

**Informe técnico sobre análisis de código estático para el**

**Sistema ÁGORA**

**Versión 1.0**

**Perito:**



**Nombre: Laura Marcela Estévez Joya**

**Cedula: 1049647364**

**Email: laura.estevez@usantoto.edu.co**

**Contenido del informe**

[1. Propósito de la evaluación 2](#_Toc43331355)

[2. Producto a evaluar 2](#_Toc43331356)

[3. Especificación de la(s) herramientas usadas para medición 2](#_Toc43331357)

[4. Especificación de la Norma de calidad 3](#_Toc43331358)

[5. Requerimientos específicos de calidad funcionales y técnicos. 3](#_Toc43331359)

[5.1. Análisis de cumplimiento 4](#_Toc43331360)

[6. Atributos de calidad. 4](#_Toc43331361)

[6.1. Asignación de puntajes para atributos de calidad. 5](#_Toc43331362)

[6.2. Atributos internos. 5](#_Toc43331363)

[6.2.1. Tamaño de sistemas y código fuente (20%) 5](#_Toc43331364)

[6.2.2. Complejidad del software(20%) 5](#_Toc43331365)

[6.2.3. Deuda técnica (20%) 5](#_Toc43331366)

[6.2.4. Seguridad(20%) 5](#_Toc43331367)

[6.2.5. 3d code metrics (20%) 5](#_Toc43331368)

[6.3. Atributos Externos. 5](#_Toc43331369)

[6.3.1. Usabilidad (20%) 5](#_Toc43331370)

[6.3.2. Fiabilidad (30%) 6](#_Toc43331371)

[6.3.3. Mantenibilidad (50%) 6](#_Toc43331372)

[7. Recomendaciones y conclusiones 6](#_Toc43331373)

[7.1. Seguridad 6](#_Toc43331374)

[7.2. Confiabilidad 6](#_Toc43331375)

[7.3. Usabilidad 6](#_Toc43331376)

[8. Bibliografía 6](#_Toc43331377)

[9. Firma del perito. 6](#_Toc43331378)

# Propósito de la evaluación

Es importante tener en cuenta al momento de crear código fuente que, no solo su funcionamiento y compilación son importantes, sino también la calidad del código, es decir; evitar y corregir errores de escritura de código, bugs, código duplicado, código muerto, vulnerabilidades, entre otros.

Por tal razón, por medio de un analizador estático de código, se hizo una inspección de este al presente proyecto para evidenciar que no presentara ninguno de los errores anteriormente mencionados y así poder medir la calidad del mismo o en su defecto evitar estas “malas prácticas” de escritura de código para futuras versiones y mantener una calidad aceptable.

# Producto a evaluar

La Universidad Distrital Francisco José de Caldas, en su marco de contratación requirió de un sistema que permitiera al público del sector comercial dar a conocer los productos y servicios que ofrecen para promover relaciones mercantiles favoreciendo a ambas partes: a la universidad para satisfacción de una necesidad y a las personas para que den a conocer sus productos. El Sistema de Registro Único de Personas y Banco de Proveedores ÁGORA, cuenta con la versión 1.0 y con seis módulos que son:

* Módulo Acceso.
* Módulo Registro (Persona Natural y Persona Jurídica, Actividades Económicas).
* Módulo Actualización Persona.
* Módulo Gestión Actividades Económicas.
* Módulo Certificados.
* Módulo Gestión Usuario.

# Especificación de la(s) herramientas usadas para medición

Para el análisis que se realizó al código del presente proyecto se usaron dos herramientas: SONARQUBE y SonarScanner.

**SONARQUBE**: es una herramienta para la inspección automática de código fuente que busca errores, malas prácticas de escritura de código o incidentes. Posteriormente, realiza un cálculo estadístico de los mismos y genera posibles métricas que pueden ayudar a mejorar la calidad del código.

* Versión 8.3.1 para Windows.
* SonarScanner – Versión 4.3 para Windows.

