Plataforma de serviços de Lisboa

Requisitos para fornecedores de soluções SaaS

Versão preliminar

Dezembro 2024

FICHA TÉCNICA

Título

Requisitos técnicos para soluções SaaS para integração com a plataforma de serviços de Lisboa.

Promoção

Município de Lisboa

Elaboração Técnica

TECH.ID by ISEL

Equipa Técnica

António Serrador, José Simão, Nuno Cruz (coordenação), Nuno Datia

Data de Edição

Dezembro de 2024

Índice

1 Introdução

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.

Este documento está estruturado em camadas complementares que, embora possam parecer redundantes numa primeira leitura, na realidade abordam diferentes perspetivas e fases do ciclo de vida da solução, tais como:

1. **Organização por Domínios**: O documento organiza os requisitos em domínios funcionais (como segurança, integração, dados) e não-funcionais (como desempenho, disponibilidade). Cada área técnica identifica os requisitos relevantes para a sua responsabilidade específica.

2. **Requisitos Técnicos vs. Documentação**: Existe uma separação entre os requisitos técnicos (o que deve ser implementado) e os requisitos de documentação (como deve ser evidenciado e documentado).

3. **Ciclo de Vida do Sistema:** Os requisitos estão organizados seguindo as diferentes fases do ciclo de vida do sistema:

    - Requisitos de implementação;
    - Requisitos de validação e testes;
    - Requisitos de operação;
    - Requisitos de monitorização e manutenção.

2 Âmbito

Este documento deverá ser utilizado enquanto guião para a definição de requisitos de soluções *Software as a Service* (SaaS) , incluindo uma série de requisitos tipificados. Nesse sentido, estes requisitos não estão limitados a, mas serão na sua maioria utilizados por:

- Fornecedores de soluções SaaS que pretendam integrar com a plataforma de serviços da CML;
- Equipas técnicas responsáveis pela avaliação e implementação de integrações;
- Equipas de desenvolvimento que necessitem adaptar soluções existentes;
- Consultores e parceiros tecnológicos envolvidos em projetos da CML.

3 Classificação de Dados

No contexto deste documento, é fundamental estabelecer a distinção entre dados estratégicos e não estratégicos, tal como se define nas seguintes secções.

3.1 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.

3.2 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.

3.3 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. A replicação dos dados estratégicos ocorre na sua maioria no sentido do fornecedor para a plataforma centralizada de dados da CML. No entanto, para algumas verticais pode ser importante garantir a bidirecionalidade da replicação. Caberá à equipa que definir os requisitos em sede de caderno de encargos, tomar essa decisão. **Neste documento (simplificado), assume-se que a replicação de dados é unidirecional.**

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.

4 Requisitos de Gestão de Dados Estratégicos

Os requisitos que se seguem foram desenvolvidos tendo em consideração as melhores práticas da indústria, os padrões nacionais e internacionais, bem como as necessidades específicas da CML.

4.1 Identificação e Classificação de Dados

REQ.DE.01 – O fornecedor DEVE fornecer um catálogo dos dados armazenados pela solução.

REQ.DE.02 – O fornecedor DEVE documentar as dependências entre diferentes conjuntos de dados.

REQ.DE.03 – O fornecedor DEVE identificar 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 DEVE manter um catálogo dos dados atualizado que inclua a sua classificação, período de retenção e dependências.

4.2 Modelo de Dados Simplificado

REQ.DE.06 – A solução DEVE fornecer um modelo de dados simplificado para os dados replicados que inclua apenas os atributos essenciais.

REQ.DE.07 – A solução DEVE incluir metadados essenciais para contextualização dos dados.

4.3 Portabilidade e Interoperabilidade

REQ.DE.08 – A solução DEVE armazenar os dados estratégicos em formatos abertos e documentados.

REQ.DE.09 – A solução DEVE fornecer APIs normalizadas para acesso aos dados estratégicos.

REQ.DE.10 – A solução DEVE incluir documentação completa do modelo para facilitar migrações futuras.

REQ.DE.11 – A solução DEVE permitir a exportação dos dados em formatos standard da indústria.

REQ.DE.12 – A solução DEVE manter um histórico das alterações ao modelo de dados.

REQ.DE.13 – A solução DEVE gerar relatórios de exportação com meta-informação sobre o contexto dos dados.

REQ.DE.14 – A solução PODE ter a funcionalidade de importar dados em lote já pré-existentes.

4.4 Interfaces de Comunicação

O fornecedor DEVE implementar pelo menos um dos seguintes mecanismos de integração, para além da Interface Programática (API) REST que é obrigatória. Todos os mecanismos implementados DEVEM cumprir os requisitos especificados.

4.4.1 Interface Programática REST (Obrigatória)

REQ.IC.01 – A interface programática DEVE seguir as especificações OpenAPI 3.0 ou superior.

REQ.IC.02 – DEVE incluir na descrição em OpenAPI meta informação.

REQ.IC.03 – DEVE incluir na descrição em OpenAPI, para cada recurso (*endpoint*) as respostas possíveis.
REQ.IC.04 – DEVE incluir na descrição em OpenAPI, os componentes reutilizáveis, incluindo os modelos de dados.
REQ.IC.05 – DEVE produzir as respostas de erro de acordo com o RFC 7807, *Problem Details for HTTP APIs*.
REQ.IC.06 – A interface programática DEVE utilizar JSON como formato de dados, em todas as situações.
REQ.IC.07 – A interface programática DEVE implementar 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 DEVE suportar limites de taxa de utilização configuráveis (*rate limiting*).
REQ.IC.09 – A interface programática DEVE incluir a versão no URL (ex: <domínio>/v1/api/).
REQ.IC.10 – DEVE suportar paginação.
REQ.IC.11 – DEVE suportar filtragem sobre os atributos expostos nos modelos de dados.

4.4.2 Serviço de Notificações (*Webhooks*)

REQ.IC.12 – O serviço PODE permitir subscrição de eventos específicos.
REQ.IC.13 – O serviço PODE incluir assinatura digital das mensagens.
REQ.IC.14 – O serviço PODE implementar nova tentativa (*retry*) com intervalos exponenciais em caso de falha.
REQ.IC.15 – O serviço PODE suportar configuração de *endpoints* por ambiente.

4.4.3 Sistema de Publicação/Subscrição de Eventos (*Pub/Sub*)

REQ.IC.16 – A solução PODE utilizar o protocolo AMQP 1.0 ou superior.
REQ.IC.17 – A solução PODE suportar filtros de eventos.
REQ.IC.18 – A solução PODE permitir configuração de qualidade de serviço (*Quality of Service*)
REQ.IC.19 – A solução PODE implementar persistência de mensagens.

4.4.4 Exportação em Lote (*Batch*)

REQ.IC.20 – A solução PODE suportar paginação de resultados.
REQ.IC.21 – A solução PODE permitir filtragem por período temporal.
REQ.IC.22 – A solução PODE implementar compressão de dados.
REQ.IC.23 – A solução PODE suportar exportação incremental.

