

# Documentação do Prompt – Maratona Tech 2025

## 1. Prompt Final

Você é um **Engenheiro de Software** especializado em aplicações web seguras para bancos. Construa um **site interativo no formato de radar** que mostre **12 dispositivos conectados ao servidor** de um banco nacional que está sofrendo ataques de malware. Cada dispositivo deve aparecer como um ponto no radar, classificado em tempo real como **Seguro** ou **Inseguro (possível malware)**. Dispositivos inseguros devem ser representados com um **ícone de fantasma [emoji de fantasma]**, em referência a malwares, enquanto os seguros recebem um ícone de **check [emoji de check]**.

O radar deve ter **camadas concêntricas** que simbolizam a arquitetura da rede, que deve ser bem centralizado.

Quando o radar “varrer” um dispositivo, ele deve abrir no **painel lateral** um **feedback da IA**. Essa análise deve ser feita em tempo real: inicialmente mostrar a mensagem “[emoji de tempo] Analisando dispositivo...”, e após alguns segundos exibir um resultado com os campos: risco, explicacao e acoesRecomendadas. Caso não haja internet, use uma **função** que simule a resposta da IA. Comente no código o ponto onde a API Gemini seria integrada de verdade.

Cada dispositivo deve conter os seguintes dados fictícios: usuario, dispositivo, so, ip, ultimoAcesso, processosSuspeitos, porteArquivoIncomum, trafegoAnomalo, status. Use **apenas HTML, CSS e JavaScript** em um único arquivo, sem frameworks.

O site deve incluir ainda:

**Um modal para a tabela de dispositivos**, com busca, filtros por status (Seguro/Inseguro/Suspeito) e símbolos **visuais**.

- **Histórico de eventos em tempo real**, simulando logs de segurança.
- **Botão Exportar CSV** com os dados dos dispositivos.
- **Design moderno**, responsivo e acessível (semântica HTML, contraste adequado, navegação por teclado).
- Um rodapé com **boas práticas de segurança**, como: manter software atualizado, usar autenticação em duas etapas e aplicar o princípio do menor privilégio.

Deixe claro no código e na interface que **todos os dados são fictícios** e que os fantasmas são uma **metáfora lúdica para malwares**.

## 2. Explicação do raciocínio por trás do prompt

Porque o tema é segurança cibernética e o engenheiro de software com especialidade em aplicações web para bancos representa quem monitora e combate malwares em situações críticas.

A ideia foi criar uma simulação criativa e interativa (radar caça-fantasmas) para mostrar de forma divertida como dispositivos podem ser seguros ou inseguros, e como o profissional atua para detectar ameaças. Incluímos esse contexto porque é uma maratona que envolve diferentes estudantes, então usamos uma metáfora divertida (fantasma = malwares) para tornar o tema fácil de entender.

Definimos a resposta como um **site interativo**, pois combina com segurança da informação, permitindo a visualização em tempo real de dispositivos, relatórios e análise (simulada) de IA.

Durante o desenvolvimento fizemos ajustes e refinamentos:

- **Versão 0.5:** percebemos problemas no radar (mal centralizado).
- **Versão 1.0:** vimos que JSON poderia confundir o usuário e mudamos para um modal mais amigável.
- **Versão 1.5 (final):** consolidamos tudo em um protótipo responsivo, acessível e com todas as funções pedidas.

A análise de IA é **simulada** com uma função em JavaScript, mas o código indica claramente onde seria feita a integração com a API Gemini, caso fosse necessário no futuro.

---

## 3. Instruções para adaptação e uso por outras pessoas

Esse prompt pode ser adaptado para outros cenários de segurança digital. Exemplos:

- Proteger redes escolares contra softwares maliciosos.
- Treinar funcionários de uma empresa para identificar dispositivos comprometidos.
- Simular ataques de phishing em um e-commerce ou rede corporativa.

Para adaptar, basta:

- Trocar o **profissional** (ex: de engenheiro bancário para analista de redes escolares).
- Alterar o **público-alvo** (ex: estudantes, funcionários de empresa, professores).

- Ajustar o **contexto** (ex: de banco para escola ou empresa).
- Modificar as **mensagens e dicas de segurança** no rodapé.

Dessa forma, o prompt pode ser reutilizado e servir como base para diferentes projetos educativos e de conscientização em segurança cibernética.