



CADERNO DE ENCARGOS

Aquisição de serviços para o desenvolvimento de uma solução tecnológica para a Plataforma de Identidade do Cidadão e Empresa dos Açores (Azor.ID)

Parte I – Requisitos Gerais

Cláusula 1.ª

Objeto

O presente Concurso Público com publicidade internacional tem como objeto a aquisição de serviços de implementação da Plataforma de Identidade do Cidadão Açores

Cláusula 2ª

Prazo de execução

- 1 - O prazo de execução do contrato para a implementação e serviço de suporte (após colocação ao serviço) da plataforma AZOR.ID terá a duração máxima de 23 meses a contar da assinatura do contrato.
- 2 - Os prazos previstos no contrato são contínuos, correndo em sábados, domingos e dias feriados.

Clausula 3.ª

Local prestação do serviço

- 1 - As prestações do presente contrato serão executadas em regime remoto exceto quando solicitada presença nas instalações do GRA, que poderão ser em São Miguel (instalações da Direção Regional das Comunicações e Transição Digital) ou na ilha Terceira (instalações da Estrutura de Missão para a Reforma e Modernização da Administração Pública) para fins específicos tais como reunião de arranque e potencialmente algumas reuniões de gestão do projeto e de entregas parciais.
- 2 – As custas com deslocações, alojamento e estadia são da responsabilidade do cocontratante.

Clausula 4.ª

Patentes, Licenças e Marcas Registadas

- 1 - O desenvolvimento da solução deverá utilizar software aberto e isento de licenciamento pago, exceto quando expressamente indicado no presente caderno de encargos.



2 - Os cocontratantes garantem que respeitam as normas relativas à propriedade intelectual e industrial, designadamente, direitos de autor, licenças, patentes e marcas registadas, relacionadas com o *hardware*, *software* e documentação técnica que utilizam no desenvolvimento da sua atividade.

3 - O Governo Regional dos Açores (GRA) não assume qualquer responsabilidade por infrações cometidas pelo prestador dos serviços, no âmbito da execução do contrato, relativamente a direitos de propriedade intelectual e industrial, relacionados com o *hardware*, *software* e documentação técnica por este utilizado, cujos direitos e autorizações legais para o efeito devam por ele ser assegurados.

Clausula 5.^a

Formação

1 - É requisito obrigatório incluir um plano de formação e acompanhamento das equipas técnicas dos utilizadores pertencentes às equipas técnicas e operacionais do GRA, o qual deverá estar descrito na proposta.

2 - O cocontratante deverá considerar pelo menos as seguintes ações de formação:

- Formação para *Troubleshooting* e Manutenção do Sistema – Para Equipa de TI do GRA.
- Formação para os administradores de sistemas sobre o *BackOffice*;
- Formação para os utilizadores de entidades pertencentes ao GRA.

Clausula 6.^a

Equipa do projeto

1 - O cocontratante deverá disponibilizar uma equipa de desenvolvimento constituída no mínimo por 8 recursos com os seguintes perfis: 1 (um) Gestor de Projeto Sénior, 1 (um) *Frontend Web Developer* Sénior, 1 (um) *Developer Mobile* (IOS) Sénior; 1 (um) *Developer Mobile* (Android) Sénior, 1 (um) *UI/UX Designer* Sénior, 1 (um) *Backend Developer* Sénior, 1 (um) *Senior Security Engineer* (Engenheiro de Segurança) e 1 (um) *DevOps* Sénior, sendo que, devem ter os seguintes requisitos obrigatórios para execução do contrato:

Perfil Gestor de Projeto

- Experiência de pelo menos 5 anos em Gestão de Projetos em pelo menos 5 projetos de desenvolvimento de software;
- Experiência de Gestão de Projetos em pelo menos 3 projetos de gestão de identidade digital e/ou eletrónica.);



- Certificação PMP (*Project Management Professional*);
- Certificação CISSP (*Certified Information Systems Security Professional*);

Perfil Senior Security Engineer (Engenheiro de Segurança)

- Experiência como CISO de entidades que comprovadamente respeitem elevados padrões de segurança (ISO27001);
- Experiência em pelo menos 5 projetos de gestão de identidade digital e/ou eletrónica, utilizando criptografia e infraestruturas de chaves públicas no desenho e implementação dos projetos;
- Experiência de participação ativa na implementação de menos 2 projetos de soluções de identidade de acordo com o eIDAS;

Perfis técnicos

- Experiência profissional mínima de 3 anos;
- Experiência em projetos de gestão de identidade digital e/ou eletrónica, emitida pelo Estado Português ou por entidades públicas.

2 - Os recursos humanos a afetar à execução dos serviços estão no âmbito de organização e sob a autoridade da entidade adjudicatária não existindo qualquer vínculo laboral com a entidade adjudicante. Os recursos humanos deverão ter um vínculo contratual com a entidade adjudicatária à data da entrega da proposta.

3 - A entidade adjudicatária deverá adequar o perfil da equipa a afetar ao objeto do presente procedimento de acordo com os objetivos definidos nas Cláusulas Técnicas do presente Caderno de Encargos.

4 - Durante a execução da prestação de serviços, a entidade adjudicante poderá solicitar a substituição de algum dos elementos da equipa da entidade adjudicatária, caso considere que este não reúne as condições necessárias ao desempenho das respetivas funções.

5 - As férias ou outros impedimentos previsíveis por parte dos recursos afetos pela entidade adjudicatária dá lugar à sua substituição, devendo ser garantido o período mínimo de 3 (três) dias para transmissão de conhecimentos entre recursos.

6 – Os membros da equipa técnica deverão ter perfil correspondente e equivalência mínima aos requisitos do número 1 desta cláusula.

7 – Havendo o recurso a anonimização de dados pessoais, o mesmo deverá ser realizado com utilização a um número de iniciais superior a 5 carateres.

Clausula 7.ª
Gestão do projeto



1 - O cocontratante deverá designar um Gestor de Projeto que facultará ao interlocutor designado pelo GRA a informação relativa ao progresso dos trabalhos, prestando toda a informação necessária e sempre que solicitado, assegurando respostas atempadas e capazes, permitindo a boa condução dos trabalhos e o cumprimento do cronograma proposto.

2 - Com a periodicidade a combinar, serão realizadas reuniões de gestão do projeto, com a presença dos intervenientes necessários do lado do cocontratante e GRA. É nomeado um Gestor de Contrato por parte do GRA com a função de acompanhar permanentemente a execução do contrato.

3 - Sempre que solicitado, o prestador de serviços obriga-se a disponibilizar, relatórios periódicos dos trabalhos e todos os documentos em língua portuguesa, que sejam necessários para a boa e integral utilização ou funcionamento daqueles.

4 - O Gestor de Projeto deverá ser responsável pela Gestão da Equipa do cocontratante, pela execução do contrato, e o principal interlocutor com o gestor do contrato designado pelo GRA. Será ainda a pessoa responsável pelo tratamento de dados pessoais, assim como todos os mecanismos formais de acompanhamento, gestão de dados e obrigações previstas no que toca a Segurança da Informação.

5 - O cocontratante deverá garantir a manutenção do número mínimo de elementos acordado e a estabilidade da equipa de trabalho ao longo da prestação de serviços. Contudo, durante a realização do projeto, poderá substituir qualquer membro da equipa por outro de perfil equivalente, mediante comunicação prévia e aceitação do GRA, sem que tal prejudique o normal decurso dos trabalhos inerentes ao projeto e o cumprimento dos prazos acordados.

6 - Na memória descritiva da proposta do concorrente, o mesmo deverá apresentar um cronograma detalhado com os serviços e entregáveis que se propõe realizar.

7 – O Gestor de Projeto do cocontratante, para a gestão geral do projeto, deverá seguir por base a metodologia PM² ou similar para a implementação deste projeto. Nomeadamente deverá estar previsto a criação e atualização (durante a fase de projeto) dos seguintes artefactos:

- a) Ficha Inicial de Projeto;
- b) Matriz das Partes Interessadas;
- c) Plano de Trabalho do Projeto;
- d) Plano de Gestão de Riscos;
- e) Plano de Gestão de Incidentes;
- f) Plano de Gestão de Requisitos;
- g) Plano de Gestão de Alterações;
- h) Plano de Aceitação de Entregáveis;
- i) Plano de Aplicação Operacional;



- j) Matriz de Requisitos;
- k) Pedido e Registo de Alterações;
- l) Registo de Entregáveis;
- m) *Checklist* da Qualidade (Lista de Verificação da Qualidade);
- n) Relatório de Progresso do Projeto (*template* que será usado para os relatórios regulares de acompanhamento de projeto);
- o) Relatório Final do Projeto;
- p) *Checklist* de Encerramento;
- q) Registo das Lições Aprendidas;

8 – Para o desenvolvimento pretende-se que seja adotada uma metodologia ágil de gestão de projeto, por exemplo SCRUM, ou seja, uma metodologia ágil que permita a criação de pacotes de funcionalidades a serem desenvolvidas em períodos mais curtos (1 ou 2 semanas), estabelecendo segmentação de planos de testes parciais.

