual

1. A subcontratação ou a cessão da posição contratual pelo adjudicatário depende da autorização da entidade adjudicante, nos termos do CCP.
2. Em caso de incumprimento, pelo adjudicatário, das suas obrigações, que reúna os pressupostos para a resolução do contrato, aquele cederá, nos termos do disposto no artigo 318.º-A do CCP, a sua posição contratual ao concorrente do procedimento pré-contratual na sequência do presente procedimento, pela ordem sequencial de classificação dos concorrentes, sempre que tal seja aplicável.

16ª. Comunicações e notificações

1. Sem prejuízo de poderem ser acordadas outras regras quanto às notificações e comunicações entre as partes do contrato, estas devem ser dirigidas, através de correio eletrónico, nos termos do artigo 468.º do CCP, para os respetivos endereços eletrónicos, identificados no contrato.
2. Qualquer alteração das informações de contacto constantes do contrato deve ser comunicada à outra parte.

17ª. Critérios ambientais

1. O adjudicatário deve garantir as melhores práticas ambientais por forma a incluir as medidas necessárias a fim de assegurar a proteção do ar, da água, do solo, e de prevenir ou reduzir a poluição sonora, a produção de resíduos e o consumo energético, com o objetivo de alcançar um nível elevado de proteção do ambiente e minimizar os impactes ambientais.
2. Garantir o correto encaminhamento dos eventuais resíduos produzidos no decorrer da execução do contrato, respeitando as boas práticas ambientais previstas na legislação em vigor.

18ª. Execução do contrato

Os serviços serão executados mediante requisição da entidade adjudicante.

19ª. Direção e Fiscalização da Execução do Contrato

1. Os poderes de direção e a fiscalização do modo de execução do contrato serão exercidos pela entidade adjudicante nos termos do disposto nos artigos 303.º a 305.º do CCP.
2. Para efeitos da concretização dos poderes de direção e fiscalização do modo de execução do contrato a entidade adjudicante será representada pelo Gestor do Contrato, ao qual se delega:
 - a. A competência para a emissão de ordens, diretivas ou instruções, bem como para proceder à notificação prevista no art.º 325.º do CCP para que o adjudicatário cumpra, em prazo fixado para o efeito, todas as obrigações emergentes do contrato, a quem o adjudicatário fica obrigado a prestar toda a colaboração que se mostrar necessária e toda a informação que lhe seja solicitada, sem prejuízo dos relatórios de acompanhamento previstos no presente caderno de encargos.
 - b. A competência para decidir sobre a verificação da existência de uma impossibilidade temporária de cumprimento do contrato que determina a suspensão do prazo (nos termos do disposto no art.º 297.º do CCP) e sobre a respetiva retoma logo que cessem as causas que determinaram a suspensão (nos termos do disposto no art.º 298.º do CCP).
3. O Gestor do Contrato, no exercício das funções de fiscalização será responsável pela medição e a avaliação dos níveis de serviço exigidos de acordo com a cláusula 3.ª do presente caderno de encargos.

20ª. Legislação aplicável

O contrato é regulado pelo disposto no CCP e restante legislação aplicável.

Anexo A – Caderno de Requisitos

1 Introdução

1.1 Objetivo

O objetivo deste caderno de requisitos é descrever as funcionalidades que deverão ser desenvolvidas no âmbito da reformulação da plataforma de registo e autenticação das entidades externas, que se relacionam com os serviços de informação, prestados pela Câmara Municipal do Porto (CMP).

1.2 Âmbito

A plataforma a desenvolver denomina-se “Plataforma de Registo e Autenticação de Munícipes”, e tem como principal objetivo gerir o ciclo de vida do processo de registo, certificação, autenticação e autorização do conjunto de acessos privilegiados de utilizadores das plataformas digitais do município, sejam eles munícipes, ou representantes de entidades externas, de acordo com os requisitos funcionais identificados neste documento.

Pretende-se que a ferramenta tenha o seu próprio interface de gestão, mas com componentes modulares que possam ser a partir de outros portais tais como o BAV (Balcão de Atendimento Virtual) e o Portal do Município, assim como com aplicações mobile, e ainda uma API para integrações com outras ferramentas e eventuais processos de federação.

2 Contextualização da Situação Atual

2.1 Processo de Registo

O mecanismo atual de registo de utilizadores (munícipes ou representantes de entidades externas), para acesso aos sistemas de informação disponibilizados pela CMP, traduz-se por um processo de pré-qualificação em que o interessado faz a requisição (presencial ou através de requerimento) de um acesso aos serviços online, em que após validação é atribuído um nome de utilizador e uma palavra passe. O nome de utilizador traduz-se no NIF (Número de Identificação Fiscal) da entidade.

Este par de informação (utilizador, password), que designamos de credenciais de acesso, ficam registados, de forma segura, numa tabela da base de dados pertencente ao sistema de Gestão Documental DocInPorto.

Através destas credenciais e com base em mecanismos simples de controlo de acessos e autorização, os utilizadores podem ter, por exemplo, acesso ao ponto de situação dos processos, preenchimentos dos formulários online, entre outros.

2.2 Processo de Autenticação e gestão de sessões atual

O mecanismo de autenticação atual está centralizado no BAV, desenvolvido em tecnologia Sharepoint, e que se baseia num mecanismo simples de manutenção de gestão de sessões entre as várias

“aplicações web” baseada na RFC 6265 (HTTP State Management Mechanism), vulgarmente denominada de “HTTP Cookie”.

2.3 Proteção de Dados

Este processo, de validação ou certificação do munícipe, parte do princípio que quem faz um requerimento aos serviços da CMP terá que passar por um conjunto de etapas e procedimentos que, de alguma forma, garantem que a entidade que o pediu é autêntica e fidedigna.

No entanto, neste processo, coloca-se um problema de proteção de dados. Efetivamente existe o risco de alguém, de forma intencional e maliciosa, fazer um pedido de registo com um NIF que não lhe pertença, e dessa forma aceder a informação confidencial e sensível.

É neste sentido que o desenvolvimento desta nova plataforma poderá produzir benefícios na medida em que se pretende a certificação da entidade, utilizando mecanismos normalizados com diversos níveis de segurança, qualidade e disponibilidade de serviço, nomeadamente os serviços comuns da AMA ou por mecanismos de reconhecimento facial com prova de vida. Pretende-se assim, aumentar o nível de confiança e qualidade da dos acessos e da informação, garantido os critérios de confidencialidade, integridade, disponibilidade e autenticidade.