4.4.5 Conectores de Base de Dados

REQ.IC.24 – Os conectores PODEM suportar JDBC/ODBC para acesso direto aos dados.
REQ.IC.25 – Os conectores PODEM implementar agrupamento de ligações (*connection pooling*).
REQ.IC.26 – Os conectores PODEM permitir configuração de tempo limite em que as ligações estão abertas em idle (*connection timeout*).
REQ.IC.27 – Os conectores PODEM permitir configuração de tempo limite da execução de um comando (*timeout*)

REQ.IC.28 – Os conectores PODEM suportar TLS 1.3 para ligações seguras.

4.4.6 Requisitos Comuns (Aplicáveis a todos os mecanismos implementados)

REQ.IC.29 – O mecanismo DEVE fornecer documentação técnica completa em português de Portugal.

REQ.IC.30 – O mecanismo DEVE suportar monitorização através de métricas normalizadas.

REQ.IC.31 – O mecanismo DEVE implementar registo estruturado (*logging*) em formato JSON.

REQ.IC.32 – O mecanismo DEVE suportar rastreabilidade através de cabeçalhos de correlação.

REQ.IC.33 – Todas as interfaces de comunicação utilizarão a sua versão mais segura, como por exemplo HTTPS (com TLS 1.3) em detrimento de HTTP.

4.5 Sincronização de Dados

O fornecedor DEVE implementar capacidades de sincronização que garantam a consistência dos dados entre o seu sistema e a plataforma central da CML. Todos os mecanismos de sincronização implementados DEVEM cumprir os seguintes requisitos:

4.5.1 Mecanismo de Sincronização Base

REQ.SD.01 – A solução DEVE replicar para o *datacentre* da CML apenas os dados classificados como estratégicos.

REQ.SD.02 – A solução DEVE manter um registo temporal (*timestamp*) da última atualização para cada registo.

REQ.SD.03 – A solução DEVE registar o momento temporal (*timestamp*) de cada operação de sincronização.

REQ.SD.04 – A solução DEVE implementar replicação incremental dos dados estratégicos.

REQ.SD.05 – A solução DEVE garantir a ordem cronológica das atualizações.

REQ.SD.06 – A solução DEVE permitir a configuração dos intervalos de sincronização por tipo de dados.

REQ.SD.07 – A solução DEVE manter um registo detalhado de todas as operações de sincronização.

REQ.SD.08 – A solução DEVE calcular e verificar *checksums* para validar a integridade dos dados replicados.

REQ.SD.09 – A solução DEVE garantir a consistência dos dados replicados através de validações periódicas.

REQ.SD.10 – A solução DEVE emitir alertas em tempo real quando forem detetadas discrepâncias na sincronização.

4.5.2 Operação em Modo Desligado (Offline)

REQ.SD.11 – A solução DEVE manter uma fila de alterações pendentes quando em modo desligado.

REQ.SD.12 – A solução DEVE sincronizar automaticamente as alterações pendentes quando a conectividade for restabelecida.

REQ.SD.13 – A solução DEVE implementar mecanismos de controlo de versões (*versioning*) para alterações em modo desligado.

REQ.SD.14 – A solução DEVE garantir a consistência dos dados após sincronização de alterações em modo desligado.

REQ.SD.15 – A solução DEVE implementar mecanismo de nova tentativa (*retry*) com espera exponencial para todas as operações de sincronização falhadas.

4.5.3 Controlo e Monitorização

REQ.SD.16 – A solução DEVE fornecer métricas detalhadas sobre o processo de sincronização.

REQ.SD.17 – A solução DEVE emitir notificações em caso de falhas de sincronização.

REQ.SD.18 – A solução DEVE manter um registo detalhado (*audit log*) de todas as operações de sincronização.

REQ.SD.19 – A solução DEVE permitir a configuração de limites de taxa de sincronização (*throttling*).

4.5.4 Recuperação e Resiliência

REQ.SD.20 – A solução DEVE implementar mecanismos de nova tentativa (*retry*) com intervalos exponenciais em caso de falha.

REQ.SD.21 – A solução DEVE suportar pontos de verificação (*checkpoints*) para recuperação de sincronizações interrompidas.

REQ.SD.22 – A solução DEVE manter um histórico de estados anteriores para possibilitar reversão (*rollback*).

REQ.SD.23 – A solução DEVE implementar mecanismos de validação de integridade dos dados sincronizados.

4.6 Formatos e Protocolos

O fornecedor DEVE garantir a conformidade com os formatos e protocolos padrão definidos pela CML para garantir a interoperabilidade com a plataforma central. Todos os mecanismos implementados DEVEM cumprir os seguintes requisitos:

4.6.1 Compatibilidade Nacional

REQ.FD.01 – A solução DEVE suportar as diretivas da plataforma MOSAICO da AMA (Agência para a Modernização Administrativa).

REQ.FD.02 – A solução DEVE seguir os princípios definidos no Regulamento Nacional de Interoperabilidade Digital (RNID).

Os requisitos seguintes são aplicados à solução completa e não apenas à componente de replicação de dados.

5 Requisitos de Segurança e Conformidade da Solução

5.1 Autenticação e Autorização

5.1.1 Protocolo OAuth 2.0

REQ.AA.01 – A solução DEVE implementar o protocolo OAuth 2.0, RFC 5849 e atualizações, com fluxo de código de autorização (*authorization code flow*).

REQ.AA.02 – A solução DEVE suportar o fluxo de credenciais do cliente (*client credentials flow*).

REQ.AA.03 – A solução DEVE suportar o mecanismo de revogação previsto no RFC 7009.

REQ.AA.04 – A solução DEVE suportar *tokens* de atualização (*refresh tokens*) com tempo de vida configurável.

5.1.2 Integração com Sistemas de Identidade

REQ.AA.05 – A solução DEVE integrar com o fornecedor de identidade da CML via SAML 2.0.
REQ.AA.06 – A solução DEVE suportar autenticação via OpenID Connect.
REQ.AA.07 – A solução DEVE implementar a autenticação através da Chave Móvel Digital.
REQ.AA.08 – A solução DEVE suportar autenticação multifator (Multi-Factor Authentication).

5.1.3 Gestão de Permissões

REQ.AA.09 – A solução DEVE implementar controlo de acesso baseado em funções (Role-Based Access Control).
REQ.AA.10 – A solução DEVE suportar controlo de acesso baseado em atributos (Attribute-Based Access Control).
REQ.AA.11 – A solução DEVE permitir a delegação temporária de acessos com validade configurável.
REQ.AA.12 – A solução DEVE implementar segregação de funções para operações críticas.