9 – Cabe ao cocontratante a elaboração dos planos de testes parciais e do plano de testes para a aceitação final, nos quais se devem incluir testes de carga e testes de segurança, enviando para o Business Manager (a ser nomeado pelo GRA) para respetiva aprovação.

Clausula 8.ª

Descrição dos Serviços de Implementação

1 – É pretendido o desenvolvimento e entrega “chave na mão” da futura plataforma AZOR.ID, para tal deverão ser consideradas as fases de implementação descritas de seguida, ou poderá o cocontratante apresentar um modelo de implementação semelhante, desde que devidamente descrito e estruturado.

2 – Os serviços devem assentar-se em 3 fases, sendo elas seguidamente descritas.

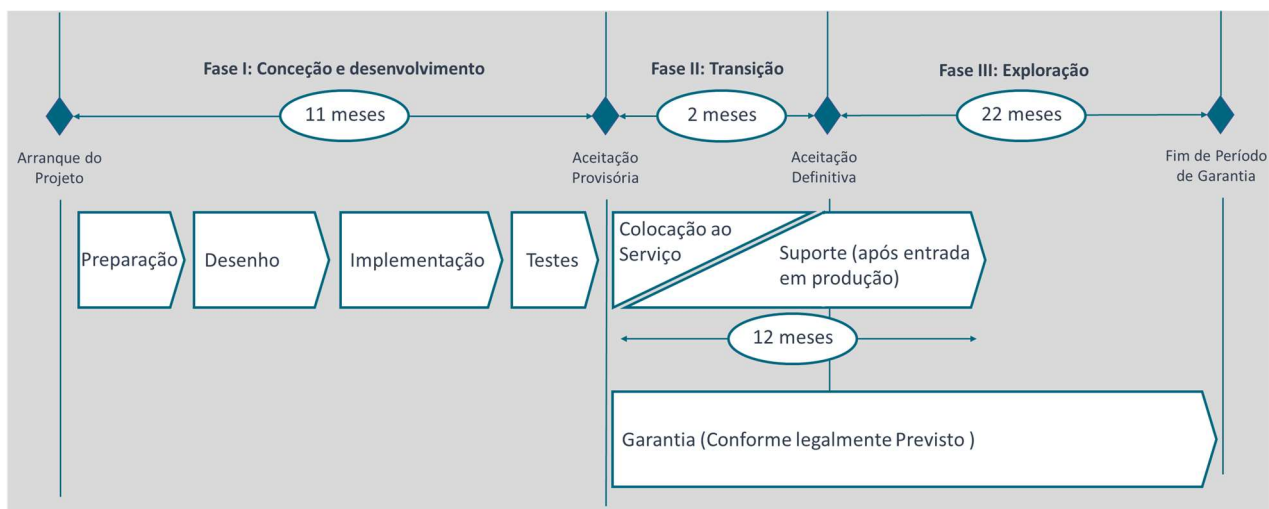
- a) Fase I: Conceção e Desenvolvimento – a qual consiste nas seguintes atividades:
 - a. Preparação – na qual é feita a análise de requisitos e infraestrutura existente e criado Ambientes de Desenvolvimento e Testes;
 - b. Desenho - na qual são apresentados os requisitos finais, desenho da arquitetura da solução e identificação das tecnologias, interfaces de comunicação, plano de proteção de dados, recuperação e segurança da aplicação;
 - c. Desenvolvimento / Implementação da solução - na qual é feito o desenvolvimento da solução (SingleSignOn; Frontend; Backend e Aplicação Móvel para onboarding), Integrações necessárias com a arquitetura e infraestrutura do GRA;
 - d. Testes – que deverão ser executados de forma faseada, de acordo com metodologias ágeis – por exemplo SCRUM; respetiva correção de bugs, Testes de interoperabilidade, qualidade e integração em produção.



- b) Fase II: Transição – que inclui as seguintes atividades:
- Colocação ao Serviço – que inclui todas as configurações necessárias para o início de operação do sistema;
 - Início da Etapa de suporte (após entrada em produção), a qual compreende suporte direto do fornecedor da solução, inclusive bolsa de horas de desenvolvimentos adicionais, não previstos nos requisitos deste contrato.
 - Formação.
 - Início do período de Garantia.
- c) Fase III: Exploração – que inclui as atividades:
- Continuação da Etapa de suporte (após entrada em produção), a qual compreende suporte direto do fornecedor da solução às equipas técnicas do Governo Regional dos Açores, inclusive bolsa de horas de desenvolvimentos adicionais, não previstos nos requisitos deste contrato.
 - Continuação do período de Garantia.

Cláusula 9.^a

Prazos de prestação de serviços



As prestações de serviços deverão ser realizadas nos seguintes prazos:

Fase I: Conceção e Desenvolvimento – Prazo Máximo 11 meses;

Fase II: Transição - Duração mínima 2 meses (na qual inclui já o início do serviço de suporte (após entrada em produção));

Fase III: Exploração – duração mínima 10 meses, referentes ao período remanescente do Serviço de Suporte (após entrada em produção). O período de vigência da garantia deverá continuar até aos limites previstos legais;



Cláusula 10.ª

Preço-base e condições de pagamento

- 1 – O preço-base é de 500.000,00€ acrescido de IVA à taxa legal em vigor.
- 2 - As quantias devidas pelo contraente público devem ser pagas após a receção da respetiva fatura, a qual só pode ser emitida após validação pelo contraente público dos serviços objeto do contrato.
- 3 - As faturas devem discriminar os serviços a que se reportam, bem como o número de compromisso financeiro associado, o qual será indicado pelo contraente público sob pena de devolução das mesmas.
- 4 - O contraente público comunicará o novo número de compromisso financeiro, nas situações em que haja alteração do mesmo.
- 5 - Deverão ser emitidas faturas eletrónicas, a submeter para a Plataforma da Faturação Eletrónica da Administração Pública (<https://www.feap.gov.pt>).
- 6 - O pagamento será efetuado em prestações, após validação do integral cumprimento das prestações previstas na cláusula 8.ª, com as seguintes condições:
 - a) 25% após a preparação e desenho, conforme previsto nas subalíneas a. e b. da alínea a) da Cláusula 8.ª;
 - b) 15% após a implementação prevista na subalínea c. da alínea a) da Cláusula 8.ª;
 - c) 20% após os testes previstos na subalínea d. da alínea a) da Cláusula 8.ª;
 - d) 15% após a colocação ao serviço prevista na subalínea a. da alínea b) da Cláusula 8.ª;
 - e) 10% com o início da subalínea b. da alínea b) e 10% após formação prevista na subalínea c. da alínea b) da Cláusula 8.ª;
 - f) 5% no termo da vigência do contrato, após validação e receção de todo o processo.

Cláusula 11.ª

Preço Contratual

- 1 - Pela prestação dos serviços objeto do contrato, bem como pelo cumprimento das demais obrigações constantes do presente Caderno de Encargos, o cocontratante deve pagar ao contraente público o valor resultante da aplicação dos preços constantes da proposta adjudicada, aos serviços efetivamente prestados, acrescido de IVA à taxa legal em vigor, se este for legalmente devido.
- 2 - O preço referido no númeroº 1 da presente cláusula inclui todos os custos, encargos e despesas cuja responsabilidade não esteja expressamente atribuída à entidade adjudicante, bem como a remuneração especial prevista no n.º 4 do artigo 14.º do Código do Direito de Autor e Direitos Conexos.
- 3 - Todos os Encargos derivados da apresentação da proposta, assinatura do contrato, prestação de garantias e seguros são igualmente da conta do cocontratante.
- 4 – São igualmente da conta do cocontratante os encargos associados a deslocações, viagens e alojamento no âmbito da presente prestação de serviços.



Cláusula 12.ª

Faturação

- 1 - As quantias devidas pela entidade adjudicante devem ser pagas após a receção da respetiva fatura, a qual só pode ser emitida após validação pelo contraente público dos serviços objeto do contrato.
- 2 - As faturas devem discriminar os serviços a que se reportam, bem como o número de compromisso financeiro associado, o qual será indicado pelo contraente público sob pena de devolução das mesmas.
- 3 - O contraente público comunicará o novo número de compromisso financeiro, nas situações em que haja alteração do mesmo.
- 4 - Serão emitidas faturas eletrónicas, devendo as mesmas ser submetidas para a Plataforma da Faturação Eletrónica da Administração Pública (<https://www.feap.gov.pt>).
- 5 - O prazo de pagamento das faturas será de acordo com a lei vigente, ou seja, 30 dias.

Cláusula 13.ª

Adiantamento e revisão de preços

- 1 - No âmbito da presente prestação de serviços não há lugar a adiantamentos.
- 2 - Os preços acordados no ato da adjudicação são válidos, sem revisão de preços, para os serviços prestados durante a vigência do contrato.

