CONSULTA PRELIMINAR

"Novo ERP para a CML"

Anexo C -

Requisitos para Fornecedores de Soluções SaaS – Solução Completa

(inclui a componente de replicação de dados)

LISBOA

Anexo C – Requisitos para Fornecedores de Soluções SaaS – Solução Completa (inclui a componente de replicação de dados)

A Câmara Municipal de Lisboa (CML) está a implementar uma estratégia de transformação digital que visa modernizar e otimizar os seus serviços, garantindo simultaneamente a soberania e segurança dos dados municipais. Como parte desta iniciativa, a CML está a desenvolver uma plataforma centralizada de serviços que servirá como ponto de integração para todas as soluções tecnológicas do município.

Neste documento encontram-se elencados um conjunto de requisitos que devem integrar as propostas apresentadas pelos fornecedores para soluções "Software as a Service" (SaaS), pretendendo-se, assim, auscultar o mercado sobre a existência da sua exequibilidade nas soluções propostas.

1. Requisitos de Segurança e Conformidade da Solução		
1.1 Autenticação e Autorização **1.1.1 Protocolo OAuth 2.0**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.AA.01	A solução implementa o protocolo OAuth 2.0, RFC 5849 e atualizações, com fluxo de código de autorização (authorization code flow).	
REQ.AA.02	A solução suporta o fluxo de credenciais do cliente (client credentials flow).	
REQ.AA.03	A solução suporta o mecanismo de revogação previsto no RFC 7009.	
REQ.AA.04	A solução suporta tokens de atualização (refresh tokens) com tempo de vida configurável.	

1. Requisitos de Segurança e Conformidade da Solução		
1.1 Autenticação e Autorização **1.1.2 Integração com Sistemas de Identidade**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.AA.05	A solução integra com o fornecedor de identidade da CML via SAML 2.0.	
REQ.AA.06	A solução suporta autenticação via OpenID Connect.	
REQ.AA.07	A solução implementa a autenticação através da Chave Móvel Digital.	
REQ.AA.08	A solução suporta autenticação multifator (Multi-Factor Authentication).	

1. Requisitos de Segurança e Conformidade da Solução		
1.1 Autenticação e Autorização **1.1.3. Gestão de Permissões**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.AA.09	A solução implementa controlo de acesso baseado em funções (Role-Based Access Control).	
REQ.AA.10	A solução suporta controlo de acesso baseado em atributos (Attribute-Based Access Control).	
REQ.AA.11	A solução permite a delegação temporária de acessos com validade configurável.	
REQ.AA.12	A solução implementa segregação de funções para operações críticas.	

1. Requisitos de Segurança e Conformidade da Solução		
1.1 Autenticação e Autorização **1.1.4 Integração com Microsoft Entra ID**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.AA.13	A solução suporta autenticação através do Microsoft Entra ID (anteriormente Azure AD) utilizando o protocolo OpenID Connect.	
REQ.AA.14	A solução sincroniza e utiliza os grupos do Microsoft Entra ID para gestão de permissões.	
REQ.AA.15	A solução suporta mapeamento configurável entre grupos do Entra ID e permissões da aplicação.	
REQ.AA.16	A solução atualiza automaticamente as permissões quando houver alterações nos grupos do Entra ID.	
REQ.AA.17	A solução suporta grupos encadeados (nested groups) do Entra ID.	
REQ.AA.18	A solução permiti a utilização de evidências (claims) do Entra ID para atributos do utilizador.	

1. Requisitos de Segurança e Conformidade da Solução		
1.1 Autenticação e Autorização **1.1.5 Auditoria e Monitorização**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.AA.19	A solução regista todas as tentativas de autenticação, sucedidas ou falhadas.	
REQ.AA.20	A solução mantém um histórico completo de alterações de permissões.	
REQ.AA.21	A solução gera alertas para tentativas de acesso suspeitas.	
REQ.AA.22	A solução fornece relatórios detalhados de atividade de autenticação.	

1.Requisitos de Segurança e Conformidade da Solução		
1. 1 Autenticação e Autorização **1.1.6 Proteção e Segurança**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.AA.23	A solução implementa proteção contra ataques de força bruta (brute force).	
REQ.AA.24	A solução bloqueia contas após número configurável de tentativas falhadas.	
REQ.AA.25	A solução força a alteração de palavras-passe temporárias no primeiro acesso.	
REQ.AA.26	A solução valida a força das palavras-passe segundo política configurável.	

1. Requisitos de Segurança e Conformidade da Solução		
1.2 Proteção de Dados		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.PD.01	A solução adota os princípios necessários ao cumprimento do Regulamento Geral de Proteção de Dados (RGPD), **REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016** e respetiva Lei de Execução Nacional (Lei n.º 58/2019, de 8 de agosto).	
REQ.PD.02	A solução implementa os requisitos técnicos definidos na Resolução do Conselho de Ministros n.º 41/2018 (arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais).	
REQ.PD.03	O fornecedor demonstra conformidade com as deliberações e orientações da CNPD aplicáveis ao setor público.	

1. Requisitos de Segurança e Conformidade da Solução		
1.2 Proteção de Dados **1.2.1 - Conformidade RGPD**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.PD.04	A fornecedor prepara e fornece todos os elementos necessários (ver Anexo D – *Formulário para Orientação na Recolha de Informação junto de Subcontratantes ou Responsáveis Conjuntos, numa Fase Inicial do Procedimento Contratual*) ao cumprimento das obrigações previstas nos artigos 32.º a 36.º do RGPD [conforme alínea f) do art.º 28.º do RGPD] e celebra um Acordo de Tratamento de Dados nos termos definidos pela CML (ver Anexo E) em sede de assinatura de contrato.	

1. Requisitos de Segurança e Conformidade da Solução		
1.2 Proteção de Dados **1.2.2 - API de Proteção de Dados**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.PD.05	A solução fornece uma API REST documentada para execução de ações relacionadas com o cumprimento do RGPD.	
REQ.PD.06	A solução disponibiliza através da API endpoints específicos para: · Pedido de acesso aos dados (right of access) · Pedido de eliminação de dados (right to erasure) · Pedido de portabilidade de dados (right to data portability) · Pedido de retificação de dados (right to rectification) · Gestão de consentimentos (consent management) · Limitação do tratamento (right to restriction of processing)	
REQ.PD.07	A solução retorna através da API o estado e progresso de cada pedido RGPD.	

1. Requisitos de Segurança e Conformidade da Solução		
1.2 Proteção de Dados **1.2.3 Encriptação**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.PD.08	A solução utiliza TLS 1.3 ou superior para todas as comunicações em rede.	
REQ.PD.09	Todos os certificados utilizados são emitidos por uma Autoridade de Certificação (CA) conhecida.	
REQ.PD.10	A solução implementa encriptação em repouso (encryption at rest) utilizando AES-256 e modos de operação seguros (como o CBC ou GCM).	
REQ.PD.11	A solução suporta a gestão de chaves de encriptação através de um sistema de gestão de chaves (key management system).	
REQ.PD.12	A solução roda automaticamente as chaves de encriptação segundo política configurável.	
RE.PD.13	A solução encripta dados sensíveis em registos de auditoria (audit logs).	

1. Requisitos de Segurança e Conformidade da Solução		
1.2 Proteção de Dados **1.2.4 Exportação e Portabilidade**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.PD.14	A solução mantém um registo detalhado de todas as operações de exportação de dados.	
REQ.PD.15	A solução implementa limites configuráveis para operações de exportação em massa.	

1. Requisitos de Segurança e Conformidade da Solução		
1.2 Proteção de Dados **1.2.4 Exportação e Portabilidade**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.PD.16	A solução inclui assinaturas digitais nas exportações de dados para garantir integridade.	

