



CONCURSO PÚBLICO INTERNACIONAL
N.º 152/21/DCP/GACD/SOFTWARE DE ADESÃO BIOMÉTRICA A
IDENTIDADE DIGITAL

Caderno de Encargos

AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA

PRESIDÊNCIA DO CONSELHO DE MINISTROS

RUA ABRANCHES FERRÃO Nº10 3º | 1600-001 LISBOA – PORTUGAL | + 351 217 231 200

www.ama.gov.pt/ | facebook.com/ama.gov.pt



PÁGINA [1 de 26](#)







Cláusulas jurídicas	4
<i>Cláusula 1.ª Objeto</i>	4
<i>Cláusula 2.ª Local da prestação de bens</i>	4
<i>Cláusula 3.ª Duração</i>	4
<i>Cláusula 4.ª Preço contratual</i>	4
<i>Cláusula 5.ª Preços base Unitários</i>	5
<i>Cláusula 6.ª Condições de pagamento</i>	5
<i>Cláusula 7.ª Propriedade intelectual</i>	6
<i>Cláusula 8.ª Sigilo</i>	6
<i>Cláusula 10.ª Cessão da posição contratual e subcontratação</i>	9
<i>Cláusula 11.ª Comunicações e notificações</i>	9
<i>Cláusula 12.ª Penalidades contratuais</i>	9
<i>Cláusula 13.ª Foro competente</i>	10
<i>Cláusula 14.ª Legislação aplicável</i>	10
<i>Cláusula 15.ª Descrição técnica do contrato</i>	11
<i>Cláusula 16.ª Níveis de serviço</i>	25
<i>Cláusula 17.ª Planeamento</i>	25
<i>Cláusula 18.ª Entregáveis e documentação</i>	25
<i>Cláusula 19.ª Mecanismos formais de acompanhamento</i>	25
<i>Cláusula 20.ª Regulamento Geral de Proteção de Dados</i>	26





CLÁUSULAS JURÍDICAS

Cláusula 1.ª

Objeto

O presente caderno de encargos compreende as cláusulas a incluir no contrato a celebrar com a Agência para a Modernização Administrativa, IP, (doravante abreviadamente designada por “AMA”), na sequência de procedimento pré-contratual que tem por objeto fornecimento de software de adesão biométrica a identidade digital, incluindo validação de segurança de documentos de identificação, reconhecimento facial, deteção de vida (“liveness”), e videoconferência e respetivos serviços acessórios, termos melhor definidos nas cláusulas técnicas do presente caderno de encargos.

Cláusula 2.ª

Local da prestação de bens

Os bens serão fornecidos nas instalações da AMA e do adjudicatário.

Cláusula 3.ª

Duração

1. O contrato terá a duração estimada de 36 meses contados da data da sua celebração, sem prejuízo das obrigações acessórias que devam perdurar para além da sua cessação.
2. Sem prejuízo do disposto no número anterior, o contrato cessa assim que os serviços prestados atinjam o preço contratual de 749.750,00€ (setecentos e quarenta e nove mil e setecentos e cinquenta euros).

Cláusula 4.ª

Preço contratual

1. Pelo fornecimento objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente caderno de encargos, a AMA deve pagar ao adjudicatário o valor resultante da aplicação dos preços unitários constantes da proposta adjudicada, até perfazer o preço contratual de 749 750,00€ (setecentos e





quarenta e nove mil setecentos e cinquenta euros), acrescido do IVA à taxa legal em vigor, se este for legalmente devido.

2. O preço referido no n.º 1 inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída à AMA, designadamente:
 - a) Despesas com deslocações, estadias e despesas de alimentação;
 - b) Encargos com telecomunicações;
 - c) Seguro de acidentes de trabalho.

Cláusula 5.ª

Preços base Unitários

1. Os preços base unitários aplicáveis ao objeto do contrato são os seguintes:
 - a) Verificação de presença de vida (liveness): 0,20 €
 - b) Comparação da Foto visível no Documento de Identificação com foto obtida da verificação de liveness (selfie): 0,12 €
 - c) Comparação da Foto na Base de dados com foto obtida da verificação de liveness (selfie): 0,12 €
 - d) Verificação de segurança avançada Cartão de Cidadão: 1,50 €
2. Para a componente de “Recolha de informação constante de Cartão de Cidadão e verificação básica de segurança” é definido um preço base de 12 000,00 € para uma utilização ilimitada durante o período do contrato.
3. São excluídas as propostas cujo valor seja superior aos preços base indicados nos números anteriores.

Cláusula 6.ª

Condições de pagamento

1. A faturação é efetuada mensalmente de acordo com o nº de processos iniciados de adesões à Chave Móvel Digital recorrendo ao software fornecido, de acordo com o preço unitário proposto.
2. O pagamento será efetuado no prazo 30 dias a contar da data da receção das faturas correspondentes, as





quais só podem ser emitidas após o vencimento da obrigação a que se referem.

3. As faturas devem discriminar os serviços a que se reportam, o número do contrato bem como o número de compromisso financeiro associado, o qual será indicado pela AMA, sob pena da sua devolução.
4. Caso as faturas apresentadas não sejam validadas pela AMA esta comunicará tal decisão ao cocontratante para que proceda à sua substituição.
5. As faturas deverão revestir a forma eletrónica, caso em que devem ser remetidos à AMA através de meio de transmissão escrita e eletrónica de dados para o Portal FEAP (Faturação Eletrónica na Administração Pública) disponibilizado pela ESPAP.
6. Só serão devidos os valores referentes às tarefas efetivamente prestadas e aceites nos termos do presente caderno de encargos.
7. O pagamento será realizado para o NIB/IBAN indicado em documento bancário apresentado pelo cocontratante o qual deverá ser atualizado sempre que necessário.
8. Em caso de atraso no cumprimento das obrigações pecuniárias por parte da AMA, o cocontratante tem o direito aos juros de mora sobre o montante em dívida, nos termos previstos no artigo 326.º do CCP e da Lei n.º 3/2010, de 27 de abril.

Cláusula 7.ª

Propriedade intelectual

1. Correm inteiramente por conta do cocontratante, os encargos e responsabilidades decorrentes da utilização, na execução do fornecimento dos equipamentos, de materiais, de elementos de construção, de hardware, de software ou de outros a que respeitem quaisquer patentes, licenças, marcas, desenhos registados e outros direitos de propriedade industrial ou direitos de autor ou conexos.
2. Se a AMA vier a ser demandada por ter sido infringido, na execução do contrato, qualquer dos direitos mencionados no ponto anterior, o cocontratante responderá nos termos do disposto no artigo 447.º, n.º 2, do Código dos Contratos Públicos.

