P.PORTO

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

UNIVERSIDADE POLITÉCNICA DO INTERIOR (UPI)

AQUISIÇÃO DE SERVIÇOS DE PROGRAMAÇÃO E ANÁLISE DE SISTEMAS

"Middleware Portal@UPI"

EXEMPLO DE CADERNO DE ENCARGOS

ÍNDICE

CADERNO DE ENCARGOS

Capítulo I
Disposições gerais

Cláusula 1.ª
Objeto

O presente Caderno de Encargos compreende as cláusulas a incluir no contrato a celebrar na sequência do procedimento pré-contratual de concurso público que tem por objeto principal a aquisição pela Universidade Politécnica do Interior (UPI), de **Serviços de Programação e Análise de Sistemas**, de acordo com os termos e condições previstas no Anexo I ao presente Caderno de Encargos, que dele faz parte integrante.

Cláusula 2.ª
Contrato

1. O contrato é composto pelo respetivo clausulado contratual e os seus anexos.
2. O contrato a celebrar integra ainda os seguintes elementos:
   a) (...);

Cláusula 3.ª
Prazo de execução

Sem prejuízo de prazo inferior que o concorrente eventualmente proponha, o prazo máximo para a execução total dos serviços é de 304 dias.

Capítulo II
Obrigações contratuais

Secção I
Obrigações do Prestador de Serviços

Cláusula 4.ª
Obrigações principais do prestador de serviços

1. Sem prejuízo de outras obrigações previstas na legislação aplicável, no presente Caderno de Encargos ou nas cláusulas contratuais, da celebração do contrato decorrem para o Prestador de Serviços, a título principal, as seguintes obrigações principais:
   a) Desenvolvimento de um Portal único (*Workplace*), doravante denominado Portal@UPI, que fará a interação e integrará todos os processos e sistemas existentes na UPI e servirá para centralizar o acesso aos diversos sistemas da UPI e, ao mesmo tempo, como plataforma para partilhar serviços entre colaboradores não docentes;
   b) Cumprir integralmente com os termos e condições técnicas constantes do **Anexo I**;
2. Decorrente das obrigações atrás elencadas deverão ser obtidos os resultados constantes do Capítulo III do **Anexo I** do presente caderno de encargos;
3. A título acessório, o Prestador de Serviços fica ainda obrigado, designadamente, a:

a) Cumprir os requisitos de governança definidos no **Anexo VIII,** do presente Caderno de Encargos;
b) Recorrer a todos os meios humanos, materiais e informáticos que sejam necessários e adequados à prestação do serviço, bem como ao estabelecimento do sistema de organização necessário à perfeita e completa execução das tarefas a seu cargo.

Cláusula 5.ª

Forma de prestação do serviço

Para acompanhamento da execução do contrato, o Prestador de Serviços fica obrigado a, sempre que solicitado, reunir nas instalações dos Serviços da UPI com os seus representantes.

Cláusula 6.ª

Fases da prestação do serviço

Os serviços objeto do contrato compreendem as seguintes fases (detalhadas no **Capítulo II** do **Anexo I,** do presente CE):

FASE A – Análise Funcional e Técnica

FASE B – Implementação

FASE C – Testes de Aceitação

FASE D – *Go-Live*

Cláusula 7.ª

Referencial técnico, normativos nacionais ou internacionais

A execução dos serviços deverá considerar os referenciais e normas relevantes na área, nomeadamente:

1. Regulamento Nacional de Interoperabilidade Digital (RNID[1]);
2. Princípios de Desenho Universal[2];
3. Regulamento Geral de Proteção de Dados[3]
4. Guia de Usabilidade para entidades da Administração Pública[4]

Cláusula 8.ª

Local e condições da prestação de serviços

Os serviços serão prestados nas instalações da UPI ou noutro local acordado com a entidade adjudicante.

[1] Resolução do Conselho de Ministros n.º 91/2012, de 8 de novembro
[2] http://www.inr.pt/content/1/5/desenho-universal
[3] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016
[4] https://usabilidade.gov.pt

Cláusula 9.ª

Objeto do dever de sigilo

1. O Prestador de Serviços deve guardar sigilo sobre toda a informação e documentação, técnica e não técnica, comercial ou outra, (...).

Cláusula 10.ª

Prazo do dever de sigilo

O dever de sigilo mantém-se em vigor por tempo indeterminado (...)

Secção II

Obrigações da Universidade do Interior

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, a UPI deve pagar ao Prestador de Serviços o preço constante da proposta adjudicada, o qual não pode, em qualquer caso, exceder o montante global de **€130.000,00 (cento e trinta mil euros)**, valor acrescido de IVA à taxa legal em vigor.
2. O preço referido no número anterior inclui todos os custos, encargos e despesas (...)

Cláusula 12.ª

Condições de pagamento

1. A quantia devida nos termos da cláusula anterior deve ser paga no final de cada uma das Fases referidas na cláusula 6.ª, ou conjunto de Fases, (...)

Capítulo III

Caução, Penalizações e Força Maior

Cláusula 13.ª

Caução

Nos termos do n.º 2 do artigo 88.º do CCP, não é necessária a prestação de caução para garantia do presente contrato.

Cláusula 14.ª

Retenção no valor dos pagamentos

1. A UPI pode proceder à retenção de até (...)
2. A retenção a que se refere o número anterior destina-se a garantir o exato e pontual cumprimento de todas as obrigações legais e contratuais que o Prestador de Serviços assume.

Cláusula 15.ª

Penalizações

1. Pelo incumprimento de obrigações emergentes do contrato, a Entidade Adjudicante pode exigir do Adjudicatário o pagamento de uma pena pecuniária, (...)

Cláusula 16.ª

Força Maior

1. Não podem ser impostas penalidades ao Cocontratante, nem é havida como incumprimento, a não realização pontual das prestações contratuais a cargo de qualquer das partes que resulte de caso de força maior, (...)

Capítulo IV
Resolução de litígios

Cláusula 17.ª

Foro competente

Para resolução de todos os litígios decorrentes do contrato fica estipulada a competência do Tribunal (...)

Capítulo V
Disposições finais

Cláusula 18.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 CCP, para o domicílio ou sede contratual de cada uma, identificados no contrato.
2. Qualquer alteração das informações de contacto constantes do contrato deve ser comunicada à outra parte.

