

## **CORPORACIÓN UNIVERSITARIA MINUTO DE DIOS – UNIMINUTO**

### **ACTIVIDAD 3 - 4**

**LUIS ALIRIO TARAZONA PALACIO  
ANDRES CAMILO OSPINA PRIETO  
JUAN DAVID TELLEZ MONROY**

**DESARROLLO DE SOFTWARE SEGURO  
TUTOR: EDWIN ALBEIRO RAMOS VILLAMIL**

**BOGOTÁ D.C 03 DE OCTUBRE 2025**

## Introducción

El presente informe tiene como objetivo presentar los hallazgos relacionados con la seguridad del código fuente del proyecto de inventario tecnológico, a partir del análisis realizado con la herramienta SonarQube.

Esta herramienta permite detectar vulnerabilidades críticas, errores de seguridad y malas prácticas que pueden comprometer la integridad, confidencialidad y disponibilidad del sistema.

## DESCRIPCIÓN DEL PROYECTO: SISTEMA DE INVENTARIO TECNOLÓGICO

### OBJETIVO GENERAL

Desarrollar una aplicación web que permita la gestión eficiente de inventarios de equipos tecnológicos, facilitando el control de registros, la autenticación de usuarios y la administración de artículos, garantizando seguridad, trazabilidad y accesibilidad desde un entorno centralizado.

### Objetivos Específicos:

- Implementar un módulo de autenticación de usuarios con registro, inicio de sesión y recuperación de contraseñas.
- Desarrollar un sistema CRUD (crear, leer, actualizar y eliminar) para los artículos tecnológicos del inventario.
- Asegurar la integridad y seguridad de los datos, evitando accesos no autorizados y protegiendo la información sensible.
- Ofrecer una interfaz web amigable para la interacción de los usuarios finales.
- Permitir la escalabilidad del sistema para que pueda integrarse con otros módulos o crecer en funcionalidades futuras.

## Informe de Seguridad – Resultados de SonarQube

### Hallazgos Principales.

Durante el análisis, SonarQube identificó un total de 3 vulnerabilidades de seguridad catalogadas como “Bloqueadoras” (Blocker), lo que significa que son de máxima prioridad y requieren corrección inmediata:

#### Inyección SQL (2 bloqueadores):

- **Ubicación:** src/controllers/authController.js (líneas 24 y 46).
- **Descripción:** El código construye consultas SQL directamente con datos proporcionados por el usuario, lo que abre la posibilidad a ataques de SQL Injection.
- **Riesgo:** Un atacante podría manipular la base de datos, extraer información confidencial, modificar registros o incluso eliminar datos críticos.
- **Recomendación:** Implementar consultas preparadas (Prepared Statements) o utilizar un ORM que gestione la seguridad de las consultas de manera automática.

#### Seguridad en la configuración (1 bloqueador)

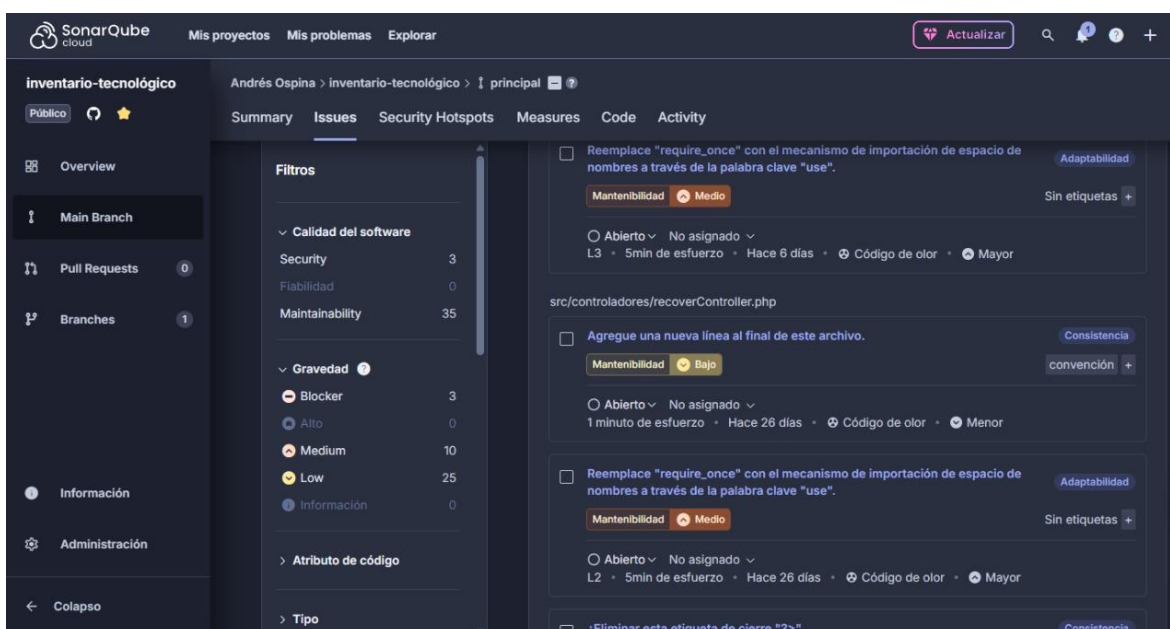
- **Ubicación:** config/db.php.
- **Descripción:** Se detectó que el archivo de configuración de la base de datos contiene credenciales inseguras o carece de protección adecuada.
- **Riesgo:** Un atacante que acceda al archivo podría comprometer las credenciales de conexión y obtener acceso completo a la base de datos.
- **Recomendación:** Establecer contraseñas seguras, almacenar credenciales en variables de entorno y restringir el acceso al archivo de configuración.