Cláusula 8.ª

Sigilo





1. O cocontratante obriga-se a observar sigilo quanto a informação e documentação, técnica e não técnica, comercial ou outra, relacionada com a atividade da AMA ou qualquer outra entidade envolvida na execução do contrato.
2. A informação e documentação cobertas pelo dever de sigilo não podem ser transmitidas a terceiros, nem ser objeto de qualquer uso ou modo de aproveitamento que não o destinado direta e exclusivamente à execução do contrato.
3. O cocontratante obriga-se ainda a respeitar a confidencialidade sobre todos os dados ou informações de carácter funcional ou processual dos serviços da Administração Pública a que tenha acesso na execução do contrato.
4. O cocontratante assume igualmente o compromisso de remover e destruir, no final do contrato, todo e qualquer registo, eletrónico ou em papel, relacionado com os dados e processos analisados e que a AMA lhe indique para esse efeito.
5. O cocontratante obriga-se, de um modo especial, a guardar sigilo quanto ao conteúdo e utilização dos sistemas de informação da responsabilidade da AMA, nos termos legalmente previstos, relativamente à proteção de dados pessoais e à proteção jurídica de bases de dados.
6. Após ter conhecimento de alguma violação de dados pessoais o cocontratante notifica a AMA sem demora injustificada, em prazo inferior a 48 horas.
7. O cocontratante garante que terceiros que envolva na execução dos serviços respeitem as obrigações de sigilo e confidencialidade constantes nos números anteriores.

Cláusula 9.ª

Proteção de dados

1. O Cocontratante é obrigado a tratar todos os dados pessoais a que tiver acesso, de acordo com o previsto no Regulamento Geral de Proteção de Dados Pessoais aprovado pelo Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 (RGPD), devendo, nomeadamente:
 - a) Tratar os dados pessoais apenas mediante instruções documentadas da Entidade Adjudicante, incluindo no que respeita às transferências de dados para países terceiros ou organizações





- internacionais, a menos que seja obrigado a fazê-lo pelo direito da União ou do Estado-Membro a que está sujeito, informando nesse caso a Entidade Adjudicante desse requisito jurídico antes do tratamento, salvo se a lei proibir tal informação por motivos importantes de interesse público;
- b) Assegurar que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade;
 - c) Adotar todas as medidas exigidas nos termos do artigo 32.º do RGPD;
 - d) Garantir o cumprimento do RGPD, nas condições aqui previstas, quando pretenda contratar um subcontratante;
 - e) Tomar em conta a natureza do tratamento, e na medida do possível, prestar assistência à Entidade Adjudicante pelo tratamento através de medidas técnicas e organizativas adequadas, para permitir que este cumpra a sua obrigação de dar resposta aos pedidos dos titulares dos dados tendo em vista o exercício dos direitos previstos no capítulo III do RGPD;
 - f) Prestar assistência à Entidade Adjudicante no sentido de assegurar o cumprimento das obrigações previstas nos artigos 32.º a 36.º do RGPD, tendo em conta a natureza do tratamento e a informação ao seu dispor;
 - g) Consoante a escolha da Entidade Adjudicante, apagar ou devolver-lhe todos os dados pessoais depois de concluído o contrato, apagando as cópias existentes, a menos que a conservação dos dados seja exigida ao abrigo do direito da União ou dos Estados-Membros;
 - h) Disponibilizar à Entidade Adjudicante todas as informações necessárias para demonstrar o cumprimento das obrigações previstas na presente cláusula, facilitando e contribuindo para as auditorias, inclusive as inspeções, conduzidas pela Entidade Adjudicante ou por outro auditor por esta mandatado.
2. A Entidade Adjudicante, no caso de suspeitar de incumprimento do RGPD, pode notificar o Cocontratante para este, no prazo de 5 dias, demonstrar o total cumprimento do referido regulamento.
 3. Caso o Cocontratante não demonstre o total cumprimento do RGPD, seja porque não o demonstrou, seja porque não o cumpre, a Entidade Adjudicante fica autorizada a proceder à auditoria aos sistemas de informação do Cocontratante, ficando este responsável por todos os custos dessa auditoria.
 4. No caso previsto no número anterior, a Entidade Adjudicante poderá compensar os custos que tenha suportado com eventuais quantias que sejam devidas ao Cocontratante, ou através do acionamento da caução, caso esta tenha sido prestada, ou através do recurso às retenções que eventualmente tenham sido efetuadas.
 5. No caso de se verificar algum incumprimento do RGPD por parte do Cocontratante, este deverá, no prazo





de 10 dias, por fim ao incumprimento e demonstrá-lo à Entidade Adjudicante.

6. O não cumprimento do RGPD, por facto imputável ao cocontratante, é considerado, para todos os efeitos, incumprimento definitivo, podendo a Entidade Adjudicante resolver o contrato, ao abrigo da alínea a) do n.º 1 do artigo 333.º do CCP.
7. Caso o Cocontratante impeça ou não colabore na realização da auditoria referida no n.º 3 da presente cláusula, a Entidade Adjudicante poderá resolver o contrato, por oposição reiterada ao exercício dos poderes de fiscalização, ao abrigo da alínea c) do n.º 1 do artigo 333.º do CCP.

Cláusula 10.ª

Cessão da posição contratual e subcontratação

O cocontratante pode ceder a sua posição no contrato ou subcontratar parcialmente o objeto do presente procedimento, desde que previamente autorizado pela AMA.

Cláusula 11.ª

Comunicações e notificações

1. Sem prejuízo de se acordarem outras regras quanto às notificações e comunicações entre as partes, estas devem ser dirigidas para o domicílio ou sede contratual de cada uma nos termos previstos no contrato.
2. Qualquer alteração das informações de contacto constantes do contrato deve ser comunicada à outra parte.

Cláusula 12.ª

Penalidades contratuais

1. Pelo incumprimento de obrigações emergentes do contrato, a AMA pode exigir ao cocontratante o pagamento de uma sanção pecuniária, num montante a fixar em função da gravidade do incumprimento, nos seguintes termos:
 - a) Pelo incumprimento nos níveis de serviço de Alojamento da CMD e Entidade Certificadora serão aplicadas penalidades de 1% do preço contratual por 0,1% abaixo do nível de serviço aferido mensalmente;
 - b) Pelo incumprimento nos níveis de serviço de Processamento pedidos de adesão CMD online, por





cada carta entregue em incumprimento do nível de serviço contratualizado, será descontado o valor equivalente ao processamento de 10 pedidos de adesão em território nacional.

2. Na determinação da gravidade do incumprimento, a AMA tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do cocontratante e as consequências do incumprimento.
3. A sanção aplicada será descontada na fatura imediatamente seguinte ao facto que a originou ou, caso tal não seja possível, será emitida nota de crédito.
4. O valor acumulado das sanções pecuniárias não pode exceder 20 % do preço contratual, sem prejuízo do poder de resolução do contrato.
5. Nos casos em que seja atingido o limite previsto no número anterior e a AMA decida não proceder à resolução do contrato, por dela resultar grave dano para o interesse público, aquele limite é elevado para 30 %.
6. A aplicação das sanções previstas na presente cláusula será objeto de audiência prévia, nos termos previstos no n.º 2 do artigo 308.º do Código dos Contratos Públicos.