1. Requisitos de Segurança e Conformidade da Solução		
1.2 Proteção de Dados **1.2.5 Auditoria e Rastreabilidade**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.PD.17	A solução regista todos os acessos a dados pessoais, incluindo visualizações.	
REQ.PD.18	A solução mantém um histórico completo de alterações a dados pessoais (change tracking).	
REQ.PD.19	A solução incluí a finalidade do processamento em todos os registos de auditoria.	
REQ.PD.20	A solução permite a pesquisa e filtragem avançada nos registos de auditoria.	
REQ.PD.21	A solução preserva os registos de auditoria por um período configurável.	

1. Requisitos de Segurança e Conformidade da Solução		
1.2 Proteção de Dados **1.2.6 Isolamento e Segmentação**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.PD.22	A solução implementa segregação lógica de dados entre diferentes clientes (multitenancy).	
REQ.PD.23	A solução suporta a definição de políticas de retenção por tipo de dados.	
REQ.PD.24	A solução implementa controlos de acesso ao nível do campo (field-level security).	
REQ.PD.25	A solução permite a classificação de dados segundo níveis de sensibilidade.	
REQ.PD.26	A solução aplica políticas de proteção baseadas na classificação dos dados.	
REQ.PD.27	A solução está toda sediada dentro da União Europeia e não permite o armazenamento nem qualquer fluxo transfronteiriço de dados para países terceiros ou organizações internacionais.	

1. Requisitos de Segurança e Conformidade da Solução		
1.3 Conformidade Regulamento Jurídico de Segurança do Ciberespaço		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.SC.01	A solução cumpre com os requisitos do Regime Jurídico de Segurança do Ciberespaço (Leis n.º 46/2018 e n.º 65/2021) para operadores de serviços essenciais, bem como com as suas revisões futuras, em particular com a transposição da diretiva SRI 2 (NIS 2) para a lei nacional.	

1. Requisitos de Segurança e Conformidade da Solução		
1.3 Conformidade Regulamento Jurídico de Segurança do Ciberespaço **1.3.1 Gestão de Incidentes**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.SC.02	O fornecedor implementa mecanismos de deteção e notificação de incidentes de segurança.	
REQ.SC.03	O fornecedor fornece toda a informação necessária para notificação ao CNCS em caso de incidente.	
REQ.SC.04	O fornecedor mantém um registo detalhado de todos os incidentes de segurança, incluindo tentativas de intrusão.	
REQ.SC.05	O fornecedor suporta a categorização de incidentes segundo a taxonomia definida pelo CNCS/CERT.PT.	

1. Requisitos de Segurança e Conformidade da Solução		
1.3 Conformidade Regulamento Jurídico de Segurança do Ciberespaço **1.3.2 Monitorização Contínua**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.SC.06	O fornecedor implementa monitorização contínua de segurança (continuous security monitoring).	
REQ.SC.07	A solução integra com o SIEM da CML através de API ou protocolo normalizado a definir durante a implementação da solução.	
REQ.SC.08	O fornecedor gera alertas em tempo real para atividades suspeitas.	
REQ.SC.09	A solução fornece métricas de segurança alinhadas com os requisitos do RJSC (Regime Jurídico de Segurança do Ciberespaço).	
REQ.SC.10	A solução suporta a realização de verificações periódicas de segurança (security assessments).	

1. Requisitos de Segurança e Conformidade da Solução		
1.3 Conformidade Regulamento Jurídico de Segurança do Ciberespaço **1.3.3 Controlos de Segurança**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.SC.11	A solução implementa todos os controlos de segurança obrigatórios definidos no RJSC.	

1. Requisitos de Segurança e Conformidade da Solução		
1.3 Conformidade Regulamento Jurídico de Segurança do Ciberespaço **1.3.3 Controlos de Segurança**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.SC.12	A solução suporta autenticação forte (strong authentication) para todas as contas privilegiadas.	
REQ.SC.13	A solução mantém registos de auditoria (audit logs) num formato não repudiável.	
REQ.SC.14	A solução implementa mecanismos de proteção contra ataques conhecidos (known attack patterns).	
REQ.SC.15	A solução garante a segmentação de redes conforme as melhores práticas do RJSC.	

1. Requisitos de Segurança e Conformidade da Solução		
1.3 Conformidade Regulamento Jurídico de Segurança do Ciberespaço **1.3.4 Relatórios e Documentação**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.SC.16	A solução gera relatórios de conformidade com o RJSC automaticamente.	
REQ.SC.17	A solução mantém um inventário atualizado de todos os ativos de informação.	
REQ.SC.18	O fornecedor documenta todas as medidas de segurança implementadas.	
REQ.SC.19	O fornecedor fornece evidências para auditorias de conformidade com o RJSC.	
REQ.SC.20	O fornecedor mantém registos de todas as avaliações de risco realizadas.	

1. Requisitos de Segurança e Conformidade da Solução		
1.3 Conformidade Regulamento Jurídico de Segurança do Ciberespaço **1.3.5 Gestão de Vulnerabilidades**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.SC.21	A solução implementa proteções contra-ataques comuns, como: • Cross-Site Scripting (XSS); • Cross-Site Request Forgery (CSRF); • SQL Injection; • Session Hijacking.	
REQ.SC.22	A solução suporta a realização de análises regulares de vulnerabilidades.	
REQ.SC.23	O fornecedor implementa processo formal de gestão de vulnerabilidades.	
REQ.SC.24	A solução permite a integração com ferramentas de análise de vulnerabilidades da CML.	

1. Requisitos de Segurança e Conformidade da Solução		
1.3 Conformidade Regulamento Jurídico de Segurança do Ciberespaço **1.3.5 Gestão de Vulnerabilidades**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.SC.25	A solução mantém um registo do estado de correção das vulnerabilidades identificadas.	
REQ.SC.26	A solução prioriza a correção de vulnerabilidades segundo critérios do RJSC.	

1. Requisitos de Segurança e Conformidade da Solução		
1.4 Armazenamento **1.4.1 Proteção de Cópias de Segurança (Backups)**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.AS.01	A solução encripta todas as cópias de segurança.	
REQ.AS.02	A solução armazena os backups em localização física distinta dos dados primários.	
REQ.AS.03	A solução implementa controlo de acesso baseado em funções para operações de backup.	
REQ.AS.04	A solução mantém registos de auditoria de todas as operações de backup e restauro.	
REQ.AS.05	A solução verifica a integridade dos backups através de checksums criptográficos.	

1. Requisitos de Segurança e Conformidade da Solução		
1.4 Armazenamento **1.4.2 Gestão de Dados Sensíveis**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.AS.06	A solução suporta máscaras de dados (data masking) para ambientes não produtivos.	
REQ.AS.07	A solução implementa controlos especiais para dados pessoais sensíveis.	
REQ.AS.08	A solução mantém registos de localização de todos os dados sensíveis.	
REQ.AS.09	A solução implementa mecanismos de eliminação segura de dados (secure deletion).	
REQ.AS.10	A solução suporta diferentes políticas de retenção baseadas na sensibilidade dos dados.	

2. Requisitos Operacionais		
2.1 Disponibilidade e Resiliência **2.1.1 Recuperação de Desastres**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.DR.01	A solução suporta pontos de restauro (recovery points) configuráveis, com período mínimo de 30 dias.	
REQ.DR.02	A solução realiza testes automáticos periódicos dos procedimentos de recuperação.	
REQ.DR.03	A solução mantém um registo detalhado (audit log) de todas as operações de recuperação executadas.	
REQ.DR.04	A solução valida a integridade dos dados após cada operação de recuperação.	