## Impacto en el Proyecto

Las vulnerabilidades encontradas tienen un impacto directo sobre la seguridad del sistema:

- Riesgo de robo o alteración de datos del inventario.
- Posible acceso no autorizado a información sensible.
- Inestabilidad del sistema si los atacantes logran manipular consultas.
- Afectación en la confianza de los usuarios y stakeholders respecto a la aplicación.

## Capturas de pantalla



**SonarQube cloud** Mis proyectos Mis problemas Explorar Actualizar 🔍 🗨️ ⚙️ +

inventario-tecnológico Andrés Ospina > inventario-tecnológico > principal ⓘ

Summary Issues Security Hotspots Measures Code Activity

**Filtros**

- Calidad del software
  - Security 3
  - Fiabilidad 0
  - Maintainability 35
- Gravedad ⓘ
  - Blocker 3
  - Alto 0
  - Medium 10
  - Low 25
  - Información 0
- Atributo de código
- Tipo

**Issues**

- ☐ ¿Eliminar esta etiqueta de cierre ">". Consistencia  
 Mantenibilidad Bajo malas prácticas por +  
 Abierto No asignado L57 2min de esfuerzo Hace 26 días Código de olor Menor
- ☐ Agregue una nueva línea al final de este archivo. Consistencia  
 Mantenibilidad Bajo convención +  
 Abierto No asignado 1 minuto de esfuerzo Hace 26 días Código de olor Menor
- ☐ Reemplace "require\_once" con el mecanismo de importación de espacio de nombres a través de la palabra clave "use". Adaptabilidad  
 Mantenibilidad Medio Sin etiquetas +  
 Abierto No asignado L3 5min de esfuerzo Hace 26 días Código de olor Mayor

**SonarQube cloud** Mis proyectos Mis problemas Explorar Actualizar 🔍 🗨️ ⚙️ +

inventario-tecnológico Andrés Ospina > inventario-tecnológico > principal ⓘ

Summary Issues Security Hotspots Measures Code Activity

**Filtros**

- Calidad del software
  - Security 3
  - Fiabilidad 0
  - Maintainability 35
- Gravedad ⓘ
  - Blocker 3
  - Alto 0
  - Medium 10
  - Low 25
  - Información 0
- Atributo de código
- Tipo

**Issues**

- ☐ Agregue una nueva línea al final de este archivo. Consistencia  
 Mantenibilidad Bajo convención +  
 Abierto No asignado 1 minuto de esfuerzo Hace 6 días Código de olor Menor
- ☐ Agregue una nueva línea al final de este archivo. Consistencia  
 Mantenibilidad Bajo convención +  
 Abierto No asignado 1 minuto de esfuerzo Hace 6 días Código de olor Menor
- ☐ Agregue una nueva línea al final de este archivo. Consistencia  
 Mantenibilidad Bajo convención +  
 Abierto No asignado 1 minuto de esfuerzo Hace 26 días Código de olor Menor

SonarQube cloud Mis proyectos Mis problemas Explorar Actualizar

inventario-tecnológico Andrés Ospina > inventario-tecnológico > principal

Summary Issues Security Hotspots Measures Code Activity

Overview

Main Branch

Pull Requests 0

Branches 1

Información

Administración

Colapso

Filtros

Calidad del software

Security 3

Fiabilidad 0

Maintainability 35

Gravedad

Blocker 3

Alto 0

Medium 10

Low 25

Información 0

Atributo de código

Tipo

Reemplace "require\_once" con el mecanismo de importación de espacio de nombres a través de la palabra clave "use". Adaptabilidad