5.1.4 Integração com Microsoft Entra ID

REQ.AA.13 – A solução DEVE suportar autenticação através do Microsoft Entra ID (anteriormente Azure AD) utilizando o protocolo OpenID Connect.
REQ.AA.14 – A solução DEVE sincronizar e utilizar os grupos do Microsoft Entra ID para gestão de permissões.
REQ.AA.15 – A solução DEVE suportar mapeamento configurável entre grupos do Entra ID e permissões da aplicação.
REQ.AA.16 – A solução DEVE atualizar automaticamente as permissões quando houver alterações nos grupos do Entra ID.
REQ.AA.17 – A solução DEVE suportar grupos encadeados (*nested groups*) do Entra ID.
REQ.AA.18 – A solução DEVE permitir a utilização de evidências (*claims*) do Entra ID para atributos do utilizador.

5.1.5 Auditoria e Monitorização

REQ.AA.19 – A solução DEVE registar todas as tentativas de autenticação, sucedidas ou falhadas.
REQ.AA.20 – A solução DEVE manter um histórico completo de alterações de permissões.
REQ.AA.21 – A solução DEVE gerar alertas para tentativas de acesso suspeitas.
REQ.AA.22 – A solução DEVE fornecer relatórios detalhados de atividade de autenticação.

5.1.6 Proteção e Segurança

REQ.AA.23 – A solução DEVE implementar proteção contra ataques de força bruta (*brute force*).
REQ.AA.24 – A solução DEVE bloquear contas após número configurável de tentativas falhadas.
REQ.AA.25 – A solução DEVE forçar a alteração de palavras-passe temporárias no primeiro acesso.
REQ.AA.26 – A solução DEVE validar a força das palavras-passe segundo política configurável.

5.2 Proteção de Dados

REQ.PD.01 – A solução DEVE adotar os princípios necessários ao cumprimento do Regulamento Geral de Proteção de Dados (Lei n.º 58/2019).

REQ.PD.02 – A solução DEVE implementar 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 DEVE demonstrar conformidade com as deliberações e orientações da CNPD aplicáveis ao setor público.

5.2.1 Conformidade RGPD

REQ.PD.04 – A solução deve apresentar a documentação mencionada na Recomendação 1/2023 da Encarregada de Proteção de Dados - Formulário para orientação na recolha de informação em matéria de proteção de dados junto de Subcontratantes ou Responsáveis Conjuntos, numa fase inicial do procedimento contratual (Anexo III), bem como a respetiva celebração de um ACORDO DE TRATAMENTO DE DADOS, designadamente:

a. Diagrama de Contexto da Arquitetura, com a apresentação do desenho da solução proposta, identificando as suas componentes; breve descrição da finalidade; identificação das categorias dos titulares dos dados pessoais e dos destinatários; fluxos de dados pessoais tratados para efeitos da interpretação da rastreabilidade do tratamento de dados realizado e indicação do Encarregado de Proteção de Dados e respetivo contacto;
b. Classificação e Identificação dos Dados Pessoais a tratar:
    i. Dados Genéricos - Dados de identificação; Dados de contacto; Dados de faturação; Dados de tráfego e de localização; Dados de navegação na internet; Dados de perfis e; outras categorias de dados pessoais não sensíveis.
    ii. Dados Pessoais de Categorias Especiais - Dados biométricos (ex: controlo de acesso físico, controlo de acesso lógico, impressão digital, voz, fotografia, imagem, ...) e; outros.
c. Identificação e descrição dos produtos e serviços propostos incluindo a lista dos seguintes componentes da solução proposta:
    i. Os dispositivos/equipamentos (anexar documentos relativos às especificações técnicas).
    ii. Os softwares/sistemas aplicacionais (anexar documentos relativos às funcionalidades).
d. Operações de tratamento a realizar no âmbito da execução dos serviços prestados.
e. Avaliação de Impacto sobre a Proteção de Dados (AIPD). Existindo uma AIPD validada pelo EPD do subcontratante, deve ser anexado o respetivo documento (incluindo a matriz de risco e a tabela de nível de risco que foi aplicada). A não existência da AIPD deve ser fundamentada.

5.2.2 API de Proteção de Dados

REQ.PD.05 – A solução PODE fornecer uma API REST documentada para execução de ações relacionadas com o cumprimento do RGPD.

REQ.PD.06 – A solução PODE disponibilizar 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 PODE retornar através da API o estado e progresso de cada pedido RGPD.

5.2.3 Encriptação

REQ.PD.08 – A solução DEVE utilizar TLS 1.3 ou superior para todas as comunicações em rede.

REQ.PD.09 – Todos os certificados utilizados DEVEM ser emitidos por uma Autoridade de Certificação (CA) conhecida.

REQ.PD.10 – A solução DEVE implementar encriptação em repouso (*encryption at rest*) utilizando AES-256 e modos de operação seguros (como o CBC ou GCM).

REQ.PD.11 – A solução DEVE suportar a gestão de chaves de encriptação através de um sistema de gestão de chaves (*key management system*).

REQ.PD.12 – A solução DEVE rodar automaticamente as chaves de encriptação segundo política configurável.

REQ.PD.13 – A solução DEVE encriptar dados sensíveis em registos de auditoria (*audit logs*).

5.2.4 Exportação e Portabilidade

REQ.PD.14 – A solução DEVE manter um registo detalhado de todas as operações de exportação de dados.

REQ.PD.15 – A solução DEVE implementar limites configuráveis para operações de exportação em massa.

REQ.PD.16 – A solução DEVE incluir assinaturas digitais nas exportações de dados para garantir integridade.

5.2.5 Auditoria e Rastreabilidade

REQ.PD.17 – A solução DEVE registar todos os acessos a dados pessoais, incluindo visualizações.

REQ.PD.18 – A solução DEVE manter um histórico completo de alterações a dados pessoais (*change tracking*).

REQ.PD.19 – A solução DEVE incluir a finalidade do processamento em todos os registos de auditoria.

REQ.PD.20 – A solução DEVE permitir a pesquisa e filtragem avançada nos registos de auditoria.

REQ.PD.21 – A solução DEVE preservar os registos de auditoria por um período configurável.

5.2.6 Isolamento e Segmentação

REQ.PD.22 – A solução DEVE implementar segregação lógica de dados entre diferentes clientes (*multitenancy*).

REQ.PD.23 – A solução DEVE suportar a definição de políticas de retenção por tipo de dados.

REQ.PD.24 – A solução DEVE implementar controlos de acesso ao nível do campo (*field-level security*).

REQ.PD.25 – A solução DEVE permitir a classificação de dados segundo níveis de sensibilidade.

REQ.PD.26 – A solução DEVE aplicar políticas de proteção baseadas na classificação dos dados.

5.3 Conformidade Regulamento Jurídico de Segurança do Ciberespaço

REQ.SC.01 – A solução DEVE cumprir 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.

5.3.1 Gestão de Incidentes

REQ.SC.02 – O fornecedor DEVE implementar mecanismos de deteção e notificação de incidentes de segurança.

REQ.SC.03 – O fornecedor DEVE fornecer toda a informação necessária para notificação ao CNCS em caso de incidente.