3 Requisitos Funcionais

Nesta secção pretende-se identificar o conjunto de requisitos funcionais que permitam, em paralelo com a reformulação do Balcão de Atendimento Virtual, criar uma nova plataforma autónoma de Registo (aprovisionamento) e Autenticação (gestão de identidades) de utilizadores (Munícipes e representantes de entidades).

Esta necessidade de autonomizar a plataforma, prende-se com a necessidade de escalabilidade e traduz-se na possibilidade de vir a implementar no futuro algumas soluções que se antecipam possam vir a revelar-se numa mais valia para o munícipe, bem como a implementação de soluções mais modernas de disponibilização da informação, nomeadamente o conceito do cartão do munícipe com um conjunto de funcionalidades e benefícios, e aplicações mobile.

Assim, pretende-se um processo que permita um registo de novos utilizadores “na hora”, ou seja de forma imediata (devendo existir uma confirmação de e-mail e/ou telemóvel). Este processo deverá ser automático, sem intervenção humana, sendo criado um registo com, pelo menos, nome e contacto, sendo atribuído um número de utilizador NUM. Este processo de registo de utilizadores dará origem a utilizadores do tipo “Utilizador não Verificado”

Este processo poderá ser posteriormente completado com uma certificação da entidade. Isto significa que perante a realização de procedimentos posteriores como, por exemplo, a apresentação de documentos, a confirmação de morada, ou o login através da AMA (Cartão de Cidadão ou Chave Móvel

Digital), podemos considerar a entidade “certificada”, confiando nos campos apresentados e comprovados e “fazendo” fé nos restantes.

Como anexo, é incluído um resumo onde são detalhados casos de uso que abordam e ajudam a compreender as situações referenciadas neste documento.

A Plataforma de Registo e Autenticação de Utilizadores deverá funcionar em qualquer equipamento fixo ou móvel, garantindo sempre a confidencialidade, integridade, disponibilidade e autenticidade da informação, apresentando uma interface responsiva, simples e facilmente compreensível para que os munícipes não tenham dificuldade na sua utilização e garantindo um conjunto de benefícios, nomeadamente:

- Aumentar a adesão do munícipe aos serviços disponibilizados online pela CMP;
- Diminuir gastos e tempo na formação de utilização da plataforma;
- Reduzir tempo na implementação da plataforma;
- Facilitar o “onboarding” na plataforma;
- Simplificar a execução das tarefas realizadas dentro do sistema;
- Acelerar os resultados obtidos através da plataforma.

As funcionalidades pretendidas deverão estar estruturadas numa lógica funcional e agrupadas de forma modular, nomeadamente:

- **Módulo 1** - Registo certificado da entidade – Registo “normal” a efetuar por qualquer entidade com CC/CMD ou através de Reconhecimento Facial;
- **Módulo 2** - Registo simplificado da entidade – Registo sem CC/CMD ou sem Reconhecimento Facial;
- **Módulo 3** – Reconhecimento facial e prova de vida (Frontend);
- **Módulo 4** - Registo certificado do representante legal da empresa – Registo prévio pelo representante legal com CC/CMD ou Reconhecimento Facial (Módulo 1) e Código de Acesso à Certidão Permanente;
- **Módulo 5** - Autenticação da entidade;
- **Módulo 6** – Utilitário de consolidação e normalização de identidades
- **Módulo 7** - Gestão de entidades – Área de administração, configuração e gestão das entidades;

3.1 Módulo 1 - Registo Certificado da Entidade

Este requisito traduz-se na necessidade de um processo de registo ágil, sem burocracias, que permitam à grande maioria dos munícipes, de uma forma rápida, iniciar o processo de Registo “onboarding” sem necessidade de burocracias ou tempos de espera como resultado de validação por parte dos serviços. Pretende-se também que este processo garanta que a entidade que pretende o acesso aos serviços

online é fidedigna e verdadeira, e que forneça um conjunto de informação necessária que lhe permita ser considerada certificada e desta forma aceder a um maior conjunto de funcionalidades e benefícios. Para este efeito pretende-se implementar duas possibilidades de registo certificado:

- Registo com CC/CMD utilizando as plataformas de serviços comuns de autenticação já existentes na Agência para a Modernização Administrativa (AMA) para a leitura dos dados;
- Na impossibilidade de utilizar o CC/CMD, efetuar o registo através de Cópia/Fotografia do CC e Reconhecimento Facial (ou outro mecanismo de prova de vida) que garantam que a entidade é fidedigna.

Pretende-se também que, durante este processo de registo, seja possível ao requerente definir um par “username/password” que lhe possibilite o acesso através de mecanismo de duplo fator de verificação, combinando informação que o utilizador tem conhecimento com algo que ele possua (telefone, mail, autenticador, etc...). Desta forma pretende-se mitigar o risco de registos de entidades e acessos não fidedignos.

Os dados pessoais recolhidos nos formulários serão sincronizados com a Gestão Central de Entidades com a atribuição do NUM (Numero de Múncipe).

Com este processo de registo o requerente ficará caracterizado como de nível de confiança alto (certificado).

Pretende-se que um utilizador caracterizado com este nível de confiança possa submeter e consultar processos associados ao seu NIF.

Os casos de uso que detalham este processo são referenciados no Anexo B do presente CE, como A1 e A2.

ID	Requisito funcional
M1 – 1	Deverá ser dado conhecimento ao utilizador de que métodos de registo é que lhe estão disponíveis de escolher (CC/CMD ou Reconhecimento facial)
M1 – 2	Deverá ser explicado ao utilizador a vantagem de cada um dos métodos de registo. O que pode ou não fazer com cada método.
M1 - 3	Se o utilizador optar pelos serviços comuns da AMA, deverá ser redirecionado para essa plataforma de autenticação de forma a poder escolher qual o método pretendido: CC ou CMD.
M1 – 4	Se o utilizador cancelar o processo de autenticação através da AMA deverá ser redirecionado para a página inicial e informado que o seu registo não foi concluído.
M1 – 5	Após autenticação através da AMA com sucesso deverá ser redirecionado para a página de recolha de atributos.
M1 – 6	Deve existir a possibilidade de definir campos de preenchimento obrigatório, e o sistema deverá avisar da necessidade do seu preenchimento.

