

# Análise Comparativa de Segurança: Plataformas de Gerenciamento de Código-Fonte

Assunto: Decisão Estratégica sobre a Plataforma de SCM (Source Code Management) On-Premise

Data: 05 de agosto de 2025

## 1. Sumário Executivo

Este documento analisa três soluções de gerenciamento de código-fonte sob a ótica da Segurança da Informação, visando selecionar a plataforma on-premise que hospedará o código-fonte dos produtos da Intelltech.

A solução atual, GitLab Community Edition (CE), apesar do custo de licença ser zero, apresenta lacunas de segurança e conformidade devido à falta de controles nativos de segurança e auditoria. A análise para a decisão se concentra em duas opções principais:

- GitLab Enterprise Edition (EE) On-Premise: Uma plataforma com abordagem integrada ("All-in-One") de DevSecOps. Seu diferencial é a unificação de ferramentas de segurança (SAST, DAST, etc) no fluxo de trabalho, o que pode simplificar a governança e a automação de políticas.
- GitHub Enterprise Server (GHES) On-Premise: Uma plataforma com reconhecida pelo controle de versão e por sua ferramenta de análise estática de código (SAST/CodeQL), que requer o complemento Advanced Security.

A escolha dependerá da prioridade estratégica da empresa: optar pela simplicidade operacional e governança unificada (foco do GitLab EE) ou pela adoção de ferramentas técnicas específicas, o que pode exigir maior esforço de integração (foco do GitHub ES).

## 2. Contexto

Dada a criticidade do código-fonte, a plataforma de SCM é um pilar da estratégia de segurança da Intelltech.




## 3. As Soluções Analisadas

Solução	Descrição Breve	Modelo
GitLab Community Edition (CE)	(Em Uso) Versão gratuita e de código aberto. Funcionalidades básicas de repositório Git.	Gratuito
GitLab Enterprise Edition (EE)	Versão paga com foco em governança, segurança e compliance. Oferece uma suíte completa de DevSecOps nativa.	Licença Paga
GitHub Enterprise Server (GHES)	Versão paga líder de mercado, com forte foco na experiência do desenvolvedor e segurança avançada (add-on).	Licença Paga + Add-on

## 4. Matriz Comparativa de Segurança

A tabela abaixo resume os recursos de cada plataforma de acordo com os critérios definidos.

Legenda:

-  Nativo e Robusto: Funcionalidade presente, madura e integrada.
-  Parcial ou via Integração: Funcionalidade existe, mas é limitada, ou requer integração com ferramentas de terceiros.
-  Ausente ou Básico: Funcionalidade inexistente ou insuficiente para uso corporativo.

Critério de Segurança	GitLab CE	GitLab EE	GitHub ES (+ Advanced Security)	Importância Estratégica
Autenticação e Autorização (SSO, MFA)	●	✓	✓	Crítica: Controla o acesso inicial à plataforma.
Controle de Permissões Granulares	✗	✓	✓	Crítica: Evita que usuários vejam ou alterem código indevidamente.
Registro e Auditoria de Atividades	✗	✓	✓	Crítica: Essencial para compliance e investigação de incidentes.
SAST (Análise de Código Estático)	✗	✓	✗ (✓ se Advanced Security incluso)	Alta: Encontra vulnerabilidades diretamente no código-fonte.
DAST (Análise de Aplicação Dinâmica)	✗	✓	●	Alta: Encontra vulnerabilidades na aplicação em execução.
Análise de Dependências	✗	✓	✗ (✓ se Advanced Security incluso)	Alta: Encontra vulnerabilidades em bibliotecas de terceiros.
Detecção de Segredos (Secrets Detection)	✗	✓	✗ (✓ se Advanced Security incluso)	Crítica: Previne o vazamento de senhas e chaves de API no código.
Automação de Políticas de Segurança	✗	✓	✓	Alta: Garante que as regras de segurança sejam aplicadas em escala.
Gestão do Ciclo de Vida de Vulnerabilidades	✗	✓	✗ (✓ se Advanced Security incluso)	Alta: Centraliza e gerencia os riscos de segurança encontrados.
Suporte a Compliance (SOC 2, ISO 27001)	✗	✓	●	Crítica: Facilita a geração de evidências para auditorias.
Suporte Técnico e SLA On-Premise	✗	✓	✓	Crítica: Garante a continuidade do negócio em caso de falhas.

