Sumário

CONSIDERAÇÕES SOBRE OS DOCUMENTOS DOS SISTEMAS DE GESTÃO

- *Todos os documentos aplicáveis ao Sistemas 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

Os princípios, boas práticas e recomendações descritos a seguir, visam reforçar a importância do tema segurança da informação de maneira geral, mas principalmente aplicado aos serviços que tenham desenvolvimento de software (i.e., produção de código-fonte), independente da modalidade do serviço.

2. ABRANGÊNCIA

As diretivas definidas neste documento complementam o PR-PS-01 Processo de Desenvolvimento de Software, devendo ser seguidas por todos os colaboradores envolvidos nas atividades de desenvolvimento de software da Imagem Geosistemas, principalmente no que tange a produção ou alteração de código-fonte para software.

Os princípios, boas práticas e recomendações aqui descritos se aplicam ao ciclo de vida dos serviços de desenvolvimento de software da Imagem Geosistemas, principalmente nas fases de Pré-vendas, Planejamento, Execução, Monitoramento & Controle e Garantia – ou equivalentes, conforme modalidade do serviço:

- **Atividades de Pré-vendas e passagem do projeto:** Os profissionais técnicos que atuam em tempo de pré-vendas devem verificar se o cliente possui a necessidade de atendimento explícito de algum Requisito Não Funcional de Segurança da Informação. As características para atendimento destes requisitos de segurança devem constar na proposta técnica ou equivalente e os esforços necessários devem ser estimados pela equipe técnica executora e constar na aba REQUISITOS da planilha de estimativas F-COM-02.rxx. Caso o cliente não explicite nenhum requisito de segurança, apenas a validação automatizada via SonarQube será feita. Todas as informações relevantes, levantadas em tempo de pré-vendas, relacionadas

ao Desenvolvimento Seguro devem ser repassadas ao Gerente de Projetos e equipe técnica executora durante a reunião inicial de passagem de informações de vendas;

- **Planejamento ou equivalente:** No início do serviço, o Gerente de Projetos junto com a Equipe Técnica do Projeto deve planejar as atividades relacionadas a implementação, validação e testes dos requisitos de segurança da informação e demais requisitos funcionais solicitados pelos clientes, considerando a avaliação dos riscos relacionados à segurança da informação – as formas de registrar os planejamentos poderão variar, conforme a modalidade do serviço;

- **Execução, Monitoramento & Controle e Garantia ou equivalentes:** Os requisitos não funcionais de segurança da informação solicitados formalmente pelos clientes deverão ser levantados, detalhados, especificados, implementados e testados internamente, bem como homologados junto aos clientes – as formas de registrar os planejamentos poderão variar, conforme a modalidade do serviço. Adicionalmente, a Imagem deverá aplicar formas automatizadas de testar vulnerabilidades e falhas de segurança no código-fonte produzido, através de ferramentas de mercado, como é caso do SonarQube.

- **Pós Garantia:** Os princípios, boas práticas e recomendações não se aplicam.

IMPORTANTE: A responsabilidade da Imagem para adequação e/ou correção das vulnerabilidades identificadas pela varredura automatizada do SonarQube restringir-se apenas aos códigos-fontes produzidos ou alterados pela equipe técnica da Imagem ou parceiros subcontratados, não se estendendo a códigos nativos, APIs ou bibliotecas da Esri ou de outros fornecedores de mercado.

3. DEFINIÇÕES

- OWASP: "*Open Web Application Security Project*" é uma entidade sem fins lucrativos e com reconhecimento internacional, atuando com foco na colaboração para o fortalecimento da segurança de softwares. Apresenta uma relação das Top 10 vulnerabilidades no desenvolvimento de software que são averiguadas através da varredura automatizada feita pelo SonarQube https://owasp.org/Top10/ e https://docs.sonarqube.org/latest/user-guide/security-reports/

- PCI DSS: *"Payment Creditcard Industry Data Security Standard"* consiste em doze requisitos significativos, incluindo vários sub-requisitos, que contêm inúmeras diretivas em relação às quais as empresas podem

medir suas próprias políticas, procedimentos e diretrizes de segurança de cartões de pagamento. Apresenta, nas versões 4.0 e 3.2.1, uma relação de vulnerabilidades no desenvolvimento de software que são averiguadas através da varredura automatizada feita pelo SonarQube https://www.pcisecuritystandards.org/ e https://docs.sonarqube.org/latest/user-guide/security-reports/

- CWE: *"Common Weakness Enumetation"* é uma lista desenvolvida pela comunidade de tipos de vulnerabilidades de software e hardware. Ele serve como uma linguagem comum, uma medida para ferramentas de segurança e como uma linha de base para esforços de identificação, mitigação e prevenção de fraquezas. Apresenta uma relação das Top 25 vulnerabilidades no desenvolvimento de software que são averiguadas através da varredura automatizada feita pelo SonarQube https://cwe.mitre.org/top25/archive/2021/2021_cwe_top25.html e https://docs.sonarqube.org/latest/user-guide/security-reports/

- API: "*Application Programming Interface*" conjunto de rotinas e padrões de programação para acesso a um aplicativo de software ou plataforma baseado na Web;

- 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.