Cláusula 13.ª

Foro competente

Para a resolução de todos os litígios relativos, designadamente, à interpretação, execução, incumprimento, invalidade, resolução ou redução do contrato é competente o Tribunal Administrativo de Círculo de Lisboa.

Cláusula 14.ª

Legislação aplicável

Em tudo o omissa neste Caderno de Encargos, observar-se-á o previsto no Código dos Contratos Públicos e demais legislação aplicável.





Cláusulas Técnicas

Cláusula 15.ª

Descrição técnica do contrato

- **1. Enquadramento**

A AMA – Agência para a Modernização Administrativa, IP é a entidade responsável pela operacionalização de vários processos transversais que têm por objetivo melhorar a Administração Pública Portuguesa e disponibilizar serviços públicos pelo canal que o cidadão considere mais adequado.

A identificação inequívoca do cidadão perante os serviços públicos é uma necessidade premente à massificação na utilização dos serviços públicos na sua eletrónica, tendo a AMA vindo a desenvolver um conjunto de soluções de autenticação e de assinatura eletrónica qualificada com o Cartão de Cidadão (CC) de forma a garantir a toda a Administração Pública a possibilidade de integrar estas funcionalidades nos seus portais de forma simples e eficiente.

A Chave Móvel Digital (CMD) surgiu em 2015 como um meio simples e seguro de autenticação dos cidadãos em portais e sítios da Administração Pública na Internet, com dois fatores de segurança: uma palavra-chave e um código recebido por SMS.

No contexto da medida SIMPLEX “CMD SIMPLEX” e de autorização legislativa prevê-se a simplificação do processo de adesão à CMD, nomeadamente:

- Adesão em aplicação móvel (de forma autónoma), recorrendo à validação de documento de identificação, deteção de vida (liveness) e reconhecimento facial.
- Adesão através de Videoconferência, assistido por Operador, procedendo-se à validação de documento de identificação, e a reconhecimento facial.

2. Processos de adesão à CMD que utilizarão software no âmbito deste fornecimento





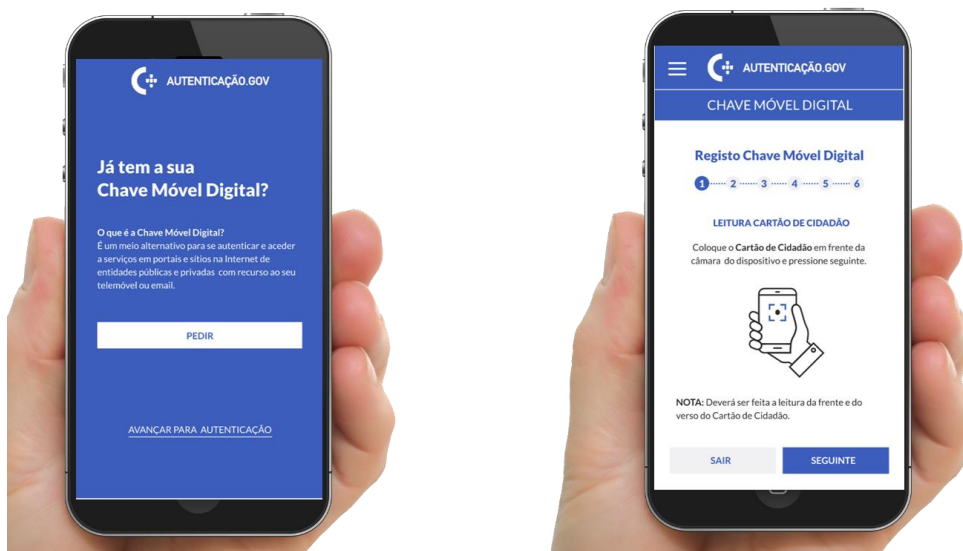
2.1 Processo de adesão à CMD em Aplicação móvel

Nesta secção apresenta-se uma descrição do processo preconizado para adesão à CMD tendo por base a recolha e comparação de dados biométricos do cidadão.

A utilização dos mecanismos de biometria no processo de adesão à CMD irá permitir, a titulares do Cartão de Cidadão, à disponibilização de mais uma forma de registo *online*.

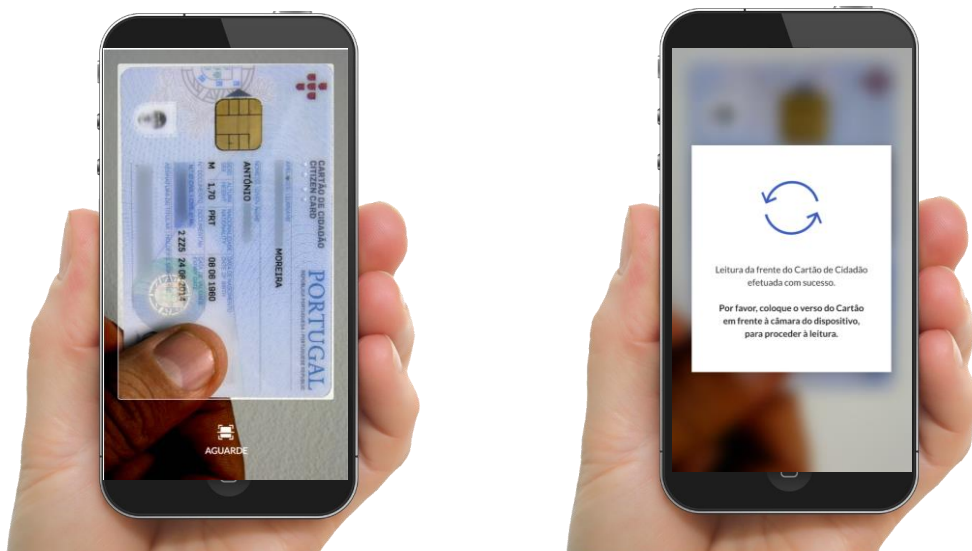
O modelo preconizado, utiliza o reconhecimento facial, com deteção de vida como mecanismo de validação da identidade, e também leitura automática dos dados do Cartão de Cidadão.

Assim, na primeira utilização de App móvel disponibilizada pela AMA (ou em qualquer momento) é possível ao utilizador iniciar um processo de registo na Chave Móvel Digital.