Cláusula 19.ª

Contagem dos prazos

1. Os prazos previstos no contrato são contínuos, não se suspendendo nos sábados, domingos e dias feriados.
2. A contagem dos prazos na fase de execução do contrato efetua-se nos termos do artigo 471.º do Código dos Contratos Públicos.

Cláusula 20.ª

Subcontratação e cessão da posição contratual

A subcontratação pelo prestador de serviços e a cessão da posição contratual por qualquer das partes depende da autorização da outra, nos termos do Código dos Contratos Públicos.

Cláusula 21.ª

Legislação aplicável

O contrato é regulado pelo CCP e pela demais legislação portuguesa aplicável.

ANEXO I

TERMOS E CONDIÇÕES TÉCNICAS

O âmbito do sistema a implementar encontra-se detalhado no **Anexo II**.

Capítulo I
Ações

A prestação de serviços deverá contemplar, pelo menos, as seguintes ações:

a) Implementar e disponibilizar um portal único de acesso aos diversos sistemas da UPI (Portal@UPI), que observe todos os requisitos:
   i) Funcionais, identificados no **Anexo IV**, do presente CE;
   ii) Não funcionais, identificados no **Anexo V**, do presente CE;
   iii) Outros requisitos, identificados no **Anexo VI**, do presente CE;
b) Instalar e configurar adequadamente o Portal@UPI em sistemas informáticos detidos pela UPI;
c) Disponibilizar nas App Stores iOS e Android uma App Mobile que, sempre que seja necessária autenticação forte para aceder a uma determinada aplicação, exija a aprovação explícita e em tempo real do utilizador;
d) Efetuar as integrações e parametrizações necessárias para que, para além de poder exigir a aprovação explícita do utilizador mediante interação com o seu disposito móvel, as credenciais de acesso por este apresentadas sejam validadas no serviço de diretoria LDAP da UPI;
e) Disponibilizar SDKs[5] de integração e respetiva documentação dos passos necessários para que a UPI possa integrar as suas aplicações com o portal único;
f) Apoio às equipas da UPI na utilização da documentação referida no ponto anterior;
g) Produção e disponibilização de todos os entregáveis descritos no **Anexo VII**, do presente CE.

Capítulo II
Plano de ação

A proposta deverá apresentar um plano de ação detalhado, subdividido nas seguintes fases:

FASE A – Análise Funcional e Técnica

Esta fase compreenderá um conjunto de ações preparatórias essenciais para uma definição clara e inequívoca dos processos a suportar pelo portal de acesso único e das condições base necessárias, assim como das parametrizações específicas a efetuar ao mesmo para que se adeque às necessidades da UPI.

Entre outras, esta fase deverá incluir (pelo menos) as seguintes atividades:

[5] *Software Development Kits*.

1) Documentação, em colaboração com a equipa da UPI, dos processos a suportar pelo portal de acesso único e das aplicações que irão ser integradas com o mesmo, documentando (para cada uma):
   a) O nome da aplicação;
   b) O logótipo da aplicação;
   c) O protocolo de integração (ex: SAML, OAUTH2, etc.) a utilizar e respetivas configurações necessárias;
   d) Os URLs de ligação do:
      i) Ambiente de homologação;
      ii) Ambiente de produção;
2) Analisar e documentar, em colaboração com a equipa da UPI, eventuais mudanças a realizar ao documento de âmbito do projeto necessárias para implementar adequadamente os processos identificados, carecendo as mesmas de aprovação explícita do;
3) Efetuar, em colaboração com a equipa da UPI, o desenho técnico de um portal de acesso único que:
   a) Garanta uma implementação óptima dos processos documentados;
   b) Garanta o fornecimento da informação necessária e suficiente em cada momento aos seus stakeholders;
   c) Assegure um investimento mínimo em cliques e navegação por parte dos utilizadores;
   d) Tenha um design *fully responsive* para todos os ecrãs: telemóvel, tablet e computador;
4) Identificação, em colaboração com a equipa da UPI, dos dados de acesso ao:
   a) Serviço de Diretoria LDAP de homologação;
   b) Serviço de Diretoria LDAP de produção;
   c) Servidor SMTP a utilizar para envio de-mails;
5) Identificação, em colaboração com a equipa da UPI, das aplicações que a UPI irá integrar programaticamente com o portal de acesso único, documentando (para cada uma):
   a) A tecnologia em que se encontra implementada;
   b) O SDK de integração a utilizar;
   c) Os ambientes existentes (homologação, produção, etc);
   d) As credenciais de acesso a utilizar junto do sistema de autenticação forte;
6) Documentação, em colaboração com a equipa da UPI, da infraestrutura de suporte a disponibilizar pela UPI, detalhando nomeadamente:
   a) Características e parametrizações da(s) máquina(s) virtual(is) a disponibilizar pela UPI;
   b) Os servidores/ portas/protocolos de ligação à Internet necessárias à utilização e bom funcionamento do sistema e portal de autenticação forte;
   c) Os servidores/portas/protocolos de ligação que o adjudicatário poderá utilizar para proceder à instalação, parametrização, manutenção e suporte remoto da solução contratada;
   d) Bases de dados e outros serviços (ex: monitorização, backup, etc.) a disponibilizar/assegurar pela UPI.

FASE B – Implementação

Durante esta fase a adjudicatária procederá ao desenvolvimento do portal.

Entre outras, esta fase deverá incluir (pelo menos) as seguintes atividades:

1) Disponibilização (pela UPI) da infraestrutura de suporte necessária à concretização do projecto, de acordo com os detalhes documentados na fase anterior;
2) Construção de um design para o portal que, cumprindo as normas da UPI, suporte de forma eficaz e eficiente a implementação do desenho e especificações elaboradas;
3) Implementação e parametrização do portal para que observe todos os requisitos:
    i) Funcionais, identificados no **Anexo IV**;
    ii) Não funcionais, identificados no **Anexo V**;
    iii) Outros requisitos, identificados no **Anexo VI**;
4) Desenvolvimento dos casos de teste para as diversas funcionalidades e perfis de utilizadores;
5) Preparação do plano de testes e homologação para entrega;
6) Instalação e parametrização do portal na UPI, utilizando os recursos disponibilizados por este;
7) Efetuar as integrações e parametrizações necessárias para que as credenciais de acesso dos utilizadores sejam validadas no serviço de diretoria LDAP da UPI;
8) Disponibilizar SDKs de integração e respetiva documentação dos passos necessários para que a UPI possa integrar as suas aplicações com o portal único.