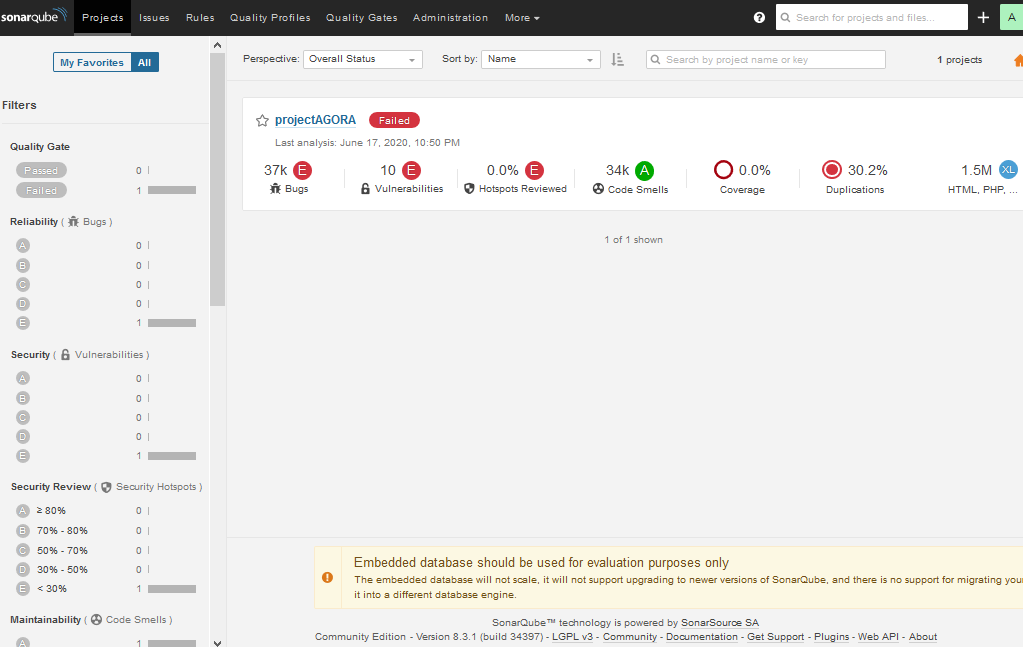


Figura 1. Pantalla Principal SonarQube

# Especificación de la Norma de calidad

La norma ISO 25000 es sumamente importante ya que nos orienta a un buen manejo y cumplimiento de normas para la recolección de requisitos de calidad de software y evaluación. Esta norma es importante implementarla en todos los proyectos y productos, debido a que contiene especificaciones y criterios a nivel global lo cual asegura calidad, seguridad y eficiencia para estos. Está compuesta por:

* ISO 2500n: gestión de calidad.
* ISO 2501n: modelo de calidad: fiabilidad, seguridad, mantenibilidad y usabilidad.
* ISO 2502n: medición de calidad.
* ISO 2503n: requisitos de calidad.
* ISO 2504n: evaluación de calidad.

# Requerimientos específicos de calidad funcionales y técnicos.

La empresa requiere que se evalué los siguientes requerimientos funcionales y técnicos específicos

|  |  |  |
| --- | --- | --- |
| Ítem | Requerimiento de calidad | Prioridad |
| 1 | Que el software pueda funcionar en sistemas operativos Android, MacOS, Windows XP, Windows 7 y Windows 10 (en 32 y 64 bits) | Alta |
| 2 | Que permita trabajar en forma rápida e intuitiva (cuente con ayudas visuales y auditivas interactivas en el software). | Alta |
| 3 | Que tenga soporte multiidiomas, especialmente inglés y español | Media |
| 4 | Que permita adecuar su estilo de visualización para adecuarse a personas con limitaciones visuales (Ley 1680 de 20 de noviembre de 2013) | Baja |
| 5 | Implementación de Ley 1581 del 2012 – Protección de datos (HABEAS DATA) | Alta |
| 6 | Permita generar reportes en EXCEL Y PDF. | Alta |
| 7 | Funcionalidad/modulo para reportar errores técnicos o funcionales desde el software. | Baja |
| 8 | Permitir acceso a 100 usuarios simultáneos | Alta |
| 9 | Tolerancia a fallos (caída de red, apagones eléctricos frecuentes). | Media |
| 10 | Integración con office | Alta |
| 11 | Cumplimiento del 80% con el estándar OWASP, priorizando en las vulnerabilidades de robo de información, XSS, SQL injection y ransomware. | Alta |
| 12 | Capacidad de respaldo y recuperación de información desde el software. | Media |
| 13 | El software debe demandar mínimos recursos de hardware (cpu Intel celeron, 2 gigas de Ram) | Alta |