M1 – 7	Os dados autorizados e recolhidos na plataforma AMA deverão ser preenchidos automaticamente na ficha do perfil do munícipe.
M1 – 8	Independentemente dos campos obrigatórios poderem ser configurados em backoffice (ver modulo de administração), o campo de 'nome' e 'nif' deverão ser sempre obrigatórios, bem como o 2FA (email ou telefone).
M1 – 9	Deverá ser dada a opção de criar um par "utilizador/password". Esta password deverá cumprir os requisitos de complexidade mínimos de segurança (ver requisitos não funcionais). O utilizador poderá ser o NUM.
M1 – 10	O utilizador obrigatoriamente deverá definir um email ou número de telefone como 2FA (2º fator de autenticação).
M1 – 11	Para concluir o processo de registo deverá ser feita a validação do 2FA gerando um OTP de, no mínimo, 4 dígitos a enviar por email ou SMS.
M1 – 12	Em caso de conclusão do processo com sucesso, deverão os dados ser sincronizados com o GCE (Gestão Central de Entidades) e gerado o NUM (Nº do Munícipe)
M1 – 13	Em caso de conclusão do processo com sucesso, deverá o sistema enviar um email de confirmação ao utilizador contendo os detalhes principais e o respetivo NUM
M1 – 14	O utilizador deverá ter a possibilidade de cancelar o processo de registo em qualquer fase até à sua conclusão, e nenhum dado ou atributo deverá ficar persistente na base de dados da plataforma.
M1 – 15	O tempo de <i>Idle Timeout</i> , para fecho automático da sessão, no caso de inatividade deverá ser 20 minutos, ou outro valor a definir.
M1 – 16	O munícipe deverá ser sempre notificado se alguma informação do seu perfil for alterada sem a sua ação direta.
M1 – 17	Todos as informações deverão ter associados registos de auditoria sobre a data, hora e autor desse registo.
M1 – 18	Deverá ser possível ao utilizador mudar o idioma da página, tendo como opção PT, EN
M1 – 19	No final do processo de registo o utilizador deverá ficar caracterizado como certificado e de nível de confiança alto.

3.2 Módulo 2 - Registo Simplificado da Entidade

Este requisito traduz-se na necessidade de um processo de registo ágil, sem burocracias, que permitam aos munícipes que não possuam forma de utilizar CC/CMD ou efetuar o processo de Reconhecimento Facial (ou outro mecanismo de prova de vida) possam aceder a um conjunto mínimo de funcionalidades que lhes permita a submissão e consulta de pedidos.

Pretende-se que durante este processo de registo seja possível ao requerente definir um par “username/password” que lhe possibilite o acesso através de mecanismo de duplo fator de verificação, combinando informação que o utilizador tem conhecimento com algo que ele possua (telefone, autenticador, etc...). Desta forma pretende-se mitigar o risco de registos de entidades e acessos não fidedignos.

Os dados pessoais recolhidos nos formulários serão sincronizados com a Gestão Central de Entidades com a atribuição do NUM (Numero de Município).

Com este processo de registo o requerente ficará caracterizado como de nível de confiança baixo (não certificado), existindo a possibilidade de, posteriormente, passar para nível de confiança alto, utilizando os mecanismos previstos no ponto 3.1.

Pretende-se que um utilizador caracterizado com este nível de confiança possa submeter e consultar processos associados ao seu NUM.

Os casos de uso que detalham este processo são referenciados no Anexo B do presente CE como A3.

ID	Requisito funcional
M2 - 1	Deverá existir a possibilidade de mostrar textos explicativos das várias alternativas de registo, configuráveis em backoffice.
M2 - 2	Deve existir a possibilidade de definir campos de preenchimento obrigatório, e o sistema deverá avisar da necessidade do seu preenchimento.
M2 – 3	Independentemente dos campos obrigatórios poderem ser configurados em backoffice (ver administração), o campo de ‘nome’ e ‘nif’ deverão ser sempre obrigatório, bem como o 2FA (email ou telefone).
M2 – 4	Deverá ser obrigatório criar um par “utilizador/password”. Esta password deverá cumprir os requisitos de complexidade mínimos de segurança (ver requisitos não funcionais)
M2 – 5	O utilizador obrigatoriamente deverá definir um email ou número de telefone como 2FA (2º fator de autenticação).
M2 – 6	Para concluir o processo de registo deverá ser feita a validação do 2FA gerando um OTP de 4 dígitos a enviar por email ou SMS.
M2 – 7	Em caso de conclusão do processo com sucesso, deverão os dados ser sincronizados com o GCE (Gestão Central de Entidades) e gerado o NUM (Nº do Município)
M2 – 8	Em caso de conclusão do processo com sucesso, deverá o sistema enviar um email de confirmação ao utilizador contendo os detalhes principais e o respetivo NUM
M2 – 9	O utilizador deverá ter a possibilidade de cancelar o processo de registo em qualquer fase até à sua conclusão, e nenhum dado ou atributo deverá ficar persistente na base de dados da plataforma.

M2 – 10	O tempo de Idle Timeout, para fecho automático da sessão, no caso de inatividade deverá ser 20 minutos
M2 – 11	O munícipe deverá ser sempre notificado se alguma informação do seu perfil for alterada sem a sua ação direta.
M2 – 12	Todas as informações deverão ter associados registos de auditoria sobre a data, hora e autor desse registo.
M2 – 13	Deverá ser possível ao utilizador mudar o idioma da página, tendo como opção PT, EN
M2 - 14	No final do processo de registo o utilizador deverá ficar caracterizado como certificado e de nível de confiança baixo.

3.3 Módulo 3 - Reconhecimento facial com prova de vida

Como alternativa à plataforma dos serviços comuns da AMA (enquanto esta não disponibilizar este serviço), e prevendo a impossibilidade de utilização do CC/CMD de forma rápida, pretende-se implementar um módulo de reconhecimento facial, em tempo real com prova de vida, que permita ao munícipe efetuar o registo na Plataforma de Registo e Autenticação e ficar certificado e caracterizado como sendo de nível de confiança alto.

Para o efeito, pretende-se que o utilizador tenha a possibilidade de confrontar a fotografia do seu cartão de cidadão, com a biometria do seu rosto em tempo real, ou através de uma fotografia ou de um vídeo. O sistema deverá recolher os atributos constantes na fotografia do CC, mediante autorização expressa do utilizador.

Por uma questão de privacidade e garantia de proteção de dados, pretende-se preferencialmente que este módulo esteja implementado numa estrutura “on-premise”, ficando alojada nos servidores da CMP. Na impossibilidade desta opção, deverá a solução ser implementada numa solução “On-Cloud”, que permita a escalabilidade dos recursos e que garanta a disponibilidade da solução, sem custos adicionais para a CMP. Uma opção de “Cloud” deverá ser sempre equacionada ao abrigo das regras do RGPD, com especial relevância para a localização do datacenter respetivo.

