REGIÃO AUTÓNOMA DOS AÇORES
VICE PRESIDÊNCIA DO GOVERNO
DIREÇÃO REGIONAL DAS COMUNICAÇÕES E DA TRANSIÇÃO DIGITAL

Exmos.(as) Srs.(as)
Chefes do Gabinete dos Membros do Governo
Secretária-Geral da Presidência do Governo
Diretores Regionais
Inspetores Regionais

Vossa referência	Sua comunicação de	Nossa referência	Data
		Circular n.º 1/DRCTD/2024	10-07-2024

ASSUNTO: Desenvolvimento de Software, de Aplicações e de Sistemas de Informação da Administração Pública Regional.

Exmo.(a) Senhor(a),

Para os devidos efeitos, junto se remete a presente Circular n.º 1/DRCTD/2024, sobre o mencionado em assunto.

Com os melhores cumprimentos,

O DIRETOR REGIONAL

Assinado por: **PEDRO MIGUEL VASCONCELOS RAPOSO DE MEDEIROS BATISTA**
Num. de Identificação: 10145471
Data: 2024.07.12 15:06:31+00'00'
Certificado por: **Governo Regional dos Açores**
Atributos certificados: **Diretor Regional das Comunicações e da Transição Digital**
CHAVE MÓVEL

Circular n.º 1/DRCTD/2024

Considerando o disposto na alínea g) do n.º 1 do artigo 36.º do Decreto Regulamentar Regional n.º 4/2023/A, de 14 de fevereiro, relativo à emissão de parecer por parte da Direção Regional das Comunicações e da Transição Digital, sobre propostas de aquisição de serviços, sistemas, aplicações e equipamentos, no âmbito dos sistemas de informação e da segurança, das redes informáticas e de comunicações e da transição digital, para a administração pública regional;

Considerando a necessidade de se promover a normalização das tecnologias afetas ao desenvolvimento e aquisição de sistemas de informação e de aplicações informáticas pelos diversos departamentos e serviços da administração pública regional com o objetivo de acautelar a eficiência dos licenciamentos, a integração das soluções, a sua interoperabilidade, o reaproveitamento das soluções e do seu código, a adoção de tecnologias aceleradoras na entrega de resultados à atividade, a urgente substituição de soluções legadas, obsoletas e sem possibilidade de manutenção, com impacto negativo no que concerne à comunicação e à cibersegurança da administração publica regional;

Considerando a necessidade de acautelar a integração dos diversos departamentos do Governo Regional no novo ecossistema LINKA - ARQUITETURA DE SISTEMAS DE INFORMAÇÃO DA ADMINISTRAÇÃO PÚBLICA REGIONAL (https://linka.azores.gov.pt/) de utilização transversal;

Considerando a aposta estratégica de adoção de uma plataforma de *LowCode*, licenciada para a utilização transversal de toda a administração pública regional direta;

Considerando o esforço de formação e capacitação efetuado, em articulação com a DROPEP através do CEFAPA, de 75 técnicos e especialistas de informática, da administração pública regional, com atividade no desenvolvimento de software, promovendo a sua valorização, atualização tecnológica, capacidades e requalificação;

Considerando que a Vice-Presidência do Governo dos Açores, através da DRCTD, disponibiliza um sistema de incentivos à modernização administrativa, SIMA (https://portal.azores.gov.pt/web/drcomunicacoes/sima-sistema-de-incentivos-à-modernização-administrativa), com o objetivo de apoiar iniciativas que promovam a concentração das diversas presenças WEB de um determinado departamento num único e novo portal da atividade, que

promovam a criação de serviços eletrónicos sustentáveis, baseados na interoperabilidade de sistemas e aplicações no ecossistema LINKA e na utilização dos dados para um aumento de transparência e eficiência governativa, incluindo a promoção de uma cultura participativa dos cidadãos e empresas;

Serve esta Circular e Anexo, que dela faz parte integrante, para estabelecer os requisitos que devem ser observados nas atividades do desenvolvimento aplicacional e de sistemas de informação e na aquisição deste tipo de soluções por parte dos departamentos do Governo Regional.