REQ.SC.04 – O fornecedor DEVE manter um registo detalhado de todos os incidentes de segurança, incluindo tentativas de intrusão.

REQ.SC.05 – O fornecedor DEVE suportar a categorização de incidentes segundo a taxonomia definida pelo CNCS/CERT.PT.

5.3.2 Monitorização Contínua

REQ.SC.06 – O fornecedor DEVE implementar monitorização contínua de segurança (*continuous security monitoring*).

REQ.SC.07 – A solução DEVE integrar com o SIEM da CML através de API ou protocolo normalizado a definir durante a implementação da solução.

REQ.SC.08 – O fornecedor DEVE gerar alertas em tempo real para atividades suspeitas.

REQ.SC.09 – A solução DEVE fornecer métricas de segurança alinhadas com os requisitos do RJSC (Regime Jurídico de Segurança do Ciberespaço).

REQ.SC.10 – A solução DEVE suportar a realização de verificações periódicas de segurança (*security assessments*).

5.3.3 Controlos de Segurança

REQ.SC.11 – A solução DEVE implementar todos os controlos de segurança obrigatórios definidos no RJSC.

REQ.SC.12 – A solução DEVE suportar autenticação forte (*strong authentication*) para todas as contas privilegiadas.

REQ.SC.13 – A solução DEVE manter registos de auditoria (*audit logs*) num formato não repudiável.

REQ.SC.14 – A solução DEVE implementar mecanismos de proteção contra ataques conhecidos (*known attack patterns*).

REQ.SC.15 – A solução DEVE garantir a segmentação de redes conforme as melhores práticas do RJSC.

5.3.4 Relatórios e Documentação

REQ.SC.16 – A solução DEVE gerar relatórios de conformidade com o RJSC automaticamente.

REQ.SC.17 – A solução DEVE manter um inventário atualizado de todos os ativos de informação.

REQ.SC.18 – O fornecedor DEVE documentar todas as medidas de segurança implementadas.

REQ.SC.19 – O fornecedor DEVE fornecer evidências para auditorias de conformidade com o RJSC.

REQ.SC.20 – O fornecedor DEVE manter registos de todas as avaliações de risco realizadas.

5.3.5 Gestão de Vulnerabilidades

REQ.SC.21 – A solução DEVE implementar proteções contra ataques comuns, como:

- Cross-Site Scripting (XSS);
- Cross-Site Request Forgery (CSRF);
- SQL Injection;
- Session Hijacking.

REQ.SC.22 – A solução DEVE suportar a realização de análises regulares de vulnerabilidades.

REQ.SC.23 – O fornecedor DEVE implementar processo formal de gestão de vulnerabilidades.

REQ.SC.24 – A solução DEVE permitir a integração com ferramentas de análise de vulnerabilidades da CML.

REQ.SC.25 – A solução DEVE manter um registo do estado de correção das vulnerabilidades identificadas.

REQ.SC.26 – A solução DEVE prioritizar a correção de vulnerabilidades segundo critérios do RJSC.

5.4 Armazenamento

5.4.1 Segurança do Armazenamento

Os requisitos associados à segurança dos dados encontram-se em capítulo dedicado ao tema da segurança.

5.4.2 Proteção de Cópias de Segurança (*Backups*)

REQ.AS.01 – A solução DEVE encriptar todas as cópias de segurança.

REQ.AS.02 – A solução DEVE armazenar os backups em localização física distinta dos dados primários.

REQ.AS.03 – A solução DEVE implementar controlo de acesso baseado em funções para operações de backup.

REQ.AS.04 – A solução DEVE manter registos de auditoria de todas as operações de backup e restauro.

REQ.AS.05 – A solução DEVE verificar a integridade dos backups através de *checksums* criptográficos.

5.4.3 Gestão de Dados Sensíveis

REQ.AS.06 – A solução DEVE suportar máscaras de dados (*data masking*) para ambientes não produtivos.

REQ.AS.07 – A solução DEVE implementar controlos especiais para dados pessoais sensíveis.

REQ.AS.08 – A solução DEVE manter registos de localização de todos os dados sensíveis.

REQ.AS.09 – A solução DEVE implementar mecanismos de eliminação segura de dados (*secure deletion*).

REQ.AS.10 – A solução DEVE suportar diferentes políticas de retenção baseadas na sensibilidade dos dados.

6 Requisitos Operacionais

6.1 Disponibilidade e Resiliência

6.1.1 Recuperação de Desastres

REQ.DR.01 – A solução DEVE suportar pontos de restauro (*recovery points*) configuráveis, com período mínimo de 30 dias.

REQ.DR.02 – A solução DEVE realizar testes automáticos periódicos dos procedimentos de recuperação.

REQ.DR.03 – A solução DEVE manter um registo detalhado (*audit log*) de todas as operações de recuperação executadas.

REQ.DR.04 – A solução DEVE validar a integridade dos dados após cada operação de recuperação.

6.2 Monitorização

O fornecedor deverá fornecer formas de monitorizar a funcionalidade da solução de acordo com os seguintes requisitos.

6.2.1 Monitorização da Disponibilidade

REQ.MO.01 – A solução DEVE fornecer métricas em tempo real sobre o estado de disponibilidade do serviço.

REQ.MO.02 – A solução DEVE implementar alertas automáticos para falhas de disponibilidade que excedam limiares configuráveis.

REQ.MO.03 – A solução DEVE manter histórico de disponibilidade com granularidade mínima de 5 minutos.

6.2.2 Alarmística

REQ.MO.04 – A solução DEVE implementar sistema de alertas para eventos críticos com suporte para múltiplos canais de notificação.

REQ.MO.05 – A solução DEVE permitir a definição de limiares (*thresholds*) configuráveis para geração de alertas.

REQ.MO.06 – A solução DEVE suportar agregação de alertas para evitar sobrecarga de notificações.

REQ.MO.07 – A solução DEVE implementar mecanismo de escalamento (*escalation*) de alertas baseado em regras configuráveis.

6.2.3 Dashboards e Visualização

REQ.MO.08 – A solução DEVE fornecer painéis de controlo (*dashboards*) pré-configurados para monitorização da solução.

REQ.MO.09 – A solução DEVE permitir visualizar, em *dashboard*, as métricas de desempenho dos diferentes serviços e integrações.

REQ.MO.10 – A solução DEVE permitir a exportação de dados de monitorização em formatos standard (CSV, JSON).

6.3 Suporte e Manutenção

6.3.1 Suporte Técnico

REQ.SM.01 – O fornecedor da solução SaaS PODE integrar 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 PODE receber todos os pedidos de suporte referentes à solução.

REQ.SM.03 – O fornecedor DEVE disponibilizar suporte técnico em português de Portugal durante o horário laboral (9h-18h).

REQ.SM.04 – O fornecedor DEVE alimentar a base de conhecimento (*knowledge base*) da CML com soluções para problemas comuns.