ID	Requisito funcional
M3 - 1	Deverá ser dada a opção ao utilizador de enviar a fotografia do cartão do cidadão em formato jpg, png, tif e pdf.
M3 - 2	Deverá ser possível efetuar a biometria e prova de vida com qualquer dispositivo que possua uma câmara que permita tirar fotografias e/ou vídeo.
M3 - 3	Deverá ser solicitada a autorização ao utilizador de recolha de atributos pessoais. Essa autorização deverá ficar registada na base de dados.

M3 - 4	Se o utilizador cancelar o processo de autenticação através de reconhecimento facial deverá ser redirecionado para a página inicial e informado que o seu registo não foi concluído.
M3 - 5	Após autenticação através de reconhecimento facial com sucesso deverá ser redirecionado para a página de recolha de atributos.
M3 - 6	Os dados autorizados e recolhidos na plataforma de reconhecimento facial do cartão do cidadão deverão ser preenchidos automaticamente na ficha do perfil do munícipe.
M3 - 7	Não deverá ser solicitado mais nenhuma informação ao utilizador além da fotografia do CC e da prova de vida (imagem/vídeo) para se concluir o processo de reconhecimento facial.
M3 - 8	Todas as imagens ou vídeos utilizados para efetuar o reconhecimento facial, deverão ser eliminados do servidor, no final do processo.
M3 - 9	Deverá ser possível ao utilizador mudar o idioma da página, tendo como opção PT, EN
M3 - 10	O tempo de Idle Timeout, para fecho automático da sessão, no caso de inatividade deverá ser 20 minutos

3.4 Módulo 4 - Registo Certificado do Representante Legal da Empresa

Pretende-se neste processo disponibilizar funcionalidades de acessos aos serviços de informação municipais aos representantes legais das empresas, ou a terceiros nomeados por si através de procuração, que permitam a submissão e consulta de informação relativa à empresa.

Para este efeito pretende-se implementar um mecanismo de registo ágil, sem burocracias, que garanta, perante a informação constante na Conservatória do Registo Comercial, que os utilizadores que estejam caracterizados como certificados de nível alto (ponto 3.1) sejam efetivamente os representantes legais, através da consulta e utilização do Código de Acesso da Certidão Permanente. Em alternativa, pretende-se garantir que o registo certificado de representante legal de empresa possa ser efetuado através da entrega da documentação/procurações, de forma presencial nos serviços municipais, o qual terá que passar por um processo de validação e certificação, e posterior gestão através de backoffice de gestão de identidades (ver ponto 3.5).

Com este processo de registo o requerente ficará caracterizado como de nível de confiança alto (certificado) e como representante legal da empresa.

Pretende-se que um utilizador caracterizado com este nível de confiança possa submeter e consultar processos associados ao NIF da entidade que representa.

Os casos de uso que detalham este processo são referenciados no Anexo B do presente CE, como A4, A5 e B3.

ID	Requisito funcional
M4 - 1	O utilizador certificado, que efetuou autenticação pelos métodos previstos em B1 tem a opção de assumir o papel de representante legal e seleciona numa lista, qual das empresas pretende representar.
M4 - 2	O utilizador certificado, que efetuou autenticação pelos métodos previstos em B1 tem a opção de proceder ao registo de novo papel de representante de empresa, fornecendo o NIF e código de acesso à certidão permanente. A plataforma deverá procurar os dados da empresa no GCE e tentar de forma automática reconhecer na conservatória do registo comercial se o utilizador é representante legal da empresa.
M4 - 3	O processo de reconhecimento automático do representante legal deverá ter em consideração se está definido na certidão permanente a exigência de mais assinaturas de outros representantes legais.
M4 - 4	Caso não seja possível fazer o reconhecimento automático através da certidão permanente, deverá o sistema exigir a submissão de documentos, que comprovem o papel de representante, para serem analisados e validados em backoffice.
M4 - 5	Deverá ser possível ao munícipe que pretende iniciar o processo de reconhecimento de representante legal, anexar documentos pdf (procurações, certidões).
M4 - 6	Em caso de conclusão do processo com sucesso, deverá o sistema enviar um email de confirmação ao utilizador.
M4 - 7	O tempo de Idle Timeout, para fecho automático da sessão, no caso de inatividade deverá ser 20 minutos
M4 - 8	No final do processo de registo o utilizador deverá ficar caracterizado como representante legal da empresa.
M4 - 9	A qualidade de representante legal deverá ter uma validade de 1 ano, ou uma data limite, devendo o sistema voltar a solicitar a validação dos elementos constantes da certidão permanente no final desse período.
M4 - 10	Deverá ser possível ao utilizador mudar o idioma da página, tendo como opção PT, EN

3.5 Módulo 5 - Autenticação da Entidade

Pretende-se disponibilizar ao munícipe duas formas de autenticação:

- Para os utilizadores cujo nível de confiança é alto (certificados), a utilização do CC/CMD. Os casos de uso que detalham este processo são referenciados em documento anexo como B1.
- Para todos os utilizadores (nível de confiança baixo ou nível de confiança alto), a utilização do par “username/password” previamente configurados, e nestes casos, sempre com o duplo fator de autenticação (email, telemóvel, autenticador, etc...). Os casos de uso que detalham este processo são referenciados no Anexo B do presente CE, como B2.