1. O desenvolvimento de software, aplicacional e de sistemas de informação deve ser efetuado preferencialmente por recurso à tecnologia *LowCode Outsystems*;
2. Na impossibilidade de se observar o disposto no ponto anterior, deve optar-se pelo desenvolvimento aplicacional e de sistemas de informação em tecnologia *open source* de utilização massiva, aplicando-se a mesma regra na utilização de sistemas de gestão de bases de dados e de sistemas operativos;
3. As soluções adquiridas, devem considerar um contrato de manutenção que garanta a sua atualização e necessidades corretivas;
4. As soluções adquiridas e aquelas que se encontram em exploração, devem ser alojadas na Infraestrutura AzoresCloud, a sua arquitetura e conceção deve cumprir com as regras de exploração daquela infraestrutura e com as disposições em vigor em matéria de cibersegurança;
5. As soluções adquiridas e aquelas que se encontram em exploração devem observar os requisitos que constam do Anexo a esta circular e que dela faz parte integrante;
6. A não observação das disposições anteriores só poderá ocorrer mediante autorização excecional da DRCTD para o efeito, a qual deverá ser requerida de forma fundamentada onde se demonstre cabalmente a impossibilidade da não observação destas disposições.

O cumprimento dos requisitos ora estabelecidos não dispensa o pedido de parecer prévio à Direção Regional das Comunicações e da Transição Digital a que alude a alínea g) do n.º 1 do artigo 36.º do Decreto Regulamentar Regional n.º 4/2023/A, de 14 de fevereiro.

ANEXO

Os requisitos adiante apresentados encontram-se identificados como obrigatórios ou facultativos (sugestões) e não impedem a fixação de outros requisitos identificados pelas entidades como necessários ao desenvolvimento da solução pretendida e concretização dos objetivos do projeto, sugere-se que estes requisitos sejam incluídos nos cadernos de encargos dos procedimentos de aquisição deste tipo de soluções.

Importa realçar que o Governo Regional dos Açores (GRA) prossegue uma estratégia de desenvolvimento dos seus sistemas de informação através uma plataforma de tecnologia Low Code da Outsystems, licenciada e em operação na infraestrutura on-premises do GRA.

A referida plataforma de Low Code disponibiliza ambientes de desenvolvimento, testes e produção, garantindo ainda a disponibilização de uma biblioteca de componentes desenvolvidos de acordo com as normas vigentes e que podem ser reutilizadas pelas entidades do GRA, como por exemplo Design Systems e autenticação GRA-ID.

A infraestrutura da plataforma de Low Code é gerida e mantida pela DRCTD e a sua utilização garante, desde logo, o cumprimento de alguns dos requisitos seguidamente enunciados.

REQUISITOS GERAIS:

− **[OBRIGATÓRIO]** Proteção de dados pessoais: A Solução deverá garantir o cumprimento do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, na sua redação atual, sendo concebida e implementada de modo a respeitar os seus princípios e direitos do utilizador.

− [SUGESTÃO] Exigir a apresentação de uma proposta de avaliação de impacto sobre a proteção de dados (AIPD), sempre que a mesma seja exigível nos termos do artigo 35.º do RGPD, designadamente quando forem tratados em larga escala os dados pessoais previstos no artigo 9.º ou no artigo 10.º do RGPD.

− **[OBRIGATÓRIO]** Usabilidade e acessibilidade: A solução deverá adotar as regras de acessibilidade nos sítios e portais da Administração Pública de acordo a legislação vigente e constantes em http://www.acessibilidade.gov.pt, em consonância com a última atualização da norma europeia EN 301 549 na versão 2.1.2 (2018-08). Desta forma os utilizadores devem usufruir

de procedimentos simplificados e padronizados que lhes permitam beneficiar da simplicidade da interface de utilizador.

