Boas práticas para evitar “Componentes Desatualizados e Vulneráveis”.

1. Manter um Inventário de Dependências

- **Documente e Gerencie**: Mantenha um inventário atualizado de todas as dependências e componentes que sua aplicação utiliza. Use ferramentas de gerenciamento de pacotes (como npm para JavaScript, pip para Python, Maven para Java) para registrar e acompanhar as versões.

2. Atualizar Regularmente

- **Acompanhe Atualizações**: Monitore e aplique atualizações para suas dependências e bibliotecas regularmente. Configure alertas para notificações de novas versões ou vulnerabilidades conhecidas.
- **Automatize Atualizações**: Use ferramentas de automação, como Renovate ou Dependabot, que ajudam a manter suas dependências atualizadas automaticamente.

3. Auditar e Avaliar Vulnerabilidades

- **Ferramentas de Análise**: Utilize ferramentas de análise de segurança que verificam suas dependências em busca de vulnerabilidades conhecidas.

4. Seguir Boas Práticas de Configuração

- **Configurações Seguras**: Garanta que suas dependências e bibliotecas estejam configuradas de maneira segura. Algumas bibliotecas podem ter configurações padrão que não são seguras, então ajuste-as conforme necessário.

5. Usar Repositórios Confiáveis

- **Origem das Dependências**: Utilize apenas pacotes e bibliotecas de fontes confiáveis e reconhecidas. Evite baixar pacotes de fontes desconhecidas ou não verificadas.

6. Realizar Revisões e Testes

- **Revisões de Código**: Faça revisões regulares do código que utiliza bibliotecas e dependências para garantir que não haja uso inadequado de componentes.
- **Testes de Segurança**: Realize testes de segurança e análise de código para identificar e mitigar possíveis vulnerabilidades associadas às suas dependências.

7. Implementar Políticas de Segurança

- **Políticas de Atualização**: Estabeleça políticas e procedimentos claros para a atualização de dependências. Isso inclui definir responsabilidades e frequências para a revisão e aplicação de atualizações.

8. Treine a Equipe

- **Treinamento**: Forneça treinamento para sua equipe sobre a importância da gestão de dependências e como identificar e responder a vulnerabilidades.

9. Uso de Ferramentas de Monitoramento

- **Monitoramento Contínuo**: Implemente ferramentas e serviços que monitoram e alertam sobre vulnerabilidades em tempo real. Estes serviços podem informar rapidamente sobre novas vulnerabilidades que afetam as bibliotecas que você usa.

10. Documentar e Controlar

- **Documentação**: Mantenha uma documentação clara sobre as versões e atualizações dos componentes utilizados, e sobre quaisquer alterações feitas em suas configurações ou uso.