Clausula 14.ª

Requisitos de implementação para o tratamento de dados pessoais

- 1 - A entidade cocontratante deverá apresentar credenciação do GNS demonstrando que está credenciada para o acesso e manuseamento de informação classificada.
- 2 - A entidade cocontratante deverá identificar projetos de âmbito nacional /internacional nos quais tenha implementado soluções de gestão de identidade, na forma digital e/ou eletrónica, sendo, contudo, valorizado o conhecimento em documentos emitidos pelo Estado Português, como por exemplo o Cartão de Cidadão, Passaporte Eletrónico Português, Título de Residência, Carta de Condução, entre outros. O GRA reserva-se no direito de confirmar junto das referidas entidades a veracidade das informações prestadas, independentemente do grau e marca de segurança do referido projeto.

Cláusula 15.ª

Suporte (após entrada em produção)

- 1 - Após a fase I: Conceção e desenvolvimento (assinatura do Auto de Aceitação Provisória) deverá iniciar o Serviço de suporte (após entrada em produção) válido por 1



ano, a incluir na proposta. Deverão igualmente apresentar preço para + 2 anos como opcional.

2 - Os serviços de suporte devem incluir:

- **Suporte Corretivo** – Suporte de 2ª linha a prestar às equipas técnicas do GRA, incluindo correção de bugs e anomalias técnicas / funcionais da plataforma e serviços a disponibilizar;

Os níveis de serviço de suporte e manutenção corretiva a considerar são:

- Correções críticas (paralisação total do sistema) – Intervenção até 4 horas x 7 dias úteis, 24 horas;
- Correções anomalias (que não paralise a utilização do sistema) – Intervenção até 8 horas x 5 dias úteis, das 09h00 às 18h00, hora dos Açores;

- **Suporte evolutivo (Mínimo Pack de 200 horas)** – Serviço de implementação de atualizações de software que não estejam previstas nos requisitos técnicos deste contrato, que inclui a implementação de melhorias ao produto que advenham de regulamentos europeus, standards internacionais ou do quadro legislativo português (exemplo: apoio na integração novos sítios Web, adoção de novos documentos ao processo de onboarding ou de autenticação, alterações na integração com o serviço de Chave Móvel Digital, etc). Outros exemplos de utilização do pack de horas são alterações requeridas pelo GRA que possam implicar mudanças profundas ao serviço e obriguem à revisão dos processos de negócio, de interfaces, inclusão de novos fornecedores de autenticação ou desenvolvimento de novas funcionalidades.

Cláusula 16.ª

Cessão da Posição Contratual

O cocontratante não poderá ceder a sua posição contratual ou qualquer dos direitos e obrigações decorrentes do contrato.

Cláusula 17.ª

Subcontratados

1 - A responsabilidade pela execução de todos os serviços prestados e contratados será sempre do cocontratante e só dele, o qual deverá submeter, com a Proposta, as empresas com quem venha a subcontratar a execução de parte dos serviços que constituem a presente prestação.

2 - Caso se verifique a necessidade de o cocontratante recorrer, por razões de natureza excecional, à subcontratação ou execução de tarefas por terceiros, requererá, para os casos em que tal não esteja claramente indicado na sua Proposta, prévia autorização ao



contraente público, fazendo acompanhar esse pedido dos elementos comprovativos da necessidade invocada e da capacidade e competência do Subcontratado que propõe, sendo os eventuais atrasos derivados de autorização exclusivamente imputáveis ao cocontratante

Cláusula 18.ª

Responsabilidades

- 1 - O cocontratante assume integral responsabilidade pelos serviços contratados, sendo o único responsável perante a entidade adjudicante pela boa prestação dos mesmos.
- 2 - O cocontratante responde nomeadamente por quaisquer erros, deficiências ou omissões na prestação de serviços, qualquer que seja a sua origem e qualquer que seja o momento em que forem detetados, salvo quando prove que os mesmos decorreram de dados fornecidos por escrito pela entidade adjudicante.
- 3 - O cocontratante responde por quaisquer erros, deficiências ou omissões, sempre que a sua atuação resulte numa incorreta identificação dos mecanismos de acompanhamento e controlo dos trabalhos a realizar.
- 4 - Sempre que os erros, deficiências ou omissões na prestação de serviços resultem de dados fornecidos pelo contraente pública, o apuramento das responsabilidades far-se-á de acordo com o previsto no artigo 378.º do Código dos Contratos Públicos.
- 5 - Em qualquer altura, e logo que solicitado pelo cocontratante o contraente público obriga-se a corrigir os erros, as deficiências ou omissões no prazo razoável que lhe vier a ser fixado, sob pena de esta mandar executá-los por conta do cocontratante, sempre que a responsabilidades dos mesmos lhe seja imputável.
- 6 - As ações de supervisão e controlo do contraente pública em nada alteram ou diminuem a responsabilidade do cocontratante no que se refere à sua prestação dos serviços.
- 7 - O contraente público tem direito de regresso contra o cocontratante responsável pelos atos ou omissões geradores de responsabilidade da entidade adjudicante no presente procedimento.

Cláusula 19.ª

Penalidades contratuais

- 1 - O contraente público pode exigir ao cocontratante o pagamento de uma sanção pecuniária, pelo incumprimento das datas e prazos de entrega dos serviços e/ou documentação solicitados, de montante a fixar em função da gravidade do incumprimento, até 20% do preço contratual, nos termos dispostos no n.º 2 do artigo 329.º do Código dos Contratos Públicos.
- 2 - Em caso de resolução do contrato por incumprimento do cocontratante, o contraente público pode exigir-lhe uma pena pecuniária de até 20% do preço contratual, sem prejuízo do disposto no n.º 3 do artigo 329.º do Código dos Contratos Públicos.



3 - Ao valor da pena pecuniária prevista no número anterior são deduzidas as importâncias pagas pela entidade adjudicatária ao abrigo do n.º 1, relativamente aos serviços cujo atraso na respetiva conclusão tenha determinado a resolução do contrato.

4 - Na determinação da gravidade do incumprimento, o contraente público tem em conta, nomeadamente, a duração da infração, a sua eventual reiteração, o grau de culpa do cocontratante, e as consequências do incumprimento.

5 - 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.

6 - A cobrança das eventuais sanções em que o cocontratante incorra, será efetuada, a critério do contraente público, designadamente por desconto no pagamento ou pagamentos subsequentes à verificação do facto que tenha dado origem à penalidade ou por acionamento das garantias em poder do contraente público.

7 - As sanções pecuniárias previstas na presente cláusula não obstam a que o contraente público exija uma indemnização pelo dano excedente.

Cláusula 20.ª

Resolução por parte do contraente público

1 - O contraente público poderá resolver o contrato em caso de incumprimento definitivo pelo cocontratante das suas obrigações contratuais, nos termos do disposto na parte final do n.º 1 do artigo 325.º e ainda do disposto nos artigos 333.º e 448.º do Código dos Contratos Públicos.

2 - O exercício do direito de resolução previsto no número anterior pelo contraente público não preclude o direito de a mesma vir a ser ressarcida pelos prejuízos que lhe advirem da conduta do cocontratante da resolução.

3 - O contraente público, independentemente da conduta do cocontratante, reserva-se o direito de resolver o contrato nos termos e com os fundamentos previstos nos artigos 334.º e 335.º do Código dos Contratos Públicos.

4 - O direito de resolução exerce-se mediante declaração escrita enviada à entidade adjudicatária e não determina a repetição das prestações já realizadas, a menos que tal seja determinado pela entidade adjudicante.

Cláusula 21.ª

Resolução por parte do cocontratante

O cocontratante pode resolver o contrato nos termos dos artigos 332.º e 449.º do Código dos Contratos Públicos.

Cláusula 22.ª

Cumprimentos de obrigações relativas aos investimentos financiados pelo Plano de Recuperação e Resiliência (PRR)



REGIÃO AUTÓNOMA DOS AÇORES
Secretaria Regional das Finanças, Planeamento e Administração Pública
Gabinete do Secretário Regional

O cocontratante garantirá o cumprimento das orientações e diretrizes emitidas pelos órgãos de coordenação regional e nacional do PRR (PRR) aplicáveis ao presente procedimento.

Cláusula 23.ª

Comunicação e Publicidade

O cocontratante assegurará o cumprimento das orientações emitidas pelos órgãos de coordenação regional e nacional do PRR em matéria de Comunicação e Publicidade.

Cláusula 24.ª

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, nos termos do Código dos Contratos Públicos, para o domicílio ou sede contratual de cada uma, identificados no contrato, através de correio, correio eletrónico ou de telecópia, nos termos dos artigos 467.º e 468.º do Código dos Contratos Públicos.

2 - Qualquer alteração das informações de contacto constantes do contrato deve ser comunicada à outra parte.

Cláusula 25.ª

Foro Competente

Para resolução de todos os litígios decorrentes da interpretação, validade ou execução do contrato fica estipulada a competência do Tribunal Administrativo e Fiscal de Ponta Delgada, com expressa renúncia a qualquer outro.