2. Requisitos Operacionais		
2.2 Monitorização **2.2.1 Monitorização da Disponibilidade**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.MO.01	A solução fornece métricas em tempo real sobre o estado de disponibilidade do serviço.	
REQ.MO.02	A solução implementa alertas automáticos para falhas de disponibilidade que excedam limiares configuráveis.	
REQ.MO.03	A solução mantém histórico de disponibilidade com granularidade mínima de 5 minutos.	

2. Requisitos Operacionais		
2.2 Monitorização **2.2.2 Alarmística**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.MO.04	A solução implementa sistema de alertas para eventos críticos com suporte para múltiplos canais de notificação.	
REQ.MO.05	A solução permite a definição de limiares (thresholds) configuráveis para geração de alertas.	
REQ.MO.06	A solução suporta agregação de alertas para evitar sobrecarga de notificações.	
REQ.MO.07	A solução implementa mecanismo de escalamento (escalation) de alertas baseado em regras configuráveis.	

2.Requisitos Operacionais		
2.2 Monitorização **2.2.3 Dashboards e Visualização**		
N.° Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.MO.08	A solução fornece painéis de controlo (dashboards) pré-configurados para monitorização da solução.	
REQ.MO.09	A solução permite visualizar, em dashboard, as métricas de desempenho dos diferentes serviços e integrações.	
REQ.MO.10	A solução permite a exportação de dados de monitorização em formatos standard (CSV, JSON).	

2. Requisitos Operacionais		
2.3 Suporte e Manutenção **2.3.1 Suporte Técnico**		
N.° Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.SM.01	A solução SaaS integra com o sistema de gestão de pedidos (tickets) da CML, a definir durante a fase de implementação.	
REQ.SM.02	O sistema de gestão de pedidos da CML recebe todos os pedidos de suporte referentes à solução.	
N.° Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.SM.03	O fornecedor disponibiliza suporte técnico em português de Portugal durante o horário laboral (9h-18h).	
REQ.SM.04	O fornecedor alimenta a base de conhecimento (knowledge base) da CML com soluções para problemas comuns.	
REQ.SM.05	O fornecedor disponibiliza um canal de suporte prioritário para incidentes críticos com disponibilidade 24x7.	
REQ.SM.06	Os pedidos de suporte são classificados nas prioridades: Baixa, Alta, Muito Alta e Crítica.	

2. Requisitos Operacionais		
2.3 Suporte e Manutenção **2.3.2 Níveis de Serviço**		
N.° Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.SM.07	A solução tem um Acordo de Nível de Serviço Service Level Agreement (SLA) que especifique: • Tempo máximo de resposta para incidentes críticos. • Tempos máximos de resolução por tipo de incidente. • Disponibilidade mínima mensal do serviço de _____%. **(indicar o valor percentual da solução proposta).**	
REQ.SM.08	O fornecedor disponibiliza um portal onde a CML possa consultar em tempo real: • Estado atual do serviço.	

2. Requisitos Operacionais		
2.3 Suporte e Manutenção **2.3.2 Níveis de Serviço**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
	• Histórico de disponibilidade. • Registo de incidentes e tempos de resolução. • Cálculo automático de penalizações.	
REQ.SM.09	Os pedidos de suporte de prioridade Baixa têm: **(indicar os valores da solução proposta).** • Tempo de resposta máximo é de _____ horas úteis. • Tempo de resolução máximo é de _____ dias úteis.	
REQ.SM.10	Os pedidos de suporte de prioridade Alta têm: **(indicar os valores da solução proposta).** • Tempo de resposta máximo é de _____ horas úteis. • Tempo de resolução máximo de _____ dias úteis.	
REQ.SM.11	Os pedidos de suporte de prioridade Muito Alta têm: **(indicar os valores da solução proposta).** • Tempo de resposta máximo de _____ horas úteis. • Tempo de resolução máximo de _____ horas úteis.	
REQ.SM.12	Os pedidos de suporte de prioridade Crítica terão: **(indicar os valores da solução proposta).** • Tempo de resposta máximo de _____ horas úteis. • Tempo de resolução máximo de _____ horas úteis.	

2. Requisitos Operacionais		
2.3 Suporte e Manutenção **2.3.3 Gestão de Atualizações**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.SM.13	A solução fornece um plano de gestão de alterações (change management) documentado para todas as atualizações.	
REQ.SM.14	A solução notifica com antecedência mínima de 15 dias sobre atualizações planeadas que afetem a integração.	
REQ.SM.15	A solução mantém um ambiente de testes atualizado para validação de alterações antes da implementação em produção.	
REQ.SM.16	A solução fornece procedimentos de retrocesso (rollback) documentados para todas as atualizações.	

2. Requisitos Operacionais		
2.3 Suporte e Manutenção **2.3.4 Manutenção Preventiva**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.SM.17	A solução executa verificações preventivas periódicas dos mecanismos de sincronização.	

2. Requisitos Operacionais		
2.3 Suporte e Manutenção **2.3.4 Manutenção Preventiva**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.SM.18	A solução realiza análises regulares de desempenho e capacidade.	
REQ.SM.19	A solução fornece recomendações proativas para otimização da integração.	
REQ.SM.20	A solução mantém um calendário de manutenção preventiva acordado com a CML.	

3. Documentação Requerida		
3.1 Documentação Técnica **3.1.1 Especificação de API**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.DT.01	O fornecedor entrega documentação completa das API em formato OpenAPI 3.0 ou superior, incluindo todos os endpoints, respostas, metadados, modelos de dados e exemplos de utilização.	
REQ.DT.02	O fornecedor fornece documentação detalhada dos mecanismos de autenticação e autorização implementados.	
REQ.DT.03	O fornecedor documenta todos os limites de taxa de utilização (rate limits) e quotas aplicáveis às API.	
REQ.DT.04	A solução mantém um catálogo atualizado de todos os serviços e interfaces disponíveis.	

3.Documentação Requerida		
3.1 Documentação Técnica **3.1.2 Arquitetura e Fluxos**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.DT.05	O fornecedor fornece diagramas de arquitetura detalhados em formato padrão UML ou C4 Model, ilustrando todos os componentes do sistema.	
REQ.DT.06	O fornecedor documenta todos os fluxos de dados entre o sistema SaaS e a plataforma da CML, incluindo diagramas de sequência.	
REQ.DT.07	O fornecedor fornece documentação sobre a topologia de rede necessária para a integração, incluindo requisitos de firewall e portos de comunicação.	

3. Documentação Requerida		
3.1 Documentação Técnica **3.1.3 Modelos de Dados**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.DT.08	O fornecedor documenta o modelo de dados completo, identificando claramente as entidades consideradas estratégicas ou de alto valor.	
REQ.DT.09	O fornecedor fornece mapeamentos (mappings) detalhados entre o modelo de dados completo e o modelo simplificado para replicação.	
REQ.DT.10	O fornecedor documenta todas as restrições de integridade referencial e regras de negócio aplicáveis aos dados estratégicos.	

3. Documentação Requerida		
3.1 Documentação Técnica **3.1.4 Mecanismos de Sincronização**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.DT.11	O fornecedor documenta detalhadamente os mecanismos de sincronização implementados, incluindo gestão de conflitos.	
REQ.DT.12	O fornecedor documenta os mecanismos de validação e garantia de integridade dos dados sincronizados.	

3. Documentação Requerida		
3.1 Documentação Técnica **3.1.5 Monitorização e Diagnóstico**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.DT.13	O fornecedor fornece documentação detalhada sobre os registos (logs) gerados pelo sistema, incluindo formato e estrutura.	
REQ.DT.14	O fornecedor documenta procedimentos de diagnóstico e resolução para cenários comuns de problemas.	

3.Documentação Requerida		
3.1 Documentação Técnica **3.1.6 Migração e Transição**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.DT.15	O fornecedor fornece documentação detalhada dos procedimentos de migração de dados.	
REQ.DT.16	O fornecedor documenta o plano de transição para cenários de término de contrato.	
REQ.DT.17	O fornecedor fornece documentação sobre os procedimentos de exportação de dados em formatos padrão da indústria.	

