1. OBJETIVO

O objetivo deste documento é informar, para Parceiros e/ou Fornecedores que estejam prestando serviços de desenvolvimento de software para a Imagem Geosistemas, a necessidade de passar a realizar a varredura automatizada, utilizando o SonarQube nos códigos-fontes produzidos ou modificados em serviços contratados a partir da data de publicação deste documento.

2. ABRANGÊNCIA

A responsabilidade dos Parceiros e/ou Fornecedores subcontratados para adequação e/ou correção das vulnerabilidades identificadas pela varredura automatizada do SonarQube restringir-se apenas aos códigos-fontes produzidos ou alterados por sua equipe técnica, não se estendendo a códigos nativos, APIs ou bibliotecas da Esri ou de outros fornecedores de mercado. Cabe ainda ressaltar que é responsabilidade dos Parceiros e/ou Fornecedores utilizar apenas códigos nativos, APIs, bibliotecas, ferramentas etc. de fontes idôneas, confiáveis e devidamente licenciados.

3. DEFINIÇÕES

- **Esri:** empresa americana especializada na produção de soluções para a área de informações geográficas, responsável pelo desenvolvimento dos softwares ArcGIS, sobre os quais são realizados os desenvolvimentos de software pela Imagem Geosistemas;
- **API:** *"Application Programming Interface"* conjunto de rotinas e padrões de programação para acesso a um aplicativo de software ou plataforma baseado na Web.

4. REFERÊNCIAS

- NBR ISO/IEC 27001:2013 – Anexo 14;
- F-PS-13 – Contrato Sintético.

5. DESCRIÇÃO

5.1. Qualidade do Software

5.1.1. Varredura Automatizada de Vulnerabilidades e Falhas de Segurança no Código-Fonte

A partir da publicação deste documento, todos os novos projetos da Imagem Geosistemas, incluindo serviços terceirizados a Parceiros ou Fornecedores, deverão ter todo código-fonte produzido ou que foi alterado sendo verificado pela varredura automatizada de vulnerabilidades e falhas de segurança do SonarQube.

Neste caso, é necessário que a empresa parceira e/ou terceirizada tenha uma assinatura do SonaQube em nuvem https://www.sonarsource.com/plans-and-pricing/#sonarcloud (acessado em 31/03/2023), ao custo mensal de € 10,00, para análise de até 100 mil linhas de código-fonte/mês. O parceiro e/ou terceirizado deve submeter seu código para análise do SonarQube e somente após atingir aos requisitos de **NOTA A** de qualidade, o código deverá ser disponibilizado para a Imagem, acompanhado da evidência de atingimento da **NOTA A**, bem como a indicação de quais pastas foram verificadas e demais evidências de testes aplicáveis.

A varredura pode ser vinculada a um pipeline do Microsoft DevOps do fornecedor, ou direto no SonarCloud, criando um projeto, conforme instruções apresentadas pelo próprio site da ferramenta:

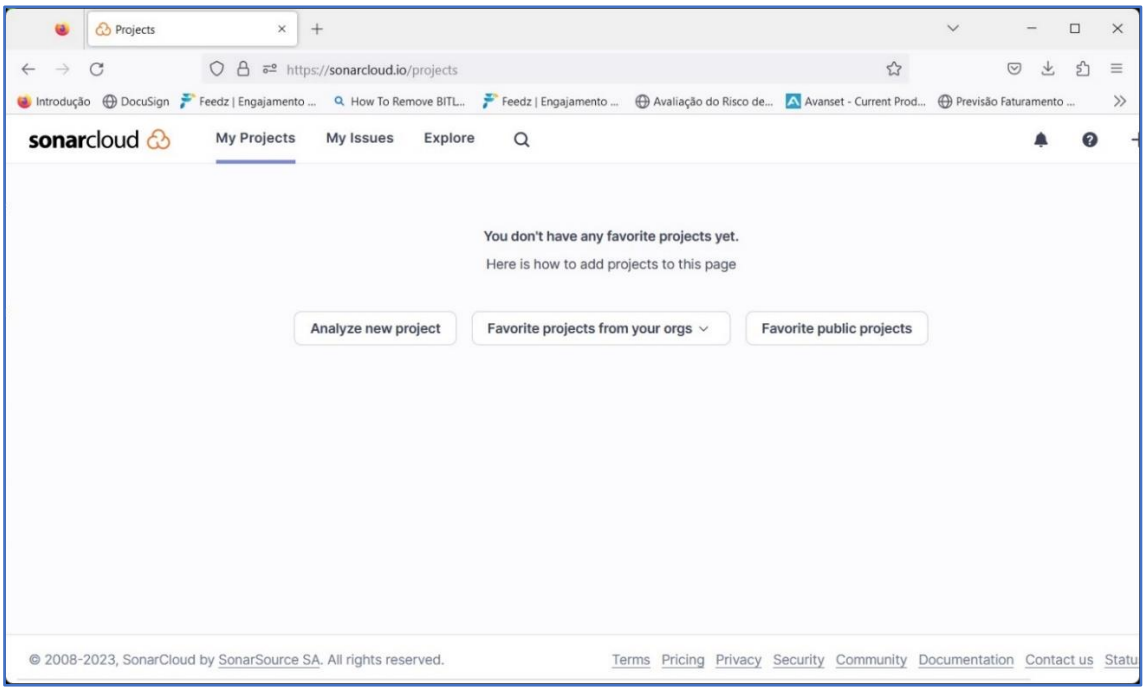

Figura 1 – Novo projeto no SonarCloud

A varredura de vulnerabilidade e qualidade do código-fonte deve ocorrer seguindo as configurações default da ferramenta SonarCloud (Security Hotspots Reviewed e Security Rating), apresentadas a seguir:

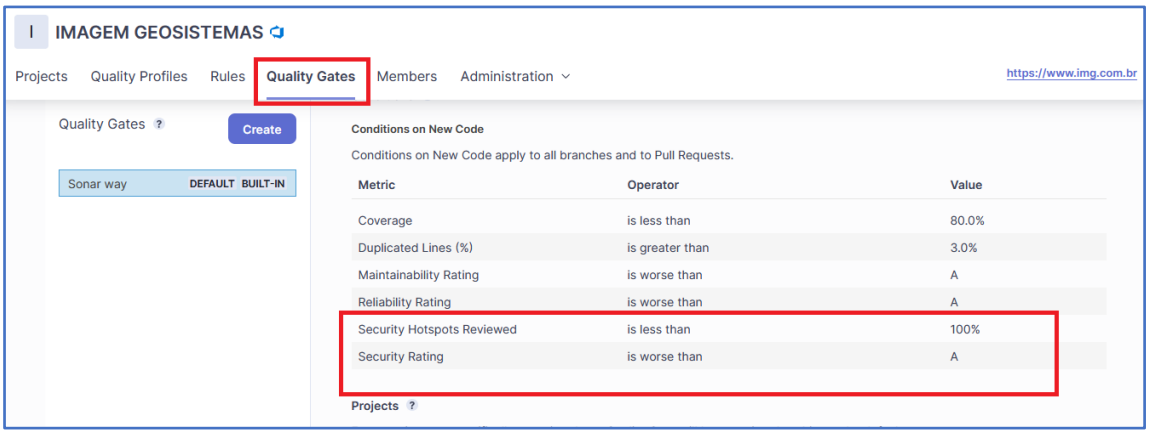

Figura 2 – Configuração Default – Nível A

Esta configuração verifica várias vulnerabilidades e problemas de segurança, além de estar em constante evolução, sendo adicionadas novas verificações, periodicamente:

Figura 3 – 319 Vulnerabilidades e 480 Focos de Segurança tratados pela varredura automática

Com o resultado **NOTA A** aprovado, o código-fonte e demais evidências de testes podem ser encaminhados para a Imagem. Caso o resultado seja diferente que **NOTA A**, a entrega deve ser postergada e retornar para que o desenvolvedor do Parceiro ou Fornecedor realizar as devidas correções.

