

VARREDURA AUTOMATIZADA DO CÓDIGO-FONTE PRODUZIDO POR PARCEIROS OU FORNECEDORES

Sumário

1. OBJETIVO	2
2. ABRANGÊNCIA.....	2
3. DEFINIÇÕES.....	2
4. REFERÊNCIAS.....	3
5. RESPONSABILIDADES.....	3
6. DESCRIÇÃO	3
6.1. Qualidade do Software.....	3
6.1.1. Varredura Automatizada de Vulnerabilidades e Falhas de Segurança no Código-Fonte.....	3
6.2. Demais Testes.....	7
7. ANEXOS	7

CÓPIA CONTROLADA

CONSIDERAÇÕES SOBRE OS DOCUMENTOS DOS SISTEMAS DE GESTÃO

- *Todos os documentos aplicáveis ao Sistema de Gestão devem ser acessados, consultados e utilizados exclusivamente por meio da ferramenta oficial de Gestão de Documentos da Imagem Tecnologia.*
- *A versão disponibilizada na plataforma é a única considerada válida e vigente para uso operacional.*
- *Não é permitida a utilização de cópias armazenadas localmente, impressões não controladas ou documentos compartilhados fora do sistema oficial.*
- *É responsabilidade de cada colaborador assegurar que está utilizando a versão atual do documento, verificando código, revisão e status de vigência antes de sua aplicação.*
- *Quaisquer divergências, inconsistências ou necessidade de atualização devem ser comunicadas ao responsável pelo documento e posteriormente à equipe da Qualidade.*

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. RESPONSABILIDADES

Atividade	Responsável
• Realizar varredura automatizada de código-fonte utilizando SonarQube	Parceiros e/ou Fornecedores
• Corrigir vulnerabilidades apenas nos códigos produzidos ou alterados pela própria equipe	Parceiros e/ou Fornecedores
• Utilizar apenas códigos, APIs e bibliotecas de fontes confiáveis e licenciadas	Parceiros e/ou Fornecedores
• Garantir que novos projetos tenham código analisado por varredura automatizada	Imagem Geosistemas / Parceiros / Fornecedores
• Contratar e manter assinatura do SonarCloud	Parceiros e/ou Fornecedores
• Submeter código para análise e atingir NOTA A de qualidade	Parceiros e/ou Fornecedores
• Disponibilizar código com evidências de qualidade e testes	Parceiros e/ou Fornecedores
• Configurar e executar varredura (pipeline DevOps ou SonarCloud)	Parceiros e/ou Fornecedores

6. DESCRIÇÃO

6.1. Qualidade do Software

6.1.1. 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>, 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

VARREDURA AUTOMATIZADA DO CÓDIGO-FONTE PRODUZIDO POR PARCEIROS OU FORNECEDORES

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:

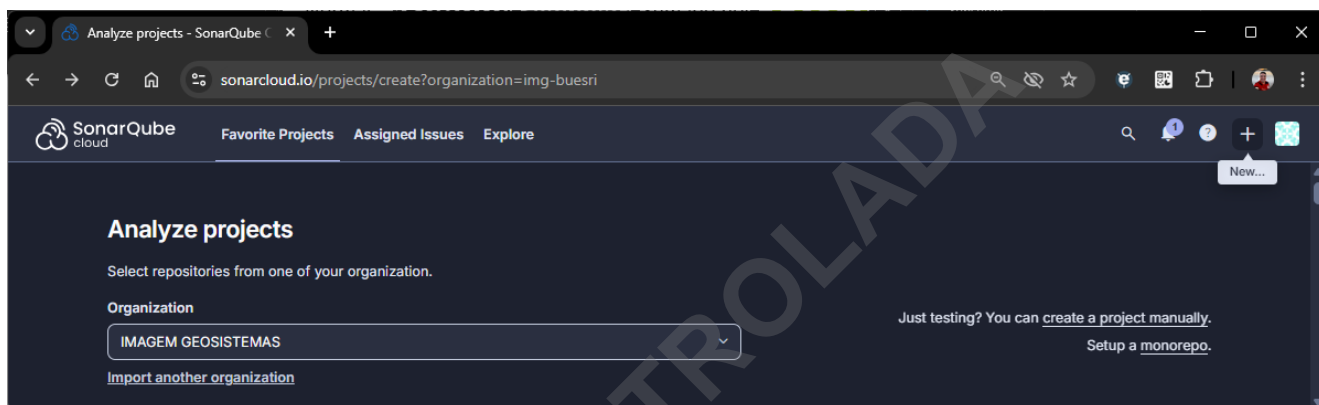
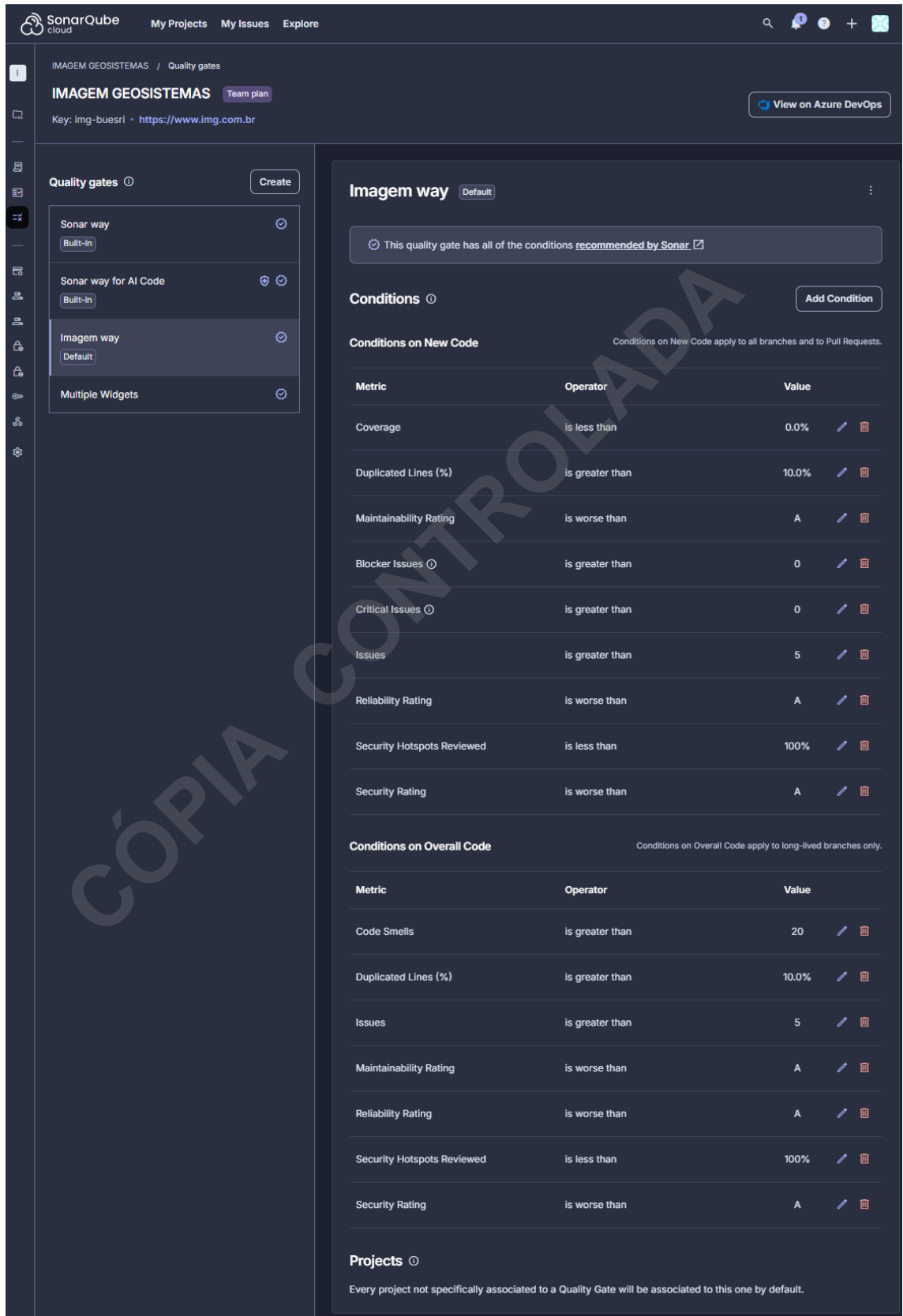


Figura 1 – Novo projeto no SonarCloud

A varredura de vulnerabilidade e qualidade do código-fonte deve ocorrer seguindo as configurações da ferramenta SonarCloud (Security Hotspots Reviewed e Security Rating) de acordo com o Imagem Way, apresentado a seguir:

CÓPIA CONTROLADA

VARREDURA AUTOMATIZADA DO CÓDIGO-FONTE PRODUZIDO POR PARCEIROS OU FORNECEDORES



The screenshot shows the SonarQube interface for configuring a Quality Gate named 'Imagem way'. The interface is in dark mode and includes a sidebar with navigation options like 'Quality gates', 'Sonar way', and 'Multiple Widgets'. The main content area is divided into sections for 'Conditions on New Code' and 'Conditions on Overall Code', each with a table of metrics, operators, and values. A 'Projects' section at the bottom indicates that all projects not specifically associated with a Quality Gate will be associated with this one by default.

