

SELEÇÃO PÚBLICA MCTI/FINEP/FNDCT/MGISP/ENAP

Subvenção Econômica à Inovação

Soluções de IA para o Poder Público – Rodada 3

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;

b) Obrigatoriamente:

- Durante a execução do projeto, observar 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.
- Durante a execução do projeto, buscar observar a metodologia e diretrizes de desenvolvimento de software, metodologia de segurança digital e o modelo de administração de dados da EPP, se for o caso.
- Elaborar documentações pertinentes ao processo de desenvolvimento de software, buscando seguir modelos pré-definidos pela EPP, a exemplo de Modelo de Dados, Arquitetura dos Sistemas e Histórias de usuários, com entregas em ferramentas de gestão de configuração da EPP.

2. AMBIENTE COMPUTACIONAL

2.1. AMBIENTE COMPUTACIONAL – ENTIDADE PÚBLICA PARTICIPANTE CVM

Para subsidiar a(s) beneficiária(s) com informações sobre o ambiente computacional da Comissão de Valores Mobiliários (CVM), segue a lista, não exaustiva, de tecnologias e ferramentas utilizadas na CVM, com foco no desenvolvimento de soluções:

- Resumo de tecnologias e métodos:

- Princípios da metodologia ágil, DevOps, plataforma Java EE (Enterprise Edition), padrões e frameworks: HTML5, CSS3, JavaScript, JQuery, Ajax, AngularJS, Angular, JSP, Bootstrap, e-MAG.

- Linguagens de Programação:

- Java SE versão 8 ou superior;
- Framework .NET 4.6.1 ou superior / .NET Core 5.x ou superior;
- PHP 8.2 ou superior;
- Microsoft T-SQL;
- Python 3.8 ou superior;
- Javascript puro e bibliotecas JQuery (2.x e 3.x) / AngularJS (1.x ou superior) / Angular (2.0 ou superior);
- HTML5 e CSS puro, Twitter Bootstrap ou qualquer outro framework de componentes de interface com o usuário compatível com HTML5 ou superior.

- Servidores de Aplicação:

- Internet Information Services (IIS);
- Wildfly;
- Nginx;
- Jboss EAP.

- Outras ferramentas:

- Visual Studio;
- Apache Subversion (SVN);
- Jenkins;
- Artifactory;
- Sonar;
- JobScheduler.

- Banco de dados:

- Microsoft SQL Server versão 2016 ou superior;
- MySQL 8.2 ou superior;
- PostgreSQL 14 ou superior;
- Até o momento, a CVM não possui bancos de dados orientados a grafos em seu ambiente de produção. Provas de conceito utilizaram-se de Neo4J e MemGraph (em Docker), com carga via Cypher, Python ou Apache Hop.

- Repositórios de documentos:

- Microsoft SQL Server;
- Sistema Eletrônico de Informações (SEI);

- Servidores de arquivos;
- Sharepoint;
- Microsoft OneDrive.

- Ferramentas para indexação de documentos:

- Apache Solr;
- iPED (Indexador da Polícia Federal).

- Ferramentas de BI:

- Microsoft SQL Server;
- SQL Server Integration Services (SSIS);
- SQL Server Analysis Services (SSAS);
- Power BI Report Server (PBIRS);
- Power BI Desktop;
- Power BI Pro.

- Linguagens para software de IA:

- Python 3.8 ou superior;
- Cypher.

- Técnicas de IA recomendadas para os Projetos:

- Aprendizado supervisionado;
- Aprendizado não supervisionado;
- Aprendizado por Reforço;
- Processamento de Linguagem Natural (NLP);
- *Large Language Models* (LLM);
- Aprendizado Profundo (*Deep Learning*);
- Redes Neurais Convolucionais (CNN);
- Redes Neurais em *Grapho* (GNN).

- Ambientes:

- Ambiente Local – consiste na estação de trabalho do desenvolvedor, em que estão instaladas as ferramentas necessárias para o desenvolvimento e teste das aplicações;
- Ambiente de Integração/Testes – ambiente corporativo, em servidor, para publicação de aplicações em desenvolvimento;
- Ambientes de Pré-produção e de Homologação – ambientes corporativos, em servidor, que permitem os testes homologatórios necessários por parte dos usuários da aplicação;
- Ambiente de Produção – ambiente corporativo, em servidor, que hospeda as aplicações em produção da CVM.

2.2. AMBIENTE COMPUTACIONAL – ENTIDADE PÚBLICA PARTICIPANTE INMETRO

Para subsidiar a(s) beneficiária(s) com informações sobre o ambiente computacional do Instituto Nacional de Metrologia, Qualidade e Tecnologia (Inmetro), segue lista, não exaustiva, de tecnologias e ferramentas utilizadas atualmente nos sistemas novos e legados, de forma a garantir a integração com os sistemas existentes:

- **Métodos:**

- Princípios metodologia ágil, Scrum.

- **Linguagens para software de IA:**

- Não utilizamos IA hoje no ambiente de TI Corporativo do Inmetro.

- **Linguagens de Programação e Tecnologias para Sistemas Atuais e Legado:**

- ASP.NET-MVC 4; Html; Java; Java script; PHP; T-SQL; Visual Basic 6.0; Delphi 5; Oracle Forms; LotusNotesScript; XML; COM +; DRUPAL; Framework Angular; Nhibernate ; WEB SERVICE WCF; WEBAPI; Access; API REST.