FASE C – Testes de Aceitação

Durante esta fase a adjudicatária procederá, em conjugação com a UPI, a testes de aceitação da solução fornecida.

Entre outras, esta fase deverá incluir (pelo menos) as seguintes atividades:

1) Definição da estratégia de testes;
2) Efetuar, em colaboração com a equipa da UPI, testes de aceitação.

FASE D – Go-Live

Ao longo desta fase terão lugar as acções necessárias para iniciar o uso do portal único em ambiente produtivo.

Entre outras, esta fase deverá incluir (pelo menos) as seguintes atividades:

1) Preparação do ambiente de formação e apresentação para os *Key users* e Utilizadores finais;
2) Parametrização;
3) Validação;
4) Formação para administração do portal e para *key users*;
5) Preparação de manual para utilizadores finais.

Os outputs esperados de cada uma das fases definidas anteriormente encontram-se elencados no **Anexo VII**, do presente CE.

Capítulo III
Resultados

Com a implementação deste caderno de encargos a UPI deverá obter os seguintes resultados:

1) Passar a dispor de um ponto único de entrada para os diversos sistemas da UPI e, ao mesmo tempo, como plataforma para partilhar serviços entre colaboradores não docentes;

2) Ter condições para integrar as suas aplicações com o referido portal, utilizando as interfaces e protocolos disponibilizadas por este;

3) Aumentar o nível de controlo e proteção no acesso às aplicações e, consequentemente, à informação da UPI, ao permitir a proteção da mesma por tecnologias de autenticação forte do atual estado da arte de segurança, baseadas na utilização de um duplo fator "algo que sabemos/algo que temos e/ou somos";

4) Todos os entregáveis detalhados no **Anexo VII**, do presente CE.

ANEXO II

ÂMBITO DO SISTEMA A IMPLEMENTAR

Com o presente concurso pretende-se contratar o desenvolvimento de um Portal único (Workplace), designado Portal@UPI, que fará a interação e integrará todos os processos e sistemas existentes na UPI, acedido por docentes, funcionários e alunos.

Este novo portal será o ponto único de entrada (balcão único) e servirá para centralizar o acesso aos diversos sistemas da UPI e, ao mesmo tempo, como plataforma para partilhar serviços entre colaboradores não docentes.

Do ponto de vista de segurança, o referido portal deverá ainda permitir à UPI assegurar que os acessos às suas aplicações possam ser protegidos por tecnologias de autenticação forte do atual estado da arte de segurança, baseadas na utilização de um duplo fator "algo que sabemos/algo que temos e/ou somos"[6].

Com a utilização das mesmas, para além das suas credenciais utilizador/senha, deverá ser exigida a aprovação explícita e em tempo real por parte do utilizador, utilizando um dispositivo móvel[7] previamente associado ao seu perfil.

Dessa forma, será possível observar as atuais boas práticas de segurança e evitar acessos não autorizados de aplicações/atacantes maliciosos que, conseguindo obter por meio ilegítimo as credenciais de acesso de outro utilizador, procurem usurpar a sua identidade e respetivos privilégios.

Capítulo I
Objetivos do projeto

Com a concretização deste projeto, a UPI visa permitir:

a) Passar a dispor de um ponto de acesso único de entrada para todos os stakeholders da UPI (candidatos, estudantes, alumni, docentes, investigadores, empresas, e outras entidades), permitindo aa UPI resolver alguns aspectos de distribuição de sistemas;
b) Aumentar o nível de controlo e proteção no acesso às aplicações e, consequentemente, à informação da UPI, ao:
    i) possibilitar a utilização de autenticação de duplo fator "algo que sabemos/algo que temos e/ou somos", integrada com o serviço de diretoria LDAP em uso na UPI para validação de credenciais;
    ii) permitir que, para que lhe seja concedido acesso a uma aplicação considerada sensível pela UPI, um utilizador necessite de interagir com o seu dispositivo móvel para comprovar a sua identidade mediante a introdução de um código PIN ou de apresentação de elementos biométricos;

[6] "*Something you know/something you have/are*" na terminologia inglesa.
[7] Por "*dispositivo móvel*" entende-se um telemóvel/smartphone com sistema operativo Android ou iOS.

iii) possibilitar que as aplicações da UPI possam beneficiar da segurança e controlo acrescidos proporcionados pelo portal único mediante integração via protocolos de autenticação padrão reconhecidos pela indústria, como SAML[8], OAUTH2, LDAP[9] e AD[10];
iv) permitir uma gestão unificada das aplicações a que cada utilizador deverá ter acesso;
v) possibilitar uma eficaz, completa e imediata remoção das autorizações de acesso a utilizadores que, por qualquer razão, deixaram de reunir as condições de acesso às mesmas;
vi) reduzir o seu nível de exposição a risco, ao impedir acessos não autorizados de aplicações/atacantes maliciosos que, conseguindo obter por meio ilegítimo as credenciais de acesso de outro utilizador, procurem usurpar a sua identidade e respetivos privilégios;
vii) permitir utilizar canais cifrados para a transferência entre sistemas das credenciais de acesso;

c) Melhorar a usabilidade e experiência de utilizador no uso das aplicações da UPI, ao:
i) permitir que, caso pretenda, cada utilizador possa usar apenas o seu dispositivo móvel para desbloquear o acesso às mesmas, sem necessidade de introdução manual das suas credenciais em cada acesso;
ii) disponibilizar mecanismos de *single sign-on* que permitam aos utilizadores acederem a todas as aplicações a que têm acesso (de acordo com o seu perfil e privilégios) apenas autenticando-se uma vez por sessão;
iii) reduzir a necessidade de contatos com os Serviços Informáticos da UPI no sentido de recuperar o acesso a contas bloqueadas por erros na introdução de credenciais.

Secção I
Requisitos

O sistema e portal de autenticação forte a fornecer no âmbito deste concurso terão que cumprir integralmente todos os requisitos, do presente CE:

i) Funcionais, identificados no **Anexo IV**;
ii) Não funcionais, identificados no **Anexo V**;
iii) Outros requisitos, identificados no **Anexo VI**;

As propostas submetidas a concurso deverão incluir um anexo que, para cada requisito constante dos referidos anexos, explique de que forma o mesmo seria cumprido pela solução proposta, contendo todos os detalhes técnicos necessários à sua compreensão e apreciação.