REQ.SM.05 – O fornecedor DEVE disponibilizar um canal de suporte prioritário para incidentes críticos com disponibilidade 24x7.

REQ.SM.06 – Os pedidos de suporte DEVEM ser classificados nas prioridades Baixa, Alta, Muito Alta e Crítica.

6.3.2 Níveis de Serviço

REQ.SM.07 – A solução DEVE ter um Acordo de Nível de Serviço Service Level Agreement (SLA) que especifique:

- Tempo máximo de resposta para incidentes críticos;
- Disponibilidade mínima mensal do serviço de 99%;
- Tempos máximos de resolução por tipo de incidente;

REQ.SM.08 – O fornecedor DEVE disponibilizar um portal onde a CML possa consultar em tempo real:

- Estado atual do serviço;
- Histórico de disponibilidade;
- Registo de incidentes e tempos de resolução;
- Cálculo automático de penalizações.

REQ.SM.09 – Os pedidos de suporte de prioridade Baixa terão:

- Tempo de resposta máximo de 72 horas úteis;
- Tempo de resolução máximo de 15 dias úteis;

REQ.SM.10 – Os pedidos de suporte de prioridade Alta terão:

- Tempo de resposta máximo de 48 horas úteis;
- Tempo de resolução máximo de 5 dias úteis;

REQ.SM.11 – Os pedidos de suporte de prioridade Muito Alta terão:

- Tempo de resposta máximo de 8 horas úteis;
- Tempo de resolução máximo de 24 horas úteis;

REQ.SM.12 – Os pedidos de suporte de prioridade Crítica terão:

- Tempo de resposta máximo de 2 horas úteis.
- Tempo de resolução máximo de 4 horas úteis.

6.3.3 Gestão de Atualizações

REQ.SM.13 – A solução DEVE fornecer um plano de gestão de alterações (*change management*) documentado para todas as atualizações.

REQ.SM.14 – A solução DEVE notificar com antecedência mínima de 15 dias sobre atualizações planeadas que afetem a integração.

REQ.SM.15 – A solução DEVE manter um ambiente de testes atualizado para validação de alterações antes da implementação em produção.

REQ.SM.16 – A solução DEVE fornecer procedimentos de retrocesso (*rollback*) documentados para todas as atualizações.

6.3.4 Manutenção Preventiva

REQ.SM.17 – A solução DEVE executar verificações preventivas periódicas dos mecanismos de sincronização.

REQ.SM.18 – A solução DEVE realizar análises regulares de desempenho e capacidade.

REQ.SM.19 – A solução DEVE fornecer recomendações proativas para otimização da integração.

REQ.SM.20 – A solução DEVE manter um calendário de manutenção preventiva acordado com a CML.

7 Documentação Requerida

7.1 Documentação Técnica

7.1.1 Especificação de API

REQ.DT.01 – O fornecedor DEVE entregar 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 DEVE fornecer documentação detalhada dos mecanismos de autenticação e autorização implementados.

REQ.DT.03 – O fornecedor DEVE documentar todos os limites de taxa de utilização (*rate limits*) e quotas aplicáveis às API.

REQ.DT.04 – A solução DEVE manter um catálogo atualizado de todos os serviços e interfaces disponíveis.

7.1.2 Arquitetura e Fluxos

REQ.DT.05 – O fornecedor DEVE fornecer diagramas de arquitetura detalhados em formato padrão UML ou C4 Model, ilustrando todos os componentes do sistema.

REQ.DT.06 – O fornecedor DEVE documentar todos os fluxos de dados entre o sistema SaaS e a plataforma da CML, incluindo diagramas de sequência.

REQ.DT.07 – O fornecedor DEVE fornecer documentação sobre a topologia de rede necessária para a integração, incluindo requisitos de firewall e portos de comunicação.

7.1.3 Modelos de Dados

REQ.DT.08 – O fornecedor DEVE documentar o modelo de dados completo, identificando claramente as entidades consideradas estratégicas ou de alto valor.

REQ.DT.09 – O fornecedor DEVE fornecer mapeamentos (*mappings*) detalhados entre o modelo de dados completo e o modelo simplificado para replicação.

REQ.DT.10 – O fornecedor DEVE documentar todas as restrições de integridade referencial e regras de negócio aplicáveis aos dados estratégicos.

7.1.4 Mecanismos de Sincronização

REQ.DT.11 – O fornecedor DEVE documentar detalhadamente os mecanismos de sincronização implementados, incluindo gestão de conflitos.

REQ.DT.12 – O fornecedor DEVE documentar os mecanismos de validação e garantia de integridade dos dados sincronizados.

7.1.5 Monitorização e Diagnóstico

REQ.DT.13 – O fornecedor DEVE fornecer documentação detalhada sobre os registos (*logs*) gerados pelo sistema, incluindo formato e estrutura.

REQ.DT.14 – O fornecedor DEVE documentar procedimentos de diagnóstico e resolução para cenários comuns de problemas.

7.1.6 Migração e Transição

REQ.DT.15 – O fornecedor DEVE fornecer documentação detalhada dos procedimentos de migração de dados.

REQ.DT.16 – O fornecedor DEVE documentar o plano de transição para cenários de término de contrato.

REQ.DT.17 – O fornecedor DEVE fornecer documentação sobre os procedimentos de exportação de dados em formatos padrão da indústria.

7.2 Documentação Operacional

7.2.1 Procedimentos de Recuperação

REQ.DO.01 – O fornecedor DEVE entregar 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 DEVE fornecer documentação dos procedimentos de restauro (*restore*) de dados estratégicos.

REQ.DO.03 – O fornecedor DEVE documentar os procedimentos de verificação pós-recuperação.

7.2.2 Planos de Contingência

REQ.DO.04 – O fornecedor DEVE documentar 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.

7.2.3 Resolução de Problemas

REQ.DO.06 – O fornecedor DEVE fornecer 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 DEVE documentar procedimentos de recolha de informação de diagnóstico.

7.2.4 Procedimentos de Suporte

REQ.DO.08 – O fornecedor DEVE documentar os processos de suporte, incluindo:

- Canais de comunicação
- Horários de atendimento;
- Tempos de resposta por severidade;
- Procedimentos de escalamento.

REQ.DO.09 – O fornecedor DEVE fornecer documentação sobre os procedimentos de manutenção preventiva.

REQ.DO.10 – O fornecedor DEVE documentar os processos de gestão de alterações (*change management*).

7.2.5 Monitorização Operacional

REQ.DO.11 – O fornecedor DEVE documentar os procedimentos de monitorização contínua do serviço.

REQ.DO.12 – O fornecedor DEVE fornecer documentação sobre a interpretação de alertas e ações recomendadas.

REQ.DO.13 – O fornecedor DEVE documentar os procedimentos de geração de relatórios operacionais periódicos.

7.2.6 Segurança Operacional

REQ.DO.14 – O fornecedor DEVE documentar os procedimentos de resposta a incidentes de segurança.