Quality gates IMAGEM GEOSISTEMAS / Quality gates

IMAGEM GEOSISTEMAS Team plan

Key: img-buesri - <https://www.img.com.br> View on Azure DevOps

Quality gates Create

- Sonar way Built-in
- Sonar way for AI Code Built-in
- Imagem way** Default
- Multiple Widgets

Imagem way Default

This quality gate has all of the conditions recommended by Sonar. View

Conditions Add Condition

Conditions on New Code Conditions on New Code apply to all branches and to Pull Requests.

Metric	Operator	Value
Coverage	is less than	0.0%
Duplicated Lines (%)	is greater than	10.0%
Maintainability Rating	is worse than	A
Blocker Issues	is greater than	0
Critical Issues	is greater than	0
Issues	is greater than	5
Reliability Rating	is worse than	A
Security Hotspots Reviewed	is less than	100%
Security Rating	is worse than	A

Conditions on Overall Code Conditions on Overall Code apply to long-lived branches only.

Metric	Operator	Value
Code Smells	is greater than	20
Duplicated Lines (%)	is greater than	10.0%
Issues	is greater than	5
Maintainability Rating	is worse than	A
Reliability Rating	is worse than	A
Security Hotspots Reviewed	is less than	100%
Security Rating	is worse than	A

Projects

Every project not specifically associated to a Quality Gate will be associated to this one by default.