ID	Requisito funcional
M5 – 1	Deverá o utilizador ser informado que foi redirecionado do Service Provider (aplicação que faz o request de autenticação) para a plataforma de autenticação.
M5 – 2	Deverá ser apresentado ao utilizador as duas possibilidades de autenticação CC/CMD ou utilizador/password.
M5 – 3	Após autenticação com sucesso, através dos métodos previstos neste módulo, deverá ser redirecionado para a página do Service Provider que solicitou a autenticação.
M5 – 4	Após autenticação com sucesso deverá ser dada a opção ao utilizador de assumir o papel de 1. representante legal (caso se aplique), 2. iniciar novo processo de reconhecimento de representante legal, 3. Utilizador individual
M5 – 5	O sistema deverá detetar a situação em que um utilizador registado com um nível de confiança baixo (A3) efetuar o processo de autenticação utilizando o CC/CMD (B1), com o mesmo NIF e Nome, e propor ao utilizador a evolução da sua conta, solicitando o par utilizador/password da conta previamente criada no processo A3. Caso o processo decorra com sucesso, deverá o utilizador ficar caracterizado como certificado e de nível de confiança alto.
M5 – 6	Deverá o sistema bloquear temporariamente sempre que o utilizador exceder o limite de tentativas falhadas de autenticação.
M5 – 7	Deverá o sistema detetar acessos através de novos dispositivos e localizações suspeitas e avisar o utilizador para confirmar se o acesso é fidedigno.
M5 - 8	O tempo de Idle Timeout, para fecho automático da sessão, no caso de inatividade deverá ser 20 minutos
M5 – 9	Deverá ser possível ao utilizador mudar o idioma da página, tendo como opção PT, EN

3.6 Módulo 6 - Utilitário de consolidação e normalização de Identidades

Pretende-se a criação de uma área de consolidação, sincronização e normalização de identidades que se mostre eficiente em detetar um conjunto de situações de não conformidade que á partida se esperam que possa acontecer, dando opções ao utilizador.

ID	Requisito funcional
M6 – 1	Sempre que o utilizador proceda a uma ação de autenticação com sucesso através dos métodos previstos no módulo 1 (A1 e A2), sem ter efetuado previamente a ação de registo (sem NUM atribuído), deverá o sistema automaticamente informar e solicitar a criação da respetiva identidade.
M6 - 2	Sempre que um utilizador, com registo prévio através do módulo 2 (A3), proceda com sucesso a uma autenticação para utilizadores certificados com CC/CMD ou Utilizador/password com reconhecimento facial, e cujo nome e nif coincidam com o registo prévio, deverá o sistema informar o munícipe que já existe um perfil associado ao seu NIF e propor a evolução do registo para um nível de confiança alto.
M6 - 3	Para efetuar a evolução do perfil para um nível de confiança alto, deverá o sistema obrigar a autenticação com sucesso, complementando com o 2FA, na conta do registo prévio.
M6 - 4	Se o utilizador não concordar em evoluir a conta, previsto no requisito M6-2, deverá o sistema criar uma situação de alerta, identificando a conta de registo prévio, para ser analisada em backoffice.
M6 - 5	Sempre que o utilizador conclua a evolução do perfil para nível de confiança alto com sucesso, deverá o sistema enviar um email de confirmação contendo os detalhes principais e o respetivo NUM.
M6 - 6	Todas as informações deverão ter associados registos de auditoria sobre a data, hora e autor desse registo.

3.7 Módulo 7 - Gestão da Identidade (Backoffice)

Pretende-se a criação de uma área de backoffice, a ser gerida pelos serviços internos da CMP, que permita a configuração geral da plataforma, gestão do ciclo de vidas das identidades, no que diz respeito à criação, certificação, fusão, eliminação, manutenção de palavras passe, associação à gestão central de entidades, entre outras. O acesso a esta plataforma deverá ser efetuado unicamente pela rede interna da CMP, com autenticação integrada com a AD.

Níveis de Acesso:

O funcionamento do Backoffice da Plataforma de Registo e Autenticação de Municípes terá por base uma organização por níveis de acesso. A organização de acessos será feita pela segmentação de perfis de utilizador. A título de exemplo poderemos ter:

- **Administrador** –todas as funcionalidades e configurações da plataforma. Gere a lista de permissões e utilizadores.

- **Utilizador** - terá acesso a consultar o perfil dos utilizador, lista de histórico de acessos, lista de dispositivos utilizados e localização, lista de bloqueios, validar os registos de representante legal, fusão de entidades, sincronização com GCE, efetuar filtros e retirar listagens.

ID	Requisito funcional
M7 – 1	O acesso a este módulo só deverá ser possível para utilizadores autenticados através de credenciais da AD.
M7 – 2	Deve ser possível o acesso às configurações gerais do website, como por exemplo: tamanho e resolução máxima das imagens, tamanho máximo dos anexos, lista de campos obrigatórios.
M7 – 3	Deve ser possível o acesso ao histórico de acessos e logs com a informação detalhada das ações e atividades realizadas por cada utilizador do backoffice.
M7 - 4	Acesso e informações relativos a número de acessos e ao dashboard da plataforma.
M7 - 5	A solução deverá permitir aos Administradores adicionar, configurar acessos e permissões ou remover perfis de utilizadores
M7 - 6	Deverá ser possível consultar os atributos de perfil de uma identidade.
M7 - 7	Deverá ser possível consultar o histórico de acessos, dispositivos e localizações dos utilizadores.
M7 - 8	Deverá ser possível consultar a lista de utilizadores bloqueados.
M7 - 9	Deverá ser possível definir o número de tentativas e o tempo de bloqueio.
M7 - 10	A plataforma deverá implementar mecanismos de pesquisa para consulta rápida dos utilizadores, através da utilização de filtros.
M7 - 11	Possibilitar aos utilizadores CMP consultar a lista de registos de representante legal pendentes, consulta dos elementos (código da certidão permanente ou anexos) e proceder à validação.
M7 - 12	Deverá ser possível ao utilizador CMP evoluir uma conta de nível de confiança baixo (não certificada, proc A3) para uma conta de nível de confiança alto (certificada) mediante a apresentação de documentação nos serviços da CMP, ficando registado o fundamento do utilizador CMP.
M7 - 13	O utilizador CMP deverá conseguir fazer a fusão de entidades, cancelamento ou reativação de entidades.
M7 - 14	O munícipe deverá ser sempre notificado se alguma informação do seu perfil for alterada sem a sua ação direta.
M7 - 15	Todos as informações deverão ter associados registos de auditoria sobre a data, hora e autor desse registo.
M7 - 16	O tempo de Idle Timeout, para fecho automático da sessão, no caso de inatividade deverá ser 20 minutos

M7 - 17	A opção de “Terminar Sessão” deverá estar acessível em todos os ecrãs.
---------	--

4 Mockups funcionais

Apresentam-se alguns mockups relativos às funcionalidades pretendidas em termos visuais.