4. REFERÊNCIAS

- M-TI-01 – Manual de Segurança da Informação;
- ISO 9001:2015;
- ISO 37001:2017;
- ISO 27001:2022;
- ISO 27002:2022;
- PR-PS-01- Processo de Desenvolvimento de Software.
- PO-TI-04 - Dinâmica de Backup e Disaster Recovery;
- PO-TI-05 – Política de Gestão de acessos;
- PR-TI-04 - Gestão de acessos;
- PR-TI-08 – Relacionamento com a Cadeia de Suprimentos;
- PR-TI-22 - Gestão de Fornecedores TIC

- PR-GPAR-01 – Gestão de Parceiros e Fornecedores;
- P-GPAR-03 – Homologação de Parceiros de Serviços e Fornecedores;
- Acordos de confidencialidade (termos de compromissos);
- Ferramenta AMMRisk.

5. RESPONSABILIDADES

Atividade	Responsável
• Devem verificar se o cliente possui a necessidade de atendimento explícito de algum Requisito Não Funcional de Segurança da Informação e documentar as características para atendimento destes requisitos de na proposta técnica ou equivalente e apresentar estas características para que os esforços necessários sejam estimados pela equipe técnica executora; • Fazer a passagem de conhecimento, para o Gerente de Projetos e equipe técnica executora, sobre todas as informações relevantes, levantadas em tempo de pré-vendas, relacionadas ao Desenvolvimento Seguro, durante a reunião inicial de passagem de informações de vendas.	Profissionais técnicos de pré-vendas (Arquitetos de Negócio e Arquitetos de Soluções ou equivalentes)
• Estimar os esforços e recursos necessários para praticar os princípios do desenvolvimento seguro, bem como executar as atividades relacionadas a implementação, validação e testes dos requisitos de segurança da informação; • Praticar os princípios do desenvolvimento seguro e contribuir para a melhoria da segurança da informação; • Configurar o pipeline SonarQube no Azure DevOps para realizar automaticamente a varredura de vulnerabilidades e falhas de segurança; • Corrigir as vulnerabilidades apontadas pelo SonarQube; • Notificar falhas e/ou novas vulnerabilidades.	Desenvolvedores próprios ou de parceiros e/ou terceirizados
• Planejar as atividades relacionadas a implementação, validação e testes dos requisitos de segurança da informação; • Desdobrar esse procedimento para os desenvolvedores próprios ou de parceiros e/ou terceirizados; • Monitorar as entregas e desempenho dos desenvolvedores próprios ou de parceiros e/ou terceirizados; • Tratar e monitorar os riscos, principalmente relacionados à segurança da informação	Responsável pelo projeto
• Apoiar a equipe na remoção de impeditivos e no tratamento de riscos residuais, principalmente relacionados à segurança da informação;	Gerente de Soluções
• Disponibilizar recursos quando necessário para melhorias nos processos.	Alta Direção

6. DESCRIÇÃO

6.1. Princípios do Desenvolvimento Seguro – Visão Geral

- Mantenha o design do sistema o mais simples e pequeno possível – sempre que possível, cada componente deve ter uma única responsabilidade;

- Baseie as decisões de acesso em permissão implícita ao invés de negação;
- Devem existir mecanismos para que todo acesso a cada objeto deve ser verificado para autorização;
- Todo programa e todo usuário do sistema devem operar usando o mínimo dos privilégios necessários para concluir o trabalho;
- Projete o sistema para resistir a ataques, mesmo que uma única vulnerabilidade seja descoberta ou que um único recurso de segurança venha a ser subvertido. A defesa em profundidade pode envolver vários níveis de segurança ou projetar o sistema para travar, ao invés de permitir que o invasor obtenha controle completo;
- Um contraponto à defesa em profundidade é que um sistema deve ser projetado para permanecer seguro, mesmo que encontre um erro ou trave;
- É provável que nenhum sistema permaneça livre de vulnerabilidades de segurança para sempre, portanto, os desenvolvedores devem planejar a instalação segura e confiável de atualizações de segurança. A segurança de um sistema de informação é tão forte quanto o seu componente mais fraco;
- As senhas utilizadas para autenticações em projetos em desenvolvimento não podem ser compartilhadas. As credenciais de acesso (usuários e senhas) devem ser mantidas preferencialmente em cofres eletrônicos e acessadas apenas por pessoas autorizadas.

6.2. Gerenciamento de Acessos e Permissões de Usuários

Utilizar, como primeira opção, as diretrizes da Esri para a verificação da identidade de usuários ao realizarem operações nos sistemas para utilizarem os mecanismos de controle através de Usuário Nomeados (Named Users) do ArcGIS Enterprise ou ArcGIS Online, exceto quando houver solicitações diferentes do cliente.

6.2.1. Autenticação através do AD Active Directory

Sempre que possível, recomendar que os Clientes adotem a prática de vincular o controle de Usuários Nomeados ao seu Active Directory, implementando um cadastro de Usuários centralizado, com políticas de senhas fortes, trocas periódicas de senhas e outras boas práticas. Para maiores informações sobre esta configuração, consultar https://enterprise.arcgis.com/pt-br/portal/latest/administer/windows/use-your-portal-with-ldap-and-portal-tier-authentication.htm.