Secção II
Entregáveis

Por forma a responder ao objetivo deste projeto, a entidade adjudicatária terá a responsabilidade de coletar, criar e disponibilizar à entidade adjudicante diversos artefactos que no seu conjunto

[8] *Security Assertion Markup Language*.
[9] *Lightweight Directory Access Protocol*.
[10] *Active Directory*.

representam o resultado do projeto. Esses artefactos, nomeados de entregáveis, estão definidos inicialmente no **Anexo VII**, do presente CE e podem ser estendidos pelas entidades adjudicante e adjudicatária, quer na fase de preparação de proposta quer na fase de desenvolvimento do projeto.

Secção III
Responsabilidades

O adjudicatário será responsável pelo fornecimento de todos os componentes exigidos por este concurso, cumprindo os requisitos indicados neste documento. Não é permitida a transferência de responsabilidade da implementação a terceiros sem o consentimento prévio da UPI.

Secção IV
Licenciamento

1. As entidades concorrentes devem incluir nas suas propostas indicação sobre o fornecimento e licenciamento de todo o software necessário, para os ambientes de homologação e produção com exceção daquele que seja disponibilizado pela UPI, indicado no **Anexo III**, do presente CE.
2. Considerando que a UPI possui atualmente cerca de XX.000 utilizadores (dos quais apenas cerca de XX.000 registam atividade semanal) e que a cada ano há cerca de XX.000 novos utilizadores, deverá ser incluído no âmbito das propostas o licenciamento perpétuo sem restrições ao nível do número total de utilizadores e até X.000 acessos simultâneos).
3. São da responsabilidade da entidade adjudicatária quaisquer encargos decorrentes da utilização, no fornecimento, de obras protegidas por direito de autor, marcas registadas, patentes registadas ou licenças (exceto as explicitamente mencionadas no **Anexo III**).
4. São igualmente da responsabilidade da entidade adjudicatária todos os custos originados pelo desrespeito por qualquer dos direitos mencionados no ponto anterior.
5. As propostas deverão ainda incluir os respetivos serviços de manutenção corretiva pelo prazo de pelo menos dois anos (sempre que aplicável), de todo o software necessário ao funcionamento deste sistema e garantir os níveis de disponibilidade, performance e segurança descritos neste documento.
6. Os serviços de manutenção deverão também contemplar as evoluções necessárias para adaptar o uso do sistema a novas versões dos sistemas operativos, exceto em casos em que tal não seja possível devido às alterações introduzidas pelo fabricante. Findo o período de manutenção, a UPI deverá ser livre de continuar a utilizar perpetuamente todo o software fornecido, exceto quando tal acarrete prestação de serviços adicionais.

Capítulo II
Critérios de aceitação

Para cada requisito ou conjunto de requisitos identificados deverão ser definidos, conjuntamente com a UPI e sob a sua aprovação, objetivos bem identificados para completude e aceitação do requisito.

Capítulo III
Fora de âmbito

São identificados a seguir um conjunto de itens que não fazem parte do âmbito do projeto e, portanto, não devem influenciar nenhuma das ações a realizar no projeto:

- Infraestrutura, serviços de administração da mesma e outros recursos, detalhados no **Anexo III**, do presente CE;
- Alterações às aplicações da UPI.

ANEXO III

RECURSOS A DISPONIBILIZAR

Para suportar a execução do projeto, a UPI disponibilizará ao adjudicatário os seguintes recursos:

1) **Rede e Telecomunicações**
   a) A infraestrutura do centro de dados da UPI tem uma arquitetura de alta disponibilidade;
   b) É servido por uma solução de comunicações pública constituída por circuitos ponto-a-ponto de 100 Mbps (*full* duplex) que interligam as escolas ao Centro de Dados da rede da UPI, excetuando o XXX, a XXX e a XXX a 1 Gbps (*full*/duplex), e um acesso à Internet pelo nó de acesso à Rede Ciência, Tecnologia e Sociedade (RCTS), com uma largura de banda de 10 Gbps (*full*/duplex), assente no protocolo BGP;
   c) Os equipamentos ativos de rede (*routers*, *switches* e *firewalls*) estão configurados, em regra, numa topologia Ativo/Passivo;
   d) Os servidores físicos assentam numa arquitetura multi-processador "64-bit Intel Xeon" *14 core*. Em regra, todas as componentes que os integram, por razões de performance ou de disponibilidade, são redundantes (*NICs*, *HBAs*, fontes de alimentação, sistema de ventilação, ...);
   e) Os servidores virtuais estão organizados, de acordos com as respetivas funcionalidades principais, numa *farm* de servidores físicos;
   f) O balanceamento das sessões pelos servidores que compõem cada *farm*, é realizado por *appliances* virtuais, as quais integram soluções de cache;
   g) Todos os equipamentos ativos e servidores integram uma rede Gigabit Ethernet;
   h) Sistemas de *front-end*:
      i) com configuração de *load balancing* de acordo com as especificações definidas pelo adjudicatário;
      ii) que poderão albergar os conteúdos estáticos disponibilizados pela entidade adjudicatária;
   i) Sistema de monitorização Nagios 3.4;
   j) Sincronização de tempo das máquinas virtuais disponibilizadas com uma fonte de tempo confiável e precisa NTP;
   k) Backup automático de dados para um site de backup, sendo que a sincronização de dados entre as duas infraestruturas realiza-se, essencialmente, através de um link dedicado com largura de banda de 1 Gbps;
2) **Base de Dados**
   a) (a identificar em sede de projeto);
3) **Plataforma de Virtualização**
   a) A plataforma de virtualização utilizada é a VMware vSphere 6.5 Enterprise;
   b) Encontra-se assente em 1 cluster com 6 nós;
4) **Máquinas Virtuais**
   a) (a identificar em sede de projeto);
5) **Serviços**
   a) Servidor SMTP;
6) **Licenças de Software**
   a) Todo o explicitamente referido nos pontos anteriores.
7) **Certificados SSL**

a) (a identificar em sede de projeto).