REQ.DO.15 – O fornecedor DEVE fornecer documentação sobre os procedimentos de gestão de acessos e credenciais.

REQ.DO.16 – O fornecedor DEVE documentar os procedimentos de auditoria de segurança periódica.

8 Requisitos de Interface

8.1 Requisitos técnicos

REQ.IT.01 – A interface web DEVE ser compatível com as versões mais recentes dos seguintes navegadores para ambientes Desktop e para dispositivos Móveis:

- Google Chrome;
- Mozilla Firefox;
- Microsoft Edge;
- Safari.

REQ.IT.02 – A interface DEVE implementar mecanismos de cache adequados para otimizar o desempenho, seguindo as melhores práticas.

REQ.IT.03 – A interface DEVE suportar compressão de dados (gzip/deflate) para reduzir o volume de dados transferidos.

REQ.IT.04 – Os tempos de resposta da interface web DEVEM respeitar 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 DEVE implementar gestão de sessões segura incluindo:

- *Timeout* de inatividade configurável;
- Invalidação segura de sessões;
- Renovação segura de *tokens*.

REQ.IT.06 – A interface DEVE implementar validação de dados tanto no cliente como no servidor.

REQ.IT.07 – A interface DEVE implementar gestão adequada de erros com mensagens apropriadas para o utilizador.

8.2 Identidade Visual

8.2.1 Conformidade com Manual de Identidade

REQ.IV.01 – A solução DEVE implementar 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 DEVE utilizar 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.

8.2.2 Personalização e Consistência

REQ.IV.04 – A solução DEVE permitir a configuração de elementos visuais secundários mantendo a conformidade com as diretrizes principais.

REQ.IV.05 – A solução DEVE manter consistência visual em todos os seus componentes, incluindo formulários, tabelas, botões e elementos interativos.

REQ.IV.06 – A solução DEVE implementar transições e animações de forma consistente em toda a interface.

8.2.3 Domínio e Apresentação

REQ.IV.07 – A solução DEVE utilizar exclusivamente o domínio web definido pela CML para todos os acessos públicos.

REQ.IV.08 – A solução DEVE apresentar elementos de marca (*branding*) conforme definido pela CML em:

- Favicon;
- Imagens de partilha em redes sociais;
- Emails e notificações;
- Documentos gerados.

8.2.4 Responsividade/Adaptabilidade

REQ.IV.09 – A solução DEVE manter a integridade da identidade visual em todas as resoluções de ecrã e dispositivos.

REQ.IV.10 – A solução DEVE adaptar elementos visuais mantendo a hierarquia e proporções definidas no manual de identidade.

REQ.IV.11 – A solução DEVE garantir a legibilidade de todos os elementos visuais em diferentes tamanhos de ecrã.

8.2.5 Iconografia e Imagens

REQ.IV.12 – A solução DEVE utilizar apenas ícones aprovados pela CML ou que sigam as diretrizes de estilo definidas.

REQ.IV.13 – A solução DEVE implementar elementos decorativos e ilustrações conforme o estilo visual aprovado pela CML.

REQ.IV.14 – A solução DEVE manter consistência no tratamento e estilo de imagens em toda a aplicação.

8.2.6 Versões e Atualizações

REQ.IV.15 – A solução DEVE suportar atualizações da identidade visual sem necessidade de reimplementação completa.

REQ.IV.16 – A solução DEVE permitir a gestão de versões de elementos visuais, mantendo compatibilidade com versões anteriores quando necessário.

REQ.IV.17 – A solução DEVE fornecer mecanismos para teste e validação de alterações visuais antes da sua implementação em produção.

8.3 Acessibilidade e Usabilidade

8.3.1 Conformidade com Normas

REQ.IA.01 – A solução DEVE cumprir as diretrizes de acessibilidade WCAG 2.1 nível AA como mínimo, de acordo com o portal acessibilidade.gov.pt.

REQ.IA.02 – A solução DEVE seguir as normas europeias de acessibilidade EN 301 549.

REQ.IA.03 – A solução DEVE estar em conformidade com o DL n.º 83/2018, referente à acessibilidade dos websites e das aplicações móveis.

8.3.2 Navegação e Orientação

REQ.IA.04 – A solução DEVE fornecer múltiplos meios de localização dentro do conteúdo:

- Navegação estruturada;

- Função de pesquisa;
- Mapa do site;
- Navegação baseada em *breadcrumbs*.

REQ.IA.05 – A solução DEVE manter uma ordem de navegação lógica e consistente em todas as páginas.

REQ.IA.06 – A solução DEVE fornecer indicações claras sobre a localização atual do utilizador na interface.

8.3.3 Formulários e Interação

REQ.IA.07 – A solução DEVE fornecer etiquetas (*labels*) claras e instruções para todos os elementos de formulário.

REQ.IA.08 – A solução DEVE implementar validação de formulários com mensagens de erro claras e acessíveis.

REQ.IA.09 – A solução DEVE permitir correção de erros de entrada com sugestões claras de resolução.

8.3.4 Conteúdo Multimédia

REQ.IA.10 – A solução DEVE fornecer alternativas textuais para todo o conteúdo não textual:

- Descrições de imagens
- Transcrições para áudio
- Legendas para vídeo

REQ.IA.11 – A solução DEVE permitir controlo de reprodução para conteúdo multimédia temporal.

REQ.IA.12 – A solução DEVE evitar conteúdo com flash ou animações que possam causar convulsões.

8.3.5 Desempenho e Resposta

REQ.IA.13 – A solução DEVE fornecer feedback imediato para todas as ações do utilizador.

REQ.IA.14 – A solução DEVE implementar indicadores de progresso para operações longas.

REQ.IA.15 – A solução DEVE manter tempos de resposta consistentes e previsíveis em toda a interface.

8.4 Internacionalização e Localização

8.4.1 Suporte Linguístico

REQ.IL.01 – A solução DEVE ter como idioma principal o português de Portugal.

REQ.IL.02 – A solução DEVE suportar o idioma inglês como idioma secundário.

REQ.IL.03 – A solução DEVE permitir a alteração dinâmica do idioma sem necessidade de recarregamento da página.

REQ.IL.04 – A solução DEVE manter o idioma selecionado entre sessões através de persistência de preferências.

REQ.IL.05 – A solução DEVE selecionar a língua a apresentar através das preferências indicadas pelo navegador do utilizador, usando o português por omissão.

8.4.2 Interface e Documentação

REQ.IL.06 – A solução DEVE adaptar automaticamente o layout para acomodar diferentes comprimentos de texto entre idiomas.

REQ.IL.07 – A solução DEVE fornecer toda a documentação de utilizador em português de Portugal.

REQ.IL.08 – A solução DEVE apresentar todas as mensagens de erro e avisos no idioma selecionado pelo utilizador, dentro dos disponíveis.