## 5. Análise Detalhada por Solução: Prós e Contras

### GitLab Community Edition (CE)

- Prós:
  - Custo de licenciamento zero.
- Contras:
  - Lacunas de Segurança e Auditoria: Apresenta ausência de trilhas de auditoria, políticas de segurança, gestão de vulnerabilidades e suporte profissional.
  - Necessidade de Ferramentas Externas: Exige a contratação e integração de múltiplas ferramentas externas para atingir um nível mínimo de segurança.
  - Desafios de Conformidade: A geração de evidências para auditorias torna-se ineficiente pela falta de ferramentas nativas.

### GitLab Enterprise Edition (EE) Ultimate

- Prós:
  - Plataforma Unificada: A integração nativa de ferramentas de segurança (SAST, DAST, etc) reduz a complexidade e o custo de gerenciamento.
  - Governança Centralizada: Facilita a aplicação de regras em toda a organização por meio de Compliance Frameworks e políticas como código.
  - Visibilidade Completa: Oferece dashboards unificados para uma visão clara da postura de segurança e do ciclo de vida das vulnerabilidades.
- Contras:
  - Profundidade dos Scanners: Uma ferramenta de segurança individual pode não ser tão aprofundada quanto a solução especialista correspondente no mercado (GitHub Enterprise).

## GitHub Enterprise Server (GHES)

- Prós:
  - Ecossistema Maduro: O GitHub Actions oferece integrações e automações robustas e fáceis de usar.
  - Prós Adicionais (Se Advanced Security Incluso):
  - Análise Estática (SAST) de Destaque: O scanner CodeQL é reconhecido no mercado por sua precisão para análise estática.
  - Prevenção de Vazamento de Segredos: A funcionalidade de push protection, que bloqueia segredos antes de entrarem no repositório, é um recurso preventivo valioso.
- Contras:
  - Segurança Avançada como Add-on: As principais funcionalidades de segurança (SAST, detecção de segredos) não estão na licença base e exigem a contratação do complemento "Advanced Security", aumentando o custo total.
  - Ausência de DAST Nativo: A análise dinâmica de segurança (DAST) precisa ser adquirida e integrada separadamente.
  - Foco Menor em Gestão de Compliance: Possui menos funcionalidades explícitas para "gerenciar pacotes de conformidade" em comparação com o GitLab.

## 6. Recomendação Estratégica e Próximos Passos

A análise indica que a manutenção do GitLab CE, em motivos de segurança, não é muito sustentável. A decisão final deve ser baseada no alinhamento com a estratégia de tecnologia da Inteltech, considerando fortemente os dois modelos de plataforma a seguir.

É fundamental destacar que para o GitHub Enterprise Server ser uma solução comparável ao GitLab EE em termos de segurança proativa (SAST, Análise de Dependências, Detecção de Segredos), a contratação do complemento "Advanced Security" é indispensável. Sem ele, a plataforma não atende a diversos critérios de segurança críticos.

### **Cenário 1:**

Optar pelo GitLab Enterprise Edition representa uma evolução natural e de baixo risco, pois se trata de uma atualização da plataforma existente, não uma migração complexa. Do ponto de vista da segurança, esta escolha oferece uma suíte de DevSecOps completa e unificada ("All-in-One"). Isso centraliza a governança e a gestão de vulnerabilidades, garantindo que ferramentas como SAST e DAST funcionem de forma integrada, sem a complexidade de gerenciar múltiplos fornecedores.

Para este cenário, a escolha recomendada é: GitLab Enterprise Edition On-Premise

### **Cenário 2:**

A escolha pelo GitHub Enterprise Server implica em um projeto de migração de plataforma, com maior custo e complexidade. O principal benefício de segurança, condicionado à compra do "Advanced Security", é o acesso à ferramenta de análise estática (SAST/CodeQL) considerada a mais poderosa do mercado. Este cenário prioriza a excelência de uma ferramenta de segurança específica em detrimento de uma suíte integrada, aceitando o ônus da migração e a necessidade de contratar e integrar outras soluções, como DAST.

Para este cenário, a escolha recomendada é: GitHub Enterprise Server On-Premise, com a contratação do complemento Advanced Security.