SELEÇÃO PÚBLICA MCTI/FINEP/FNDCT/ME/ENAP

Subvenção Econômica à Inovação – 16/2022

Soluções de IA para o Poder Público – Rodada 1

ANEXO 3 – DIRETRIZES GERAIS DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO, AMBIENTE COMPUTACIONAL, REQUISITOS PARA A TRANSFERÊNCIA DE CONHECIMENTO, E SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

1. DIRETRIZES GERAIS DE TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO

A(s) beneficiária(s) deverá(ão) observar as seguintes diretrizes gerais de TICs para os Desafios Tecnológicos de todas as EPPs:

a) Preferencialmente:

- Adotar, durante a execução do projeto, soluções de tecnologia da informação e comunicação (TIC) suportadas pela EPP;

- Adotar, durante a execução do projeto, soluções não proprietárias, que não necessitem de aquisições e nem tampouco de subscrições por parte da EPP;

- Observar, durante a execução do projeto, a metodologia e diretivas de desenvolvimento de software, metodologia de segurança digital e o modelo de administração de dados da EPP, se for o caso.

b) Obrigatoriamente:

- Observar, durante a execução do projeto, todos os atos normativos vigentes, as políticas de segurança da informação e de privacidade aplicáveis, bem como o uso das boas práticas no desenvolvimento de soluções tecnológicas;

- Durante a execução do projeto, buscar alinhar com a EPP a infraestrutura de TIC a ser utilizada para a implantação da solução;

- Durante a execução do projeto, buscar seguir as diretrizes arquiteturais da EPP.

2. AMBIENTE COMPUTACIONAL

2.1. AMBIENTE COMPUTACIONAL – ENTIDADE PÚBLICA PARTICIPANTE ANS

A(s) beneficiária(s) deverá(ão) considerar, preferencialmente, os seguintes ambientes computacionais para os Desafios Tecnológicos da Agência Nacional de Saúde Suplementar (ANS):

- Sistemas desenvolvidos em linguagem JAVA e PHP;
- Banco de Dados Oracle e MySQL;
- Servidor de Aplicação Apache, JBOSS e IIS;
- Plataformas Web (Clusterizadas e standalone); e
- Plataformas Cliente/Servidor (Clusterizada e standalone).

Para os Desafios Tecnológicos da ANS, a(s) beneficiária(s) deverá(ão), preferencialmente, desenvolver WEBSERVICES sempre que o resultado da solução de IA servir de insumo para os sistemas da ANS. O WEBSERVICES deverão atender aos seguintes padrões:

- desenvolvimento de APIs padrão REST;
- utilização de swagger para documentação;
- autenticação via Oauth2;
- utilizando o framework SpringBoot;
- publicação em containers Docker, capazes de acessar módulos com vistas à obtenção de propriedades públicas/privadas e acesso a objetos (ou padrões) Secrets para obtenção de credenciais; e
- padrão Oauth2 para autenticação e controle de acesso das APIS.

2.2. AMBIENTE COMPUTACIONAL – ENTIDADE PÚBLICA PARTICIPANTE ANVISA

Para subsidiar a(s) beneficiária(s) com informações sobre o ambiente computacional da Agência Nacional de Vigilância Sanitária, segue a lista, não exaustiva, de tecnologias e ferramentas utilizadas na ANVISA, com foco no desenvolvimento de soluções:

- Linguagens de Programação:

- JAVA 7 e 17; PHP 5 e 7; ASP 3.0; Visual Basic 6.0; Python; Delphi; PL/SQL;

- Tecnologias utilizadas em sistemas Single Page Application (SPA):

- AngularJS; Angular 7; PrimeNG; NodeJS

- Tecnologias utilizadas no desenvolvimento de web services (back-end):

- Spring Framework; CXF; Swagger; JPA; JAX-WS; JAX-RS; Groovy

- Tecnologias de Banco de Dados:

  - Oracle; Microsoft SQL Server; PostgreSQL; MongoDB; MySQL

- Tecnologias BI e ETL:

  - Power Center; Power BI

- Tecnologias comuns (demais tecnologias):

  - Gitlab CI/CD; Gitlab package registry e container registry; Nexus; Bucket S3 (Minio); Keycloak; RabbitMQ; EMC Documentum; Html e CSS; Singular; Maven; Redis; SVN; Selenium; Docker; Kubernetes; Rancher; Mantis; Jenkins; Bootstrap; JBoss Wildfly; JQuery; Sonar; Joomla; Wordpress; Sharepoint; Liferay; Plone; Artifactory; WSO2

2.3. AMBIENTE COMPUTACIONAL – ENTIDADE PÚBLICA PARTICIPANTE MAPA

Para subsidiar a(s) beneficiária(s) com informações sobre o ambiente computacional do Ministério da Agricultura, Pecuária e Abastecimento (MAPA), segue a lista, não exaustiva, de tecnologias e ferramentas utilizadas no MAPA, com foco no desenvolvimento de soluções:

- Resumo de tecnologias e métodos:

  - The Clean Architecture (Arquitetura Limpa), princípios SOLID, método The Twelve-factor app, TypeScript, React.js, Node.js, Cypress para testes ponta a ponta, Sentry, REST-API, Swagger, cache em memória com REDIS, Microsserviços, broker de mensagens com Apache Kafka, PostgreSQL, Gitlab CI/CD, API Gateway, Docker, Kubernetes, GCP/GKE e Rancher;

- Linguagens para software de IA:

  - Python e Scikit-learn como recomendação, usando Jupyter notebooks, persistindo em banco de dados Postgres.