8.5 Integração com Sistemas CML

8.5.1 Autenticação e Autorização

REQ.IN.01 – A solução DEVE utilizar a Chave Móvel Digital através da plataforma autenticacao.gov.pt para autenticação de utilizadores externos (munícipes).

REQ.IN.02 – A solução DEVE utilizar o Microsoft Entra ID para autenticação de utilizadores internos da CML.

REQ.IN.03 – A solução DEVE implementar um mecanismo de descoberta automática do tipo de utilizador para redireccionamento para o sistema de autenticação apropriado.

REQ.IN.04 – A solução DEVE manter *tokens* de autorização separados para cada tipo de utilizador, respeitando os ciclos de vida específicos de cada sistema de autenticação.

8.5.2 Gestão de Sessões

REQ.IN.05 – A solução DEVE implementar 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 DEVE sincronizar o estado da sessão com o serviço de autenticação correspondente.

REQ.IN.07 – A solução DEVE implementar terminação de sessão apropriada para cada tipo de autenticação.

8.5.3 Perfis e Permissões

REQ.IN.08 – A solução DEVE obter os perfis de acesso dos utilizadores internos diretamente do Microsoft Entra ID.

REQ.IN.09 – A solução DEVE manter uma estrutura de permissões própria apenas para utilizadores externos.

REQ.IN.10 – A solução DEVE validar e renovar automaticamente as credenciais conforme as políticas de cada sistema de autenticação.

8.5.4 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.11 – Em caso de pedido de suporte por parte dos munícipes a solução DEVE gerar um novo email e enviá-lo para o helpdesk@cm-lisboa.pt. O email deverá conter toda a informação necessária para a identificação da origem do pedido de suporte.

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.

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.

9 Conformidade e Certificações

9.1 Conformidade e Certificações

9.1.1 Certificações Gerais de Segurança da Informação

REQ.CS.01 – A solução PODE possuir certificação ISO/IEC 27001:2022 ou superior, válida e emitida por entidade acreditada.

REQ.CS.02 – A solução PODE manter um Sistema de Gestão de Segurança da Informação (SGSI) alinhado com a ISO/IEC 27001.

REQ.CS.03 – O fornecedor PODE disponibilizar à CML a declaração de aplicabilidade (*Statement of Applicability*) da certificação ISO/IEC 27001.

REQ.CS.04 – A solução PODE possuir certificação SOC 2 Type II ou equivalente europeu, cobrindo os critérios de segurança, disponibilidade e confidencialidade.

9.1.2 Certificações Específicas para Cloud

REQ.CS.05 – A infraestrutura *cloud* que suporta o sistema, DEVE possuir certificação ISO/IEC 27017 para segurança em *cloud computing*.

REQ.CS.06 – A infraestrutura *cloud* que suporta o sistema DEVE possuir certificação ISO/IEC 27018 para proteção de dados pessoais em *cloud*.

REQ.CS.07 – A infraestrutura *cloud* que suporta o sistema DEVE apresentar certificação CSA STAR (Security, Trust, Assurance, and Risk) nível 2 ou superior.

9.1.3 Conformidade com Normas de Segurança

REQ.CS.08 – A solução DEVE estar em conformidade com as recomendações de segurança do Quadro Nacional de Referência para a Cibersegurança.

REQ.CS.09 – O fornecedor DEVE demonstrar conformidade com restantes recomendações de segurança do Centro Nacional de Cibersegurança (CNCS).

9.1.4 Validação e Manutenção de Certificações

REQ.CS.10 – O fornecedor DEVE realizar avaliações independentes de segurança (*pen testing*) por entidade certificada.

REQ.CS.11 – O fornecedor DEVE manter um processo documentado de gestão contínua das certificações, incluindo renovações e atualizações.

REQ.CS.12 – O fornecedor DEVE notificar a CML com antecedência mínima de 90 dias sobre quaisquer alterações no estado das certificações.

9.1.5 Requisitos de Documentação

REQ.CS.13 – O fornecedor DEVE disponibilizar toda a documentação comprovativa das certificações em português europeu ou inglês.

REQ.CS.14 – O fornecedor DEVE manter um repositório atualizado com todos os relatórios de auditoria e certificação.

REQ.CS.15 – O fornecedor DEVE fornecer relatórios periódicos de conformidade com as certificações (*compliance reports*).

9.1.6 Gestão de Incidentes e Continuidade

REQ.CS.16 – O fornecedor DEVE seguir as indicações do ISO/IEC 27035 para gestão de incidentes de segurança da informação.

REQ.CS.17 – A fornecedor PODE estar em conformidade com a ISO/IEC 22301 para gestão de continuidade de negócio.

REQ.CS.18 – O fornecedor DEVE seguir as diretivas da ISO/IEC 27031 para continuidade de negócio em TIC.

10 Processo de Validação

10.1 Ambientes de Validação

10.1.1 Disponibilização de Ambientes

REQ.AV.01 – O fornecedor DEVE disponibilizar um ambiente de testes dedicado que replique todas as funcionalidades do ambiente de produção.

REQ.AV.02 – O fornecedor DEVE manter o ambiente de testes sincronizado com a versão de produção com diferença máxima de 5 dias úteis.

REQ.AV.03 – O fornecedor DEVE fornecer um ambiente de validação com recursos dedicados e isolados de outros clientes.

10.1.2 Gestão de Dados de Teste

REQ.AV.04 – O ambiente de testes DEVE utilizar conjuntos de dados sintéticos que representem adequadamente os dados estratégicos.

REQ.AV.05 – O fornecedor DEVE implementar um processo de refrescamento (*refresh*) periódico dos dados de teste que não utilize dados reais de produção.

REQ.AV.06 – O fornecedor DEVE fornecer ferramentas para geração e manipulação de dados de teste que repliquem todos os cenários de integração.

10.1.3 Configuração de Ambientes

REQ.AV.07 – O fornecedor DEVE disponibilizar documentação detalhada da configuração necessária para estabelecer a ligação ao com o ambiente de testes.

REQ.AV.08 – O ambiente de testes DEVE suportar a simulação de todos os cenários de erro e exceção previstos nos requisitos de integração.

REQ.AV.09 – O fornecedor DEVE permitir a reposição (*reset*) do ambiente de testes para um estado base conhecido em menos de 60 minutos.

10.1.4 Controlo de Acesso

REQ.AV.10 – O fornecedor DEVE implementar mecanismos de autenticação e autorização específicos para o ambiente de testes.

REQ.AV.11 – O fornecedor DEVE manter um registo detalhado (*audit log*) de todas as operações realizadas no ambiente de testes.

REQ.AV.12 – O fornecedor DEVE permitir a gestão independente de utilizadores e permissões no ambiente de testes.

10.2 Testes Funcionais

10.2.1 Validação de Fluxos de Dados

REQ.TF.01 – O fornecedor DEVE disponibilizar casos de teste documentados para cada fluxo de dados estratégicos identificado.