ANEXO IV

REQUISITOS FUNCIONAIS

Nesta seção estão identificadas as funcionalidades que o portal único terá que disponibilizar para observar todas as necessidades da UPI.

A referência efetuada às operações CRUD entende-se como a criação, atualização e eliminação de registos, assim como a obtenção dos detalhes de um único registo e a listagem de todos os registos com possível aplicação de filtros apropriados aos tipos de dados constantes dos registos.

Todas as interações dos utilizadores com o sistema, para execução das operações CRUD ou restantes funcionalidades devem ser efetuadas através de uma interface gráfica ou aplicacional/API[11] disponibilizada pelo Portal@UPI. Está excluída a possibilidade de se efetuarem operações diretamente em sistema de gestão de base de dados.

ID	Funcionalidade	Tipo	Descrição	Interface(s)[12]
		Gerais		
[FUN#01]	Mecanismo RBAC	Obrigatório	Suportar a utilização de mecanismos de RBAC[13], permitindo um controlo de acessos simples definido com base em papéis e privilégios.	n.a.
		Interface Web		
[FUN#02]	Página de Entrada (utilizador não autenticado)	Obrigatório	Ao aceder ao portal único, um utilizador não autenticado deverá poder autenticar-se perante o mesmo, usando qualquer um dos mecanismos de autenticação disponibilizados (ver [FUN#16]), para: • aceder à página de entrada configurado para o seu utilizador • ativar o uso de autenticação forte, associando ao seu perfil um dispositivo móvel que lhe permita provar a sua identidade e aprovar um pedido de acesso em tempo real • alterar o dispositivo móvel que se encontra associado ao seu perfil	Web
[FUN#03]	Página de Entrada (utilizador autenticado)	Obrigatório	Ao aceder ao portal único, um utilizador autenticado deverá ter acesso a uma página de entrada que: • Por omissão, apresente: ○ Lista da aplicações a que lhe foi concedido acesso, bastando clicar no	Web

[11] *Application Programming Interface* em terminologia inglesa.
[12] Esta coluna indica para o respetivo requisito, qual(is) a(s) interface(s) mediante a(s) qual(is) a respetiva funcionalidade deverá ser disponibilizada.
[13] *Role-Based Access Control* ou Controle de Acessos Baseado em Papéis.

ID	Funcionalidade	Tipo	Descrição	Interface(s)[12]
			respetivo nome/icon para ser redirecionado[14] para a mesma • Possa ser configurada para: ○ Apresentar alertas/eventos relevantes, consoante o(s) seus) papel(éis) ○ Visualizar[15] o conteúdo do seu calendário Office 365 ○ Organizar os diversos componentes disponíveis da forma que lhe é mais intuitiva ○ Filtrar a informação apresentada por papel, visualizando apenas os elementos relativos ao papel selecionado	
[FUN#04]	Interface de Utilizador	Obrigatório	Após devidamente autenticado, um utilizador deverá ter acesso a interface Web do portal único que lhe permita: • Consultar o seu perfil de utilizador • Consultar as aplicações a que lhe foi concedido acesso	Web
[FUN#05]	Interface de Administação	Obrigatório	O portal único deverá ter uma interface Web, acessível apenas a utilizadores devidamente autenticados e com privilégios de administração, e que permita administrar o mesmo e configurar todos os parâmetros relevantes, entre os quais: • Gestão CRUD de utilizadores • Gestão CRUD de papéis/grupos de utilizadores • Gestão CRUD de aplicações integradas com o portal único • Configuração de integrações com outros sistemas a que o portal único aceda para obter informação • Aprovisionamento (gestão CRUD) de contas LDAP e associação ao utilizador do Portal@PPorto	Web
Utilizador				
[FUN#06]	Perfil de Utilizador	Obrigatório	Um utilizador autenticado deverá poder consultar o seu perfil de utilizador, com a possibilidade de definir/alterar: • A sua senha • O seu número de telemóvel • Se pretende utilizar autenticação forte, substituição a introdução manual das suas credenciais utilizador/senha pela utilização de um dispositivo móvel que lhe permita provar a sua identidade e aprovar um pedido de acesso em tempo real • Qual o dispostivo móvel (e respectiva designação) que se encontra associado ao seu perfil	Web

[14] Podendo ou não necessitar de se autenticar novamente, consoante a referida aplicação esteja configurada para o exigir ou não.
[15] Caso essa opção se encontra ativa e configurada para o utilizador em causa.

ID	Funcionalidade	Tipo	Descrição	Interface(s)[12]
[FUN#07]	Emparelhamento de Dispositivo Móvel	Obrigatório	A associação de um dispositivo móvel ao perfil um utilizador deverá decorrer da seguinte forma: • Utilizador autentica-se no portal único e seleciona a respetiva opção • Portal único apresenta um código QR code único gerado para cada emparelhamento • Utilizador abre a App de Autenticação Forte e seleciona a opção de leitura de QR Code • App de Autenticação Forte pergunta ao utilizador se autoriza o emparelhamento com o perfil em causa • Portal único associa automaticamente o dispositivo móvel associado ao perfil do utilizador	Web
			Gestão de Utilizadores	
[FUN#08]	Gestão de Utilizadores	Obrigatório	Um utilizador autenticado e com privilégios de administração deverá poder efetuar a gestão CRUD de utilizadores, que deverá permitir (pelo menos): • Listar (de forma paginada) os utilizadores existentes • Pesquisar utilizadores • Consultar os detalhes (nome, e-mail, nº de telemóvel registado) de cada utilizador • Definir/alterar dados de um utilizador • Suspender o acesso de um utilizador, para que este deixe de se conseguir autenticar no portal único (conta LDAP associada também fica suspensa) • Reativar o acesso de um utilizador (conta LDAP associada também fica reativada)	Web
[FUN#09]	Gestão de Papéis/Grupos de Utilizadores	Obrigatório	Um utilizador autenticado e com privilégios de administração deverá poder efetuar a gestão CRUD de papéis/grupos de utilizadores, que deverá permitir (pelo menos): • Consultar, criar, alterar e apagar papéis/grupos de utilizadores • Associar um utilizador a um ou mais papéis/grupos de utilizadores	Web
			Gestão de Aplicações	