− [OBRIGATÓRIO] Deverá cumprir as regras para atribuição do nível 2 - Selo Prata ou superior, Selo de Usabilidade e Acessibilidade desenvolvido pela Agência para a Modernização Administrativa (AMA) e pelo Instituto Nacional para a Reabilitação (INR), de acordo com as regras definidas em https://selo.usabilidade.gov.pt/prata.html.

− [OBRIGATÓRIO] Conformidade com Norma RNID: Sempre que aplicável, a solução tem de estar em conformidade com o RNID (regulamento nacional de interoperabilidade digital, Resolução do Conselho de Ministros n.º 2/2018, de 05 de janeiro, na redação em vigor).

− [OBRIGATÓRIO] A solução deve estar concebida e implementada de modo a respeitar os seguintes princípios:

- Adequabilidade (completude e correção): A solução assegura todos os requisitos numa lógica de resultados a alcançar, sem falhas;
- Privacidade e segurança: A solução deverá suportar e garantir a operacionalização de procedimentos de segurança e privacidade condizentes com a exigência do tipo de informação e serviços assegurados. Em particular, deve garantir a segurança das componentes aplicacionais e dos dados, recorrendo às melhores práticas, nomeadamente por utilização de controlo de acessos, encriptação, assinatura digital, etc.;
- Proteção: A solução deverá garantir a recuperação, legibilidade e integridade da informação nela armazenada e processada;
- Estruturação por camadas / perímetros de segurança: A arquitetura deve ser estruturada em camadas, com cada camada protegida por um perímetro de segurança própria, de acordo com as melhores práticas e com as diretivas emitidas pela DRCTD no que diz respeito ao alojamento e acesso à rede;
- Elevada disponibilidade: No que respeita ao ambiente de produção, deverão ser cumpridos elevados níveis de fiabilidade e disponibilidade, através da adoção de arquiteturas redundantes, com capacidades de recuperação de falhas. Neste contexto, devem ser implementados mecanismos de monitorização, quando aplicável.

- Mínima dependência de fornecedores e de tecnologias específicas: A dependência de fornecedores com tecnologias/frameworks específicas e não genericamente utilizadas por várias entidades deve ser minimizada.

− **[OBRIGATÓRIO]** Deve ser sempre exigido ao prestador de serviços documentação sobre o código-fonte, arquitetura da aplicação, segurança e processos de integração, bem como manuais na perspetiva do administrador e utilizador.

INFRAESTRUTURA:

− **[OBRIGATÓRIO]** A solução será alojada na nuvem privada do Governo Regional dos Açores - Azores Cloud. A Plataforma terá de estar em conformidade com as diretrizes de alojamento e segurança da Azores Cloud.

− [**OBRIGATÓRIO**, **exceto se desenvolvido em outsystems**] A solução proposta deve assegurar backups regulares e mecanismos de restauração como parte dos seus serviços, e a capacidade de fornecer backups seguros e descarregáveis tanto da base de dados como dos dados do sistema de ficheiros no prazo de 24 horas após qualquer pedido.

− [**OBRIGATÓRIO, para contratos que incluam suporte]** Durante a execução do contrato, o cocontratante deve efetuar uma monitorização operacional contínua da segurança do sistema, incluindo, mas não se limitando a, áreas como a gestão de vulnerabilidade, efetuando avaliações regulares por referência a uma norma de boas práticas de segurança reconhecida, como a ISO (ou equivalente).

− **[OBRIGATÓRIO, exceto se desenvolvido em outsystems]** Sempre que necessário deverá ser solicitada a criação de um servidor virtual para alojamento do site/aplicação ou em alternativa utilizar um já existente, da mesma entidade, que suporte o alojamento do site/aplicação (https://helpdesk.azores.gov.pt/ - Pedido de novo servidor).