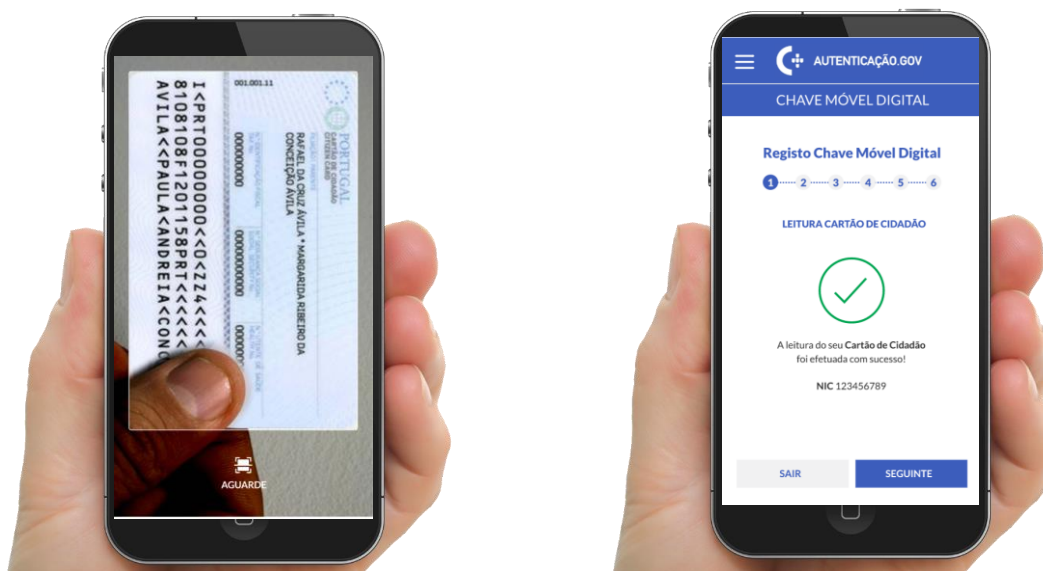


1. O primeiro passo do processo de adesão consiste na obtenção de fotografia da frente e verso do Cartão de Cidadão.

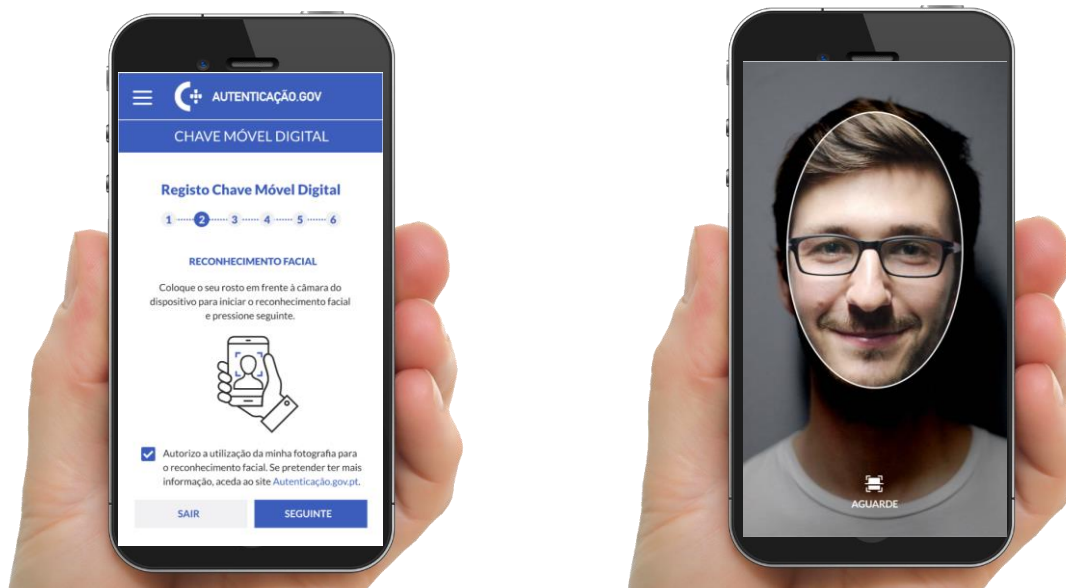




Após a obtenção da frente e verso do CC o sistema procede a uma validação básica de segurança em relação ao documento e à recolha dos dados constantes do Cartão, incluindo o Número de Identificação Civil e a fotografia constante do Cartão.