Cláusula 26.ª

Legislação aplicável

A tudo o que não esteja especialmente previsto no presente Caderno de Encargos aplica-se o estatuído no Código dos Contratos Públicos, e demais legislação aplicável.



Parte II – Requisitos Técnicos e Funcionais

Cláusula 1ª

Introdução

1 - Pretende-se a aquisição de uma plataforma de gestão de identidades do Cidadão e Empresas que tenham presença nos Açores.

2 - Nos últimos anos, o acelerar do processo de transformação e modernização do Estado e por consequência a disponibilização de um maior número de serviços digitais aos cidadãos, às empresas e entidades, criou alguns desafios relativos à sua adoção.

3 - Este desafio relativo à adoção dos serviços digitais tem por base um conjunto de fatores:

- a) Disponibilizar serviços que, verdadeiramente, respondam às necessidades dos cidadãos e empresas, em vez de serem uma mera desmaterialização de procedimentos já existentes em papel;
- b) Facilidade e consistência de utilização dos serviços – existência de diversas experiências na utilização dos serviços públicos digitais disponibilizadas pelas inúmeras entidades públicas, e tipicamente com um grau de complexidade elevado;
- c) Confiança dos serviços públicos digitais - a complexidade e heterogeneidade, apresentada pelos serviços públicos digitais atualmente disponíveis pelas diversas entidades, leva a que os cidadãos ainda tenham dúvidas e barreiras à sua utilização, levando à incerteza e à falta de confiança nestes serviços.
- d) Aumentar a interoperabilidade no ecossistema digital público dos Açores;
- e) Garantir a proteção de dados pessoais dos Cidadãos pelo cumprimento do Regulamento Geral de Proteção de Dados (RGPD);
- f) Simplificar a gestão e integração das plataformas que constituem o ecossistema digital público dos Açores;
- g) Assegurar às empresas um porto de entrada e autenticação para a realização de serviços públicos;
- h) Criação de um fluxo que permita aos cidadãos e empresas criarem pedidos de representação para realização serviços específicos disponibilizados pelo GRA, em nome de outrem.

4 - Para responder a estes desafios e num momento em que entidades públicas se encontram a desenvolver iniciativas de transformação digital (e não apenas mera desmaterialização), o GRA pretende:

- a) Adquirir uma plataforma de Gestão de Identidades e de Acessos centralizado aos sítios Web de todas as entidades que constituem o GRA, através de um Portal único onde o cidadão e empresa se possam registar e aceder num único sítio Web;
- b) Disponibilizar acesso aos portais com mecanismos de autenticação forte;
- c) Usufruir de mecanismos de “single sign-on” entre os portais;



- d) Implementar mecanismos de partilha de dados entre o ecossistema digital gerido pelo GRA, disponibilizando funcionalidades de gestão de entidades digitais e de gestão de consentimentos sobre a Proteção de Dados, respondendo assim às reais necessidades dos utilizadores das diversas plataformas digitais públicas dos Açores;
- e) As soluções a disponibilizar deverão garantir elevados critérios de usabilidade, fornecendo uma experiência consistente entre as plataformas digitais das entidades públicas;
- f) Assegurar integração e interoperabilidade com a futura arquitetura de sistemas de informação do GRA.

Cláusula 2ª

Objetivos gerais

- 1 - Desenvolvimento de um Portal de Gestão da Identidade do Cidadão e Empresas (AZOR.ID) onde este possa registar-se e aceder a diversos sítios Web do ecossistema digital público dos Açores;
- 2 - A referida plataforma deverá disponibilizar mecanismos de gestão de consentimento sobre a utilização dos dados pessoais do Cidadão, permitindo ao Cidadão decidir acerca da partilha de dados pessoais com entidades que constituem o GRA;
- 3 - Para as Empresas não há a obrigatoriedade legal de gestão de consentimento sobre a utilização dos dados da empresa, visto serem dados de pessoas coletivas e não privados.
- 4 - Esse portal único enviará as informações do cidadão para as entidades que o mesmo se registou, ficando registado esse consentimento, quer para consulta e gestão posterior do Cidadão, quer para a entidade gestora da plataforma.
- 5 - A autenticação do cidadão deverá suportar os atributos profissionais do cidadão, permitindo ao mesmo a opção de se autenticar como cidadão ou na qualidade das funções que desempenha enquanto profissional qualificado. Para isso terá de associar atributos profissionais através do Sistema de Certificação de Atributos Profissionais (SCAP).
- 6 - Na área Pessoal do cidadão, o mesmo deverá ter acesso a:
 - Dar consentimento;
 - Cancelar consentimento;
 - Possibilidade de verificação e refrescamento dos seus dados;
 - i. Solicitar o direito ao esquecimento, de acordo com os direitos emanados do RGPD e no cumprimento do quadro legal em vigor;
 - Criar pedidos de representação de realização de serviços públicos do GRA, em nome de outrem;
 - Aprovar pedidos de representação;
 - Visualizar atividades feitas em seu nome (referentes aos pedidos de representação);



- Cancelar Pedidos de Representação em seu nome.
- 7 - Na vista da empresa, a mesma deverá ter acesso a:
- Criar pedidos de representação da empresa para realização de serviços públicos do GRA;
 - Aprovar pedidos de representação;
 - Visualizar atividades feitas em seu nome (referentes aos pedidos de representação);
 - Cancelar representações em seu nome.
- 8 - Pretende-se que os dados demográficos do cidadão e empresas surjam de forma automática no sítio Web específico que visita e no qual pretende utilizar os serviços digitais desse sítio, desde que o cidadão esteja registado no AZOR.ID e utilize os mecanismos de autenticação disponibilizados;
- 9 - Em virtude de alguns cidadãos e empresas terem mais do que uma morada (ex. 1 Lisboa e 1 Ponta Delgada) é necessário permitir acrescentar as mesmas no Portal de Identidade, identificando qual a morada que se pretende que seja considerada como a morada principal;
- 10 - A solução a disponibilizar deverá disponibilizar mecanismos (APIs) que permitam a integração entre plataformas e o AZOR.ID, com segurança e performance;
- 11 - A solução deverá suportar não só a possibilidade de receber pedidos de informação (quer de cidadãos ou empresas), como também deve suportar a disseminação de informação que seja atualizada, para sistemas que tenham subscrito esse serviço;
- 12 - Pretende-se ainda que o cidadão possa rever os seus dados pessoais sempre que necessário, como por exemplo a morada, morada profissional, estado civil, e-mail, telefone, entre outros;
- 13 - Deverá ser possível ao Cidadão alterar a gestão de consentimentos de acordo com as suas preferências;
- 14 - O AZOR.ID deve possibilitar analisar quais as entidades que vão ser notificadas das alterações de dados do Cidadão e Empresas;
- 15 - É necessária a criação de uma “timeline” que permita ao cidadão a verificação das ações por si realizadas no que concerne à gestão de dados pessoais, desde a criação da conta. Assim, todas as ações realizadas pelo Cidadão que envolvam gestão de consentimentos, alteração de dados e direito ao esquecimento, devem ser registadas com referência temporal e com incorporação de mecanismos de segurança que previnam e permitam detetar tentativas de adulteração da informação. Devem ainda serem implementados mecanismos de auditoria que permitam analisar e identificar possíveis tentativas de adulteração dos referidos registos;
- 16 - Deverá ser criada uma API para integração de soluções digitais que permitam comunicar com o cidadão utilizando Push Notifications, desde que previamente autorizado pelo Cidadão. Assim, será possível ao Cidadão receber notificações sempre que altere os seus dados, assim como receber mensagens



de carácter geral e informativo que o GRA e demais entidades públicas pretendam enviar ao Cidadão;

- 17 - A autenticação nos vários portais e serviços online, disponibilizados pelas várias instituições que constituem o GRA, deverá ser feita sempre com as mesmas credenciais, devendo ser disponibilizadas soluções de “single sign-on” entre o portal AZOR.ID que realiza a primeira autenticação e serve de porta de entrada para os demais sítios Web;
- 18 - O AZOR.ID deverá disponibilizar mecanismos de autenticação forte, tais como a Chave Móvel Digital (CMD de autenticação) e ser possível a utilização de documentos que permitam leitura contactless e cumpram com a estrutura de dados prevista no Doc 9303 da ICAO/OACI, em alinhamento com o Regulamento UE 1157/2019. Também deverá ser possível realizar a autenticação com uma aplicação móvel (a considerar na proposta do concorrente) para entre outras funcionalidades, permitir receber push notifications e códigos de segurança, que o Cidadão utiliza para confirmar e finalizar o processo de autenticação multi-factor. Deverá ser adicionalmente suportar opção de MFA por intermédio de SMS e email (sendo estas opções customizáveis pelo utilizador);
- 19 - Na aplicação móvel mencionada no ponto anterior e para o registo do Cidadão que não tenha em sua posse um leitor de cartões de chip de contacto, para ler documentos como o atual Cartão do Cidadão, ou não tenha ativa a CMD, deverá ser disponibilizada nessa Aplicação móvel a possibilidade do Cidadão poder realizar total ou parcialmente o processo de onboarding para registo da conta, fornecendo os seus dados biográficos e biométricos (fotografia), prova de morada e outros elementos que sejam necessários à criação da sua identidade digital;
- 20 - Ao realizar o onboarding, ou seja, a criação de conta no Azor.ID, o cidadão poderá utilizar a leitura do cartão do cidadão ou a chave móvel digital. A solução deverá permitir a importação dos dados, preenchendo automaticamente os dados necessários para a criação da conta. Deverá permitir ao cidadão visualizar e confirmar os seus dados;
- 21 - Na aplicação móvel, deverá ser disponibilizada a funcionalidade de 2FA (Duplo Fator de Autenticação) através de *push notifications* que lhe permitam aceitar ou rejeitar determinada ação que está a ser realizada com a sua entidade digital, assim como permitir receber códigos de segurança OTP – One Time Password, permitindo desta forma realizar processos de autenticação mesmo quando os cidadãos não reúnem condições para utilizar a CMD ou o Cartão de Cidadão;
- 22 - A aplicação móvel deverá suportar a disponibilização de um QR *code* que serviria para autenticação de uma determinada ação, serviço ou evento.
- 23 - O cidadão residente nos Açores que utiliza Título (cartão) de Residência é convidado a ativar a CMD para utilização dos vários serviços online. Assim, deverá ser seguida a seguinte abordagem a este perfil de cidadãos:
 - a. Utilizar o processo de autenticação com Chave Móvel Digital (Autenticação Gov);