REQ.TF.02 – O fornecedor DEVE implementar validações automáticas para verificar a integridade dos dados durante os testes aos processos de sincronização.

REQ.TF.03 – O fornecedor DEVE fornecer mecanismos de verificação da ordem cronológica das atualizações de dados estratégicos.

10.2.2 Testes de Integração

REQ.TF.04 – O fornecedor DEVE disponibilizar uma suite completa de testes de integração que cubra todos os *endpoints* da API.

REQ.TF.05 – O fornecedor DEVE fornecer testes automatizados para validar o comportamento dos mecanismos de sincronização em modo offline.

REQ.TF.06 – O fornecedor DEVE implementar testes específicos para validar a gestão de conflitos na sincronização bidirecional.

10.2.3 Validação de Transformações

REQ.TF.07 – O fornecedor DEVE implementar testes automatizados para validar todas as transformações de dados entre o sistema SaaS e o modelo simplificado.

REQ.TF.08 – O fornecedor DEVE fornecer casos de teste específicos para validar a preservação da integridade referencial após transformações.

REQ.TF.09 – O fornecedor DEVE disponibilizar ferramentas para comparação automatizada de dados antes e após transformações.

10.2.4 Gestão de Estados

REQ.TF.10 – O fornecedor DEVE fornecer testes que validem a preservação do estado da aplicação durante falhas de conectividade.

REQ.TF.11 – O fornecedor DEVE implementar validações do processo de recuperação de estado após interrupções de sincronização.

REQ.TF.12 – O fornecedor DEVE disponibilizar testes para verificar a consistência dos dados em diferentes estados do sistema.

REQ.TF.13 – O fornecedor DEVE disponibilizar testes para verificar o funcionamento dos procedimentos de penalizações por indisponibilidade.

10.2.5 Validação de Regras de Negócio

REQ.TF.14 – O fornecedor DEVE implementar testes específicos para validar a aplicação das regras de classificação de dados estratégicos.

REQ.TF.15 – O fornecedor DEVE fornecer casos de teste que validem as restrições de acesso aos dados estratégicos.

REQ.TF.16 – O fornecedor DEVE disponibilizar testes que verifiquem a correta aplicação das políticas de retenção de dados.

10.3 Validação de Segurança

10.3.1 Análise de Vulnerabilidades

REQ.VS.01 – O fornecedor DEVE realizar análises automáticas de vulnerabilidades em todo o código relacionado com a gestão de dados estratégicos.

REQ.VS.02 – O fornecedor DEVE executar verificações de segurança do código (*code scanning*) em todas as atualizações antes da implementação.

REQ.VS.03 – O fornecedor DEVE realizar análises regulares de vulnerabilidades nas bibliotecas e dependências utilizadas na integração.

10.3.2 Validação de Encriptação

REQ.VS.04 – O fornecedor DEVE validar a correta implementação dos mecanismos de encriptação em trânsito (*in transit*) através de testes automatizados.

REQ.VS.05 – O fornecedor DEVE verificar a eficácia da encriptação em repouso (*at rest*) dos dados estratégicos através de testes de acesso direto ao armazenamento.

REQ.VS.06 – O fornecedor DEVE testar os procedimentos de rotação de chaves de encriptação sem impacto na disponibilidade dos dados.

10.3.3 Validação de Controlo de Acessos

REQ.VS.07 – O fornecedor DEVE implementar testes automatizados para validar a correta aplicação das políticas de controlo de acesso.

REQ.VS.08 – O fornecedor DEVE garantir e verificar a segregação efetiva de dados entre diferentes contextos de segurança.

REQ.VS.09 – O fornecedor DEVE testar a revogação imediata de acessos em todos os componentes da solução.

10.3.4 Auditoria de Segurança

REQ.VS.10 – O fornecedor DEVE validar a completude e precisão dos registos de auditoria (*audit logs*) através de testes de rastreabilidade.

REQ.VS.11 – O fornecedor DEVE verificar a integridade dos registos de auditoria através de testes de manipulação.

REQ.VS.12 – O fornecedor DEVE testar os mecanismos de alerta de segurança através de simulações de incidentes.

REQ.VS.13 – A solução DEVE testar a preservação dos registos de auditoria por um período configurável.

REQ.VS.14 – A solução DEVE testar a exportação dos registos de auditoria em formato standard para análise externa.

10.3.5 Testes de Resiliência

REQ.VS.15 – O fornecedor DEVE realizar testes de continuidade de segurança durante falhas de componentes críticos.

REQ.VS.16 – O fornecedor DEVE validar o comportamento seguro do sistema durante a recuperação de falhas.

REQ.VS.17 – O fornecedor DEVE testar a preservação dos controlos de segurança durante operações em modo degradado.

10.4 Certificação de Integrações

10.4.1 Validação de API

REQ.CI.01 – O fornecedor DEVE validar a conformidade de todas as API expostas com a especificação OpenAPI 3.0 através de testes automatizados.

REQ.CI.02 – O fornecedor DEVE testar a implementação correta de todos os mecanismos de controlo de versão (*versioning*) das API.

REQ.CI.03 – O fornecedor DEVE verificar a correta implementação dos limites de pedidos (*rate limiting*) e quotas em todas as API.

10.4.2 Verificação de Protocolos

REQ.CI.04 – O fornecedor DEVE validar a conformidade com o protocolo OAuth 2.0 através de um conjunto completo de testes.

REQ.CI.05 – O fornecedor DEVE certificar a implementação correta do protocolo AMQP 1.0 para comunicações assíncronas.

REQ.CI.06 – O fornecedor DEVE verificar a conformidade com os protocolos de comunicação segura (TLS 1.3) através de testes específicos.

10.4.3 Validação de Sincronização

REQ.CI.07 – O fornecedor DEVE certificar o funcionamento correto dos mecanismos de sincronização incremental.

REQ.CI.08 – O fornecedor DEVE validar a precisão dos registos temporais (*timestamps*) utilizados na sincronização.

REQ.CI.09 – O fornecedor DEVE garantir a correta implementação dos mecanismos de deteção e resolução de conflitos.

10.4.4 Verificação de Formatos

REQ.CI.10 – O fornecedor DEVE validar a conformidade dos formatos de dados com os esquemas (*schemas*) JSON definidos.

REQ.CI.11 – O fornecedor DEVE certificar a correta codificação de caracteres (UTF-8) em todas as comunicações.

REQ.CI.12 – O fornecedor DEVE verificar a conformidade com os formatos de data e hora definidos na norma ISO 8601.

10.4.5 Certificação de Resiliência

REQ.CI.13 – O fornecedor DEVE validar o comportamento das integrações durante falhas parciais do sistema.

REQ.CI.14 – O fornecedor DEVE verificar a recuperação automática das integrações após interrupções de conectividade.

REQ.CI.15 – O fornecedor DEVE certificar o correto funcionamento dos mecanismos de tentativas (*retry*) com espera exponencial.