− **[OBRIGATÓRIO, exceto se desenvolvido em outsystems]** A solução deverá estar preparada para poder funcionar com um ambiente de disaster recovery, nomeadamente no que diz respeito às questões de sincronismo de dados, transição do ambiente de produção em caso de desastre e posterior recuperação.

GESTÃO DE TRÁFEGO:

− **[OBRIGATÓRIO, exceto se desenvolvido em outsystems]** O site/aplicação deverá suportar Load Balancing e SSL Offloading do tipo Full Proxy, gerido por equipamento de gestão de tráfego externo. O endereço IP do cliente será transmitido ao servidor no cabeçalho X-Forwarded-For e o protocolo (HTTP ou HTTPS) de ligação utilizado pelo cliente no cabeçalho X-Forwarded-Proto.

− **[OBRIGATÓRIO, exceto se desenvolvido em outsystems]** Caso exista transmissão de dados pessoais entre cliente e o servidor, o tráfego entre o servidor e o equipamento de gestão de tráfego deverá ser encriptado com um certificado self-signed (em alternativa podem solicitar a assinatura de um CSR à DRCTD) utilizando no mínimo o protocolo e encriptação TLS 1.2.

− **[OBRIGATÓRIO exceto se desenvolvido em outsystems]** Desempenho e distribuição de carga: A solução deve estar adaptada a funcionar adequadamente com mecanismos de distribuição de carga, nomeadamente com os serviços de balanceamento de carga fornecidos pelo datacenter do GRA – Azores Cloud. Caso o nível de criticidade assim determine, deverá ser assente num sistema distribuído: espera-se que seja projetada para ser executada em múltiplas máquinas em simultâneo, assegurando uma distribuição de carga por intermédio de servidores aplicacionais múltiplos;

− [**OBRIGATÓRIO exceto se desenvolvido em outsystems]** Deverá existir, na raiz do site/aplicação, sem quaisquer mecanismos de redireccionamento, uma página com o nome healthcheck.(php|asp|aspx|outra extensão|sem extensão) que execute todos os testes necessários para aferir o estado de funcionamento do site (ex. ligação à base de dados) e retorne o resultado em texto “STATUS OK” caso o resultado de todos os testes seja positivo e “STATUS FAIL” caso o resultado de um dos testes seja negativo. Esta página é utilizada pelo balanceador de forma a só disponibilizar o site/aplicação quando o resultado é “STATUS OK”.

AUTENTICAÇÃO:

− **[OBRIGATÓRIO]** Utilizadores internos Administração Pública Regional: Autenticação efetuada através de Microsoft Entra ID, o sistema de autenticação atualmente utilizado pela Administração Pública Regional. A autenticação Microsoft Entra ID é efetuada através Security Assertion Markup

Language 2.0 (SAML 2.0) e/ou OpenID Connect (OIDC) estando disponível um Identity Provider (IDP) para o efeito.

− [OBRIGATÓRIO] Toda a gestão de grupos de utilizadores do site/aplicação deve ser feita na aplicação, não sendo possível utilizar a AD para o efeito. A AD apenas fornece a autenticação e atributos básicos (Nome, email, sAMAccountName e etc.)

− [OBRIGATÓRIO para soluções que prevejam disponibilização ao cidadão/empresa] Utilizadores externos (cidadãos/empresas):

- Autenticação.Gov;
- Azor.ID (IDP SAML2 / OIDC) que se encontrará em produção em setembro de 2024 e servirá como plataforma de autenticação para todos os cidadãos e empresas dos Açores perante a Administração Pública Regional;
- Formulário de registo com preenchimento dos seguintes campos: NIF, Denominação, Email, Confirmação de Email, Definição de palavra-passe, Confirmação de palavra-passe, Aceitação dos termos de utilização. A autenticação deverá ser efetuada através Security Identity Provider (IDP) para o efeito (utilização permitida apenas e até à disponibilização da plataforma Azor.ID).