- b. Possibilidade de utilizar a aplicação móvel de *Onboarding* para leitura *contactless* do Título de Residência, cumprindo o exposto anteriormente no que concerne ao formato dos dados;
 - c. A plataforma deverá suportar a utilização de cartões de cidadão europeus no *Onboarding*, que cumpram com o regulamento UE 1157/2019 e com a estrutura de dados OACI/ICAO conforme previsto no Doc 9303, e estar de acordo com a norma EIDAS;
 - d. Deverá ser entregue com o AZOR.ID, uma interface que permita a integração por *webservices* os serviços da RIAC, I.P.;
- 24 - Na interface web do Azor.ID deverá estar disponível uma secção em que o utilizador possa pedir um sincronismo de atualização dos seus dados a partir da chave móvel Digital ou cartão de cidadão (autenticação.gov). Nesta interface deverá ser disponibilizado ao cidadão uma validação da atualização dos dados – indicando de forma visual quais os campos que serão alterados;
- 25 - Deverá ser possível a utilização do AZOR.ID por um cidadão em nome de outra pessoa desde que seja apresentada uma procuração que esteja em conformidade com a Lei 49/2018 de 14 de agosto sobre o Regime do Maior Acompanhado. Como exemplo deverá ser possível os pais terem acesso em nome dos filhos ao AZOR.ID, pessoas ausentes do país, cuidadores informais, etc.
- a. Para um cidadão solicitar acesso ao AZOR.ID em nome de outra pessoa deverá ser possível criar um procedimento na plataforma onde o cidadão irá solicitar o acesso e anexar o documento tipo mandato judicial com vista ao acompanhamento, diretivas antecipadas de vontade, procuração para cuidados de saúde, testamento vital, etc;
 - b. Após o envio desse documento o cidadão que está a facultar a procuração deverá receber uma notificação onde poderá autorizar ou rejeitar o acesso por parte do terceiro que está a solicitar esse mesmo acesso;
 - c. Essa permissão deverá ficar registada no ID do cidadão sem possibilidade de adulteração;
- 26 - Deverá também ser possível a um cidadão ou empresa pedir ou receber pedidos de representação referentes à execução de serviços específicos da Administração Pública Regional. Ou seja, posso criar um pedido para que um ou mais serviços públicos possam ser realizados em seu nome:
- a. Estes serviços estão devidamente identificados e catalogados na plataforma CES-APR (que se encontra em fase de implementação, e com a qual o AZOR.ID necessitará de interoperar);
 - b. O Cidadão ou Empresa podem selecionar os serviços que pretendem que possam ser realizados em seu nome, definir o período para o qual o terceiro pode realizar o respetivo serviço, pode inclusive definir o número de vezes que o serviço pode ser executado;
 - c. Após a realização do pedido de procuração, a mesma irá aparecer na página pessoal do cidadão ou empresa visado para aceitação.



- d. Este pedido de procuração pode ser bidirecional, ou seja, um cidadão ou empresa pode criar pedido de procuração para execução de serviço em nome de um terceiro – que por sua vez recebe a notificação e aprova, ou posso tomar a iniciativa de atribuir procuração a ser realizada por um terceiro – a qual o mesmo poderá aprovar ou não.
 - e. Deverá ser sempre possível a quem atribui o pedido de representação, ter a possibilidade de estabelecer os limites da mesma. Os limites devem no mínimo permitir:
 - i. Estabelecer limites temporais da duração da representação;
 - ii. Selecionar quais os serviços (que constam na lista do CES-APR) que possam ser executados em seu nome;
 - iii. Estabelecer o número limite de vezes que pode ser realizado o respetivo serviço procurado (este limite associado a serviço específico);
 - f. Quem atribui a representação terá sempre a possibilidade de a qualquer momento cancelar a respetiva representação – tal não irá cancelar pedidos que já tenham sido realizados em seu nome.
 - g. Quem atribui a representação, deverá também na sua área pessoal visualizar quais os serviços que tenham sido executados em seu nome. Os serviços serão executados na futura Plataforma de Serviços da Administração Pública (ainda em fase de projeto).
- 27 - A plataforma AZOR.ID, deverá ter previsto na sua interface com a futura plataforma de Serviços da Administração Pública Regional, no sentido de enviar informação / aprovação relativa à representação de realizar o respetivo serviço digital em nome de outra pessoa ou empresa.
- 28 - O AZOR.ID deverá apresentar também informação de identificação do serviço, suporte, políticas de privacidade e demais elementos que o GRA entenda serem necessários publicar nas áreas públicas da plataforma;
- 29 - Para o registo das Empresas no AZOR.ID, deverá existir uma ligação com o sistema da autoridade tributária, sendo possível a partir deste interface de buscar todas as informações relativas à identificação da empresa, e criar o registo no AZOR.ID. Entre as informações, deverão incluir (se disponível na interface da Autoridade Tributária):
- a. Denominação Social da Empresa;
 - b. Moradas;
 - c. NIPC;
 - d. Domicílio fiscal;
 - e. CAE;
 - f. Sede ou estabelecimentos;
 - g. Representante Legal;
 - h. Contactos Telefónicos e/ou email;
- 30 - Deverá ser possível ao AZOR.ID receber atualizações dos dados da empresa automaticamente a partir da interface da Autoridade Tributária, caso



não seja possível, deverá ser considerada uma rotina que permita fazer o pull dos dados para os atualizar;

- 31 - Deverá ser previsto a plataforma AZOR.ID enviar mensagens de forma estruturada para a futura plataforma do GRA – *Process State Registry*. As mensagens a ser enviadas deverão no mínimo incluir:
- Logins efetuados;
 - Atualização de dados;
 - Criação de acessos;
 - Representações criadas;
 - Pedidos de acesso a dados.

Cláusula 3ª

Requisitos *Backoffice* e *Mobile APP*

- 1 - A plataforma a desenvolver deve incluir a construção de um portal Web de *BackOffice* onde as equipas do GRA irão gerir o AZOR.ID, assim como gerir as integrações com os demais sítios Web do ecossistema digital público dos Açores via *Webservices* utilizando os standards abertos SAML, OAUTH e OpenID;
- 2 - O AZOR.ID deverá ser responsiva para dispositivos móveis, como smartphones e tablets;
- 3 - A aplicação móvel a disponibilizar deverá ser nativa para iOS e Android e estar preparada para publicação nas seguintes plataformas:
 - Play Store (Google);
 - AppGallery (Huawei);
 - App Store (iOS);
- 4 - A publicação das aplicações móveis deverá ser realizada nas respetivas contas do Governo Regional dos Açores, devendo o adjudicatário providenciar o devido apoio na publicação das mesmas.
- 5 - Deve ser considerada a criação de perfis de utilizador diferenciados para utilização do *backoffice*, com diferentes permissões de acessos a funcionalidades de gestão e consulta de informação;
- 6 - Deverá ser disponibilizado um serviço de diretório com a listagem das entidades (sites) com os quais o AZOR.ID esteja integrado, devendo a entidade aparecer automaticamente assim que esteja criada a integração via *backoffice*;
- 7 - Deverá ser criada uma área no AZOR.ID para integradores externos, nomeadamente os que desenvolvem sítios web que pretendam integrar com o AZOR.ID;
- 8 - Deverá ser criada no AZOR.ID uma área de testes e qualidade onde os sítios web serão inicialmente integrados antes do lançamento para produção;
- 9 - Deverá ser criado um motor de risco onde constarão as regras de acesso predefinidas pelo GRA e implementadas em sede de projeto, assim como um mecanismo de notificações de alerta para as equipas técnicas do GRA. Entre as regras de acesso a serem criadas deverá ser possível:



- Colocar em quarentena quem tenta aceder ao website mais do que cinco vezes sem sucesso;
 - Avaliação de geolocalização do utilizador;
 - Identificação de padrões de horário de acesso e bloqueio de utilizador caso esteja a realizar acessos fora desse horário em correlação com outros fatores, como a geolocalização.
- 10 - Deverá ser disponibilizada no *backoffice* uma área de *Audit Logging*, com boa usabilidade, onde devem ser guardados e verificados os registos de acessos;
- 11 - A solução a disponibilizar deverá identificar no documento de proposta como responde aos requisitos em baixo indicados:
- Arquitetura tecnológica de elevada disponibilidade;
 - Obedecer a princípios de *Security by Design* e *Privacy by Default*;
- 12 - Os dados do Cidadão considerados como sensíveis devem ser armazenados com recurso a técnicas de encriptação e anonimização de dados;
- 13 - O concorrente deverá considerar que a solução deverá ser instalada por si com total redundância no DC GRA – que utiliza tecnologia de virtualização VMware v.7;

Cláusula 4ª

Requisitos *Frontend*

- 1 - O adjudicatário deverá disponibilizar para a plataforma AZOR.ID, e em complemento ao mencionado nos pontos anteriores e, os seguintes requisitos para o *Frontend*:

Tipos de registo e de acesso do Cidadão e Empresas ao Portal:

- Registo a partir de operador numa Loja do Cidadão;
- Registo direto via web, com validação de operador na loja do cidadão;
- Cartão do Cidadão;
- Chave Móvel Digital - CMD;
- Através de uma aplicação móvel a construir que permita realizar a jornada de onboarding e OTP – One Time Password;
- Interface com autoridade Tributária (para empresas);
- O Cidadão ao fazer autenticação deverá ter opção de se autenticar em seu nome pessoal ou com a função de acordo com os seus atributos profissionais (SCAP).

Área de dados pessoais do Cidadão:

- Consulta dos seus dados pessoais;
- Alteração dos seus dados pessoais;
- Verificação de qual o Atributo profissional ativo;
- Check List com visibilidade de todas as entidades onde o cidadão pretende partilhar (ou já partilha) os seus dados;



- Solicitar o apagamento dos seus dados pessoais, de acordo com a base legal do processo de negócio (licitude);
- Alertas sobre a expiração do documento de identificação oficial utilizado no processo de onboarding;
- Pedido de sincronismo de dados com autenticação.gov ou chave móvel digital;
- Consulta de Representações ativas em seu nome ou em representação de terceiro;
- Consulta de serviços que tenham sido realizados em seu nome com representações emitidas;
- Consulta de Procurações ativas;
- Solicitar acesso em nome de outra pessoa;
- Criação de pedido de representação em nome de outro (com respetivos critérios de serviços, validade e cadência);
- Criação de envio de pedidos de representação para outra pessoa (com respetivos critérios de serviços, validade e cadência).

Área de dados da Empresa:

- Consulta dos dados da Empresa;
- Alertas sobre a expiração do documento de identificação oficial utilizado no processo de onboarding;
- Solicitar acesso em nome de outra pessoa ou empresa (com submissão de documento oficial);
- Criação de pedido de representação em nome de outra Pessoa ou empresa (com respetivos critérios de serviços, validade e cadência);
- Consulta das representações ativas;
- Consulta de Procurações ativas;
- Consulta dos serviços realizados com a sua representação;

“Single sign-on” como serviço para os cerca de 600 portais e serviços da Região:

- Solução de integração dos mecanismos de autenticação para utilização nos sítios web a integrar;
- Disponibilização de serviço, API e documentação para integração por terceiros nos novos websites desenvolvidos para a Região;

Pedido, partilha e preenchimento automático de dados nos formulários dos vários serviços:

- É pretendido que o cidadão e empresa não precisem de estar constantemente a preencher os seus dados pessoais nos vários serviços / portais. Assim, após selecionar uma entidade/serviços, através da referida “check list”, os seus dados deverão ficar disponíveis para utilização pela(s) entidade(s) com as quais aceitou partilhar os seus dados pessoais;



Cláusula 5ª

Requisitos *Onboarding* Digital

***Onboarding* Digital – Aplicação móvel e Web**

De forma a criar o registo seguro de um cidadão e em alternativa à CMD ou por impossibilidade de utilização de um leitor de cartões para leitura do Cartão de Cidadão, pretende-se que a solução a disponibilizar contemple o desenvolvimento de uma aplicação móvel que disponibilize o processo de *onboarding* e gestão de dados pessoais, que contemple pelo menos os seguintes passos:

- Passo 1 – Tirar fotografia do Cartão de Cidadão ou leitura do documento contactless como o Passaporte, Título de Residência, etc...;
- Passo 2 – Recolha de fotografia do Cidadão com a câmara fotográfica do telemóvel;
- Passo 3 – Criação da identidade digital e respetivo dossier digital do processo de adesão;
- Passo 4 – Fornecimento de outros elementos (se obrigatórios) para processo de negócio (prova de morada, certidões, etc...), a definir em sede de projeto;

Cláusula 6ª

Requisitos para Duplo Fator de Autenticação

Duplo Fator de Autenticação – Aplicação Móvel

Para os utilizadores que não pretendem utilizar CMD ou CC, a aplicação móvel deverá possibilitar a autenticação por duplo fator com a geração de códigos OTP – One Time Password enviados por SMS, em integração com o gateway de sms do GRA, assim como realizar autenticações/autorizações utilizando push notifications enviadas para a aplicação móvel;

Cláusula 7ª

Requisitos de Backoffice de Gestão

O backoffice de gestão deverá permitir a gestão central de diversas funcionalidades, entre as quais:

Gestão de notificações:

- Cidadão deverá receber uma notificação sempre que os seus dados pessoais são alterados;
- Envio de notificações em massa para todos os utilizadores registados;



- Envio de notificações para utilizadores que obedeçam a um determinado perfil;
- Integração com SMS gateway a ser disponibilizado pelo GRA.

Motor de risco:

- Motor/serviço com regras de acordo com as políticas de acesso a definir pelo GRA:
 - Exemplo I: Colocar em quarentena utilizador se efetuar mais do que cinco tentativas de acesso sem sucesso;
 - Exemplo II: Acessos fora do país (geolocalização com análise temporal);

Gestão de perfis:

- Criação de perfis diferenciados para cada entidade do GRA com mecanismos de registo de utilizador/data/hora de atividades CRUD (Create, Read, Update, Delete) sobre dados pessoais;
- Criação de perfis diferenciados para entidades externas ao GRA e que necessitem de acesso ao portal de BackOffice;
- Criação de perfis de utilizador utente da plataforma;
- Todos os utilizadores devem efetuar autenticação com 2FA;

Audit Logging:

- Serviço de Audit Logging com registo de acessos de administração da plataforma, para fins de auditoria e conformidade com boa usabilidade na interface para a visualização destes dados;
- Serviço de Audit Logging com registo de ações do Cidadão como acessos à plataforma, alteração de dados, gestão de consentimentos e pedido de esquecimento;
- O acesso ao serviço de Audit Logging deverá ser condicionado a nível técnico e funcional de forma que só com a autorização de 2 pessoas em simultâneo e que tenham permissões para o efeito, é que será possível consultar tais registos;
- Serviço de Audit Logging de negócio com apresentação de dashboards e relatórios diários, semanais e mensais com a possibilidade de consulta de informação de atividade da plataforma (novas contas por perfil, número de utilizadores ativos por perfil, número de pedidos de direito ao esquecimento, número de ações do Cidadão por tipo de ação (refrescamento de dados, autenticações, autorização/cancelamento de consentimentos)).

Entidades



- Serviço de diretório de entidades públicas e/ou serviços;
- Disponibilizar catálogo de serviços por entidade e acesso online aos mesmos (a partir de interoperabilidade com a plataforma CES-APR);

Ambiente de Testes e qualidade

- Página onde serão inseridos os novos websites das entidades e/ou serviços a integrar com o portal ainda em ambiente de testes para posteriormente passarem à produção.

Segurança da Informação:

- O proponente deverá assegurar na sua solução os princípios da confidencialidade, integridade e disponibilidade da informação de acordo com as boas práticas de segurança da informação, nomeadamente a conformidade com a Lei 65/2021 de 30 de julho;
- É exigido que a solução a propor contemple no mínimo:
 - A encriptação e anonimização dos dados pessoais guardados nas bases de dados;
 - A encriptação dos canais de comunicação entre módulos e serviços a disponibilizar;
 - A encriptação do disco das máquinas virtuais onde vão estar instalados os módulos da solução proposta;

Cláusula 8ª

Requisitos Tecnológicos

Adequabilidade (completude e correção)

- A solução assegura todos os requisitos numa lógica de resultados a alcançar, sem falhas;

Alta disponibilidade / Redundância

- A solução deverá ser facilmente escalável de forma a garantir a performance e gestão de capacidade, com intervenções simples e sem a necessidade de revisão da arquitetura da plataforma e serviços a implementar;
- A solução, no que respeita ao ambiente de produção, deverão ser cumpridos elevados níveis de fiabilidade e disponibilidade, através da adoção de arquiteturas redundantes, com capacidades de recuperação de falhas, entre outros, através da redundância nos vários componentes



tecnológicos. Neste contexto, deverão ser implementados mecanismos de monitorização;

- A solução deverá ser desenhada e implementada de forma a ser redundante, tendo em consideração que será instalada em máquinas virtuais nos centros de dados do GRA;
- A solução deverá suportar sincronismo entre servidores ou Bases de dados instaladas em sites geograficamente distintos (na ilha Terceira e São Miguel) com tempos de latência inferiores a 20 ms.