3. Documentação Requerida		
3.2 Documentação Operacional **3.2.1 Procedimentos de Recuperação**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.DO.01	O fornecedor entrega um plano detalhado de recuperação de desastres (disaster recovery) que inclua: • Procedimentos passo-a-passo; • Responsabilidades e papéis; • Tempos máximos de recuperação Recovery Time Objective (RTO); • Pontos de recuperação garantidos Recovery Point Objective (RPO).	
REQ.DO.02	O fornecedor fornece documentação dos procedimentos de restauro (restore) de dados estratégicos.	
REQ.DO.03	O fornecedor documenta os procedimentos de verificação pós-recuperação.	

3. Documentação Requerida		
3.2 Documentação Operacional **3.2.2 Planos de Contingência**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.DO.04	O fornecedor documenta planos de contingência para cenários críticos, incluindo: • Falhas de conectividade • Corrupção de dados • Comprometimento de segurança • Indisponibilidade de serviço	
REQ.DO.05	O fornecedor DEVE documentar procedimentos alternativos para operação em modo degradado.	

3. Documentação Requerida		
3.2 Documentação Operacional **3.2.3 Resolução de Problemas**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.DO.06	O fornecedor fornece guias de resolução de problemas (troubleshooting) com: • Cenários comuns de erro; • Procedimentos de diagnóstico; • Soluções recomendadas; • Árvores de decisão para resolução.	
REQ.DO.07	O fornecedor documenta procedimentos de recolha de informação de diagnóstico.	

3.Documentação Requerida		
3.2 Documentação Operacional **3.2.4 Procedimentos de Suporte**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.DO.08	O fornecedor documenta os processos de suporte, incluindo: • Canais de comunicação • Horários de atendimento; • Tempos de resposta por severidade; • Procedimentos de escalamento.	
REQ.DO.09	O fornecedor fornece documentação sobre os procedimentos de manutenção preventiva.	
REQ.DO.10	O fornecedor documenta os processos de gestão de alterações (change management).	

3.Documentação Requerida		
3.2 Documentação Operacional **3.2.5 Monitorização Operacional**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.DO.11	O fornecedor documenta os procedimentos de monitorização contínua do serviço.	
REQ.DO.12	O fornecedor fornece documentação sobre a interpretação de alertas e ações recomendadas.	
REQ.DO.13	O fornecedor documenta os procedimentos de geração de relatórios operacionais periódicos.	

3. Documentação Requerida		
3.2 Documentação Operacional **3.2.6 Segurança Operacional**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.DO.14	O fornecedor documenta os procedimentos de resposta a incidentes de segurança.	
REQ.DO.15	O fornecedor fornece documentação sobre os procedimentos de gestão de acessos e credenciais.	
REQ.DO.16	O fornecedor documenta os procedimentos de auditoria de segurança periódica.	

4.Requisitos de Interface		
4.1 Requisitos técnicos		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.IT.01	A interface web é compatível com as versões mais recentes dos seguintes navegadores para ambientes Desktop e para dispositivos Móveis:	

4. Requisitos de Interface		
4.1 Requisitos técnicos		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
	• Google Chrome; • Mozilla Firefox; • Microsoft Edge; • Safari.	
REQ.IT.02	A interface implementa mecanismos de cache adequados para otimizar o desempenho, seguindo as melhores práticas.	
REQ.IT.03	A interface suporta compressão de dados (gzip/deflate) para reduzir o volume de dados transferidos.	
REQ.IT.04	Os tempos de resposta da interface web respeitam os seguintes limites: • Carregamento inicial da página: máximo 2 segundos; • Operações interativas: máximo 1 segundo; • Apresentação de feedback visual: máximo 0.1 segundos.	
REQ.IT.05	A interface implementa gestão de sessões segura incluindo: • Timeout de inatividade configurável; • Invalidação segura de sessões; • Renovação segura de tokens.	
REQ.IT.06	A interface implementa validação de dados tanto no cliente como no servidor.	
REQ.IT.07	A interface implementa gestão adequada de erros com mensagens apropriadas para o utilizador.	

4. Requisitos de Interface		
4.2 Identidade Visual **4.2.1 Conformidade com Manual de Identidade**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.IV.01	A solução implementa todas as diretrizes definidas no Manual de Normas Gráficas da Marca Lisboa, incluindo: • Logótipo e suas variantes; • Paleta de cores institucional; • Tipografia aprovada.	
REQ.IV.02	A solução utiliza apenas as cores definidas no manual de identidade, respeitando os códigos cromáticos especificados.	
REQ.IV.03	A conformidade visual será aferida pela CML e aprovada durante o desenvolvimento.	

4. Requisitos de Interface		
4.2 Identidade Visual **4.2.2 Personalização e Consistência**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.IV.04	A solução permite a configuração de elementos visuais secundários mantendo a conformidade com as diretrizes principais.	

4. Requisitos de Interface		
4.2 Identidade Visual **4.2.2 Personalização e Consistência**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.IV.05	A solução mantém consistência visual em todos os seus componentes, incluindo formulários, tabelas, botões e elementos interativos.	
REQ.IV.06	A solução implementa transições e animações de forma consistente em toda a interface.	

4. Requisitos de Interface		
4.2 Identidade Visual **4.2.3 Domínio e Apresentação**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.IV.07	A solução utiliza exclusivamente o domínio web definido pela CML para todos os acessos públicos.	
REQ.IV.08	A solução apresenta elementos de marca (branding) conforme definido pela CML em: • Favicon; • Imagens de partilha em redes sociais; • Emails e notificações; • Documentos gerados.	

4. Requisitos de Interface		
4.2 Identidade Visual **4.2.4 Responsividade/Adaptabilidade**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.IV.09	A solução mantém a integridade da identidade visual em todas as resoluções de ecrã e dispositivos.	
REQ.IV.10	A solução adapta elementos visuais mantendo a hierarquia e proporções definidas no manual de identidade.	
REQ.IV.11	A solução garante a legibilidade de todos os elementos visuais em diferentes tamanhos de ecrã.	

4. Requisitos de Interface		
4.2 Identidade Visual **4.2.5 Iconografia e Imagens**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.IV.12	A solução utiliza apenas ícones aprovados pela CML ou que sigam as diretrizes de estilo definidas.	
REQ.IV.13	A solução implementa elementos decorativos e ilustrações conforme o estilo visual aprovado pela CML.	

4. Requisitos de Interface		
4.2 Identidade Visual **4.2.5 Iconografia e Imagens**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.IV.14	A solução mantém consistência no tratamento e estilo de imagens em toda a aplicação.	

4. Requisitos de Interface		
4.2 Identidade Visual **4.2.6 Versões e Atualizações**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.IV.15	A solução suporta atualizações da identidade visual sem necessidade de reimplementação completa.	
REQ.IV.16	A solução permite a gestão de versões de elementos visuais, mantendo compatibilidade com versões anteriores quando necessário.	
REQ.IV.17	A solução fornece mecanismos para teste e validação de alterações visuais antes da sua implementação em produção.	

4. Requisitos de Interface		
4.3 Acessibilidade e Usabilidade **4.3.1 Conformidade com Normas**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.IA.01	A solução cumpre as diretrizes de acessibilidade WCAG 2.1 nível AA como mínimo, de acordo com o portal acessibilidade.gov.pt.	
REQ.IA.02	A solução segue as normas europeias de acessibilidade EN 301 549.	
REQ.IA.03	A solução está em conformidade com o DL n.º 83/2018, referente à acessibilidade dos websites e das aplicações móveis.	