6.2.2. Autenticação de Múltiplos Fatores

Informar aos clientes que é possível utilizar a autenticação dos Usuários Nomeados do ArcGIS Online e Portal for ArcGIS através de múltiplos fatores. A utilização desta forma de autenticação é controlada pelo Sistema ArcGIS e não afeta outros aspectos da codificação. Esta configuração pode ser feita a partir da versão 10.9.1 do Portal for ArcGIS e na versão corrente do ArcGIS Online.

Para maiores informações sobre esta configuração, consultar https://enterprise.arcgis.com/pt-br/portal/latest/administer/windows/configure-security.htm#MULTIFACTOR.

6.3. Boas Práticas na Prevenção de Ataques Cibernéticos ou Falhas de Segurança da Informação

Nesta seção se definem os padrões mínimos de segurança para prevenção a ataques a sistemas customizados pela Imagem Geosistemas e se especificam os requisitos a serem atendidos como padrões nos desenvolvimentos de softwares.

Todas nossas aplicações fornecidas pela Esri – distribuidor ArcGIS, passam pelo processo de validação do OWASP, o que nos garante que foram adotadas as melhores práticas de segurança na aplicação.

Como os desenvolvimentos da Imagem Geosistemas se caracterizam por customizações dos Produtos e Componentes da Plataforma ArcGIS, deve-se garantir que as orientações fornecidas na documentação da Esri sejam consultadas regulamente e seguidas sempre que aplicável:

- *Security Best Practices*
- *ESRI Software Security and Privacy*
- *A Practical Guide to ArcGIS Online Security - ESRI*

NOTA: A partir de abril de 2023, a Imagem optou por utilizar a ferramenta de mercado SonarQube para fazer a varredura do código-fonte dos projetos iniciados após esta data, a procura de vulnerabilidades e falhas de segurança, em substituição do processo anterior de validação manual, por amostragem, dos requisitos não funcionais de segurança da informação.

Devido ao fato de a varredura automatizada do código-fonte ser muito mais confiável do que a inspeção manual por amostragem, podemos considerar que a mesma pode ser utilizada, mesmo de maneira retroativa (ou seja, para projetos tratados pela Revisão 2 deste documento) a fim de comprovar o atendimento dos requisitos de segurança da informação.

6.4. Prevenção, Reação e Mitigação de Falhas de Segurança

Esta seção apresenta diretrizes para a realização de procedimentos que garantam uma reação adequada à ocorrência de vulnerabilidades e falhas de segurança. Detalha-se o emprego de armazenamento de códigos, backups, testes e tratamento de ocorrências.

6.4.1. Orientações Relacionadas ao Códigos-Fonte

- Os códigos-fonte devem ser armazenados no Microsoft DevOps e os demais artefatos no Sharepoint do respectivo serviço. Os acessos serão feitos por usuários ativos devidamente autenticados via Active Directory (AD) da Imagem.
- Remover comentários do código-fonte que possam ser acessados pelos usuários e revelar detalhes internos do sistema ou outras informações sensíveis, como senhas, dados pessoais etc.
- Não armazenar senhas, strings de conexão ou outras informações confidenciais em texto claro/legível ou em qualquer forma criptograficamente insegura no lado cliente.
- Os códigos-fontes e demais documentos dos projetos são submetidos a backups regulares, conforme procedimento PR-TI-02 - Dinâmica de Backup e Disaster Recovery.

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

A partir da publicação da revisão 3 deste documento, todos os novos projetos deverão ter todo código-fonte produzido e armazenado no Microsoft DevOps e passar pela varredura automatizada de vulnerabilidades e falhas de segurança do SonarQube.


```
extraProperties: |
  sonar.sources=./widgets/zzEscalaManual
```

Figura 1 – Configuração da(s) pasta(s) a ser(em) auditada(s)

O scan de vulnerabilidade e qualidade do código ocorre na ferramenta SonarQube e o indicador determinado como resultado precisa ser = A (melhor nota possível), considerando as seguintes configurações do SonarQube:

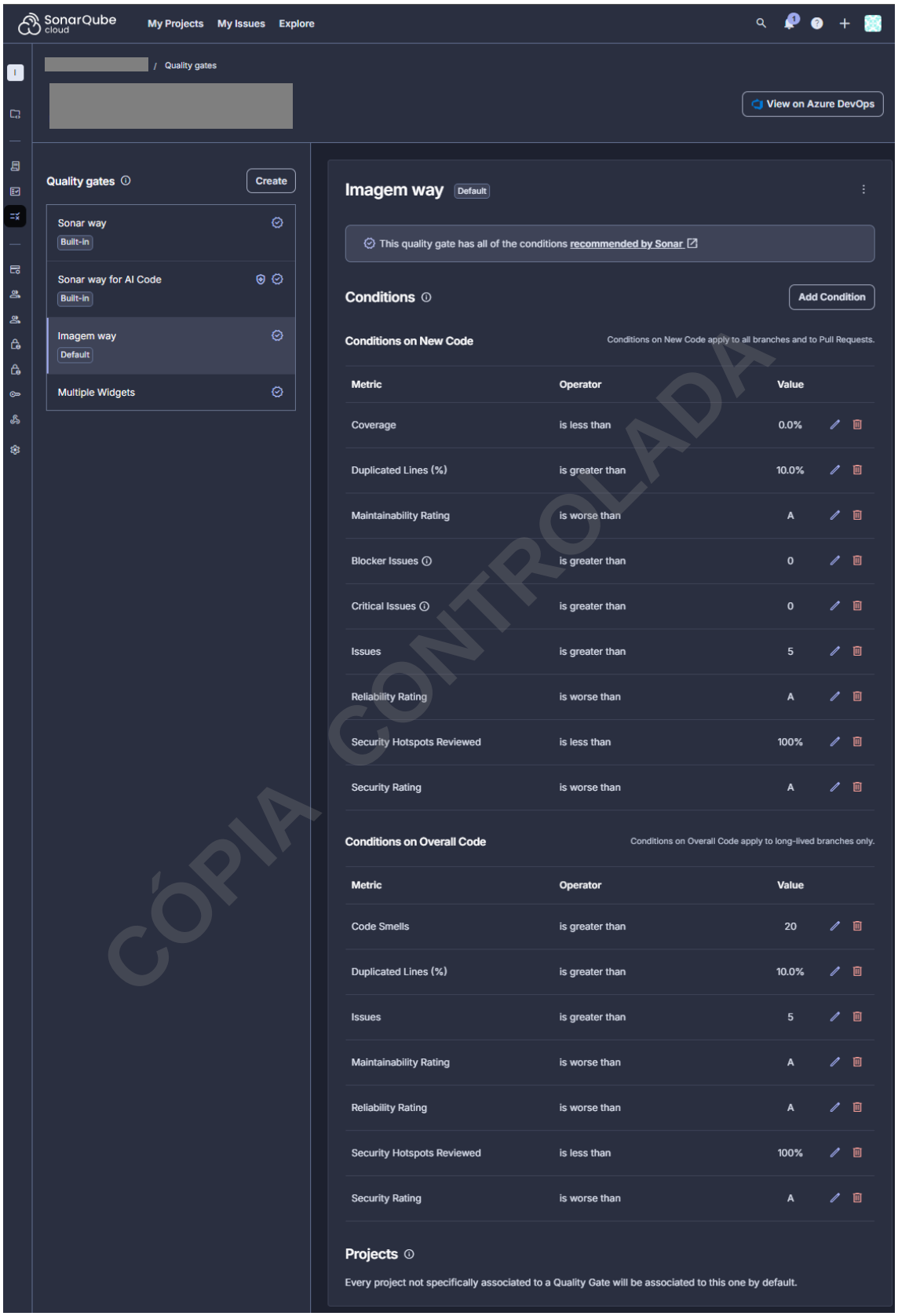

Figura 2 – Configuração Quality Gate Imagem – Nível A

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

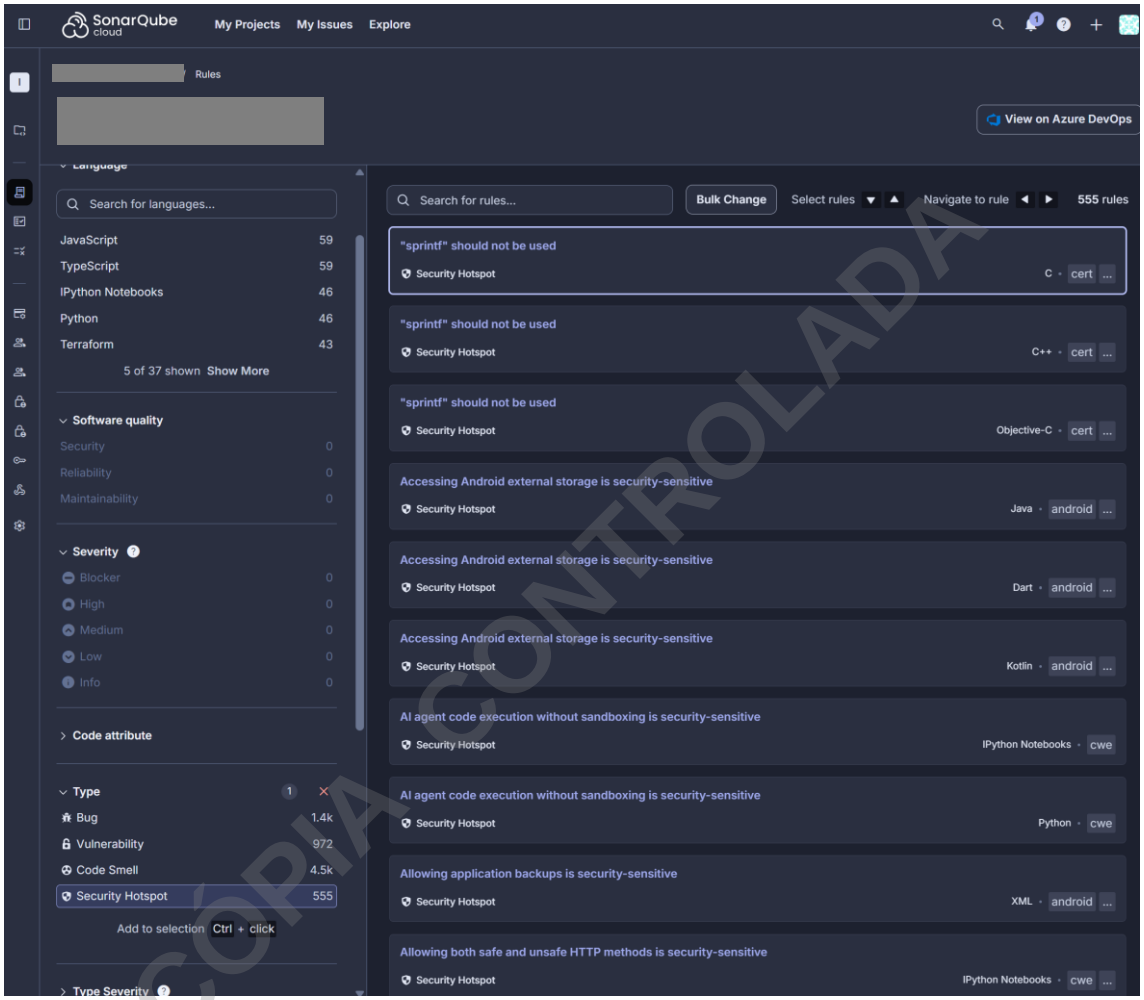

Figura 3 – 972 Vulnerabilidades e 555 Focos de Segurança tratados pela varredura automática

Com o resultado A aprovado, o código pode ser publicado para testes. Caso o resultado seja diferente que nota A, o deploy é cancelado e retorna para o desenvolvedor realizar as devidas correções.