Desempenho e distribuição de Carga

- A solução deve estar adaptada a funcionar adequadamente com mecanismos de distribuição de carga, nomeadamente aos serviços de balanceamento de carga fornecidos pelo datacenter do GRA – Azores Cloud. Deverá ser assente num sistema distribuído: espera-se que a plataforma seja projetada para ser executada em múltiplas máquinas em simultâneo, assegurando uma distribuição de carga por intermédio de servidores aplicativos múltiplos.
- Pretende-se que a solução apresente arquiteturas redundantes e com capacidades de recuperação de falhas. Neste contexto, deverão ser implementados mecanismos de monitorização eficazes e os procedimentos de recuperação da solução deverão ser bem definidos, sejam estes automáticos ou que necessitem de intervenção manual, sendo que deverá ser possível recuperar o funcionamento da solução quando se verifique uma indisponibilidade da mesma num prazo máximo de 4 horas, com a exceção das situações causadas ou condicionadas por fatores externos e/ou alheios à solução.
- A solução tem de ter a capacidade técnica para suportar até 1500 (mil e quinhentos) utilizadores em simultâneo sem degradação de desempenho.
- A solução deverá suportar comunicações previstas via interfaces desenvolvidas, sem qualquer impacto na performance do sistema.
- A previsão da quantidade de troca de mensagens deverá ser apresentada pelo cocontratante em fase de desenho de projeto e aprovado pelo GRA.
- A Solução deverá disponibilizar, na raiz do site, sem quaisquer mecanismos de redirecionamento, uma página com o nome healthcheck. (php|asp|aspx|outra extensão|sem extensão) que execute todos os testes que necessários a aferir o estado de funcionamento do site (ex. ligação à base de dados) e retorne o resultado em texto “STATUS OK”, para cada teste, caso o resultado de todos os testes seja positivo e “STATUS FAIL” caso o resultado de um dos testes seja negativo. Esta página é utilizada pelo balanceador de forma a só disponibilizar o site/aplicação quando o resultado é “STATUS OK”.



- O carregamento de uma nova página deverá demorar no máximo 1 segundo em pelo menos 90% dos casos de utilização;
- O tempo de execução de um comando ou função deverá ser inferior a 1 segundo, após o clique do botão – exceto para os comandos de processamento de listagens ou incorporação de ficheiros.

Mínima dependência de fornecedores e de tecnologias específicas

- A dependência de fornecedores com tecnologias/frameworks específicas e não genericamente utilizadas por várias entidades deve ser minimizada, recorrendo-se a estes apenas em casos onde alguma funcionalidade específica não se encontre em produtos de mercado.

Evoluções futuras:

- A arquitetura da solução deverá estar preparada para que a instalação/migração em infraestrutura cloud seja facilitada e sem necessidade de alteração da plataformas e serviços a disponibilizar;

Conformidade com Norma RNID

- Sempre que aplicável, a solução tem de estar em conformidade com o RNID (regulamento nacional de interoperabilidade digital de acordo com a RCM nº 2/2018, de 05.01, na redação em vigor);

Solução 100% web based

- A solução deverá ser 100% web based, não devendo ser requisito do posto de trabalho a instalação de plugins ou outros componentes específicos da solução para poder operar na plataforma.

Hardware do Servidor e Software Base:

- O Hardware Servidor e o Software Base, necessários para a solução, serão disponibilizados pelo contraente público através da infraestrutura do Azores Cloud.
- A solução deverá ser desenvolvida tendo por base tecnologias open source e funcionar em Sistemas Operativos e Bases de dado open source, por exemplo em Linux, PostgreSQL ou outros, em versão LTS.
- Os servidores a disponibilizar pelo GRA serão virtualizados (Vmware v.7).
- A solução deverá suportar Load Balancing e SSL Offloading do tipo Full Proxy, gerido por equipamento de gestão de tráfego. O endereço IP do cliente será transmitido ao servidor no cabeçalho X-Forwarded-For e o protocolo (HTTP ou HTTPS) de ligação utilizado pelo cliente no cabeçalho X-Forwarded-Proto.
- O cocontratante é responsável pela definição dos requisitos de Hardware Servidor e Software Base para a infraestrutura de suporte à solução,



estando obrigado a respeitar as normas especificadas nos dois últimos requisitos.

- A solução deverá permitir backups, não comprometendo a disponibilidade do serviço. Os backups serão feitos online, sem quebra de serviço.

Linguagem de Programação a ser utilizada:

- Deverá ser utilizada linguagem de programação baseada em tecnologias opensource;
- Deverá ser suportado versões tecnológicas LTS (Long Term Support);
- Deverá igualmente ser suportado gestão de versões e salvaguardas de segurança através da utilização de repositório de artefactos.

Segurança:

- A solução deverá dispor de controlos, meios e mecanismos que garantam os princípios base da segurança:
 - Confidencialidade – garantir que a informação só poderá ser acedida ou tratada por utilizadores com permissão para tal e de acordo com as estritas necessidades específicas para a realização das respetivas funções;
 - Integridade da informação – garantir que a informação tratada e gerada por qualquer dos utilizadores não é apagada, alterada ou corrompida sem autorização, intencional ou acidentalmente, desde a sua criação até à respetiva eliminação, mantendo-a completa, sem supressões ou acréscimos, com particular atenção durante a sua circulação;
 - Disponibilidade – desde que estejam reunidas as condições necessárias para acesso e tratamento da informação, nomeadamente a autenticação e autorização do utilizador, garantir que esta está atempadamente disponível.
- As comunicações deverão ser efetuadas sobre protocolos seguros e sem vulnerabilidades de forma a garantir a confidencialidade e integridade da comunicação.
- Em particular, a utilização da solução em browser deverá ser feita por ligação segura (HTTPS).
- O acesso de um utilizador a qualquer uma das componentes da solução deverá implicar apenas um único procedimento de autenticação (login), mas sempre condicionado ao respetivo perfil de acesso e autorizações definidas.
- A solução tem de regular o acesso dos utilizadores com base em permissões que poderão ser associadas a perfis, sendo estes perfis atribuídos aos utilizadores ou a grupos de utilizadores. A implementação



do sistema de permissões deverá seguir o modelo “role-based access control” (RBAC) ou “Attribute-based access control” (ABAC).

- Os grupos devem poder ser constituídos por utilizadores ou por outros grupos. As permissões de um grupo são herdadas pelos seus utilizadores ou subgrupos.
- As permissões devem ser configuradas de modo a refletir as necessidades do modelo operacional e processos de negócio suportados.
- As permissões necessárias para a manutenção e administração técnica da Solução não devem incluir o acesso aos dados em transmissão ou armazenados.
- As permissões podem ser concedidas de forma positiva ou negativa, isto é, concedendo ou retirando expressamente a autorização.
- Todas as funcionalidades descritas para a solução deverão estar sujeitas a controlo de permissões de modo a garantir que o utilizador:
 - Só tem acesso aos objetos para os quais tem autorização, direta ou indireta;
 - Este acesso aos objetos deverá estar associado à respetiva entidade a quem o utilizador pertence;
 - Deverá ser possível limitar a vista de ramificação da árvore da estrutura de entidades da Administração Pública Regional e das autarquias, de acordo com a raiz atribuída ao utilizador.
 - Só pode executar as operações para as quais tem autorização, direta ou indiretamente.
- A parametrização de permissões na solução deverá permitir uma gestão ao nível:
 - Diretamente dos utilizadores;
 - A partir da estrutura da árvore de objetos, nomeadamente, selecionando um ramo da árvore a partir do qual seja dado acesso aos conteúdos dos objetos descendentes;
 - Através de perfis funcionais, nomeadamente: produtor (aquele que criou o conteúdo), owner (aquele que está responsável pela Respetiva entidade base), aprovador (aquele que aprova o conteúdo); e/ou
 - De grupos aos quais os utilizadores pertençam, incluindo grupos genéricos como everyone (todos os utilizadores), administradores, etc.
- Os grupos devem poder ser constituídos por utilizadores ou por outros grupos. As permissões de um grupo são herdadas pelos seus utilizadores ou subgrupos.
- A solução deve suportar a gestão de identidades, permitindo criar, gerir, suspender, auditar e apagar utilizadores e grupos, bem como, as associações entre estes dois conceitos.
- A solução deverá suportar a encriptação das bases de dados.