INTERFACES:

− [OBRIGATÓRIO] A solução deve dispor de capacidade de integração com sistemas informáticos terceiros e de mecanismos que facilitem a expansão dessa capacidade, estando em conformidade com as normas técnicas utilizadas para integração. A comunicação entre a aplicação e os serviços externos será realizada mediante a implementação de uma plataforma de interface de programação (API), reduzindo a quantidade de pontos de ligação e otimizando a informação obtida.

− **[OBRIGATÓRIO]** A integração entre a solução e os sistemas de informação deverá ser realizada através de web services, a integrar numa base SOA, exceto quando tecnicamente justificável por motivos de criação de uma interface mais rica ou de desempenho superior;

− **[OBRIGATÓRIO]** Caso sejam disponibilizados web services, os mesmos devem ser fornecidos pelo próprio site/aplicação e não por aplicações extra em portos diferentes ou proxies através do

servidor web (ex. aplicação/site em apache/php/mysql e webservice em java no porto 8080), exceto quando tecnicamente justificável a sua não adoção.

− **[OBRIGATÓRIO Caso a Solução inclua disponibilização de serviços para dentro do GRA ou para fora (cidadão/empresas) ou necessidade de atualização orgânica]** Integração com o Catálogo Eletrónico de Entidades e Serviços da Administração Pública Regional (CES) - Sistema que irá ter o catálogo central das entidades da Administração Pública Regional e dos serviços por estas prestados, bem como os pontos de atendimento. Qualquer alteração que ocorra na orgânica da APR terá de ser registada neste sistema e terá uma interface que todos podem consumir. Esta plataforma disponibiliza um canal de comunicação de eventos utilizando a tecnologia Apache Kafka e terá uma interface para consumo por serviços terceiros.

− **[OBRIGATÓRIO caso a Solução inclua disponibilização de serviços para dentro do GRA ou para fora (cidadão/empresas) ou portais de negócio – SUJEITO A AVALIAÇÃO DRCTD]** Integração com o Módulo de fluxos: Desenvolvido em Outsystems, o módulo de fluxos integra os sistemas, orquestrando toda a informação que deve ir de um sistema para o outro.

− [OBRIGATÓRIO] Sempre que seja necessário integrar com outras plataformas do GRA a comunicação deverá ser feita através da plataforma de interoperabilidade e-HUB: O e-HUB é a plataforma do Governo Regional dos Açores suportada em web-services criada com o objetivo de abstrair os serviços/aplicações/sistemas uns dos outros permitindo assim a sua substituição sem afetar os restantes.

SEGURANÇA:

− [OBRIGATÓRIO exceto se desenvolvido em outsystems] A solução deverá dispor de controlos, meios e mecanismos que garantam o cumprimento de princípios base de segurança, designadamente:

- a informação só poderá ser acedida ou tratada por utilizadores com permissão para tal e de acordo com as estritas necessidades específicas para a realização das respetivas funções;
- a informação tratada e gerada por qualquer dos utilizadores não é apagada, alterada ou corrompida sem autorização desde a sua criação até à respetiva eliminação, mantendo-a completa, sem supressões ou acréscimos, com particular atenção durante a sua circulação;

- as comunicações devem ser efetuadas sobre protocolos seguros e sem vulnerabilidades de forma a garantir a confidencialidade e integridade da comunicação.
- a utilização da solução em browser deverá ser feita por ligação segura (HTTPS).

− [OBRIGATÓRIO] No que diz respeito à segurança no alojamento de aplicações/sistemas nas redes do GRA, quer sejam desenvolvidos de raiz ou parametrizados de acordo com um determinado projeto (ex. parametrização de wordpress), devem ser aplicados os seguintes princípios:

- Sistemas/aplicações acedidos a partir da Internet não podem aceder a serviços/sistemas/aplicações acedidos apenas internamente, por exemplo Active Directory, com a exceção de acessos a web services desde que devidamente autorizados para DRCTD;
- Sistemas/aplicações acedidos apenas a partir das redes do GRA podem aceder a serviços/sistemas/aplicações acedidos apenas internamente, por exemplo Active Directory, bem como a serviços/sistemas/aplicações acedidos a partir da Internet;
- Sobrepõem-se a todos os princípios anteriores o princípio geral de que um sistema/aplicação acedido a partir da Internet, em caso de comprometimento, não deverá poder aceder aos restantes serviços/sistemas/aplicações ficando isolado.