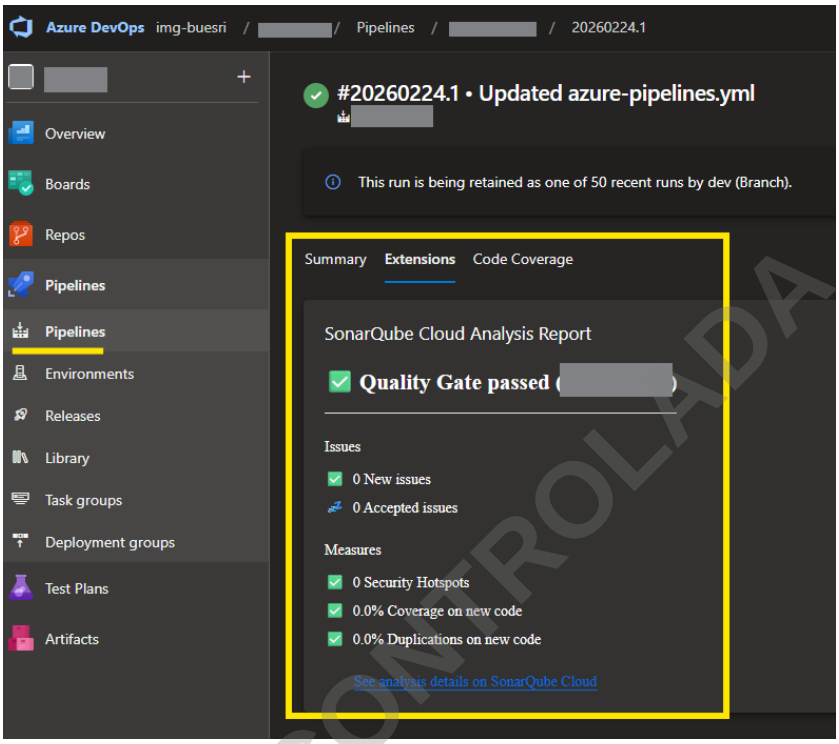

Figura 4 – Pipeline com a Extensão SonarCloud executado com Sucesso, Nota A

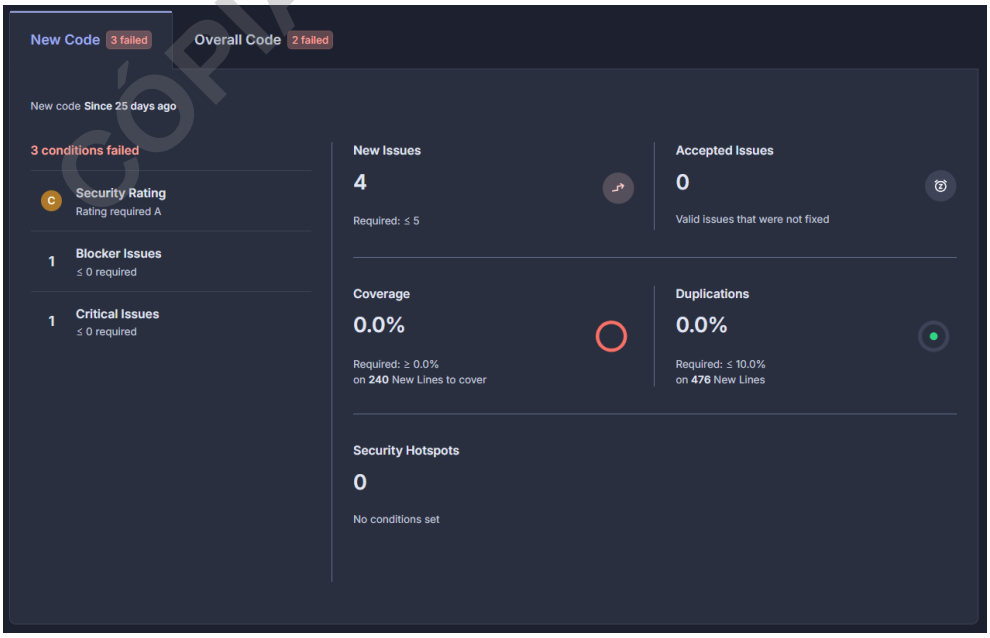

Figura 5 – Exemplo de Reprovação, precisa de atenção em security e issues

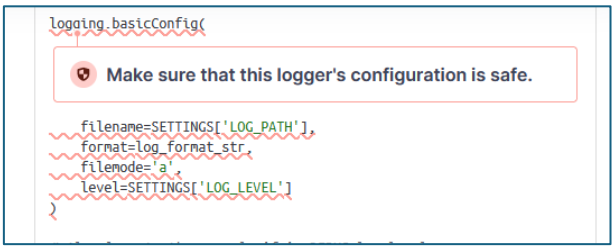

Figura 6 – Exemplo de Detalhamento de Apontamento de Segurança

Também é possível consultar os resultados das varreduras através [do site do Sonar]():

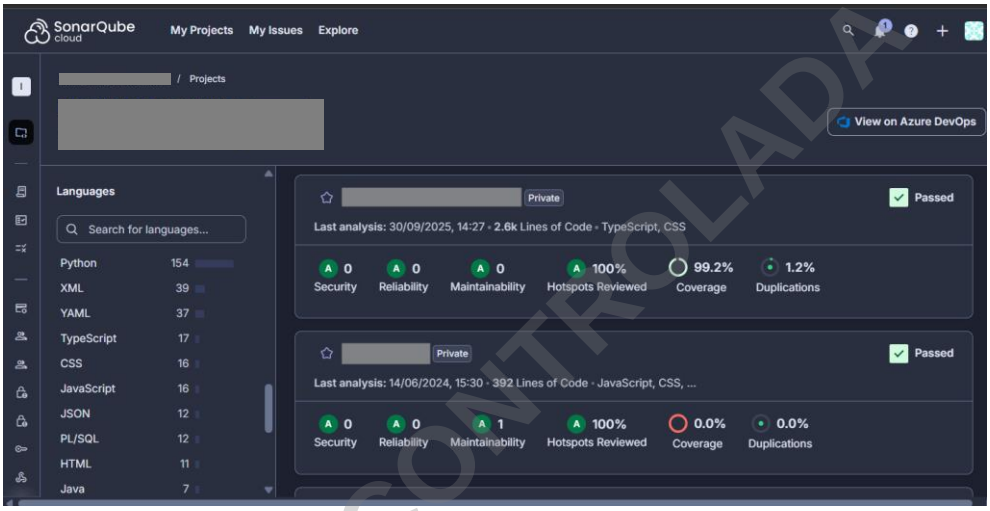

Figura 7 – Listagem de Projetos no SonarCloud

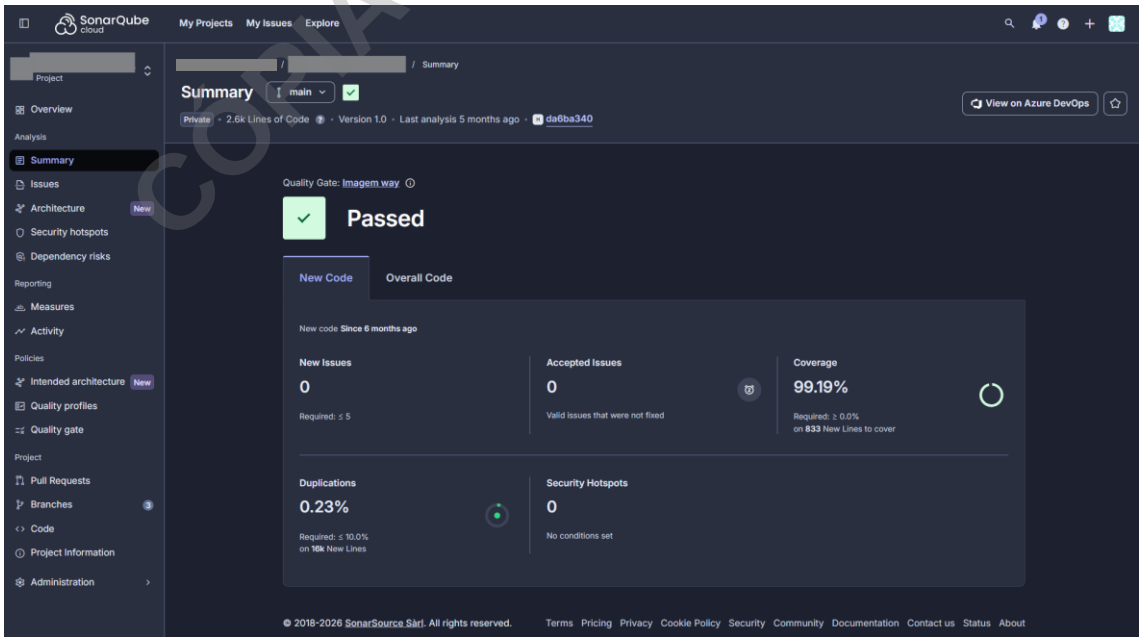

Figura 8 – Detalhes do Projeto aprovado em todos os aspectos

6.4.3. Ambientes de Desenvolvimento, Homologação e Produção

Sempre que possível, deve-se utilizar ambientes distintos para Desenvolvimento, Homologação e Produção, salvo os casos que o cliente não tenha adquirido as licenças de Homologações. A Imagem e a Esri recomendam, como boas práticas, conforme consta na documentação online, item Environment Isolation, que sejam instalados e se utilizem os ambientes de Produção, Homologação e Desenvolvimento de maneira isolada, principalmente para soluções de uso crítico.