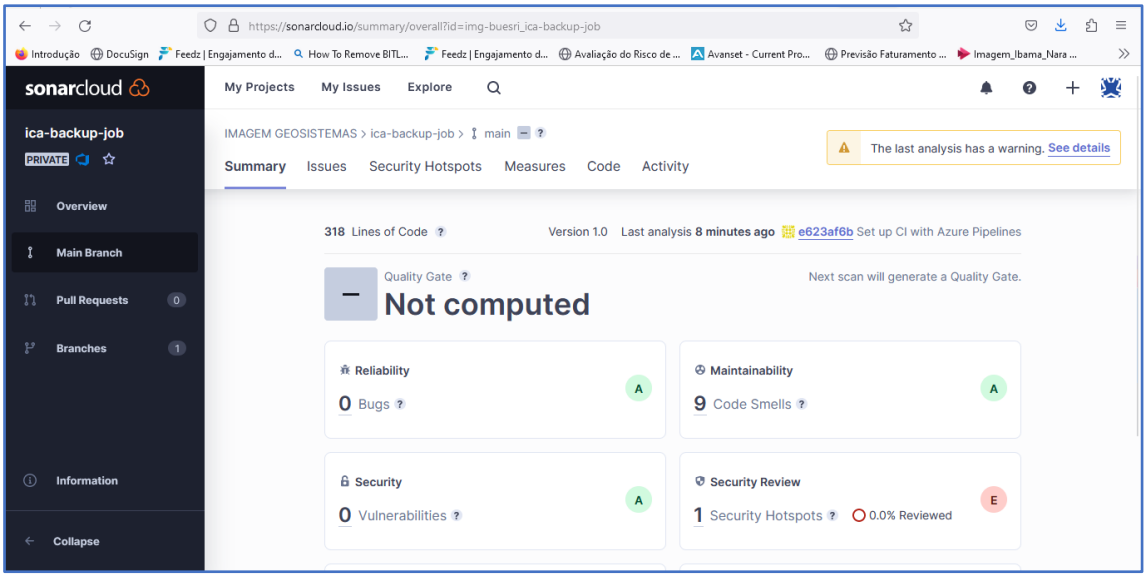

Figura 4 – Exemplo de Reprovação, nota E, com 1 Apontamento de Segurança

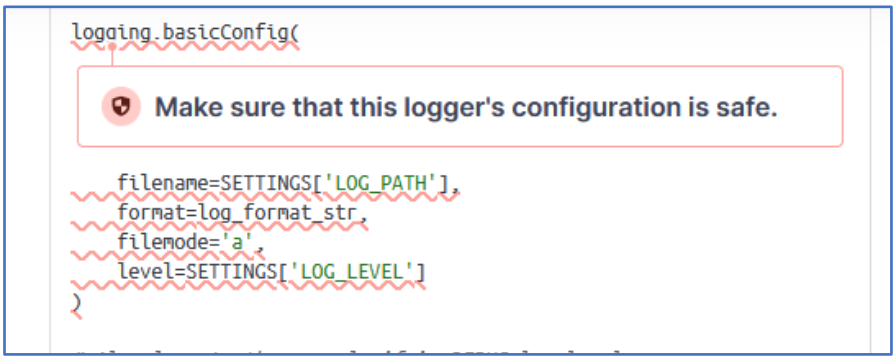

Figura 5 – Exemplo de Detalhamento de Apontamento de Segurança

5.2. Demais Testes

O fato de realizar a varredura do SonarCloud, atingindo a **NOTA A**, não substitui a necessidade de testar e documentar outros testes de Requisitos Funcionais e Não Funcionais do escopo da contratação – as funcionalidades e demais característica solicitadas pela Imagem devem ser testadas antes da entrega e as evidências testes devidamente apresentadas.

6. ANEXOS

N/A