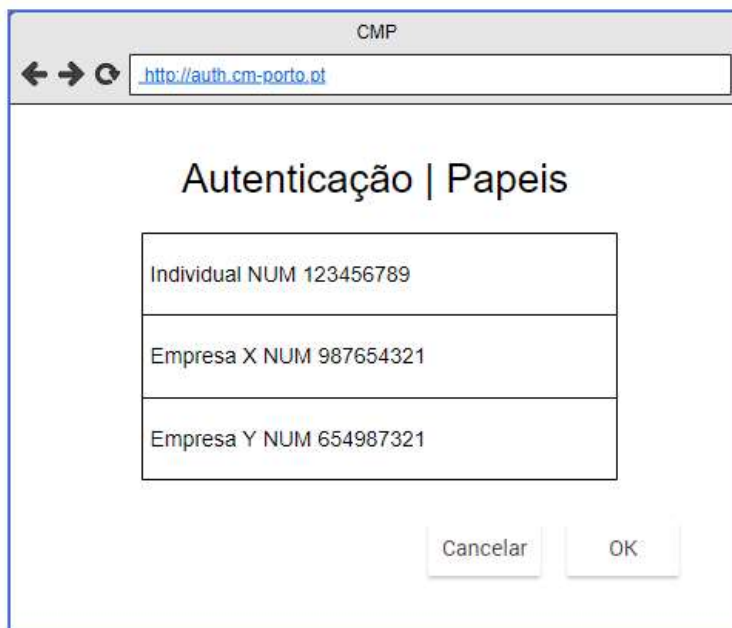
Esta sugestão de representação gráfica é meramente indicativa e poderá ser alterada para que a plataforma consiga apresentar os elementos visuais de acordo com as boas práticas de usabilidade gráfica e de experiência de utilização (UI/UX) para este tipo de sistema.



Figura 1 - Página inicial de autenticação



Figura 2 - Confirmação por OTP - 2º Fator Autenticação



Individual NUM 123456789
Empresa X NUM 987654321
Empresa Y NUM 654987321

Esta janela poderá ser opcional, mediante parametro do service provider que requisitou a autenticação

Figura 3 - Página de seleção de papeis



[Cartão do Cidadão ou Chave Móvel Digital](#)

[Reconhecimento com Prova de Vida](#)

[Registo Simplificado](#)

[Registo de Empresa](#)

Figura 4 - Página de Registo



Figura 5 - Detalhes e Credenciais de Acesso



Figura 6 - Registo de Empresas

5 Requisitos não funcionais

ID	Requisito funcional
NFR - 1	A versão <i>desktop</i> e <i>mobile</i> deve ter uma interface com design responsivo. <i>Responsive web design</i> : os elementos que o compõem a plataforma devem adaptar-se automaticamente à largura de janela do dispositivo no qual ele está a ser visualizado.
NFR - 2	Todas as interfaces devem ser simples e intuitivas, e orientar-se pelas boas práticas de usabilidade. A estrutura das páginas web devem ser desenhadas tendo em conta as boas práticas de UX&UI (user experience & user interface).
NFR - 3	A plataforma deve fornecer os termos e condições de uso.
NFR - 4	A plataforma deve fornecer a política de privacidade de dados.
NFR - 5	A plataforma deve fornecer a política de <i>cookies</i> .
NFR - 6	A plataforma deve orientar-se pelo Manual de identidade do Porto., seguindo as regras de uso da marca.
NFR - 7	A plataforma deve ser compatível com as normas Web Content Accessibility Guidelines (WCAG) 2.1 ⁷ e pelo Selo de Usabilidade e Acessibilidade ⁸ . O cumprimento destas diretrizes fará com que o conteúdo se torne acessível a um maior número de pessoas com incapacidades, incluindo cegueira e baixa visão, surdez e baixa audição, dificuldades de aprendizagem, limitações cognitivas, limitações de movimentos, incapacidade de fala, fotossensibilidade bem como as que tenham uma combinação destas limitações. Após concluído, o <i>website</i> deve passar pelo validador nacional de acessibilidade para cidadãos ⁹ , com percentagem de 80%.
NFR - 8	A plataforma deve cumprir com a norma ISO 9241-11, relativa à Usabilidade.
NFR - 9	A plataforma deve utilizar a família tipográfica Neue Haas Unica Pro, como fonte principal, e tipo de letra Regular, para elementos pontuais, a indicar.
NFR - 10	A plataforma deverá disponibilizar diferentes tamanhos e estilos da fonte tipográfica, com as seguintes orientações: • Títulos: ○ H1: 48px (<i>desktop</i>); 36px (<i>mobile</i>) ○ H2: 36px (<i>desktop</i>); 24px (<i>mobile</i>) ○ H3: 24px (<i>desktop</i>); 20px (<i>mobile</i>) ○ H4: 20px (<i>desktop</i>); 18px (<i>mobile</i>) • Parágrafo: ○ Parágrafo <i>default</i>: 18px (<i>desktop</i>); 16px (<i>mobile</i>) ○ Parágrafo pequeno: 16px (<i>desktop</i>); 14px (<i>mobile</i>)

⁷ W3C Accessibility Standards (<https://www.w3.org/TR/WCAG21/> e <https://www.w3.org/Translations/WCAG20-pt-PT/#visual-audio-contrast>).

⁸ Portal de Usabilidade e Acessibilidade do Governo Português (<http://www.acessibilidade.gov.pt/>).

⁹ Validador nacional de acessibilidade (<http://www.acessibilidade.gov.pt/web/checklist-10aspetos.html>).

	- Estilo da fonte: - Regular - Bold - Itálico - Sublinhado Espaço entre linha e parágrafo: min. 1.4px
NFR - 11	A plataforma deve aplicar o seguinte estilo de texto e paleta de cores no conteúdo de texto, orientada à marca Porto. e à usabilidade e acessibilidade do <i>website</i>: - Cor principal: Azul #243E8B - Texto principal: Preto #0b0c0c - Texto secundário: Cinzento escuro #626a6e - Hiperligações de texto: - Link: Azul #243E8B <u>underline</u> - Link hover: Azul #243E8B <u>underline</u> bold - Link visited: Vermelho escuro #7E184B <u>underline</u> - Link desativado: Cinzento claro #D1D1D1 <u>underline</u> :normal <u>Ocupação da via pública - reapreciação</u> :hover <u>Ocupação da via pública - reapreciação</u> :visited <u>Ocupação da via pública - reapreciação</u> :disable <u>Ocupação da via pública - reapreciação</u> - Hiperligação de texto para <i>website</i> externo: adicionar ícone (16 x 16 px) representativo de link externo: :external-link <u>Ocupação da via pública - reapreciação</u> ↗ - Estilo de texto <i>underline</i> deverá ter uma distância de cerca de 5 a 6px da linha base do texto, com <i>border</i> de 1px; - Estado de erro (apenas para mensagens de erro): Vermelho #d4351c - Estado de alerta (apenas para mensagens de alerta): Amarelo #ffdd00 e Preto #0b0c0c
NFR - 12	A plataforma deve aplicar a seguinte paleta de cores no desenho de interface do <i>frontend</i>:

¹⁰ Política de privacidade e política de cookies da Câmara Municipal do Porto: <http://www.cm-porto.pt/politica-de-privacidade/politica-de-privacidade>

6 Requisitos tecnológicos

ID	Requisito funcional
TR - 1	A plataforma deverá permitir a integração com outras plataformas internas e externas através de APIs, por exemplo: Gestão Central de Entidades
TR - 2	A plataforma deverá expor web-services SOAP/REST que permitam a aplicações cliente autenticar por utilizador/password e validar o OTP.
TR - 3	A plataforma deverá prever a integração com o sistema de notificações por email e SMS da CMP.
TR – 4	A plataforma deverá ter todos os módulos de funcionamento <i>on-premises</i> , utilizando servidores aplicacionais e de base de dados internos.
TR – 5	A plataforma deve ser desenvolvida utilizando (preferencialmente): Sistema Operativo: Linux Centos 7 Sistema de BD: PostgreSQL 11 Servidor web: Apache Motor de pesquisa: Elasticsearch 7.3 (ou posterior)
TR – 6	A plataforma deverá garantir a autenticação SSO num formato federado baseado na RFC 6265 garantindo a integração multidomínio para as aplicações existentes na CMP de forma a assegurar temporariamente a compatibilidade da autenticação das aplicações legadas, nomeadamente os formulários online e a consulta de processos online.
TR – 7	A plataforma deve conter um sistema de apoio à de continuidade do negócio, nomeadamente sistema de backup e restauro.
TR – 8	Assegurar critérios de segurança e confidencialidade HTTPS. Solução com nível de segurança elevado e certificações. Todas as comunicações entre os equipamentos e o servidor deverão ser feitas de forma segura SSL/HTTPS.
TR – 9	Integração no sistema de backups e restauro dos sistemas informáticos da Câmara Municipal do Porto.
TR – 10	Desenvolvimento e disponibilização de ambiente interno de pré-produção atualizado, para testes e formação, durante o decorrer do presente contrato;
TR – 11	A plataforma deverá funcionar como Identity Provider Federado, e/ou como proxy de autenticação, implementando protocolos de autenticação (OAuth, OpenID Connect, SAML2.0) que permitam a interoperabilidade futura com aplicações moveis, cartão do munícipe, SSO multidomínio, entre outros.
TR – 12	Disponibilização de manuais e documentação de suporte à plataforma;

7 Metodologia de Gestão de Projeto

De forma a garantir o sucesso do projeto, a entidade adjudicatária deve apresentar uma proposta de plano de execução do projeto, que deverá seguir as melhores práticas de desenvolvimento, tais como:

- Entrega inicial de proposta de *mockups* para análise e validação de design e navegabilidade.
- Agendamento de pontos de situação regulares (semanais/quinzenais) com a equipa do Município do Porto alocada ao projeto;

Deverá ser entregue o calendário com a descrição e metodologia para todas as fases de implementação do projeto, e indicando os principais marcos (milestones), as dependências de tarefas e respetivos formatos de documentação.

Devem ser apresentadas competências ou formação comprovada na metodologia escolhida, assim como a ferramenta ou plataforma de gestão de projeto a utilizar.

O Município do Porto, por si ou através de uma entidade por si indicada, assumirá a responsabilidade de acompanhamento de projeto.

8 Instalação, customização, formação e manutenção

Deve ser garantido, pela entidade adjudicatária, a instalação, customização e manutenção da Plataforma de Registo e Autenticação de Múncipes, durante o período de desenvolvimento do projeto e, posteriormente, no período de adaptação, no acompanhamento e formação das equipas envolvidas. De forma generalizada, devem ser consideradas as seguintes ações:

- A empresa deve alocar ao projeto uma equipa de técnicos e consultores tecnológicos, *web designers* e UX & UI's, que devem estar presentes nos serviços da Câmara Municipal do Porto sempre que solicitados;
- A empresa deve garantir o acompanhamento e validação do desenvolvimento da plataforma, pela equipa do Município do Porto alocada ao projeto;
- A empresa deve garantir a validação de requisitos não funcionais, funcionais e tecnológicos pela equipa do Município do Porto alocada ao projeto;
- A empresa deve garantir a realização de testes de usabilidade da plataforma, ao longo do seu desenvolvimento, com os diferentes tipos de utilizadores, com a apresentação do respetivo relatório;
- A empresa deve garantir a realização de testes de acessibilidade à plataforma, com a apresentação do respetivo relatório;
- A empresa deve garantir a realização de testes de segurança da plataforma de produção, com a apresentação do respetivo relatório;
- A empresa deve garantir a realização de testes de performance/carga da plataforma de produção, com a apresentação do respetivo relatório;
- A plataforma deverá passar nos testes de auditoria de segurança e performance, a realizar por entidade externa credenciada solicitada pela CMP, e proceder às correções identificadas, sob pena de não aceitação do produto final.

- A empresa deve garantir a formação técnica antecipada aos técnicos do Município do Porto para administração e gestão da nova plataforma, com a disponibilização de manuais de instalação, suporte e administração da mesma;
- A empresa deve garantir a formação antecipada à equipa do Município do Porto para utilização da nova plataforma, com a disponibilização de manuais de utilização;
- A empresa deve fornecer os requisitos e instruções de instalação de todos os componentes da plataforma, na fase inicial do projeto;
- A empresa deve garantir a correta instalação e funcionamento da plataforma nos seus diversos componentes.
- O código que venha a ser desenvolvido será propriedade do Município do Porto. O código (fontes e respetiva documentação) devem ser entregues na entrada em produção da plataforma.

9 Compatibilidade, Escalabilidade e Segurança

É fundamental assegurar que os desenvolvimentos inerentes a esta nova plataforma tenham especial consideração os aspetos da compatibilidade com as soluções atuais no universo dos sistemas de informação da CMP, nomeadamente o Balcão de Atendimento Virtual, Plataforma de Formulários Online e Processo de Consultas Online, bem como assegurar a migração das contas de utilizadores existentes na plataforma atual.

Outro aspeto de grande importância na gestão estratégica dos sistemas de informação é assegurar a escalabilidade e interoperabilidade desta nova plataforma para futuras soluções que possam vir a ser desenvolvidas num futuro próximo, nomeadamente o Portal do Município, Cartão do Município, aplicações móveis, bem como ligação com outros providers de autenticação (Google, Microsoft, etc).