4. Requisitos de Interface		
4.3 Acessibilidade e Usabilidade **4.3.2 Navegação e Orientação**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.IA.04	A solução fornece múltiplos meios de localização dentro do conteúdo: • Navegação estruturada; • Função de pesquisa; • Mapa do site; • Navegação baseada em breadcrumbs.	
REQ.IA.05	A solução mantém uma ordem de navegação lógica e consistente em todas as páginas.	
REQ.IA.06	A solução fornece indicações claras sobre a localização atual do	

4. Requisitos de Interface		
4.3 Acessibilidade e Usabilidade **4.3.2 Navegação e Orientação**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
	utilizador na interface.	

4. Requisitos de Interface		
4.3 Acessibilidade e Usabilidade **4.3.3 Formulários e Interação**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.IA.07	A solução fornece etiquetas (labels) claras e instruções para todos os elementos de formulário.	
REQ.IA.08	A solução implementa validação de formulários com mensagens de erro claras e acessíveis.	
REQ.IA.09	A solução permite correção de erros de entrada com sugestões claras de resolução.	

4. Requisitos de Interface		
4.3 Acessibilidade e Usabilidade **4.3.4 Conteúdo Multimédia**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.IA.10	A solução fornece alternativas textuais para todo o conteúdo não textual: • Descrições de imagens • Transcrições para áudio • Legendas para vídeo	
REQ.IA.11	A solução permite controlo de reprodução para conteúdo multimédia temporal.	
REQ.IA.12	A solução evita conteúdo com flash ou animações que possam causar convulsões.	

4. Requisitos de Interface		
4.3 Acessibilidade e Usabilidade **4.3.5 Desempenho e Resposta**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.IA.13	A solução fornece feedback imediato para todas as ações do utilizador.	
REQ.IA.14	A solução implementa indicadores de progresso para operações longas.	
REQ.IA.15	A solução mantém tempos de resposta consistentes e previsíveis em toda a interface.	

4. Requisitos de Interface		
4.4 Internacionalização e Localização **4.4.1 Suporte Linguístico**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.IL.01	A solução tem como idioma principal o português de Portugal.	
REQ.IL.02	A solução suporta o idioma inglês como idioma secundário.	
REQ.IL.03	A solução permite a alteração dinâmica do idioma sem necessidade de recarregamento da página.	
REQ.IL.04	A solução mantém o idioma selecionado entre sessões através de persistência de preferências.	
REQ.IL.05	A solução seleciona a língua a apresentar através das preferências indicadas pelo navegador do utilizador, usando o português por omissão.	

4. Requisitos de Interface		
4.4 Internacionalização e Localização **4.4.2 Interface e Documentação**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.IL.06	A solução adapta automaticamente o layout para acomodar diferentes comprimentos de texto entre idiomas.	
REQ.IL.07	A solução fornece toda a documentação de utilizador em português de Portugal.	
REQ.IL.08	A solução apresenta todas as mensagens de erro e avisos no idioma selecionado pelo utilizador, dentro dos disponíveis.	

4. Requisitos de Interface		
4.5 Integração com Sistemas CML **4.5.1 Autenticação e Autorização**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.IN.01	A solução utiliza a Chave Móvel Digital através da plataforma autenticacao.gov.pt para autenticação de utilizadores externos (munícipes).	
REQ.IN.02	A solução utiliza o Microsoft Entra ID para autenticação de utilizadores internos da CML.	
REQ.IN.03	A solução implementa um mecanismo de descoberta automática do tipo de utilizador para redireccionamento para o sistema de autenticação apropriado.	
REQ.IN.04	A solução mantém tokens de autorização separados para cada tipo de utilizador, respeitando os ciclos de vida específicos de cada sistema de autenticação.	

4. Requisitos de Interface		
4.5 Integração com Sistemas CML **4.5.2 Gestão de Sessões**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.IN.05	A solução implementa tempos de sessão diferenciados: • Para utilizadores internos conforme política da CML; • Para utilizadores externos conforme regulamentação da autenticacao.gov.pt.	
REQ.IN.06	A solução sincroniza o estado da sessão com o serviço de autenticação correspondente.	
REQ.IN.07	A solução implementa terminação de sessão apropriada para cada tipo de autenticação.	

4. Requisitos de Interface		
4.5 Integração com Sistemas CML **4.5.3 Perfis e Permissões**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.IN.08	A solução obtém de acesso dos utilizadores internos diretamente do Microsoft Entra ID.	
REQ.IN.09	A solução mantém uma estrutura de permissões própria apenas para utilizadores externos.	
REQ.IN.10	A solução valida e renova automaticamente as credenciais conforme as políticas de cada sistema de autenticação.	

4.Requisitos de Interface		
4.5 Integração com Sistemas CML **4.5.4 Ajuda e Suporte para Munícipes** Além dos fluxos de pedidos de suporte da CML para o fornecedor SaaS, deverá ser fornecida uma forma de receção de pedidos de suporte do munícipe referentes a funcionalidades da solução SaaS.		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.IN.11	Em caso de pedido de suporte por parte dos munícipes a solução gera um novo email e envia para o helpdesk@cm-lisboa.pt. O email deverá conter toda a informação necessária para a identificação da origem do pedido de suporte.	

4. Requisitos de Interface		
4.5 Integração com Sistemas CML **4.5.4 Ajuda e Suporte para Munícipes** Além dos fluxos de pedidos de suporte da CML para o fornecedor SaaS, deverá ser fornecida uma forma de receção de pedidos de suporte do munícipe referentes a funcionalidades da solução SaaS.		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.IN.12	A solução pode vir a integrar com o sistema centralizado de ajuda da CML, a definir durante a fase de implementação da solução.	

4. Requisitos de Interface		
4.5 Integração com Sistemas CML **4.5.4 Ajuda e Suporte para Munícipes** Além dos fluxos de pedidos de suporte da CML para o fornecedor SaaS, deverá ser fornecida uma forma de receção de pedidos de suporte do munícipe referentes a funcionalidades da solução SaaS.		
REQ.IN.13	A solução pode vir a disponibilizar documentação de utilizador na base de conhecimento central da CML, a definir durante a fase de implementação da solução.	

5.Conformidade e Certificações		
5.1 Conformidade e Certificações **5.1.1 Certificações Gerais de Segurança da Informação**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.CS.01	A solução possuí certificação ISO/IEC 27001:2022 ou superior, ou compatível válida e emitida por entidade acreditada.	
REQ.CS.02	A solução mantém um Sistema de Gestão de Segurança da Informação (SGSI) alinhado com a ISO/IEC 27001 ou compatível.	
REQ.CS.03	O fornecedor disponibiliza à CML a declaração de aplicabilidade (Statement of Applicability) da certificação ISO/IEC 27001 ou compatível.	
REQ.CS.04	A solução possuí certificação SOC 2 Type II ou equivalente europeu, cobrindo os critérios de segurança, disponibilidade e confidencialidade.	

5.Conformidade e Certificações		
5.1 Conformidade e Certificações **5.1.2 Certificações Específicas para a Cloud**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.CS.05	A infraestrutura cloud que suporta o sistema, possuí certificação ISO/IEC 27017 para segurança em cloud computing.	
REQ.CS.06	A infraestrutura cloud que suporta o sistema possuí certificação ISO/IEC 27018 para proteção de dados pessoais em cloud.	
REQ.CS.07	A infraestrutura cloud que suporta o sistema apresenta certificação CSA STAR (Security, Trust, Assurance, and Risk) nível 2 ou superior.	

5.Conformidade e Certificações		
5.1 Conformidade e Certificações **5.1.3 Conformidade com Normas de Segurança**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.CS.08	A solução está em conformidade com as recomendações de segurança do Quadro Nacional de Referência para a Cibersegurança.	
REQ.CS.09	O fornecedor demonstra conformidade com restantes recomendações de segurança do Centro Nacional de	

5.Conformidade e Certificações		
5.1 Conformidade e Certificações **5.1.3 Conformidade com Normas de Segurança**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
	Cibersegurança (CNCS).	