[FUN#10]	Gestão de Aplicações	Obrigatório	Um utilizador autenticado e com privilégios de administração deverá poder efetuar a gestão CRUD de aplicações integradas com o portal único, permitindo configurar para cada uma (pelo menos):
			• Parâmetros gerais, incluindo:
			  ○ Nome
			  ○ Logotipo
			  ○ URL de acesso à aplicação
			  ○ Se os utilizadores devem ter acesso por omissão à aplicação (ou apenas caso o mesmo lhes seja explicitamente concedido)
			  ○ Protocolo de integração
			  ○ Nível de segurança mínimo exigido (single sign-on, autenticação forte, etc.)
				Web

ID	Funcionalidade	Tipo	Descrição	Interface(s)[12]
[FUN#11]	Gestão de Permissões de Acesso a Aplicações	Obrigatório	Um utilizador autenticado e com privilégios de administração deverá poder efetuar: • Conceder/retirar acesso a uma aplicação a um determinado utilizador/papel/grupo de utilizadores • Definir que, por omissão, qualquer novo utilizador tem acesso a uma determinada aplicação.	Web
[FUN#12]	Configuração Simplificada de Aplicações	Obrigatório	O portal único deverá permitir a configuração simplificada de aplicações COTS[16], solicitando apenas a introdução da informação que não possa ser automaticamente preenchida. Esta opção deverá ser possível, obrigatoriamente, para as seguintes aplicações: • Office 365 • Gitlab • Github • Jira • Confluence Esta opção deverá ser possível, opcionalmente, para (pelo menos) as seguintes aplicações: • AWS	Web
		Painel de Controlo		
[FUN#13]	Eventos de Sistema e Estatísticas	Obrigatório	Um utilizador autenticado e com privilégios de administração deverá poder consultar (pelo menos): • Para um determinado utilizador: ○ Data/hora dos últimos acessos realizados e a que aplicações ○ Tentativas de acesso bem sucedidas ○ Tentativas de acesso fracassadas • Para uma determinada aplicação: ○ Data/hora dos últimos acessos realizados e por que utilizadores ○ Número de acessos diários ○ Percentagem de acessos à mesma para um determinado período de tempo, quando comparada com a totalidade de acessos registados	Web
[FUN#14]	Distribuição Geográfica	Obrigatório	Um utilizador autenticado e com privilégios de administração deverá poder consultar (pelo menos): • Para todas a aplicações: ○ Localização geográfica (em mapa) dos acessos realizados num determinado período de tempo • Para uma determinada aplicação: ○ Localização geográfica (em mapa) dos acessos realizados num determinado período de tempo	Web

[16] *Commercial off-the-shelf*, aplicações comerciais disponíveis no mercado.

ID	Funcionalidade	Tipo	Descrição	Interface(s)[12]
		Políticas		

[FUN#15]	Suporte para Políticas	Obrigatório	Um utilizador autenticado e com privilégios de administração deverá poder ativar/desativar as seguintes políticas (pelo menos):
			• Para um determinado utilizador/papel/grupo de utilizadores:
			  ○ Possibilidade de acesso apenas em dias úteis/horário laboral
			  ○ Possibilidade de acesso apenas a partir de determinada zona geográfica[17]
			• Para uma determinada aplicação:
			  ○ Possibilidade de acesso apenas em dias úteis/horário laboral
			  ○ Possibilidade de acesso apenas a partir de determinada zona geográfica[18]
				Web

		Autenticação		
[FUN#16]	Mecanismos de Autenticação	Obrigatório	Um utilizador deverá poder autenticar-se: • Introduzindo o seu utilizador/senha registado no serviço de diretoria LDAP da UPI • Utilizando a App de Autenticação Forte, utilizando o seu dispositivo móvel para aprovar explicitamente/em tempo real o seu pedido de acesso e, se o nível de segurança assim o exigir, autenticando-se mediante código PIN, biometria, etc. • Com o seu Cartão de Cidadão, inserido num leitor de smartcards conectado a um sistema operativo suportado oficialmente pelo Cartão de Cidadão • Com a sua Chave Móvel Digital	Web
[FUN#17]	Single Sign-on	Obrigatório	Por omissão, o portal único deverá permitir que um utilizador aceda a todas as aplicações a que tem acesso (de acordo com o seu perfil e privilégios) autenticando-se apenas uma vez por sessão. Esta possibilidade não se aplicará quando, uma determinada aplicação, seja configurada para exigir autenticação forte.	Web
[FUN#18]	Autenticação Forte	Obrigatório	O acesso a uma determinada aplicação pode ser configurado para exigir autenticação forte, que requeira a utilização de autenticação de duplo fator "algo que sabemos" (credenciais na diretoria LDAP em uso na UPI)/"algo que temos e/ou somos" (interação do utilizador com o dispositivo móvel que este tiver associado ao seu perfil). Nesse caso: • Deverá ser possível definir vários níveis de segurança, desde uma simples aprovação explícita até a autenticação biométrica do utilizador • O portal único deverá despoletar o envio de uma *push notification* para o dispositivo móvel	Web

[17] Apenas para uso de autenticação forte.
[18] Apenas para uso de autenticação forte.

ID	Funcionalidade	Tipo	Descrição	Interface(s)[12]
			associado ao perfil do respetivo utilizador sempre que for necessária uma ação deste • Quando necessário, o portal único deverá despoletar o envio de uma mensagem SMS para o dispositivo móvel associado ao perfil do respetivo utilizador • O utilizador deverá instalar no seu dispositivo Android ou iOS a respetiva App de Autenticação Forte.	
[FUN#19]	Apps de Autenticação Forte	Obrigatório	Deverá ser disponibilizada nas App Stores Google e Apple uma App Android e iOS (respetivamente) que, sempre que o acesso a uma determinada aplicação careça de autenticação forte, exija (consoante o nível de segurança definido) que o utilizador: • aprove explicitamente e em tempo real o pedido de acesso • introduza um código PIN (previamente definido por si) • (opcional) faça prova da sua biometria[19] As referidas Apps deverão: • Permitir que, caso o utilizador assim o deseje, o uso da App substitua a introdução manual das suas credenciais utilizador/senha • Ter interface disponível em Português e Inglês • Cifrar toda a informação sensível armazenada no dispositivo móvel • Impedir a captura vídeo da sua utilização • Comunicar com os sistemas centrais através de web socket, utilizando tecnologia PKI para comunicar e se autenticar perante os mesmos	n.a.
			Integração	
[FUN#20]	Calendário Office 365	Obrigatório	Um utilizador autenticado deverá poder configurar a integração (via link para ficheiro .ics) do portal único com o Office 365, de modo a permitir que visualize no portal único os eventos do seu calendário Office 365.	Web
[FUN#21]	Fontes de Informação REST	Obrigatório	Um utilizador autenticado deverá poder configurar a integração (via serviço REST) do portal único com um serviço externo, de modo a permitir que visualize no portal único alertas/eventos relevantes para si.	Web
[FUN#22]	Suporte para Protocolo SAML[20] (Inbound/Outbound)	Obrigatório	No sentido de facilitar a sua integração com as aplicações da UPI, o portal único deverá disponibilizar uma interface SAML	n.a.