O Ambiente de desenvolvimento e os recursos, incluindo pessoas, processos e tecnologias devem ser disponibilizados considerando os riscos associados com o desenvolvimento. Os controles aplicáveis devem considerar os riscos associados e estes são controlados conforme diretrizes estabelecidas no PR-TI-04 - Gestão de Acessos.

6.4.4. Testes

- **Requisitos Funcionais e Não Funcionais do Cliente** – as funcionalidades e demais característica solicitadas pelos clientes devem ser testadas antes da entrega para os usuários e as evidências teste devidamente armazenadas, conforme PR-PS-01- Processo de Desenvolvimento de Software.

6.5. Desenvolvimento Terceirizado

Todos os princípios, boas práticas e recomendações aplicáveis ao ciclo de vida dos projetos de desenvolvimento de software da Imagem Geosistemas devem ser comunicados, acordados e cobrados das empresas parceiras e/ou terceirizadas, pois estas regras também se aplicam a serviços executados desta forma.

As empresas parceiras e/ou terceirizadas devem garantir que seus processos e infraestrutura proporcionem um nível de segurança aceitável, devendo estes (processo e ambientes para desenvolvimento de software) serem avaliados no processo de homologação dos fornecedores (PR-TI-08 - Relacionamento com a Cadeia de Suprimentos, PR-TI-22 - Gestão de Fornecedores TIC, PR-FP-01 – Gestão de Parceiros e Fornecedores, P-FP-01 - Homologação de Parceiros de Serviços e Fornecedores).

Durante a execução de um serviço, o Gerente de Projetos da Imagem deve ser responsável por garantir que os códigos-fontes produzidos por empresas parceiras e/ou terceirizadas estejam armazenados no Microsoft DevOps da Imagem e que eles atendam aos requisitos de **NOTA A** para a varredura de vulnerabilidades, falhas de segurança e as outras definidas no SonarQube, para isso é necessário que:

- **Opção 1:** A empresa parceira e/ou terceirizada tenha uma assinatura do Sonaqube em nuvem, ao custo mensal de € 10,00, para análise de até 100 mil linhas de código-fonte. 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** (print de tela, conformes figuras 7 e 8 apresentadas anteriormente) bem como o arquivo YAML de configuração do pipeline do SonarQube e demais evidências de testes aplicáveis;

- **Opção 2:** Caso o Gerente de Projetos determine que a opção 1 não seja viável, existe a possibilidade que, após aprovação do seu Gerente de Atendimento, seja dado um acesso individual, não administrador e restrito ao projeto desenvolvido pelo parceiro e/ou terceirizado para que este possa armazenar os códigos-fontes no DevOps da Imagem, rodar os testes no SonarQube da Imagem e verificar os ajustes necessários a fim de corrigir estas inconsistências e o código-fonte atinja a **NOTA A**. O apoio de Usuário Administrador Imagem será necessário para dar os acessos e fazer as configurações iniciais necessárias. Os custos destes acessos deverão ser contabilizados no projeto;

- **Opção 3:** Caso o Gerente de Projetos determine que as opções anteriores não sejam viáveis, existe a possibilidade um profissional técnico da Imagem apoie o Gerente de Projetos na interface com o parceiro e/ou terceirizado para o armazenamento e configuração do pipeline de varredura. Caso sejam encontradas inconsistências pelo SonarQube, o código-fonte será encaminhado para que a empresa parceira e/ou terceirizada faça os ajustes necessários a fim de corrigir estas inconsistências e o código-fonte atinja a **NOTA A**. Os custos da alocação deste profissional técnico Imagem deverão ser contabilizados no projeto.

6.6. Gestão de Configuração

6.6.1. Tags no Código-Fonte

Toda vez que for necessário gerar uma versão de código-fonte para entrega a clientes, deverá ser criada uma tag identificando unicamente como estava o código-fonte no momento desta entrega.