5.Conformidade e Certificações		
5.1 Conformidade e Certificações **5.1.4 Validação e Manutenção de Certificações**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.CS.10	O fornecedor realiza avaliações independentes de segurança (pen testing) por entidade certificada.	
REQ.CS.11	O fornecedor mantém um processo documentado de gestão contínua das certificações, incluindo renovações e atualizações.	
REQ.CS.12	O fornecedor notifica a CML com antecedência mínima de 90 dias sobre quaisquer alterações no estado das certificações.	

5. Conformidade e Certificações		
5.1 Conformidade e Certificações **5.1.5 Requisitos de Documentação**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.CS.13	O fornecedor disponibiliza toda a documentação comprovativa das certificações em português europeu ou inglês.	
REQ.CS.14	O fornecedor mantém um repositório atualizado com todos os relatórios de auditoria e certificação.	
REQ.CS.15	O fornecedor fornece relatórios periódicos de conformidade com as certificações (compliance reports).	

5. Conformidade e Certificações		
5.1 Conformidade e Certificações **5.1.6 Gestão de Incidentes e Continuidade**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.CS.16	O fornecedor segue as indicações do ISO/IEC 27035 ou compatível para gestão de incidentes de segurança da informação.	
REQ.CS.17	A solução está em conformidade com a ISO 22301 ou compatível para gestão de continuidade de negócio.	
REQ.CS.18	O fornecedor mantém certificação ISO/IEC 27031 ou compatível para continuidade de negócio em TIC.	

6. Processo de Validação		
6.1 Ambientes de Validação **6.1.1 Disponibilização de Ambientes**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.AV.01	O fornecedor disponibiliza um ambiente de testes dedicado que replique todas as funcionalidades do ambiente de produção.	
REQ.AV.02	O fornecedor mantém o ambiente de testes sincronizado com a versão de produção com diferença máxima de 5 dias úteis.	
REQ.AV.03	O fornecedor fornece um ambiente de validação com recursos dedicados e isolados de outros clientes.	

6. Processo de Validação		
6.1 Ambientes de Validação **6.1.2 Gestão de Dados de Teste**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.AV.04	O ambiente de testes utiliza conjuntos de dados sintéticos que representem adequadamente os dados estratégicos.	
REQ.AV.05	O fornecedor implementa um processo de refrescamento (refresh) periódico dos dados de teste que não utilize dados reais de produção.	
REQ.AV.06	O fornecedor fornece ferramentas para geração e manipulação de dados de teste que repliquem todos os cenários de integração.	

6. Processo de Validação		
6.1 Ambientes de Validação **6.1.3 Configuração de Ambientes**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.AV.07	O fornecedor disponibiliza documentação detalhada da configuração necessária para estabelecer a ligação com o ambiente de testes.	
REQ.AV.08	O ambiente de testes suporta a simulação de todos os cenários de erro e exceção previstos nos requisitos de integração.	
REQ.AV.09	O fornecedor permite a reposição (reset) do ambiente de testes para um estado base conhecido em menos de _____ horas/dias. **(indicar o valor da solução proposta).**	

6. Processo de Validação		
6.1 Ambientes de Validação **6.1.4 Controlo de Acesso**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.AV.10	O fornecedor implementa mecanismos de autenticação e autorização específicos para o ambiente de testes.	

6. Processo de Validação		
6.1 Ambientes de Validação **6.1.4 Controlo de Acesso**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.AV.11	O fornecedor mantém um registo detalhado (audit log) de todas as operações realizadas no ambiente de testes.	
REQ.AV.12	O fornecedor permite a gestão independente de utilizadores e permissões no ambiente de testes.	

6. Processo de Validação		
6.2 Testes Funcionais **6.2.1 Validação de Fluxos de Dados**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.TF.01	O fornecedor disponibiliza casos de teste documentados para cada fluxo de dados estratégicos identificado.	
REQ.TF.02	O fornecedor implementa validações automáticas para verificar a integridade dos dados durante os testes aos processos de sincronização.	
REQ.TF.03	O fornecedor fornece mecanismos de verificação da ordem cronológica das atualizações de dados estratégicos.	

6. Processo de Validação		
6.2 Testes Funcionais **6.2.2 Testes de Integração**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.TF.04	O fornecedor disponibiliza uma suite completa de testes de integração que cubra todos os endpoints da API.	
REQ.TF.05	O fornecedor fornece testes automatizados para validar o comportamento dos mecanismos de sincronização em modo offline.	
REQ.TF.06	O fornecedor implementa testes específicos para validar a gestão de conflitos na sincronização bidirecional.	

6. Processo de Validação		
6.2 Testes Funcionais **6.2.3 Validação de Transformações**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.TF.07	O fornecedor implementa testes automatizados para validar todas as transformações de dados entre o sistema SaaS e o modelo simplificado.	
REQ.TF.08	O fornecedor fornece casos de teste específicos para validar a preservação da integridade referencial após transformações.	

6. Processo de Validação		
6.2 Testes Funcionais **6.2.3 Validação de Transformações**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.TF.09	O fornecedor disponibiliza ferramentas para comparação automatizada de dados antes e após transformações.	

6. Processo de Validação		
6.2 Testes Funcionais **6.2.4 Gestão de Estados**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.TF.10	O fornecedor fornece testes que validem a preservação do estado da aplicação durante falhas de conectividade.	
REQ.TF.11	O fornecedor implementa validações do processo de recuperação de estado após interrupções de sincronização.	
REQ.TF.12	O fornecedor disponibiliza testes para verificar a consistência dos dados em diferentes estados do sistema.	
REQ.TF.13	O fornecedor disponibiliza testes para verificar o funcionamento dos procedimentos de penalizações por indisponibilidade.	

6. Processo de Validação		
6.2 Testes Funcionais **6.2.5 Validação de Regras de Negócio**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.TF.14	O fornecedor implementa testes específicos para validar a aplicação das regras de classificação de dados estratégicos.	
REQ.TF.15	O fornecedor fornece casos de teste que validem as restrições de acesso aos dados estratégicos.	
REQ.TF.16	O fornecedor disponibiliza testes que verifiquem a correta aplicação das políticas de retenção de dados.	

6. Processo de Validação		
6.3 Validação de Segurança **6.3.1 Análise de Vulnerabilidades**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.VS.01	O fornecedor realiza análises automáticas de vulnerabilidades em todo o código relacionado com a gestão de dados estratégicos.	
REQ.VS.02	O fornecedor executa verificações de segurança do código (code scanning) em todas as atualizações antes da implementação.	
REQ.VS.03	O fornecedor realiza análises regulares de vulnerabilidades nas bibliotecas e dependências utilizadas na integração.	

6. Processo de Validação		
6.3 Validação de Segurança **6.3.2 Validação de Encriptação**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.VS.04	O fornecedor valida a correta implementação dos mecanismos de encriptação em trânsito (in transit) através de testes automatizados.	
REQ.VS.05	O fornecedor verifica a eficácia da encriptação em repouso (at rest) dos dados estratégicos através de testes de acesso direto ao armazenamento.	
REQ.VS.06	O fornecedor testa os procedimentos de rotação de chaves de encriptação sem impacto na disponibilidade dos dados.	

6. Processo de Validação		
6.3 Validação de Segurança **6.3.3 Validação de Controlo de Acessos**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.VS.07	O fornecedor implementa testes automatizados para validar a correta aplicação das políticas de controlo de acesso.	
REQ.VS.08	O fornecedor garante e verifica a segregação efetiva de dados entre diferentes contextos de segurança.	
REQ.VS.09	O fornecedor testa a revogação imediata de acessos em todos os componentes da solução.	