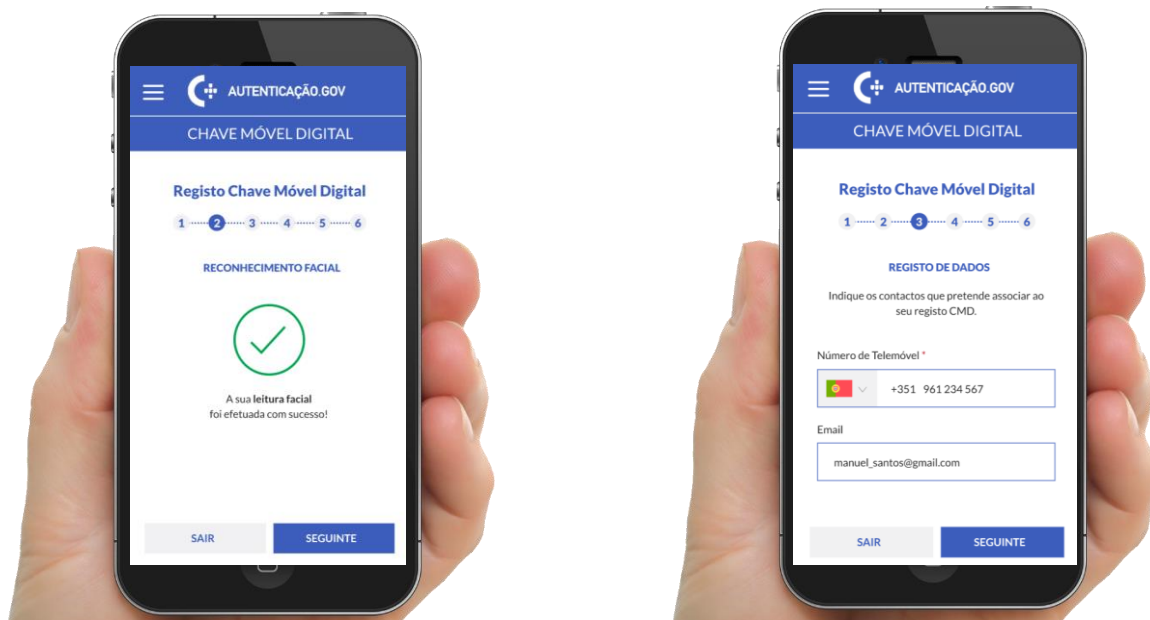


2. No passo seguinte, são recolhidas um conjunto de frames de fotografias ou vídeo do cidadão.

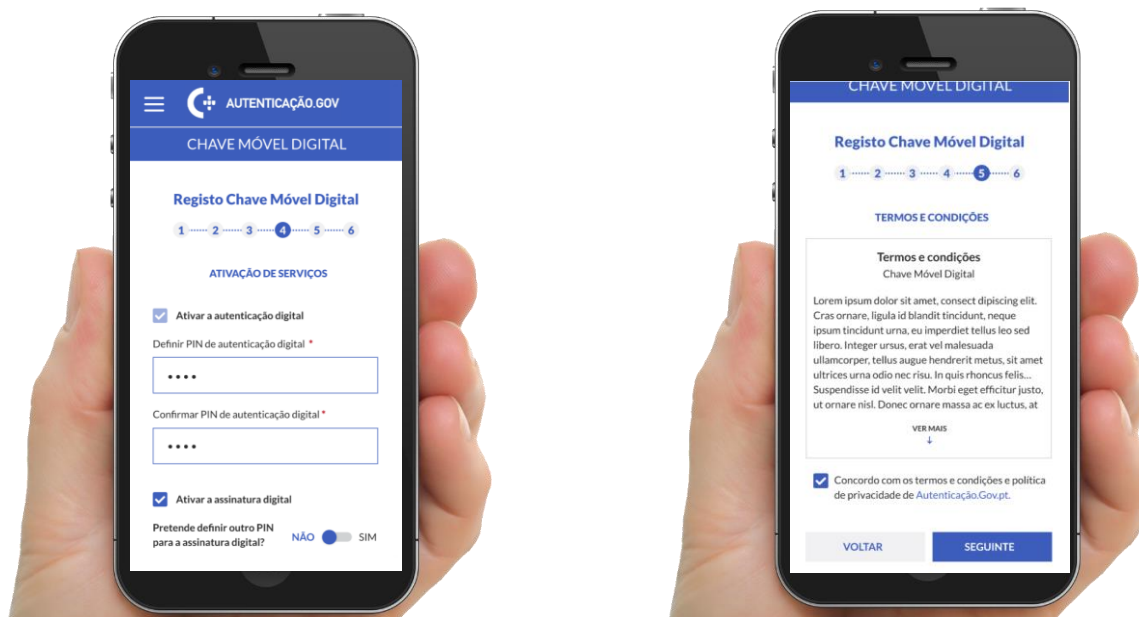


O conjunto de frames de fotografias ou vídeo são verificados em relação à presença de vida (liveness) e é comparada a fotografia do cidadão com a recolhida do Cartão de Cidadão (passo 1) e com a fotografia de alta resolução recolhida aquando do pedido de Cartão de Cidadão. Em caso de dúvidas é ainda feita uma verificação adicional de segurança à veracidade do Cartão de Cidadão.

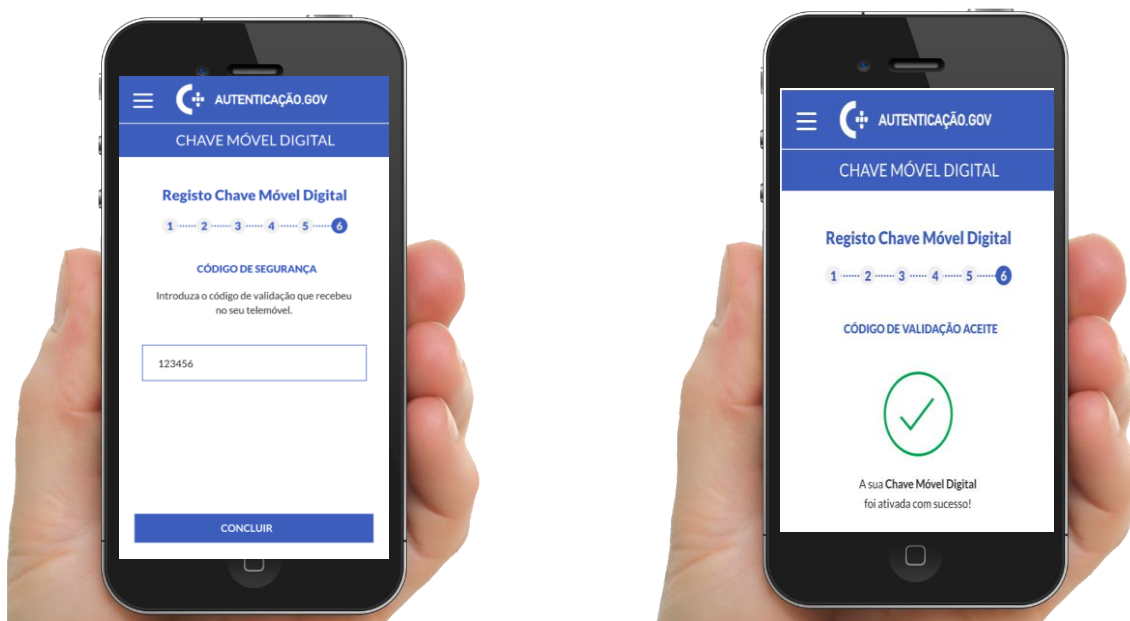
3. Efetuado com sucesso o processo de reconhecimento facial são solicitados os dados específicos da CMD, nomeadamente o nº de telemóvel e o email.



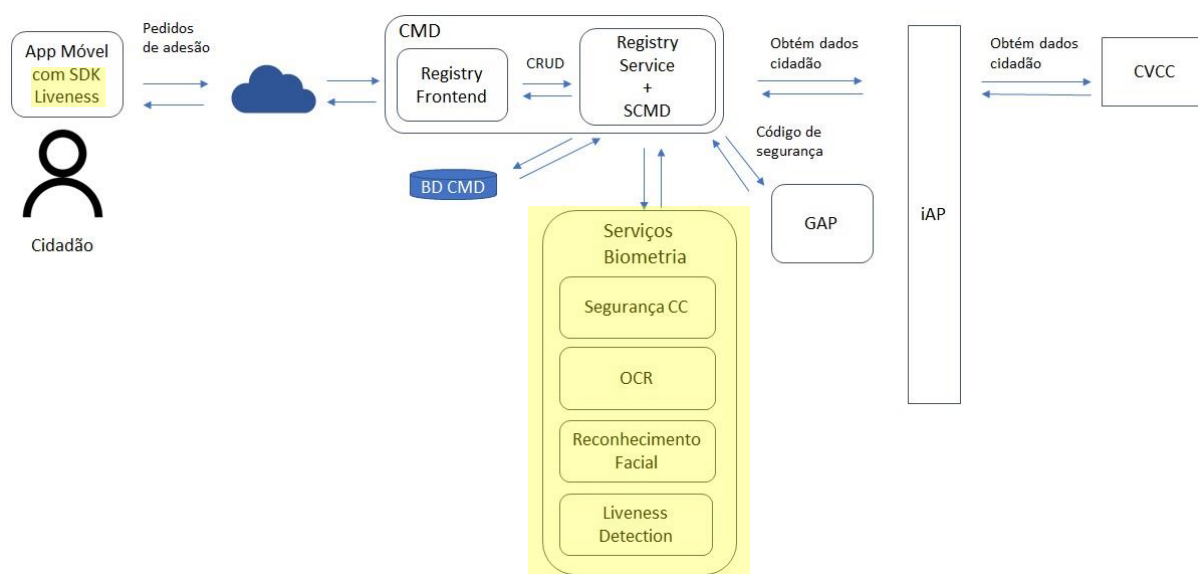
4. Em seguida o utilizador pode definir o PIN que pretende usar e, opcionalmente, aderir à assinatura da CMD.
5. Seguidamente são apresentados os termos e condições do serviço prestado que o utilizador deve ler e concordar.



