BIX TECNOLOGIA · DOCUMENTO CORPORATIVO

Plano de Treinamento e Conscientização em Segurança e Privacidade

Programa periódico de treinamento técnico do time de software, com tópicos, formato e frequência definidos.

Versão 1.0 **Status** Aprovada e publicada **Revisão** Anual ou sob mudança

1. Objetivo e público-alvo

Programa interno de capacitação contínua, com foco em **desenvolvimento seguro** de aplicações de IA e agentes, para disseminar conhecimento técnico e boas práticas — incluindo segurança e privacidade — na equipe.

- **Público-alvo:** time de software.
- **Onboarding:** todos os membros recebem treinamento de **segurança da informação** na admissão.

2. Formato e frequência

- **Formato:** apresentação seguida de **sessão de Q&A**.
- **Frequência:** quinzenal — toda **sexta-feira, a cada duas semanas**.

3. Tópicos do programa

Os temas são abordados com **enfoque de segurança e privacidade** sempre que aplicável:

- **MCP** (Model Context Protocol) — integração segura com ferramentas e contexto (escopos e autorização).
- **RAG** (Retrieval-Augmented Generation) — proteção e controle dos dados usados na recuperação de contexto.
- **Observabilidade** — logs e métricas sem expor segredos ou dados sensíveis; detecção de anomalias.
- **Evals** — avaliação de qualidade e robustez das saídas (incl. prompt injection e confiabilidade).
- **Skills** — uso seguro de skills (permissões e validação).
- **Tools** — uso seguro de tools (validação de entradas/saídas; sem modo auto-approve).
- **Pesquisa léxica e semântica** no **PostgreSQL (pgvector)**, sem outros bancos vetoriais — isolamento e controle de acesso aos dados.

- Uso da **API do Claude** (Anthropic) — gestão de chaves/segredos, 2FA e não envio de dados sensíveis.
- Gestão de contexto com **subagentes** — minimização de dados e menor privilégio no contexto.
- Tratamento de **retry** em agentes — resiliência e tratamento seguro de falhas.
- **Paralelismo** — limites de taxa (rate limiting) e robustez.

4. Registro e acompanhamento

- A participação é registrada a cada sessão.
- O material das apresentações é compartilhado com a equipe.

Aprovação

DOCUMENTO Plano de Treinamento e Conscientização em Segurança e Privacidade	**VERSÃO** 1.0
APROVADO POR Direção — Bix Tecnologia	**DATA DE REVISÃO** Junho de 2026
PRÓXIMA REVISÃO Junho de 2027 (ou sob mudança relevante)	**CONTATO** info@bixtecnologia.com.br

Documento oficial publicado pela Bix Tecnologia. Diretrizes de caráter geral e orientador; detalhamentos operacionais constam em normas internas complementares.