6. Processo de Validação		
6.3 Validação de Segurança **6.3.4 Auditoria de Segurança**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.VS.10	O fornecedor valida a completude e precisão dos registos de auditoria (audit logs) através de testes de rastreabilidade.	
REQ.VS.11	O fornecedor verifica a integridade dos registos de auditoria através de testes de manipulação.	
REQ.VS.12	O fornecedor testa os mecanismos de alerta de segurança através de simulações de incidentes.	
REQ.VS.13	A solução testa a preservação dos registos de auditoria por um período configurável.	
REQ.VS.14	A solução testa a exportação dos registos de auditoria em formato standard para análise externa.	

6. Processo de Validação		
6.3 Validação de Segurança **6.3.5 Testes de Resiliência**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.VS.15	O fornecedor realiza testes de continuidade de segurança durante falhas de componentes críticos.	
REQ.VS.16	O fornecedor valida o comportamento seguro do sistema durante a recuperação de falhas.	
REQ.VS.17	O fornecedor testa a preservação dos controlos de segurança durante operações em modo degradado.	

6. Processo de Validação		
6.4 Certificação de Integrações **6.4.1 Validação de API**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.CI.01	O fornecedor valida a conformidade de todas as API expostas com a especificação OpenAPI 3.0 através de testes automatizados.	
REQ.CI.02	O fornecedor testa a implementação correta de todos os mecanismos de controlo de versão (versioning) das API.	
REQ.CI.03	O fornecedor verifica a correta implementação dos limites de pedidos (rate limiting) e quotas em todas as API.	

6. Processo de Validação		
6.4 Certificação de Integrações **6.4.2 Verificação de Protocolos**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.CI.04	O fornecedor valida a conformidade com o protocolo OAuth 2.0 através de um conjunto completo de testes.	
REQ.CI.05	O fornecedor certifica a implementação correta do protocolo AMQP 1.0 para comunicações assíncronas.	
REQ.CI.06	O fornecedor verifica a conformidade com os protocolos de comunicação segura (TLS 1.3) através de testes específicos.	

6. Processo de Validação		
6.4 Certificação de Integrações **6.4.3 Validação de Sincronização**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.CI.07	O fornecedor certifica o funcionamento correto dos mecanismos de sincronização incremental.	
REQ.CI.08	O fornecedor valida a precisão dos registos temporais (timestamps) utilizados na sincronização.	

6. Processo de Validação		
6.4 Certificação de Integrações **6.4.3 Validação de Sincronização**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.CI.09	O fornecedor garante a correta implementação dos mecanismos de deteção e resolução de conflitos.	

6. Processo de Validação		
6.4 Certificação de Integrações **6.4.4 Verificação de Formatos**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.CI.10	O fornecedor valida a conformidade dos formatos de dados com os esquemas (schemas) JSON definidos.	
REQ.CI.11	O fornecedor certifica a correta codificação de caracteres (UTF-8) em todas as comunicações.	
REQ.CI.12	O fornecedor verifica a conformidade com os formatos de data e hora definidos na norma ISO 8601.	

6. Processo de Validação		
6.4 Certificação de Integrações **6.4.5 Certificação de Resiliência**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.CI.13	O fornecedor valida o comportamento das integrações durante falhas parciais do sistema.	
REQ.CI.14	O fornecedor verifica a recuperação automática das integrações após interrupções de conectividade.	
REQ.CI.15	O fornecedor certifica o correto funcionamento dos mecanismos de tentativas (retry) com espera exponencial.	

Anexo C - Componente de Replicação de Dados

A. Objetivo da Replicação Seletiva

A plataforma centralizada de dados da CML implementa uma estratégia de replicação seletiva, onde apenas os dados classificados como estratégicos são sincronizados e mantidos também nos sistemas da CML (on premises ou SaaS).

A replicação dos dados estratégicos ocorre na sua maioria no sentido do fornecedor para a plataforma centralizada de dados da CML. No entanto, neste caso é importante garantir a bidirecionalidade da replicação.

A replicação dos dados estratégicos tem como objetivos:

- Garantir a soberania sobre dados críticos;
- Facilitar a transição entre fornecedores;
- Otimizar custos de armazenamento e processamento;
- Simplificar a gestão de conformidade regulamentar;
- Garantia de operacionalidade mínima sem recurso a sistemas externos;

- Melhorar a eficiência da preservação digital.

B. Conceitos:

Dados Estratégicos

São considerados dados estratégicos aqueles que apresentam pelo menos uma das seguintes características:

- Dados essenciais para a continuidade operacional dos serviços municipais;
- Dados históricos necessários para análise e tomada de decisão;
- Dados que representam o registo oficial de interações com munícipes;
- Dados necessários para conformidade legal e regulamentar;
- Dados críticos para a transição entre fornecedores de serviços;
- Dados únicos ou de origem primária na CML, que se mantenham atuais.

Dados Não Estratégicos

São considerados dados não estratégicos:

- Dados operacionais temporários;
- Dados duplicados ou derivados de fontes primárias;
- Dados detalhados em cujos agregados sejam suficientes para análise e tomadas de decisão;
- Dados de configuração específicos da solução;
- Dados de utilização e métricas do sistema;
- Dados intermediários auxiliares resultantes de processamento.

Seguidamente, são elencados os requisitos para a "Componente de Replicação de Dados" para a Plataforma de Serviços de Lisboa, a saber:

7. Requisitos de Gestão de Dados Estratégicos		
7.1 Identificação e Classificação de Dados		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.DE.01	O fornecedor fornece um catálogo dos dados armazenados pela solução.	
REQ.DE.02	O fornecedor documenta as dependências entre diferentes conjuntos de dados.	
REQ.DE.03	O fornecedor identifica claramente os dados necessários para a continuidade do negócio.	
REQ.DE.04	A CML irá definir junto do fornecedor aquilo que são dados estratégicos durante a fase de implementação.	
REQ.DE.05	A solução mantém um catálogo dos dados atualizado que inclua a sua classificação, período de retenção e dependências.	

7. Requisitos de Gestão de Dados Estratégicos		
7.2 Modelo de Dados Simplificado		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.DE.06	A solução fornece um modelo de dados simplificado para os dados replicados que inclua apenas os atributos essenciais.	
REQ.DE.07	A solução incluí metadados essenciais para contextualização dos dados.	

7.Requisitos de Gestão de Dados Estratégicos		
7.3 Portabilidade e Interoperabilidade		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.DE.08	A solução armazena os dados estratégicos em formatos abertos e documentados.	
REQ.DE.09	A solução fornece APIs normalizadas para acesso aos dados estratégicos.	
REQ.DE.10	A solução incluí documentação completa do modelo para facilitar migrações futuras.	
REQ.DE.11	A solução permite a exportação dos dados em formatos standard da indústria.	
REQ.DE.12	A solução mantém um histórico das alterações ao modelo de dados.	
REQ.DE.13	A solução gera relatórios de exportação com meta-informação sobre o contexto dos dados.	
REQ.DE.14	A solução tem a funcionalidade de importar dados em lote já pré-existentes.	