No que diz respeito à segurança da solução a implementar é fundamental garantir mecanismos de controlo de acessos indevidos, nomeadamente o bloqueio preventivo e temporário das contas com respetivos alertas de segurança, bem como a validação no caso de alteração de plataforma, localização ou dispositivo.

No que diz respeito à componente tecnológica, carece ainda de posterior especificação mais detalhada, mas não necessariamente extensa, nomeadamente no que diz respeito à integração de federação com base nas tecnologias SAML 2.0, OpenID/OpenAuth.

Anexo B - JobStories

JobStories dos processos descritos no caderno de requisitos

#	Componente / Módulo	Opção	Requisito	Critérios	
1	Processo de Inscrição (Onboarding)	A1	Inscrição através da plataforma AMA	Dado que Quando e ou e e Então	o utilizador precisa de se autenticar através da plataforma da AMA é redirecionado para esta plataforma escolhe a autenticação através do cartão de cidadão escolhe a autenticação através da Chave Móvel Digital a autenticação é validada o utilizador autoriza a recolha de informação A plataforma da AMA comunica com a CMP enviando informação de autenticação e dos dados do utilizador
2	Processo de Inscrição (Onboarding)	A1	Inscrição através da plataforma AMA	Dado que Quando	que o utilizador foi autenticado na plataforma da AMA a CMP recebe as informações de autenticação

				e	é dada a opção para gerar um par “utilizador/password”
				e	existe validação de 2o fator de autenticação (email, sms)
				e	é criado o numero do munícipe NUM e realizada a sincronização na Gestão Central de Entidades
				Então	utilizador fica caracterizado como de nível de confiança alto (certificado)
3	Processo de Inscrição (Onboarding)	A2	Inscrição com Utilizador/Password e com Reconhecimento Facial e Prova de Vida	Dado que	o utilizador precisa de se autenticar através da plataforma de Reconhecimento Facial
				Quando	o utilizador é redirecionado para a plataforma de Reconhecimento Facial
				e	Utilizador fornece fotografia do cartão do cidadão
				e	faz prova de vida
				e	autoriza a recolha da informação
				Então	é redirecionado para a plataforma da CMP
4	Processo de Inscrição (Onboarding)	A2	Inscrição com Utilizador/Password e	Dado que	que o utilizador foi autenticado na plataforma de Reconhecimento Facial



			com Reconhecimento Facial e Prova de Vida	Quando	a CMP recebe as informações de autenticação
				e	é dada a opção para gerar um par “utilizador/password”
				e	existe validação de 2o fator de autenticação (email, sms)
				e	é criado o numero do munícipe NUM e realizada a sincronização na Gestão Central de Entidades
				Então	o utilizador fica caracterizado como de nível de confiança alto (certificado)
5	Processo de Inscrição (Onboarding)	A3	Inscrição com Utilizador e Password	Dado que	utilizador precisa de se autenticar
				Quando	Utilizador é reencaminhado para formulário de inscrição da CMP
				e	é recolhida informação relativa ao munícipe
				e	é gerado um par “utilizador/password”
				e	existe validação de 2o fator de autenticação (email, sms)

				e	é criado o número do munícipe NUM e realizada a sincronização na Gestão Central de Entidades
				Então	utilizador fica caracterizado como de nível de confiança baixo (não certificado)
6	Processo de Inscrição (Onboarding)	A4	Inscrição para Representante de Empresas	Dado que	o utilizador (gerente, ou pessoa afim) precisa de efetuar o processo de inscrição A1, ou A2 - para ser considerado certificado de nível alto
				Quando	utilizador inicia processo de inscrição como gerente de empresa
				e	fornece informação relativa à empresa
				e	fornece o código de acesso à Certidão Permanente para validação de representante autorizado (gerente)
				e	existe validação com sucesso
				Então	utilizador fica considerado como certificado e representante legal da empresa

7	Processo de Inscrição (Onboarding)	A5	Inscrição para Representante de Empresas, presencial e em Backoffice	Dado que	o utilizador (gerente, ou pessoa afim) precisa de efetuar o processo de inscrição A1, ou A2 - para ser considerado certificado de nível alto
				Quando	utilizador inicia processo de inscrição como gerente de empresa
				e	fornece informação relativa à empresa
				e	o utilizador se apresenta perante os serviços da CMP com a sua documentação pessoal e com a documentação da empresa (Pacto Social, Certidão Permanente, Procuração, etc...)
				Então	em BackOffice, é criado o perfil de gerente da empresa (representante legal)
				e	o utilizador fica considerado como certificado e representante legal da empresa
8	Processo de Autenticação (Login)	B1	Autenticação para utilizadores certificados (A1, A2), com papel de utilizador individual	Dado que	utilizador é considerado previamente certificado, por um método de autenticação certificado (AMA, Utilizador/Password com reconhecimento facial) ou apenas por Utilizador/Password com 2FA (email, sms)



			Quando	O utilizador seleciona o papel de utilizador individual
			Então	Utilizador tem acesso a submeter formulários e consultar todos os processos relativos ao seu NIF
			e	pode gerir o seu perfil, alterando a sua informação pessoal, alterar a palavra passe ou 2o fator de autenticação
			e	pode iniciar processo de registo de inscrição para gerente de empresas, sendo redirecionado para processo A4.
9	Processo de Autenticação (Login)	B2	Autenticação para utilizadores não certificados (A3), com papel de utilizador individual	Dado que O utilizador é considerado não certificado, por método de autenticação não certificado (Utilizador/Password com 2FA) Quando o utilizador acede à plataforma CMP Então o utilizador tem apenas acesso a submeter formulários e consultar todos os processos relativos ao seu NUM

			e	pode gerir o seu perfil, alterando a sua informação pessoal, alterar a palavra passe ou 2o fator de autenticação
			e	tem acesso a iniciar processo de certificação de utilizador, sendo redirecionado para o processo A1 ou A2
10	Processo de Autenticação (Login)	B3	Autenticação para utilizadores certificados (A4), com papel de utilizador representante de empresa	Dado que utilizador é considerado previamente certificado, por um método de autenticação certificado (AMA, Utilizador/Password com reconhecimento facial) ou apenas por Utilizador/Password com 2FA (email, sms) Quando o utilizador seleciona o papel de gerente Então o utilizador pode criar ou consultar informação relativa ao NIF da empresa que representa