6. Finalmente o utilizador deve introduzir o código temporário enviado por SMS para o telemóvel indicado no passo 3.
7. O utilizador é informado do sucesso do processo de adesão.



A figura seguinte sistematiza a arquitetura aplicacional subjacente.



Legenda:

Software alvo
de
fornecimento



Este processo de adesão, e o software proposto, cumpre os requisitos preconizados no Despacho n.º 2705/2021, de 11 de março do Gabinete Nacional de Segurança.

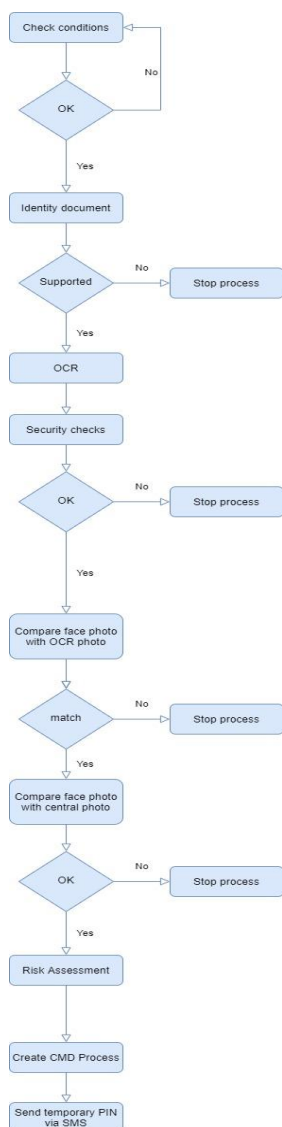
2.2 Processo de adesão à CMD em Videoconferência

A adesão à CMD em vídeo-conferência é realizada com agentes de Centros de Contacto da AMA, usando solução de software fornecida pelo adjudicatário de acordo com os seguintes passos:

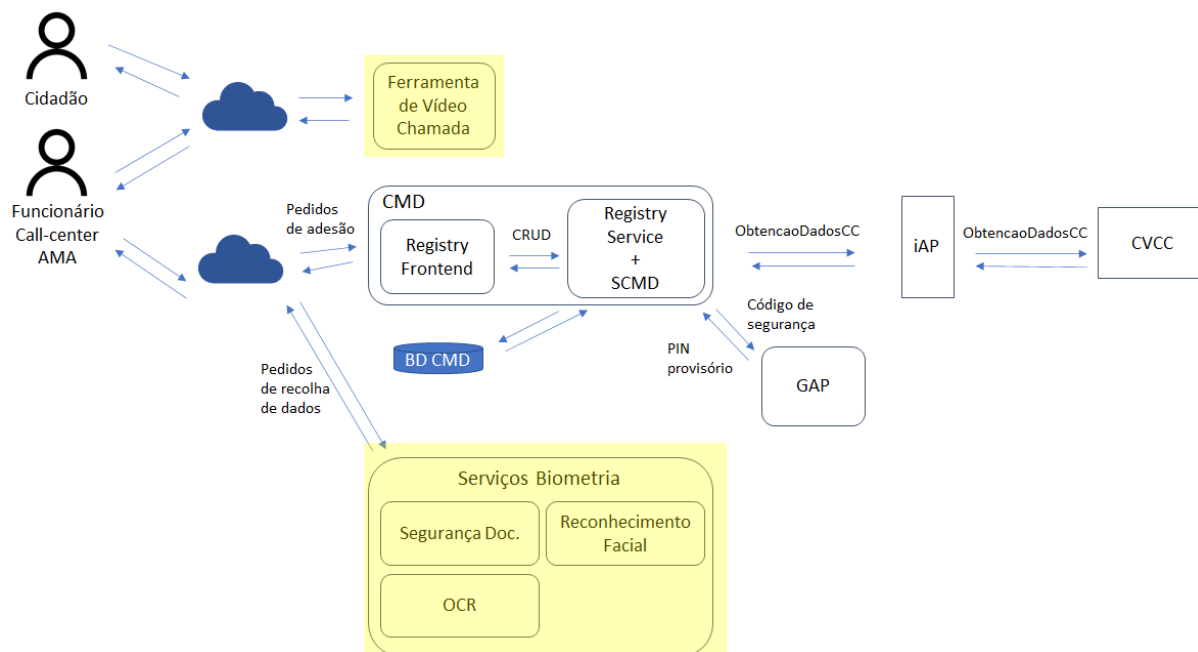
1. Processo de identificação do cidadão, incluindo:
 - a. Verificação de documento de identificação
 - b. Reconhecimento facial (frame da vide-conferencia do cidadão (selfie) vs. foto no documento)
2. Reconhecimento facial (rame da vide-conferencia do cidadão (selfie) vs. foto central)
3. Criação da conta CMD
4. Envio do PIN Provisório por SMS

O diagrama seguinte sistematiza os principais passos preconizados para este fluxo de adesão.





Na figura seguinte apresenta-se a arquitetura aplicacional preconizada (evidenciando a **amarelo** o software no âmbito do presente fornecimento)



Legenda:

Software alvo
de
fornecimento

Este processo de adesão, e o software proposto, cumpre os requisitos preconizados no Despacho n.º 154/2017 de 5 de dezembro do Gabinete Nacional de Segurança.

3. Âmbito do objeto

No âmbito do presente fornecimento pretende-se o fornecimento de software de adesão biométrica a identidade digital, incluindo validação de segurança de documentos de identificação, reconhecimento facial, deteção de vida ("liveness"), e videoconferência que assegure os seguintes requisitos:

3.1. OCR Cartão de Cidadão e verificação básica de segurança Cartão de Cidadão (CC)

O software fornecido deve assegurar a recolha de todos os dados constantes do Cartão de Cidadão (CC) e uma verificação básica de segurança, nomeadamente assegurando:

- Identificação de fotocópias a cores de elevada resolução (de cartão original).
- OCR de todos os dados constantes do Cartão (letras, algarismos e símbolos)
- Comparação dados contantes na MRZ com restantes dados do CC
- Recolha de fotografia constante do Cartão (em formato compatível com mecanismo de comparação de fotos, mais à frente descrito).