− [OBRIGATÓRIO] Devem ser submetidos os esquemas de ligações de firewall sempre que for solicitada a criação de VMs e quando for necessário fazer alterações de ligações. Deve sempre ser respeitada a nomenclatura definida.

− [OBRIGATÓRIO] Os Fornecedores de Serviço Externos (FSE) têm de fornecer a informação necessária (NIF da empresa, Nome da Empresa, Nome do funcionário, email do funcionário) à criação das contas de acesso VPN bem como respeitar e aceitar a regras definidas pelo GRA, sob pena de não lhes ser permitido o acesso à rede.

− [SUGESTÃO] O site/aplicação deve ser testado no site de testes https://internet.nl/, devendo obter resultado positivo na maioria dos "HTTP security headers" da secção "Security options". Ainda que não seja possível obter resultado positivo em alguns dos cabeçalhos, os mesmos devem ser fornecidos. O site/aplicação deve ser testado no site de testes https://internet.nl/, devendo obter resultado positivo em todos os "HTTP security headers" da secção "Security options".

DESENVOLVIMENTO:

− [OBRIGATÓRIO] Caso seja utilizado um CMS, ou outra plataforma, como base do site (ex. Drupal, Wordpress e etc.) o desenvolvimento deverá ser feito sob a forma de módulos (plugins, temas e etc.) do CMS por forma a ser possível a atualização do CMS independentemente dos módulos, permitindo assim colmatar possíveis falhas de segurança. Alerta-se para a necessidade da utilização destas plataformas e seus componentes e módulos exigirem atualizações constantes, sob pena de incorrerem em riscos de segurança e, por este motivo, terem de ser desativadas até à reposição do seu normal funcionamento.

− [OBRIGATÓRIO] Modularidade e capacidade de crescimento: A solução deverá ser modular e baseada numa arquitetura orientada a serviços (SOA), que permita a sua evolução de forma simples e com esforço de integração reduzido, seguindo as melhores práticas de mercado, tanto a nível de infraestruturas físicas como estruturação lógica do sistema. Adicionalmente, a solução deverá ser capaz de suportar de forma incremental novas funcionalidades e o acréscimo de volumes de trabalho, através da reconfiguração e reparametrização das componentes fornecidas, eventualmente aumentando o número ou capacidade dos equipamentos instalados. A conceção e evolução da solução deverá ser realizada de modo a minimizar o impacto sobre eventuais extensões ou desenvolvimentos anteriormente realizados. A solução deverá permitir a partilha de carga por vários servidores aplicacionais e de bases de dados, garantindo a manutenção da performance por scale-out.

− [SUGESTÃO] As camadas de software, bases de dados e sistemas operativos que compõem a solução a fornecer devem ser executadas/implementadas em sistemas open-source, nomeadamente Linux, sem recorrer a qualquer tipo de licenciamento adicional.

− [SUGESTÃO] Caso seja necessária a utilização de uma base de dados Microsoft SQL Server, ou outra que requeira licenciamento, deve ser analisada a possibilidade de usar uma versão que não necessite de qualquer licenciamento, por exemplo o SQL Server Express e a sua instalação em sistema operativo open-source Linux sem recorrer a qualquer tipo de licenciamento de SO.

− [SUGESTÃO] Idealmente as aplicações devem ter utilizadores locais à própria aplicação de forma a não serem necessárias credenciais extra para quaisquer operações que são internas à aplicação.