Mantenibilidad Medio Sin etiquetas +

Abierto No asignado

L3 5min de esfuerzo Hace 26 días Código de olor Mayor

Eliminar esta etiqueta de cierre ">". Consistencia

Mantenibilidad Bajo malas prácticas por +

Abierto No asignado

L95 2min de esfuerzo Hace 26 días Código de olor Menor

src/views/agregar\_item.php

Agree una nueva línea al final de este archivo. Consistencia

Mantenibilidad Bajo convención +

Abierto No asignado

1 minuto de esfuerzo Hace 26 días Código de olor Menor

Reemplace "require\_once" con el mecanismo de importación de espacio de

SonarQube cloud Mis proyectos Mis problemas Explorar Actualizar

inventario-tecnológico Andrés Ospina > inventario-tecnológico > principal

Summary Issues Security Hotspots Measures Code Activity

Overview

Main Branch

Pull Requests 0

Branches 1

Información

Administración

Colapso

Filtros

Calidad del software

Security 3

Fiabilidad 0

Maintainability 35

Gravedad

Blocker 3

Alto 0

Medium 10

Low 25

Información 0

Atributo de código

Tipo

Reemplace "require\_once" con el mecanismo de importación de espacio de nombres a través de la palabra clave "use". Adaptabilidad

Mantenibilidad Medio Sin etiquetas +

Abierto No asignado

L3 5min de esfuerzo Hace 26 días Código de olor Mayor

Eliminar esta etiqueta de cierre ">". Consistencia

Mantenibilidad Bajo malas prácticas por +

Abierto No asignado

L39 2min de esfuerzo Hace 26 días Código de olor Menor

src/views/dashboard.php

Agree una nueva línea al final de este archivo. Consistencia

Mantenibilidad Bajo convención +

Abierto No asignado

1 minuto de esfuerzo Hace 6 días Código de olor Menor

Reemplace "require\_once" con el mecanismo de importación de espacio de

**SonarQube cloud** Mis proyectos Mis problemas Explorar Actualizar 🔍 🔔 ⚙️ +

inventario-tecnológico Andrés Ospina > inventario-tecnológico > principal

Summary **Issues** Security Hotspots Measures Code Activity

**Filtros**

- Calidad del software
  - Security 3
  - Fiabilidad 0
  - Maintainability 35
- Gravedad
  - Blocker 3
  - Alto 0
  - Medium 10
  - Low 25
  - Información 0
- Atributo de código
- Tipo

**Issues**

- ☐ Reemplace "require\_once" con el mecanismo de importación de espacio de nombres a través de la palabra clave "use". Adaptabilidad  
 Mantenibilidad Medio Sin etiquetas +  
 Abierto No asignado  
 L3 · 5min de esfuerzo · Hace 26 días · Código de olor · Mayor
- ☐ ¿Eliminar esta etiqueta de cierre ">"?. Consistencia  
 Mantenibilidad Bajo malas prácticas por +  
 Abierto No asignado  
 L40 · 2min de esfuerzo · Hace 26 días · Código de olor · Menor

src/views/inventario.php

- ☐ Agregue una nueva línea al final de este archivo. Consistencia  
 Mantenibilidad Bajo convención +  
 Abierto No asignado  
 1 minuto de esfuerzo · Hace 26 días · Código de olor · Menor
- ☐ Reemplace "require\_once" con el mecanismo de importación de espacio de nombres a través de la palabra clave "use". Adaptabilidad

**SonarQube cloud** Mis proyectos Mis problemas Explorar Actualizar 🔍 🔔 ⚙️ +

inventario-tecnológico Andrés Ospina > inventario-tecnológico > principal

Summary **Issues** Security Hotspots Measures Code Activity

**Filtros**

- Calidad del software
  - Security 3
  - Fiabilidad 0
  - Maintainability 35
- Gravedad
  - Blocker 3
  - Alto 0
  - Medium 10
  - Low 25
  - Información 0
- Atributo de código
- Tipo
- Gravedad del tipo
- Estado