7. Requisitos de Gestão de Dados Estratégicos		
7.4 Interfaces de Comunicação **7.4.1 Interface Programática REST (obrigatória)**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.IC.01	A interface programática segue as especificações OpenAPI 3.0 ou superior	
REQ.IC.02	Incluí na descrição em OpenAPI meta informação	
REQ.IC.03	Incluí na descrição em OpenAPI, para cada recurso (endpoint) as respostas possíveis.	
REQ.IC.04	Incluí na descrição em OpenAPI, os componentes reutilizáveis, incluindo os modelos de dados.	
REQ.IC.05	Produz as respostas de erro de acordo com o RFC 7807, Problem Details for HTTP APIs.	
REQ.IC.06	A interface programática utiliza JSON como formato de dados, em todas as situações.	
REQ.IC.07	A interface programática implementa autenticação e autorização com OAuth 2.0 (RFC 6749 e atualizações), mecanismos de autorização nativos do HTTP (RFC 7235), objetos JWT transportados em cabeçalho 'Authorization' ou através de chaves (keys) presentes noutros cabeçalhos HTTP, a definir durante a implementação da solução.	
REQ.IC.08	A interface programática suporta limites de taxa de utilização configuráveis (rate limiting).	
REQ.IC.09	A interface programática incluí a versão no URL (ex: <domínio>/v1/api/).	
REQ.IC.10	Suporta paginação.	

7. Requisitos de Gestão de Dados Estratégicos		
7.4 Interfaces de Comunicação **7.4.1 Interface Programática REST (obrigatória)**		
N.° Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.IC.11	Suporta filtragem sobre os atributos expostos nos modelos de dados.	

7.Requisitos de Gestão de Dados Estratégicos		
7.4 Interfaces de Comunicação **7.4.1 Serviço de Notificações (Webhooks)**		
N.° Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.IC.12	O serviço permite subscrição de eventos específicos.	
REQ.IC.13	O serviço incluí assinatura digital das mensagens.	
REQ.IC.14	O serviço implementa nova tentativa (retry) com intervalos exponenciais em caso de falha.	
REQ.IC.15	O serviço suporta configuração de endpoints por ambiente.	

7.Requisitos de Gestão de Dados Estratégicos		
7.4 Interfaces de Comunicação **7.4.2 Sistema de Publicação/Subscrição de Eventos (Pub/Sub)**		
N.° Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.IC.16	A solução utiliza o protocolo AMQP 1.0 ou superior.	
REQ.IC.17	A solução suporta filtros de eventos.	
REQ.IC.18	A solução permite configuração de qualidade de serviço (Quality of Service).	
REQ.IC.19	A solução implementa persistência de mensagens.	

7. Requisitos de Gestão de Dados Estratégicos		
7.4 Interfaces de Comunicação **7.4.3 Exportação em Lote (Batch)**		
N.° Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.IC.20	A solução suporta paginação de resultados.	
REQ.IC.21	A solução permite filtragem por período temporal.	
REQ.IC.22	A solução implementa compressão de dados.	
REQ.IC.23	A solução suporta exportação incremental.	

7. Requisitos de Gestão de Dados Estratégicos		
7.4 Interfaces de Comunicação **7.4.4 Conectores de Base de Dados**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.IC.24	Os conectores suportam JDBC/ODBC para acesso direto aos dados.	
REQ.IC.25	Os conectores implementam agrupamento de ligações (connection pooling).	
REQ.IC.26	Os conectores permitem configuração de tempo limite em que as ligações estão abertas em idle (connection timeout).	
REQ.IC.27	Os conectores permitem configuração de tempo limite da execução de um comando (timeout).	
REQ.IC.28	Os conectores suportam TLS 1.3 para ligações seguras.	

7. Requisitos de Gestão de Dados Estratégicos		
7.4 Interfaces de Comunicação **7.4.5 Requisitos Comuns**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.IC.29	O mecanismo fornece documentação técnica completa em português de Portugal.	
REQ.IC.30	O mecanismo suporta monitorização através de métricas normalizadas.	
REQ.IC.31	O mecanismo implementa registo estruturado (logging) em formato JSON.	
REQ.IC.32	O mecanismo suporta rastreabilidade através de cabeçalhos de correlação.	
REQ.IC.33	Todas as interfaces de comunicação utilizam a sua versão mais segura, como por exemplo HTTPS (com TLS 1.3) em detrimento de HTTP.	

7. Requisitos de Gestão de Dados Estratégicos		
7.5 Sincronização de Dados O fornecedor implementa capacidades de sincronização que garantam a consistência dos dados entre o seu sistema e a plataforma central da CML. **7.5.1 Mecanismo de Sincronização Base**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.SD.01	A solução replica para o datacentre da CML apenas os dados classificados como estratégicos.	
REQ.SD.02	A solução mantém um registo temporal (timestamp) da última atualização para cada registo.	
REQ.SD.03	A solução regista o momento temporal (timestamp) de cada operação de sincronização.	
REQ.SD.04	A solução implementa replicação incremental dos dados	

7. Requisitos de Gestão de Dados Estratégicos		
7.5 Sincronização de Dados O fornecedor implementa capacidades de sincronização que garantam a consistência dos dados entre o seu sistema e a plataforma central da CML. **7.5.1 Mecanismo de Sincronização Base**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
	estratégicos.	
REQ.SD.05	A solução garante a ordem cronológica das atualizações.	
REQ.SD.06	A solução permite a configuração dos intervalos de sincronização por tipo de dados.	
REQ.SD.07	A solução mantém um registo detalhado de todas as operações de sincronização.	
REQ.SD.08	A solução calcula e verifica checksums para validar a integridade dos dados replicados.	
REQ.SD.09	A solução garante a consistência dos dados replicados através de validações periódicas.	
REQ.SD.10	A solução emite alertas em tempo real quando forem detetadas discrepâncias na sincronização.	

7. Requisitos de Gestão de Dados Estratégicos		
7.5 Sincronização de Dados **7.5.2 Operação em Modo Desligado (Offline)**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.SD.11	A solução mantém uma fila de alterações pendentes quando em modo desligado.	
REQ.SD.12	A solução sincroniza automaticamente as alterações pendentes quando a conectividade for restabelecida.	
REQ.SD.13	A solução implementa mecanismos de controlo de versões (versioning) para alterações em modo desligado.	
REQ.SD.14	A solução garante a consistência dos dados após sincronização de alterações em modo desligado.	
REQ.SD.15	A solução implementa mecanismo de nova tentativa (retry) com espera exponencial para todas as operações de sincronização falhadas.	

7.Requisitos de Gestão de Dados Estratégicos		
7.5 Sincronização de Dados **7.5.3 Controlo e Monitorização**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.SD.16	A solução fornece métricas detalhadas sobre o processo de sincronização.	
REQ.SD.17	A solução emite notificações em caso de falhas de sincronização.	

7.Requisitos de Gestão de Dados Estratégicos		
7.5 Sincronização de Dados **7.5.3 Controlo e Monitorização**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.SD.18	A solução mantém um registo detalhado (audit log) de todas as operações de sincronização.	
REQ.SD.19	A solução permite a configuração de limites de taxa de sincronização (throttling).	

7. Requisitos de Gestão de Dados Estratégicos		
7.5 Sincronização de Dados **7.5.4 Recuperação e Resiliência**		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.SD.20	A solução implementa mecanismos de nova tentativa (retry) com intervalos exponenciais em caso de falha.	
REQ.SD.21	A solução suporta pontos de verificação (checkpoints) para recuperação de sincronizações interrompidas.	
REQ.SD.22	A solução mantém um histórico de estados anteriores para possibilitar reversão (rollback).	
REQ.SD.23	A solução implementa mecanismos de validação de integridade dos dados sincronizados.	

7. Requisitos de Gestão de Dados Estratégicos		
7.6 Formatos e Protocolos		
O fornecedor garante a conformidade com os formatos e protocolos padrão definidos pela CML para assegurar a interoperabilidade com a plataforma central.		
7.6.1 Compatibilidade Nacional		
N.º Requisito	**Requisito**	**Proposta do Fornecedor (Sim/Não)**
REQ.FD.01	A solução suporta as diretivas da plataforma MOSAICO da AMA (Agência para a Modernização Administrativa).	
REQ.FD.02	A solução segue os princípios definidos no Regulamento Nacional de Interoperabilidade Digital (RNID).	