- **Bancos de dados:**

- MySQL; Oracle; MS SQL SERVER 2000,2008,2012.

- **Ferramentas de BPMS:**

- ZEEV/Orquestra.

- **Ferramentas de BI:**

- Solução da Microsoft.

- **Ambientes:**

- Desenvolvimento, homologação, operação e produção.

2.3. AMBIENTE COMPUTACIONAL – ENTIDADE PÚBLICA PARTICIPANTE INSS

Para subsidiar a(s) beneficiária(s) com informações sobre o ambiente computacional do Instituto Nacional do Seguro Social (INSS), segue a lista, não exaustiva, de tecnologias e ferramentas utilizadas no INSS, com foco no desenvolvimento de soluções:

- Resumo de tecnologias e métodos:

- Geral: Princípios metodologia ágil, REST-API, Gitlab CI/CD, Docker e Rancher, Kubernetes, MySQL, MariaDB PostgreSQL, AWS RDS, AWS EC2, AWS S3;
- Apache, Microsoft EntraID, Linux Debian.

- Linguagens para software de IA:

- Não temos IA hoje no INSS, excetuando-se aquelas nativas das soluções de escritório do Microsoft 365;
- Suportamos tecnologias de bibliotecas Python para IA.

- Linguagens de Programação:

- JAVA; PHP; Python; JS.

- Banco de dados:

- PostgreSQL, MySQL, MongoDB, MariaDB, AWS RDS (MySQL ou PGSQL).

- Ferramentas de desenvolvimento:

- VSCode e soluções livres.

- Ferramentas de BI:

- Solução Qlik.

- Repositório:

- Git.

- Ambientes:

- Desenvolvimento, homologação e produção;
- Nuvens Públicas AWS e GovCloud.

2.4. AMBIENTE COMPUTACIONAL – ENTIDADE PÚBLICA PARTICIPANTE SUFRAMA

Para subsidiar a(s) beneficiária(s) com informações sobre o ambiente computacional da Superintendência da Zona Franca de Manaus (SUFRAMA), segue a lista, não exaustiva, de tecnologias e ferramentas utilizadas na SUFRAMA, com foco no desenvolvimento de soluções:

- **Resumo de tecnologias e métodos:**

- Geral: Princípios metodologia ágil, Arquitetura Limpa, princípios SOLID, REST-API, Gitlab, CI/CD, IIS, Docker, Oracle, SQLServer;
- Plataforma Monolítica: Arquitetura Monolítica MVC, Wildfly AS, PrimeFaces, Hibernate, EJB - CDI - JSF (Jakarta EE 8), Selenium.

- **Linguagens para software de IA:**

- Nenhuma específica.

- **Linguagens de Programação:**

- C#, plataforma .NET.

- **Banco de dados:**

- SQLServer (preferencialmente), Oracle.

- **Ferramentas de desenvolvimento:**

- VSCode ou qualquer que seja utilizada.

- **Ferramentas de BI:**

- Solução da Microsoft PowerBI.

- **Ferramenta para modelagem de processo:**

- Bizagi.

- **Repositório:**

- GitLab.

- **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 e quaisquer outras documentações e artefatos que sejam ou tenham sido necessários 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):
 - a. Entregar relatório de análise de vulnerabilidades, que aponte não constar vulnerabilidades na solução;
 - b. Elaborar documentação conforme metodologia de administração de dados das EPPs, caso exista;
 - c. Entregar relatório de testes de carga;
 - d. Apresentar informes à EPP com o acompanhamento e status da implantação da solução;
 - e. Prestar apoio nos processos de criação de ambientes computacionais dentro das estruturas da EPP;
 - f. 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 PRIVACIDADE

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

- 4.1. Cumprir o que dispõe a legislação aplicável, inclusive 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. Não realizar cruzamento com quaisquer dados públicos sem autorização expressa da EPP;
- 4.4. Não copiar quaisquer conjuntos de dados, mesmo que públicos, para o ambiente de desenvolvimento sem autorização expressa da EPP;
- 4.5. Não tentar, de modo algum, copiar dados para outro ambiente, não importando o quão seguro o considere;
- 4.6. Não tentar de modo algum burlar as configurações de segurança realizadas pela EPP no ambiente de desenvolvimento;

- 4.7. Realizar configurações adicionais de segurança que garantam que todas as operações realizadas por todas as pessoas que trabalharem no ambiente de desenvolvimento sejam registradas em log;
- 4.8. Não tentar apagar ou alterar arquivos de log;
- 4.9. Evitar vazamento de informações, mantendo sigilo e privacidade, 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;
- 4.10. 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;
- 4.11. 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;
- 4.12. 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 não identificada ou anonimizada;
- 4.13. 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;
- 4.14. Utilizar recursos de segurança da informação e de tecnologia da informação licenciados (se requerido pelo fabricante), seguros e atualizados;
- 4.15. 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;
- 4.16. 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;
- 4.17. Manter documentação atualizada sobre ações operacionais durante o projeto (escopo, escala, finalidade de backup, cópia, duplicação de dados, descarte, quem realizou, data, hora etc.).

A não observância dos deveres acima implicará em penalidades civis, penais e administrativas.