**Issues**

- ☐ Agregue una nueva línea al final de este archivo. Consistencia  
 Mantenibilidad Bajo convención +  
 Abierto No asignado  
 1 minuto de esfuerzo · Hace 26 días · Código de olor · Menor

src/views/logout.php

- ☐ Agregue una nueva línea al final de este archivo. Consistencia  
 Mantenibilidad Bajo convención +  
 Abierto No asignado  
 1 minuto de esfuerzo · Hace 26 días · Código de olor · Menor

src/views/recover.php

- ☐ Agregue una nueva línea al final de este archivo. Consistencia  
 Mantenibilidad Bajo convención +  
 Abierto No asignado  
 1 minuto de esfuerzo · Hace 26 días · Código de olor · Menor

src/views/recuperar\_contraseña.php

- ☐ Agregue una nueva línea al final de este archivo. Consistencia  
 Mantenibilidad Bajo convención +  
 Abierto No asignado  
 1 minuto de esfuerzo · Hace 23 días · Código de olor · Menor

src/views/register.php

- ☐ Agregue una nueva línea al final de este archivo. Consistencia  
 Mantenibilidad Bajo convención +  
 Abierto No asignado  
 1 minuto de esfuerzo · Hace 23 días · Código de olor · Menor

38 de 38 mostrados



SonarQube cloud

Mis proyectos Mis problemas Explorar

Actualizar

inventario-tecnológico

Andrés Ospina > inventario-tecnológico > principal

Summary Issues Security Hotspots Measures Code Activity

Overview

Main Branch

Pull Requests

Branches

Información

Administración

Colapso

### Resumen de la sucursal principal

945 Líneas de código • Último análisis Hace 25 segundos • d1842fc0

Puerta de calidad: [Vía del sonar](#)

**No calculado**

El siguiente escaneo generará una Puerta de Calidad.

Seguridad	Fiabilidad	Mantenibilidad
3 Cuestiones abiertas	0 Cuestiones abiertas	35 Cuestiones abiertas

Problemas aceptados	Cobertura	Duplicaciones
0	Se necesitan algunos pasos adicionales para que SonarQube Cloud analice la cobertura de su código. <a href="#">Configurar el análisis de cobertura</a>	0,0% No se establecen condiciones en 2,8k Líneas

Puntos críticos de seguridad

4

SonarQube cloud

Mis proyectos Mis problemas Explorar

Actualizar

inventario-tecnológico

Andrés Ospina > inventario-tecnológico > principal

Summary Issues Security Hotspots Measures Code Activity

Overview

Main Branch

Pull Requests

Branches

Información

Administración

Colapso

### Filtros

Calidad del software

Security 3

Fiabilidad 0

Maintainability 35

Gravedad

Blocker 3

Alto 0

Medium 10

Low 25

Información 0

Atributo de código

Tipo

### Seleccione problemas para acciones masivas

Seleccionar problemas Navegue hasta el problema 38 cuestiones 3h 7min esfuerzo

☐ Cambiar

config/db.php

☐ Agregue una nueva línea al final de este archivo. [Consistencia](#)  
Mantenibilidad Bajo convención

☐ Abierto ☐ No asignado  
1 minuto de esfuerzo • Hace 26 días • Código de olor • Menor

☐ Agregue protección con contraseña a esta base de datos. [Responsabilidad](#)  
Seguridad Bloqueador CWB

☐ Abierto ☐ No asignado  
L7 • Esfuerzo de 45 minu... • Hace 26 días • Vulnerabilidad • Bloqueador

☐ ¿Eliminar esta etiqueta de cierre ">". [Consistencia](#)  
Mantenibilidad Bajo malas prácticas por