- O acesso de um utilizador a qualquer uma das componentes da solução deverá implicar apenas um único procedimento de autenticação (login), mas sempre condicionado ao respetivo perfil de acesso e autorizações definidas.
- A solução deverá suportar mecanismos de bloqueio de acesso no cliente ou logoff automático do utilizador em função de períodos de inatividade passíveis de serem configurados.
- A solução deverá estar preparada para poder funcionar com um ambiente de disaster recovery, nomeadamente no que diz respeito às questões de sincronismo de dados, transição do ambiente de produção em caso de desastre e posterior recuperação.
- Os mecanismos de segurança da solução deverão ser suficientemente robustos para suportar o não repúdio de ações realizadas pelos utilizadores.

Gestão à consulta de Arquivo de utilizadores:

- Deverá permitir colocar utilizadores (cidadãos ou empresas) em modo arquivo (nunca eliminando totalmente os dados);
- Deverá permitir aos operadores a consulta de utilizadores (cidadãos ou empresas) arquivados, assegurando anonimização dos mesmos, consoante o perfil de acesso do operador;
- O acesso à consulta do arquivo deverá ser condicionado a nível técnico e funcional de forma que só com a autorização de 2 pessoas em simultâneo e que tenham permissões para o efeito, é que será possível consultar tais registos .

Cláusula 9ª

Interfaces com Sistemas Terceiros

São descritos de seguida interfaces mínimas que o sistema deve suportar, não obstante de outras que possam ser identificadas como vitais para o funcionamento do projeto.

Autoridade Tributária

- Interface com autoridade tributária que irá permitir criar as identidades das empresas e atualizar os respetivos dados;

Chave móvel digital

- Plataforma utilizada pela AMA para autenticação dos cidadãos a nível nacional – servirá para a criação dos cidadãos no AZOR.ID.

Cartão cidadão

- Cartão de identidade dos cidadãos nacionais, que servirá para o onboarding dos utilizadores do AZOR.ID;



Portal dos dados Abertos (Em fase de Projeto)

- Futura plataforma de dados abertos da região. O AZOR.ID deverá disponibilizar listagens devidamente anonimizadas de informação útil para consumo de outros sistemas ou de análise de dados. Algumas informações relevantes:
 - Número de utilizadores registados;
 - Quantidade de logins efetuados;
 - Número de “representações” efetuadas;

eHub (em fase de Projeto)

- Plataforma central da arquitetura de sistemas do GRA – deverá servir de base para toda a troca de comunicações entre sistemas, agindo como middleware – a linguagem a ser utilizada para troca de mensagens deverá ser baseada em NGSI-LD;

Catálogo eletrónico de entidades e Serviços (CES-APR) (em implementação)

- O CES-APR contém a lista de entidades da Administração Pública Regional e respetivos serviços por elas executadas;
- A interface a prever deverá disponibilizar a listagem de serviços disponibilizados pela APR, por forma a poderem ser geradas as representações para a realização dos mesmos serviços online.

API para consumo de autenticação para as Plataformas do GRA

- Interface que irá permitir a autenticação dos cidadãos e empresas nos sistemas do GRA;

API para consulta de informação referente ao Cidadão e Empresa

- Interface que irá disponibilizar a outros sistemas do GRA os dados referentes ao Cidadão e empresas;

Process State Registry (em fase de projeto)

- Plataforma central da arquitetura de sistemas da APR, que irá guardar os registos de todos os logins efetuados, criação de utilizadores, criação de pedidos de representações, entre outros;

Portal dos Serviços – APR (em fase de projeto)

- Futuro portal que irá suportar a desmaterialização dos formulários dos serviços públicos. Irá interoperar com o AZOR.ID no sentido de poder receber informação do cidadão ou empresas para o preenchimento dos formulários;
- Deverá receber também informação relativa às representações para executar os serviços em nome de outrem.



Cláusula 10ª

Requisitos Não funcionais

Usabilidade e Acessibilidade:

- O desenvolvimento da solução deverá conter as boas práticas definidas, a nível nacional e internacional, para uma usabilidade e acessibilidade eficaz da mesma, tendo por base uma constante adaptação, sempre que necessário, atendendo ao público-alvo que irá usufruir da solução. A solução deverá adotar as regras de acessibilidade nos sítios e portais da Administração Pública Regional dos Açores, de acordo a legislação vigente e constantes em <http://www.acessibilidade.gov.pt>, em consonância com a última atualização da norma europeia EN 301 549 na versão 2.1.2 (2018-08). Desta forma os utilizadores devem usufruir de procedimentos simplificados e padronizados que lhes permitam beneficiar da simplicidade da interface de utilizador;
- A usabilidade desta solução deve-se adaptar a todo o tipo de utilizadores, desde o utilizador mais avançado para o utilizador mais limitado. A concentração de informação deve ser tida em conta de forma a melhorar a interpretação dos utilizadores.
- Como referido anteriormente, esta aplicação pode vir a ser utilizada por todo o tipo de utilizadores (potencialmente incluindo utilizadores que recorrem a tecnologias de apoio), a sua acessibilidade é, também, um ponto crucial a ter em consideração.
- As seguintes regras de usabilidade e acessibilidade devem ser cumpridas na sua totalidade, aquando do desenvolvimento da aplicação:
 - Os termos mais complexos devem ter uma definição agregada;
 - O tipo de letra do corpo do documento é adequado, com um tamanho mínimo de 12 pontos;
 - O espaçamento entre linhas não deve ser inferior a 1.5x o tamanho da letra;
 - Nenhum nível de navegação tem mais de 9 opções;
 - A navegação principal está sempre visível e sempre no mesmo local;
 - As hiperligações de texto não devem ser diferenciadas apenas com base na cor;
 - Elementos gráficos interativos têm de aparentar ser clicáveis;
 - Os formulários com mais de 2 ecrãs de altura devem ser distribuídos por várias páginas;
 - O tamanho dos campos deve refletir o tamanho previsível dos dados;
 - As legendas dos campos são breves e claras;
 - Campos obrigatórios devem ser claramente indicados como tal;



- Deve ser confirmado o sucesso da transação/envio de informação;
- A informação já introduzida deve poder ser corrigida a qualquer momento;
- As ações destrutivas nunca devem ser permanentes; deve ser sempre possível desfazer a operação;
- As mensagens de erro devem mostrar os passos concretos para a resolução dos mesmos;
- É possível selecionar as opções e as subopções do menu quer com rato quer com teclado;
- Ao clicar com o rato na etiqueta, o cursor surge no respetivo campo de edição;
- A imagem ou gráfico tem um equivalente alternativo em texto curto e correto;
- Os gráficos de análise de dados deverão ser acompanhados de uma descrição longa;
- No corpo de um documento, o contraste entre a cor do texto normal (menor que 18 pontos ou menor que 14 pontos negrito) e a cor do fundo é superior a 4,5:1;
- O rácio de contraste entre a cor do texto de tamanho grande (maior ou igual que 18 pontos ou maior ou igual que 14 pontos negrito) e a cor do fundo é superior a 3:1;

Evitar redundância de dados:

- Na forma de registos obsoletos, descrições obsoletas e duplicações. Para otimizar a qualidade e a eficiência dos catálogos será necessário descrever os registos apenas uma vez num formato machine-readable para permitir uma ampla disseminação da informação em todos os canais.

Proteção de Dados Pessoais:

- A solução deverá estar concebida e implementada de modo a respeitar os seguintes princípios:
 - Privacy by Design – a solução tem de assegurar a conformidade com o RGPD no tratamento de dados pessoais ao longo do ciclo de vida de cada processo (para SOLUÇÕES a serem desenhadas de novo), ou
 - Privacy by Default – a solução tem de assegurar a conformidade com o RGPD no que diz respeito ao limite máximo de tempo de manutenção ou acesso dos dados para prossecução do objetivo.



REGIÃO AUTÓNOMA DOS AÇORES
Secretaria Regional das Finanças, Planeamento e Administração Pública
Gabinete do Secretário Regional

- A solução deverá suportar, quando tecnicamente aplicável, o Regulamento EU 2016/679 quanto ao tratamento de dados pessoais, entre outros, através de:
 - Proteção de dados sensíveis;
 - Capacidade de registar os conteúdos relativos a um determinado indivíduo.
- Para respeitar o RGPD, a solução terá de garantir a estrita aplicação de perfis não só ao acesso a funcionalidades, mas também no acesso a dados pessoais, a segurança no manuseamento de dados pessoais internamente, nas interfaces humanas e com outros sistemas, no armazenamento de dados pessoais e nas funcionalidades da auditoria do acesso a dados pessoais.
- A solução tem de encriptar os dados em todas as comunicações e nas bases de dados, em particular, os dados pessoais terão de ser encriptados em todas as situações em que estejam acessíveis às equipas técnicas de desenvolvimento, manutenção e administração da solução.
- Em particular, o sistema de permissões deverá individualizar os dados pessoais ou as operações sobre estes.