A tag deverá ser um nome único no seu respectivo projeto, sendo criada através de funcionalidades nativas do github no Azure DevOps do projeto. Para produção, a criação da tag é obrigatória e o

formato deve ser **tag-NNN**. Para homologação, a criação da tag é **opcional** e o formato deve ser **taghom-NNN**. Abaixo segue um exemplo de criação de tag:

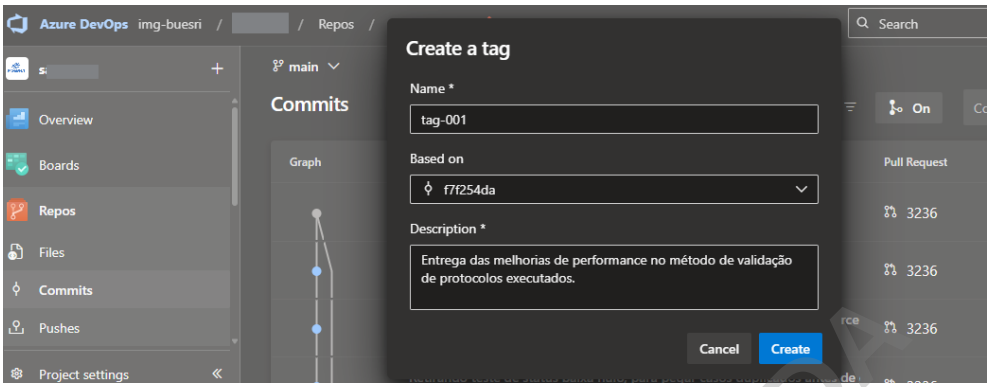

Figura 9 – Criação de uma nova tag

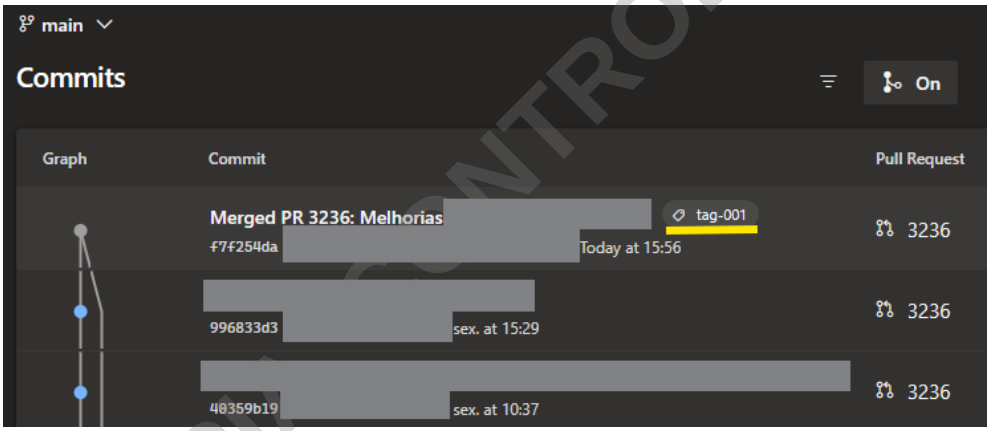

Figura 10 - Tela mostrando tag-001 associada ao código armazenado no DevOps

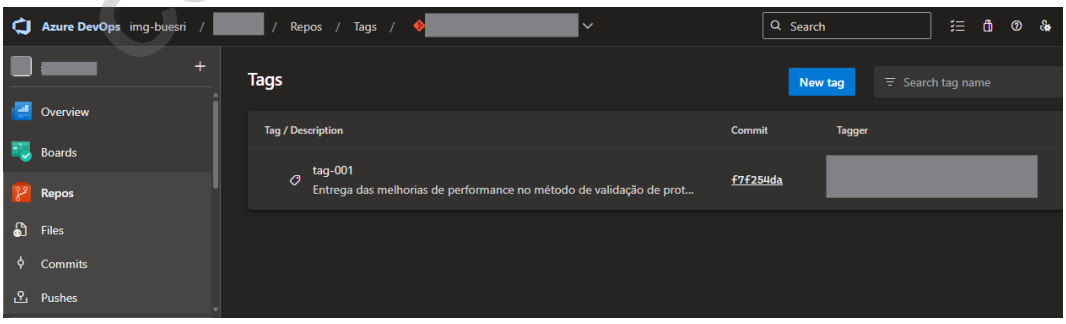

Figura 11 – Tela de consulta das tags criadas em um projeto.

A descrição da tag, no formato **tag-NNN,** para produção, e no formato **taghom-NNN,** para homologação (quando aplicável) deve constar descrita, no corpo ou título do e-mail e/ou comunicação de liberação da versão para o cliente, permitindo futuramente a consulta do código-fonte da entrega a partir da tag por quem eventualmente venha a precisar.

6.7. Evidência de Identificação do Ambiente de Testes

Sempre que aplicável, as evidências de testes funcionais registradas nos Tests Cases do DevOps ou equivalente, devem também demonstrar em qual ambiente os testes foram realizados.

Em páginas web, por exemplo, itens no ArcGIS Portal, ArcGIS Online, aplicações customizadas no ExperienceBuilder, os prints da tela devem mostrar a URL completa do item que está sendo testado.

Em execuções no servidor via Conexão Remota, o print deve mostrar a barra superior com o nome ou IP do servidor que está sendo acessado e deve também aparecer no canto inferior direito a data/hora da execução da máquina.

7. ANEXOS

- *Security Best Practices* (acessado em 24/03/2026);
- *ESRI Software Security and Privacy* (acessado em 24/03/2026);
- *A Practical Guide to ArcGIS Online Security - ESRI* (acessado em 24/03/2026).
- PR-PS-06 - Varredura Automatizada do Código-Fonte Produzido por Parceiros ou Fornecedores
- M-TI-02-Orientação do Firewall e Antivirus para Fornecedores e Parceiros de Serviços de Desenvolvimento