☐ Abierto ☐ No asignado

SonarQube cloud

Mis proyectos Mis problemas Explorar

Actualizar

inventario-tecnológico

Andrés Ospina > inventario-tecnológico > principal

Summary Issues Security Hotspots Measures Code Activity

Overview

Main Branch

Pull Requests

Branches

Información

Administración

Colapso

### Filtros

Calidad del software

Security 3

Fiabilidad 0

Maintainability 35

Gravedad

Blocker 3

Alto 0

Medium 10

Low 25

Información 0

Atributo de código

Tipo

### Seleccione problemas para acciones masivas

Seleccionar problemas Navegue hasta el problema 38 cuestiones 3h 7min esfuerzo

☐ Cambiar

público/js/scripts.js

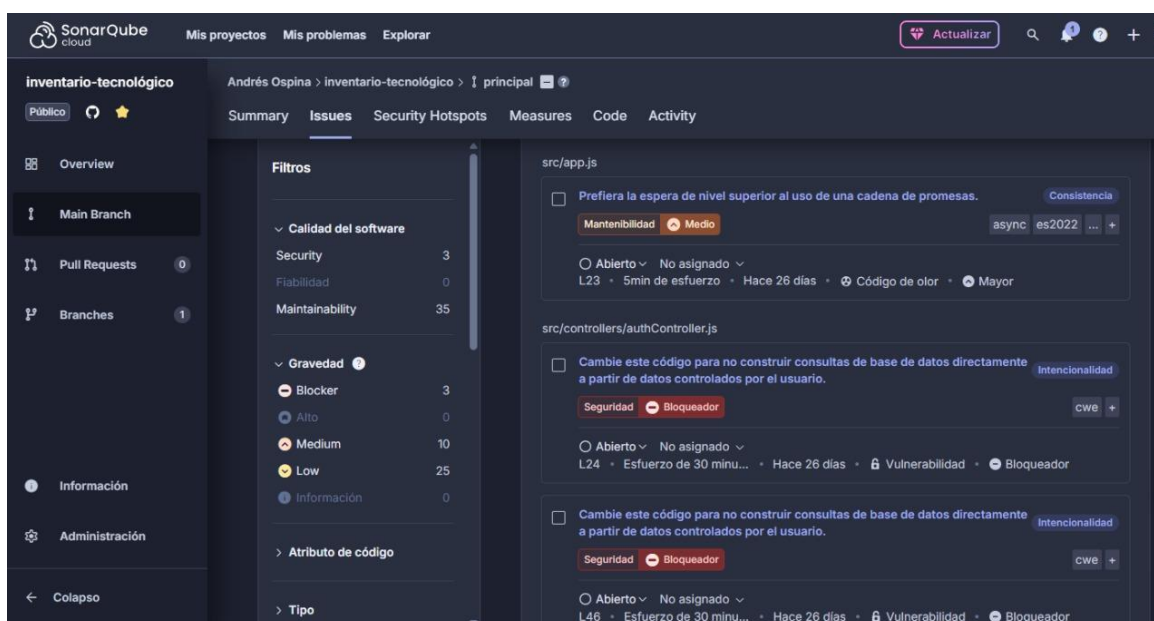
☐ Prefiera 'globalThis' a 'window'. [Consistencia](#)  
Mantenibilidad Bajo es2020 portabilidad

☐ Abierto ☐ No asignado  
L18 • 2min de esfuerzo • Hace 26 días • Código de olor • Menor

☐ Prefiera 'globalThis' a 'window'. [Consistencia](#)  
Mantenibilidad Bajo es2020 portabilidad

☐ Abierto ☐ No asignado  
L38 • 2min de esfuerzo • Hace 26 días • Código de olor • Menor

src/app.js



**SonarQube cloud** Mis proyectos Mis problemas Explorar Actualizar

inventario-tecnológico Andrés Ospina > inventario-tecnológico > principal

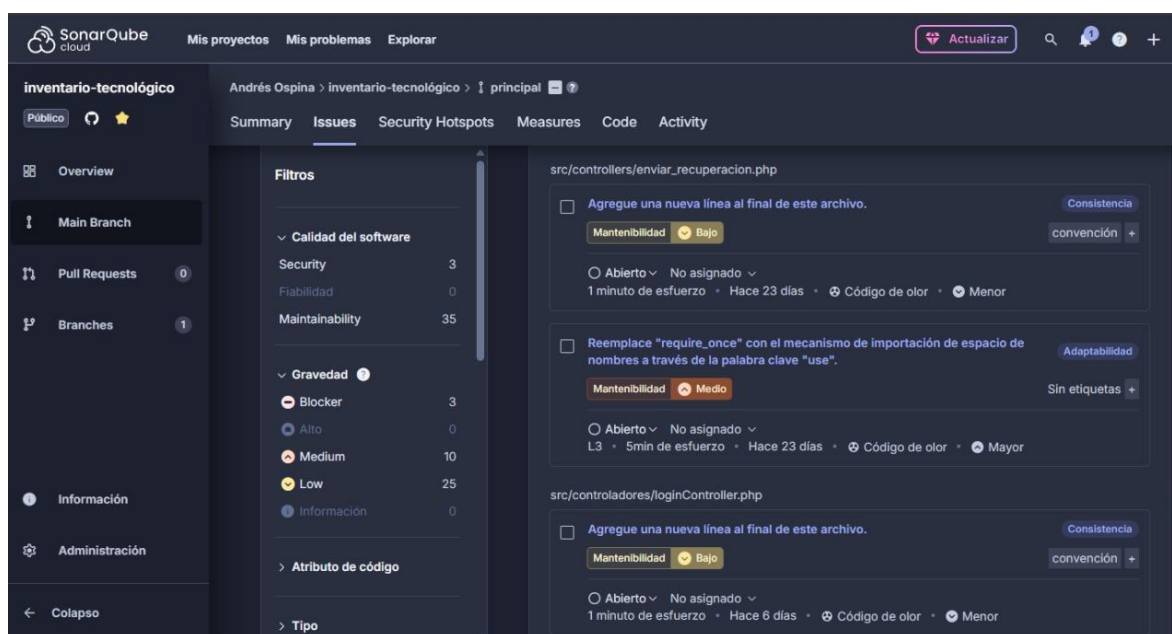
Summary **Issues** Security Hotspots Measures Code Activity