- Banco de dados:

  - PostgreSQL;

- Ferramentas de desenvolvimento:

- Para os modelos de ML, recomenda-se o uso do Jupyter. Para os sistemas de informação, recomenda-se o VS Code.

- Padrão de Interface:

- Basicamente DSGov e eMAG.

- Ferramentas de BI:

- QlikSense e/ou DataStudio;

- Repositório:

- GitLab ou Google Drive, a depender do projeto;

- Ambientes:

- desenvolvimento, homologação e produção.

3. REQUISITOS PARA A TRANSFERÊNCIA DE CONHECIMENTO

A(s) beneficiária(s) deverá(ão) observar os requisitos para a transferência de conhecimento descritos nesta seção em relação aos Desafios Tecnológicos de todas as EPPs.

3.1. A(s) beneficiária(s) será(ão) responsável(is) pela transferência de conhecimento, por meio da criação e execução de um plano de implantação, bem como pela documentação relacionada. O plano de implantação deve listar todos os requisitos de hardware e de software da solução (i.e: sistemas operacionais, servidores de aplicação, linguagens de programação, componentes necessários, etc.);

3.2. A(s) beneficiária(s) deverá(ão) disponibilizar todos os código-fonte, os scripts, os manuais dos usuários, os planos de implantação, os modelos de dados, a documentação detalhada acerca da arquitetura da solução, os requisitos ou quaisquer outras documentações e artefatos necessários e suficientes para o desenvolvimento, a implantação e a sustentação da solução;

3.3. A(s) beneficiária(s) deverá(ão) documentar e manter atualizada documentação das soluções desenvolvidas para a EPP.

3.4. ~~A~~(s) beneficiária(s) também deverá(ão):

- Entregar relatório de análise de vulnerabilidades, que aponte não constar vulnerabilidades na solução;
- Elaborar documentação conforme metodologia de administração de dados das EPPs, caso exista;
- Entregar relatório de testes de carga;
- Apresentar informes à EPP com o acompanhamento e status da implantação da solução;
- Prestar apoio nos processos de criação de ambientes computacionais dentro das estruturas da EPP;
- Prestar apoio na internalização da solução, com possibilidade de atuação em conjunto com as áreas técnicas da EPP, em observância ao processo de gestão de mudanças, caso exista.

4. SEGURANÇA DA INFORMAÇÃO E DE PRIVACIDADE

Em relação aos Desafios Tecnológicos de todas as EPPs, a(s) beneficiária(s) deverá(ão):

4.1. Cumprir o que dispõe a Lei Geral de Proteção de Dados Pessoais (LGPD) nº 13.853/2019, suas atualizações e normas complementares;

4.2. Observar a política de segurança da informação e a política de proteção de dados pessoais, ou equivalentes da EPP;

4.3. Evitar vazamento de informações, mantendo sigilo e privacidade, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto, de interesse da EPP ou de terceiros, que tomar conhecimento em razão da execução do projeto, aplicáveis aos dados, informações, regras de negócios, documentos e outros;

4.4. Implementar e manter controles e procedimentos específicos que assegurem completo e absoluto sigilo dos colaboradores participantes do projeto, a fim de que respeitem o uso dos dados somente para as finalidades previstas no projeto;

4.5. Providenciar revogação imediata dos acessos de colaborador(es) aos dados da EPP, caso haja a ocorrência de transferência, remanejamento ou demissão. Sendo necessário, deverá providenciar comunicação imediata à EPP para que tome as providências cabíveis em seu ambiente;

4.6. Obter autorização da área de negócio da EPP para a utilização dos dados pessoais em ambiente de teste, desenvolvimento e homologação, devendo, preferencialmente, utilizar os dados de maneira anonimizada;

4.7. Utilizar técnicas ou métodos apropriados durante a execução e encerramento do projeto para garantir exclusão ou destruição segura de dados pessoais (incluindo originais, cópias e registros arquivados), de modo a impedir sua recuperação no processo;

4.8. Utilizar recursos de segurança da informação e de tecnologia da informação licenciados (se requerido pelo fabricante), seguros e atualizados;

4.9. Formalizar à EPP, imediatamente, incidentes que envolvam vazamento de dados, indisponibilidade ou comprometimento da informação relacionados ao projeto, processamento não autorizado ou outro não cumprimento dos termos e condições contratuais;

4.10. Apresentar à EPP, sempre que solicitado e de maneira tempestiva, toda e qualquer informação e documentação relativa à execução do projeto e/ou que comprovem a implementação dos requisitos previstos no projeto;

4.11. Manter documentação atualizada sobre ações operacionais durante o projeto (escopo, escala, finalidade de backup, cópia, duplicação de dados, descarte, quem realizou, data, hora, etc.).