- Verificação de mecanismos base de segurança, incluindo
 - sobreposição de microtexto,
 - presença de símbolos base de Cartão de Cidadão,
 - verificação da presença e autenticidade dos mecanismos de segurança ótica (incluindo DOVID e filete holográfico)
 - verificação de presença de todos os campos

Assim, o *software* deve receber 2 fotografias da frente e verso do CC e devolver todos os dados constantes do Cartão, bem como uma indicação do nível de fidedignidade do documento.

3.2. Verificação de presença de vida (liveness)

O software fornecido deve assegurar (sem qualquer intervenção humana de backoffice) a presença de vida (liveness) de vídeo ou sequência de imagens (frames) recolhidas. Neste processo deve ser assegurado a medida da profundidade 3D, a textura da pele, as reflexões oculares, entre outras – sem necessidade de interação por parte do utilizador (e.g., sem necessidade de movimentos os olhos ou da face pelo utilizador)

Funcionalidade de Verificação de liveness com certificação ISO/IEC 30107 (Anti-Spoofing technology, a.k.a., Presentation Attack Detection) nível 1 e nível 2, ou equivalente – assegurando resistência a ataques fotos, vídeos de alta resolução, marcaras de papel, máscaras 3D de resina, látex e silicone usadas por humanos.

3.3. Comparação da Fotografia visível no Cartão com selfie

O software fornecido deve assegurar a comparação da imagem de baixa resolução da fotografia constante no cartão de cidadão com a imagem extraída do processo de prova de vida (liveness).

Taxa de falsos positivos (False accept rate - FAR) inferior ou igual a 1/1 000 000, com taxa de falsos negativos (False reject rate - FRR) inferior a 1%. (True acceptance rate - TAR superior ou igual a 99%).

3.4. Comparação da Foto na Base de dados com selfie

O software fornecido deve assegurar a comparação da fotografia de alta resolução recolhida aquando do pedido de Cartão de Cidadão com a imagem extraída do processo de prova de vida (incluindo a deteção de gémeos)

Taxa de falsos positivos (False accept rate - FAR) inferior ou igual a 1/10 000 000, com taxa de falsos negativos (False reject rate - FRR) inferior a 2%. (True acceptance rate - TAR superior ou igual a 98%).

Solução avaliada por entidade de referência independente (e.g., NIST, IARPA, WIDER, ENISA).





3.5. Verificação de segurança avançada Documento de identificação

Adicionalmente aos mecanismos de segurança em relação à fidedignidade do documento de identificação descritos no ponto 3.1, devem estar disponíveis mecanismos avançados de verificação de segurança, utilizados pela aplicação móvel sempre que se entenda. Deve ser assegurado uma verificação avançada de segurança, e se necessário humana (prestada pelo adjudicatário com um SLA de resposta inferior a 1 dia útil), do documento que assegure:

- Verificação da presença e veracidade de mecanismos de segurança do CC, incluindo:
 - Microtexto
 - Janela com *Multiple Laser Image*.
 - Tintas UV (opcional)
- Detecção de adulteração do Cartão (e.g., alteração de dados impressos, alteração de fotografia)

Consideram-se ainda neste âmbito as validações de segurança a outros documentos distintos do Cartão de Cidadão, nomeadamente Passaportes, Título e Cartão de Residência e cartões de identificação de outros Estados Membros da EU.

3.6. Quantidades Estimadas

Preveem-se as seguintes quantidades de utilização dos serviços ao longo do período da execução do contrato:

	Quantidade estimada (3 anos)
OCR Cartão de Cidadão e verificação básica de segurança CC	ilimitada
Verificação de presença de vida	1 000 000
Comparação da Foto visível no Cartão com selfie	1 330 000
Comparação da Foto na Base de dados com selfie	1 330 000
Verificação de segurança avançada Documento de Identificação	66 500
Adesão por Video-conferência (valor total por adesão até 10 minutos de duração)	333 000
Adesão por Video-conferência, minuto adicional (além dos 10 minutos iniciais, valor por minuto)	660 000

3.7. Requisitos Transversais

O software fornecido deve incluir um componente central (disponibilizada em regime SaaS, cf secção seguinte) e uma SDK para ser integrado em App móvel da AMA. O SDK deve assegurar:





- Deve ser disponibilizado um SDK para iOS e para Android
- O SDK para iOS deve ser desenvolvido Objective-C
- O SDK para Android não deve depender de bibliotecas AndroidX
- O SDK deve funcionar em redes Wi-Fi que não permitam a utilização do utilitário de rede “ping” para endereços externos à rede

3.8 SaaS

Deve ser disponibilizado os serviços tecnológicos, em regime de Software as a Service (SaaS), em infra-estrutura de servidores, redes, segurança, e administração necessários para a disponibilização do âmbito descrito no presente CE.

No mínimo devem ser disponibilizados os seguintes servidores dedicados em Datacenter localizado na EU, assegurando:

- 2x Servidor Base de Dados (CPU 4 cores, 6GB RAM, 40 GB Disco)
- 2x Servidor Front-end Biometria (CPU 4 cores, 6GB RAM, 20 GB Disco)
- 2x Servidor Aplicacional Verificação Documentos (CPU 4 cores, 6GB RAM, 20 GB Disco)
- 2x Servidor Aplicacional Face Match (CPU 4 cores, 6GB RAM, 20 GB Disco)
- 2x Servidor Aplicacional Liveness (CPU 4 cores, 6GB RAM, 20 GB Disco)
- 2x Servidor Aplicacional Video-Conferencia (CPU 4 cores, 6GB RAM, 20 GB Disco)
- 2x Servidor web Video-Conferencia (CPU 4 cores, 6GB RAM, 20 GB Disco)
- 2x (Firewalls e IDS)

Deve ainda ser disponibilizado ambiente de testes/Qualidade.

Todo o software necessário para esta infraestrutura central é da responsabilidade do adjudicatário (todos os ambientes).

De forma a responder aos requisitos constantes do CE, caso se revele maior capacidade dos equipamentos para responder aos requisitos de performance, ou segurança, tal deve ser assegurado pelo adjudicatário.