**Filtros**

- Calidad del software
  - Security: 3
  - Fiabilidad: 0
  - Maintainability: 35
- Gravedad
  - Blocker: 3
  - Alto: 0
  - Medium: 10
  - Low: 25
  - Información: 0
- Atributo de código
- Tipo

**src/app.js**

- ☐ Prefiera la espera de nivel superior al uso de una cadena de promesas. **Consistencia**
  - Mantenibilidad: Medio
  - async es2022
  - Abierto No asignado
  - L23 5min de esfuerzo Hace 26 días Código de olor Mayor
- ☐ Cambie este código para no construir consultas de base de datos directamente a partir de datos controlados por el usuario. **Intencionalidad**
  - Seguridad: Bloqueador
  - CWE
  - Abierto No asignado
  - L24 Esfuerzo de 30 minu... Hace 26 días Vulnerabilidad Bloqueador
- ☐ Cambie este código para no construir consultas de base de datos directamente a partir de datos controlados por el usuario. **Intencionalidad**
  - Seguridad: Bloqueador
  - CWE
  - Abierto No asignado
  - L46 Esfuerzo de 30 minu... Hace 26 días Vulnerabilidad Bloqueador



**SonarQube cloud** Mis proyectos Mis problemas Explorar Actualizar

inventario-tecnológico Andrés Ospina > inventario-tecnológico > principal

Summary **Issues** Security Hotspots Measures Code Activity

**Filtros**

- Calidad del software
  - Security: 3
  - Fiabilidad: 0
  - Maintainability: 35
- Gravedad
  - Blocker: 3
  - Alto: 0
  - Medium: 10
  - Low: 25
  - Información: 0
- Atributo de código
- Tipo

**src/controllers/enviar\_recuperacion.php**

- ☐ Agregue una nueva línea al final de este archivo. **Consistencia**
  - Mantenibilidad: Bajo
  - convención
  - Abierto No asignado
  - 1 minuto de esfuerzo Hace 23 días Código de olor Menor
- ☐ Reemplace "require\_once" con el mecanismo de importación de espacio de nombres a través de la palabra clave "use". **Adaptabilidad**
  - Mantenibilidad: Medio
  - Sin etiquetas
  - Abierto No asignado
  - L3 5min de esfuerzo Hace 23 días Código de olor Mayor

**src/controladores/loginController.php**

- ☐ Agregue una nueva línea al final de este archivo. **Consistencia**
  - Mantenibilidad: Bajo
  - convención
  - Abierto No asignado
  - 1 minuto de esfuerzo Hace 6 días Código de olor Menor

Enlace prueba front y backend

<https://youtu.be/jdcsWWHrkoY>

## Conclusión

La incorporación de normas de calidad de software y el seguimiento de herramientas como SonarQube constituyen un pilar esencial para el éxito de cualquier proyecto de desarrollo. Los hallazgos de seguridad y mantenibilidad no deben verse como obstáculos, sino como oportunidades para mejorar el producto y garantizar un software seguro, confiable y sostenible en el tiempo, también el implementar las mejoras propuestas no solo beneficia al equipo de desarrollo al facilitar el mantenimiento y la escalabilidad.

## Referencias

- Pragma. (2021, 19 de agosto). *Conoce las 8 ventajas de SonarQube*.  
Pragma. <https://www.pragma.co/es/blog/conoce-las-8-ventajas-de-sonarqube>  
[pragma.co](https://www.pragma.co)
- Sentries. (s. f.). *Qué es SonarQube: Verifica y analiza la calidad de tu código*.  
Sentries. <https://sentries.io/blog/que-es-sonarqube/> [Sentries](https://sentries.io)