[19] Utilizando a biometria suportada pelo dispositivo móvel do utilizador.
[20] *Security Assertion Markup Language*.

ID	Funcionalidade	Tipo	Descrição	Interface(s)[12]
			que, para cada aplicação integrada através desse protocolo, permita a consulta/configuração de: • Identificador SAML da aplicação • ID de utilizador da aplicação • URL de POST da aplicação • Algoritmo de Hash • Se a assinatura digital dos pedidos da aplicação deve ser requerida/verificada • Se as respostas à aplicação devem ser assinadas digitalmente • Algoritmo de assinatura digital das respostas • Se as respostas devem ser cifradas Certificado digital da aplicação	
[FUN#23]	Suporte para Protocolo OAUTH2 (Inbound/Outbound)	Obrigatório	No sentido de facilitar a sua integração com as aplicações da UPI, o portal único deverá disponibilizar uma interface OAUTH2 que, para cada aplicação integrada através desse protocolo, permita a consulta/configuração de: • Identificador único da aplicação • Senha • URL para onde, após a autenticação, o utilizador irá ser redirecionado Par de chaves utilizado para assinar/verificar os tokens	n.a.
[FUN#24]	Suporte para Protocolo LDAP	Obrigatório	No sentido de facilitar a sua integração com as aplicações da UPI, o portal único deverá disponibilizar uma interface LDAP compatível com a implementação atual na UPI (OpenLDAP 2.4.31).	n.a.
[FUN#25]	Suporte para Protocolo AD	Obrigatório	No sentido de facilitar a sua integração com as aplicações da UPI, o portal único deverá disponibilizar uma interface AD, compatível com a implementação atual na UPI (versão AD do Windows 2012).	n.a.

ANEXO V

REQUISITOS NÃO-FUNCIONAIS

O sistema a implementar deverá observar os seguintes requisitos não-funcionais:

ID	Descrição	Tipo	Detalhe
[NFC#01]	Escalabilidade	Obrigatório	O sistema a fornecer deverá encontrar-se implementado e configurado de forma a permitir que, se for necessário fazer face a volumes de pedidos mais elevados, possam ser adicionados mais nodos de forma apenas limitada pelos recursos da infraestrutura que dá suporte ao sistema.
[NFC#02]	Desempenho	Obrigatório	O sistema a fornecer deverá encontrar-se implementado e configurado de forma a permitir que: • O envio de push notifications para dispositivos móveis Android e iOS demore (no máximo) < 3s;
[NFC#03]	Segurança das Comunicações	Obrigatório	Assegurar a confidencialidade dos dados trocados entre as aplicações da UPI, o sistema, o portal de autenticação forte e todos os seus componentes, utilizando canais protegidos por algoritmos criptográficos considerados seguros pela boas práticas atuais.
[NFC#04]	Segurança Aplicacional	Obrigatório	O sistema a fornecer deverá encontrar-se implementado e configurado de forma a: • Mitigar o risco de vulnerabilidade a SQL *Injections* e *cross-side scripting* • Os serviços implementados, bases de dados e outros componentes do sistema façam uso de mecanismos de controlo de acesso que assegurem que cada operação/tipo de informação apenas se encontra acessível a clientes autenticados de acordo com o nível de segurança mínimo exigido para tal • Quando e onde aplicável, utilizar algoritmos criptográficos considerados seguros atualmente • Implementar as recomendações e boas práticas definidas pelo OWASP (*Open Web Application Security Project*)
[NFC#05]	Suporte Multilingue	Obrigatório	O sistema a fornecer deverá encontrar-se implementado e configurado de forma a permitir que: • As interfaces gráficas suportem, em simultâneo, vários idiomas • As interfaces gráficas estejam totalmente disponíveis em Português e Inglês
[NFC#06]	Geração de Códigos de Erro	Obrigatório	O sistema a fornecer deverá utilizar uma estruturação de códigos de erro que permitam uma rápida identificação do âmbito e localização do problema subjacente.

[NFC#07]	Clientes a suportar	Obrigatório	O sistema a fornecer deverá encontrar-se implementado e configurado de forma a permitir o acesso:
			• pela versão mais recente dos seguintes *browsers*:
			  ○ Internet Explorer
			  ○ Microsoft Edge
			  ○ Firefox
			  ○ Chrome
			  ○ Safari
			• em execução, quando aplicável, nos sistemas operativos:
			  ○ Windows 7, 8.1 e 10
			  ○ MacOS 10.8 a 10.12
			  ○ Ubuntu 14.10
			• em dispositivos móveis com plataformas:
			  ○ Android (versões 4.1 a 6.0)
			  ○ iOS (versões 8.0 a 10)

ANEXO VI

OUTROS REQUISITOS

ID	Descrição	Tipo	Detalhe

[OUT#01]	Composição da Equipa de Projeto	Obrigatório	A composição da equipa utilizada pela adjudicatária na implementação do sistema:
			• apenas poderá ser alterada caso:
			  ○ a adjudicatária informe (com pelo menos 15 dias úteis de antecedência, salvo casos de força maior) a UPI do CV (e outras informações relevantes) do(s) novo(s) elemento(s)
			  ○ a UPI manifeste por escrito a sua concordância com a(s) alteração(ões) proposta(s)