Disponibilidade de serviços com nível de disponibilidade superior ou igual a 99.9950%, em período 24hx7d, devendo assegurar-se os seguintes requisitos:

- Número máximo de pedidos de OCR Cartão de Cidadão e verificação básica de segurança CC: 1000 pedidos/minuto;
- Número máximo de pedidos de liveness: 600 pedidos/minuto;
- Número máximo de pedidos de Comparação da Foto: 1000 pedidos/minuto;
- Número máximo de pedidos de Verificação de segurança avançada: 100 pedidos/minuto;





- Tempo médio de resposta a pedidos de liveness, comparação de foto, OCR Cartão de Cidadão e verificação básica de segurança: 3 segundos em 90% dos pedidos;
- Tempo máximo de resposta a pedidos de liveness, comparação de foto, OCR Cartão de Cidadão e verificação básica de segurança: 10 segundos em 100% dos pedidos;
- Tempo médio de resposta a pedidos de verificação de segurança avançada Cartão de Cidadão: 5 segundos em 90% dos pedidos;
- Tempo máximo de resposta a pedidos de verificação de segurança avançada Cartão de Cidadão: 20 segundos em 100% dos pedidos;
- Tempo máximo de resposta de Interface web de videoconferência: 2 segundos em 90% dos pedidos;
- Tempo máximo de resposta de Interface web de videoconferência: 4 segundos em 99% dos pedidos;
- Tempo máximo de resposta de Interface web de videoconferência: 5 segundos em 100% dos pedidos;

Todos os dados pessoais (incluindo dados biométricos e de identificação) devem ser eliminados dos equipamentos (servidores e equipamentos de rede) após a resposta e, obrigatoriamente, no final de cada dia (em caso de incidentes ou erros).

O centro de dados deve assegurar entre outros:

- O acesso físico aos vários níveis de segurança, aos elementos previamente identificados pela AMA;
 - Que todos os alarmes oriundos do Sistema de Segurança, devem ser comunicados à AMA no prazo máximo de 2 horas, devendo ser integrado com o sistema de monitorização da AMA se a tecnologia o permitir;
 - Energia elétrica AC/DC socorrida com UPS, bem como gerador diesel e redundância de UPS;
 - Climatização e refrigeração – AVAC, incluindo ar condicionado industrial com condutas corta-fogo, detetor e regulador de humidade do ar e redundância de ar condicionado;
 - Chãos falsos com esteiras para cablagem;
- ❖ Informar a AMA das regras de uso do Centro de Dados;
- ❖ Manter o sigilo e a confidencialidade da informação respeitante aos equipamentos e aplicações informáticas, bem como a quaisquer dados e conhecimentos específicos, de qualquer natureza, da





plataforma tecnológica a alojar;

- ❖ Assumir a responsabilidade por quaisquer danos que a AMA venha a sofrer por causa imputável às condições de alojamento no Centro de Dados;
- ❖ Conceder apoio na remoção da plataforma tecnológica alojada após a cessação da vigência do presente Protocolo.

3.9. Manutenção e Suporte

Deve ser assegurada a Administração do software fornecido em regime SaaS, assegurando a permanente atualização das versões de software, incluindo sistema operativo, software base (com sistemas de gestão de BD, servidores aplicativos ou outros) e software específico fornecido.

Entende-se por manutenção preventiva e corretiva o conjunto das ações efetuadas pelo adjudicatário de forma a corrigir quaisquer erros, anomalias ou incorreções, incluindo revisões preventivas, manutenção remota e reparação de avarias, assegurando um tempo de reposição do serviço de acordo com o especificado mais à frente, nesta secção.

Entende-se por tempo de reposição do serviço a soma do “tempo de resposta” e do “tempo de reparação”.

Entende-se por tempo de resposta o prazo compreendido entre a comunicação da anomalia ao Adjudicatário (por telefone, ou email) e o início da sua reparação.

Entende-se por tempo de reparação o prazo compreendido entre o início da intervenção e a reposição completa do serviço em funcionamento.

Os concorrentes deverão considerar na proposta apresentada os serviços suporte e de manutenção preventiva, e corretiva, incluído no preço da proposta assegurando os SLA definidos na tabela seguinte (Em período 24x7), de acordo com nível de prioridade definido pela AMA:

Nível de Prioridade	Exemplo	Tempo resposta	Tempo reposição
Baixo	Problema que afeta menos de 1% dos pedidos	24 horas	5 dias uteis
Médio	Problema que afeta até de 10% dos pedidos	2 horas	4 horas
Elevado	Serviço indisponível, Problema que afeta mais de 10% dos pedidos	30 minutos	1 hora





Cláusula 16.ª

Níveis de serviço

Disponibilidade de serviços 99.9950%, em período 24hx7d e com os tempos indicados nos pontos 3,8 da Clausula anterior.

Cláusula 17.ª

Planeamento

1. O fornecimento e os serviços suprarreferidos deverão ser iniciados após a celebração do contrato e integralmente concluídos num prazo de 3 anos.
2. O adjudicatário deve apresentar após a celebração do contrato um calendário para o fornecimento e desenvolvimento dos serviços apresentados no ponto 3 da cláusula 14.ª, com indicação clara da alocação dos recursos e sua alocação às diferentes fases e entregáveis do projeto.
3. O planeamento apresentado pode vir a sofrer alterações em função de prioridades no decurso do projeto.

Cláusula 18.ª

Entregáveis e documentação

1. O adjudicatário entregará à AMA, conforme faseamento dos trabalhos, no mínimo, a seguinte documentação em suporte digital (.pdf e .odf):
 - a) Documentação de APIs das várias componentes do software disponibilizado;
 - b) Relatório mensal referente aos serviços prestados, incluindo níveis de serviço assegurados;
2. A AMA poderá proceder à reprodução de todos os documentos referidos no número anterior (para os fins que assim o entender).

Cláusula 19.ª

Mecanismos formais de acompanhamento

1. No âmbito do presente procedimento o adjudicatário deverá respeitar a orgânica indicada na sua proposta para a realização dos trabalhos e a coordenação conjunta do projeto com a AMA, incluindo os diversos níveis, tendo em consideração os seguintes requisitos:





- a) Todos resultados produzidos pelo adjudicatário no âmbito do presente fornecimento deverão ser alvo de aceitação por parte da AMA;
- b) A AMA terá um prazo de 2 semanas para se pronunciar em relação aos resultados apresentados pelo adjudicatário.
- c) No caso da não-aceitação, por parte da AMA, dos resultados, deverá o adjudicatário (num prazo inferior a 5 dias) proceder às alterações necessárias para nova análise da AMA (nos termos supra).

Cláusula 20.ª

Regulamento Geral de Proteção de Dados

Quando aplicável o cocontratante deve demonstrar a conformidade dos bens com os requisitos do regulamento e da RCM 41/2018.

Cláusula 21.ª

Gestor do Contrato

1. O gestor do contrato, com a função de acompanhar permanentemente a execução contratual, nos termos e para os efeitos previstos no artigo 290.º-A do CCP, será designado pela AMA no contrato.
2. O cocontratante deverá indicar a pessoa na sua organização que será responsável pela execução do contrato, e que será o interlocutor com o gestor do contrato designado pela AMA, bem como a pessoa responsável pelo tratamento de dados pessoais.