Figura 2 – Configuração Quality Gate Imagem Way – Nível A

VARREDURA AUTOMATIZADA DO CÓDIGO-FONTE PRODUZIDO POR PARCEIROS OU FORNECEDORES

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

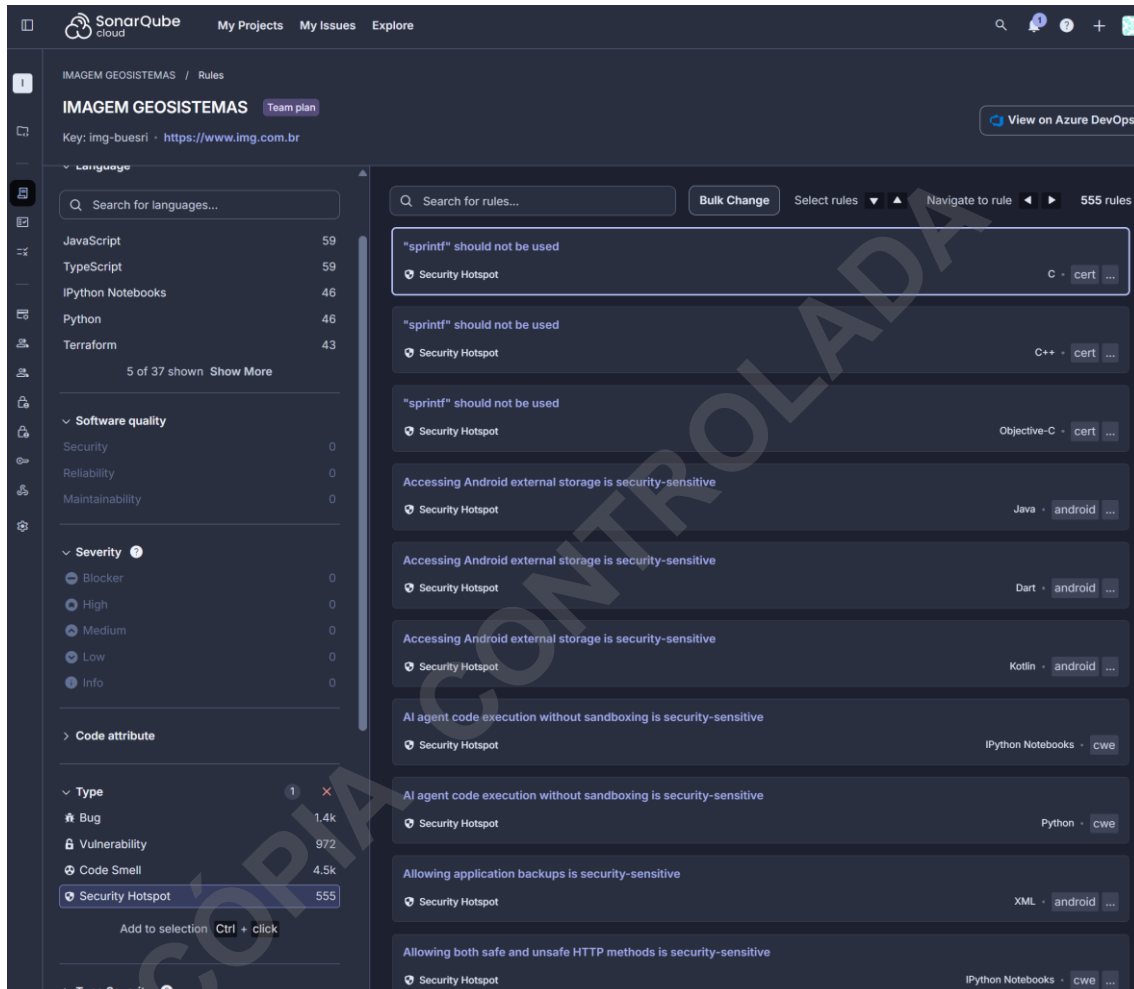


Figura 3 – 972 Vulnerabilidades e 555 Focos de Segurança tratados pela varredura automática

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.

VARREDURA AUTOMATIZADA DO CÓDIGO-FONTE PRODUZIDO POR PARCEIROS OU FORNECEDORES

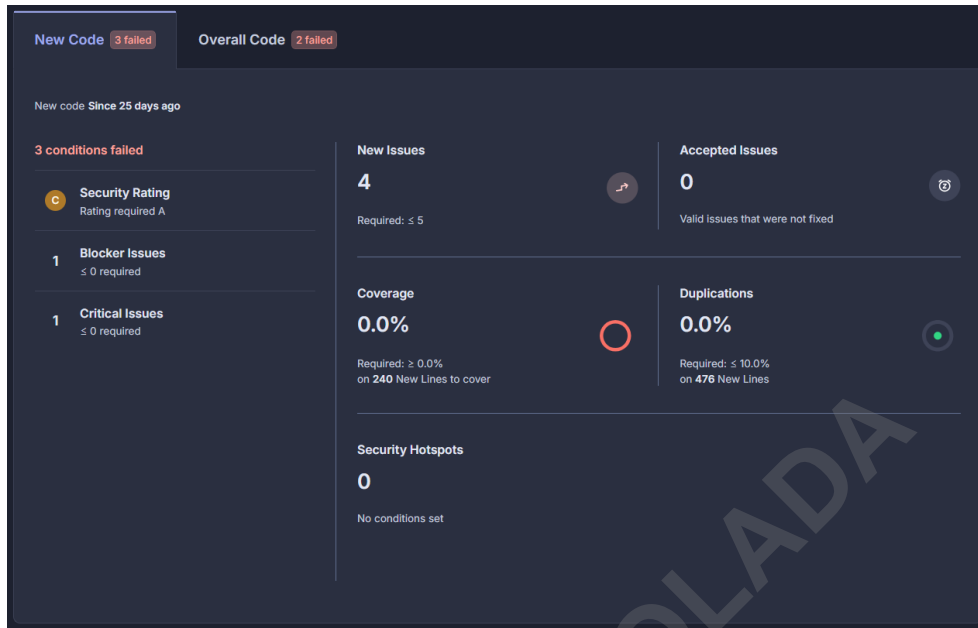


Figura 4 – Exemplo de Reprovação, precisa de atenção em security e issues

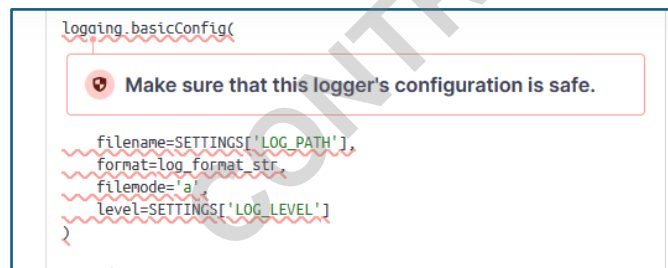


Figura 5 – Exemplo de Detalhamento de Apontamento de Segurança

6.2. 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.

7. ANEXOS

Não aplicável.