[OUT#02]	Experiência no Uso de Criptografia	Desejável	A equipa utilizada pela adjudicatária na implementação do sistema deverá possuir experiência demonstrável no uso de técnicas criptográficas, sendo explicitamente identificado(s) na proposta o(s) elemento(s) detentor(es) da mesma
[OUT#03]	Suporte para envio de *push notifications* informativas	Desejável	O portal único deverá permitir que, em situações a definir pela UPI, sejam enviadas *push notifications* informativas para os dispositivos móveis Android e/ou iOS associados aos perfis dos utilizadores.
[OUT#04]	Suporte para autenticação biométrica	Desejável	A App de Autenticação Forte deverá suportar autenticação biométrica usando o tipo de biometria (impressão digital, facial, etc.) suportada nativamente e embebida em cada dispositivo móvel.
[OUT#05]	Suporte para Protocolo OpenID Connect	Desejável	No sentido de facilitar a sua integração com as aplicações da UPI, o portal único deverá disponibilizar uma interface OpenID Connect que, para cada aplicação integrada através desse protocolo, permita a consulta/configuração de: • Identificador único da aplicação • Senha • URL para onde, após a autenticação, o utilizador irá ser redirecionado Par de chaves utilizado para assinar/verificar os tokens

ANEXO VII

ENTREGÁVEIS

Como resultado da implementação do projeto, é obrigação do adjudicatário fornecer à UPI a seguinte lista de entregáveis:

ID	Descrição	Formato	Entregue em	Observações
Arranque				
[ENT#01]	Plano de Projeto	A propor pela adjudicatária	No máximo, até 3 semanas após data de arranque de projeto	No arranque do projeto deverá ser apresentado um plano de trabalhos detalhado com as atividades e as suas datas de execução, milestones e outra informação relevante para a gestão do projeto e acompanhamento da execução;
Fase A				
[ENT#02]	Documentação de Processos a suportar pelo Portal Único	Microsoft Visio + Microsoft Word	No máximo, até 18 semanas após início da Fase A	Utilizando a notação UML e/ou BPMN, complementada com outro tipo de artefactos que permitam expressar ideias ou conceitos de forma mais percetível e/ou que não sejam suportados de forma adequada pela mesma.
Fase B				
[ENT#03]	Implementação do Portal Único	OVF Virtual Appliance	No máximo, até 6 semanas após início da Fase B	Observando todos os requisitos aplicáveis: • funcionais identificados no Anexo IV; • não funcionais identificados no Anexo V; • gerais identificados no Anexo VI.
[ENT#04]	SDK Java	ZIP	No máximo, até 6 semanas após início da Fase B	SDK em Java que permita a integração com o portal único e respectiva documentação
[ENT#05]	SDK C#	ZIP	No máximo, até 6 semanas após início da Fase B	SDK em C# que permita a integração com o portal único e respectiva documentação
[ENT#06]	SDK Node	ZIP	No máximo, até 6 semanas após início da Fase B	SDK em Node que permita a integração com o portal único e respectiva documentação
[ENT#07]	SDK PHP	ZIP	No máximo, até 6 semanas após início da Fase B	SDK em PHP que permita a integração com o portal único e respectiva documentação
[ENT#08]	Plano de Testes	Microsoft Word	No máximo, até 6 semanas após início da Fase B	Incluindo: • Casos de teste; • Procedimentos de teste; • Critérios de aceitação.
Fase C				
[ENT#09]	Relatório de Testes	Microsoft Word	No máximo, até 6 semanas após início da Fase C	Resultados da execução do Plano de Testes e respetiva análise crítica.
Fase D				
[ENT#10]	Manual de Operação e Administração	Microsoft Word	No máximo, até 7 semanas após início da Fase D	Incluindo procedimentos de monitorização e de recuperação.
[ENT#11]	Manual de Utilização	Microsoft Word	No máximo, até 7 semanas após início da Fase D	Destinado a utilizadores finais.
[ENT#12]	Conteúdos de Suporte	Knowledge Base +	No máximo, até 7 semanas após início da Fase D	Com códigos de erro, FAQs, etc.

ID	Descrição	Formato	Entregue em	Observações
		Decision Tree Kayako[21]		
[ENT#13]	Processo de Ativação de Suporte	Microsoft Word	No máximo, até 7 semanas após início da Fase D	Incluindo os contactos a usar, SLA a esperar e processo de escalamento.

Todos os entregáveis só podem ser considerados finais após a aprovação da UPI.

[21] https://www.kayako.com/

ANEXO VIII

GOVERNANÇA

No sentido de permitir um adequado acompanhamento e controlo do projeto por parte da UPI, o adjudicatário fica obrigado a cumprir os seguintes requisitos de governança:

1) Nomear formalmente um gestor de projeto, com poderes e competências profissionais suficientes para assegurar a articulação com a UPI e para representar as equipas da adjudicatária, em sede de gestão de projeto, que será responsável por:
   a) coordenar o desenrolar dos trabalhos;
   b) eliminar obstáculos às ações da equipa de projeto;
   c) assegurar a disponibilização atempada dos entregáveis identificados no **Anexo VII**;
   d) responder de forma célere, eficaz e completa às solicitações de informação e ação por parte da UPI;

2) O gestor de projeto em representação da adjudicatária deverá estar disponível para reunir com a UPI sempre que solicitado por este, e nas instalações deste.

ANEXO IX

GARANTIA TÉCNICA E SUPORTE

O Adjudicatário garante a manutenção corretiva e suporte do sistema desenvolvido no âmbito deste projeto por um período mínimo de 24 (vinte e quatro) meses, a partir do momento em que seja concluída a FASE C. Durante esse prazo, o adjudicatário garante ainda as evoluções necessárias para adaptar o uso do sistema a novas versões dos sistemas operativos, exceto em casos em que tal não seja possível devido às alterações introduzidas pelo fabricante. Findo o período de manutenção, a UPI deverá ser livre de continuar a utilizar perpetuamente todo o software fornecido, exceto quanda tal acarrete prestação de serviços adicionais.

A garantia técnica compreende as obrigações de o Adjudicatário proceder à correcção ou eliminação dos defeitos, anomalias ou desconformidades com as caraterísticas, especificações e requisitos mencionados nas especificações técnicas constantes no presente caderno de encargos.

O serviço de suporte deverá ser disponibilizado, todos os dias úteis no horário laboral compreendido entre as 09:00 e as 18:00.

O tempo de início de resposta aos pedidos (SLA) deve ser o dia útil seguinte.