## Análisis de cumplimiento

|  |  |  |
| --- | --- | --- |
| **Ítems** | **Porcentaje de cumplimiento** | **Análisis** |
| El software funciona en sistemas operativos Android, MacOS, Windows XP, Windows 7 y Windows 10 (en 32 y 64 bits) | 100% | - |
| Permite trabajar en forma rápida e intuitiva (cuente con ayudas visuales y auditivas interactivas en el software). | 100% | - |
| Tiene soporte multiidiomas, especialmente inglés y español | 50% | - La plataforma cuenta con un único idioma(español)  **- Recomendación:** implementar el idioma inglés en la mayoría de la plataforma(2meses/3’500.000) |
| Permite adecuar su estilo de visualización para adecuarse a personas con limitaciones visuales (Ley 1680 de 20 de noviembre de 2013) | 0% | - La plataforma no se adecua a la Ley 1680 del 20 de noviembre de 2013.  - **Recomendación:** adaptar la plataforma para personas con limitaciones visuales(1mes/2’000.000) |
| Implementa la Ley 1581 del 2012 – Protección de datos (HABEAS DATA) | 100% | - |
| Permite generar reportes en EXCEL Y PDF. | 100% | - |
| Funcionalidad/modulo para reportar errores técnicos o funcionales desde el software. | 0% | - La plataforma no cuenta con un módulo para reportes de errores y fallas técnicas.  - **Recomendación:** Crear módulo en el cual el usuario pueda hacer reporte de errores y fallas técnicas.(15días/800.000) |
| Permite acceso a 100 usuarios simultáneos | 100% | - |
| Tolerancia a fallos (caída de red, apagones eléctricos frecuentes). |  |  |
| Integración con office | 100% | - |
| Cumplimiento del 80% con el estándar OWASP, priorizando en las vulnerabilidades de robo de información, XSS, SQL injection y ransomware. | 60% | **-** Señala riesgos como *exposición de datos sensibles* y *mala configuración de seguridad.*  **- Recomendación:** hacer mejor uso del protocolo SSL/TLS el cual se usa para el cifrado de mensajes de punto a punto(servidor-cliente) |
| Capacidad de respaldo y recuperación de información desde el software. | 100% | - |
| El software debe demandar mínimos recursos de hardware (cpu Intel celeron, 2 gigas de Ram) | 100% | - |

# Atributos de calidad.

Los atributos de calidad que se utilizarán para la evaluación del Software ÁGORA, de acuerdo a lo especificado en el siguiente cuadro:

*Tabla 1 Atributos de calidad*

|  |  |
| --- | --- |
| ATRIBUTOS INTERNOS | Características del software que determinan su habilidad para satisfacer las necesidades propias e implícitas. |
| ATRIBUTOS EXTERNOS | Características del software que determinan su habilidad para satisfacer las necesidades explicitas e implícitas. |
| ATRIBUTOS EN USO | Características del software que determinan los requerimientos de los usuarios finales de manera que satisfagan sus necesidades. |

## Asignación de puntajes para atributos de calidad.

Los puntajes establecidos a los atributos de calidad seleccionados de acuerdo a las necesidades, se muestran en la siguiente tabla:

*Tabla 2, Asignación de pesos sobre la medición de atributos.*

|  |  |
| --- | --- |
| Tipo de atributo | Puntaje |
| Atributos internos | 65 |
| Atributos externos | 35 |
| Total | 100 |

## Atributos internos.

### Tamaño de sistemas y código fuente (20%)

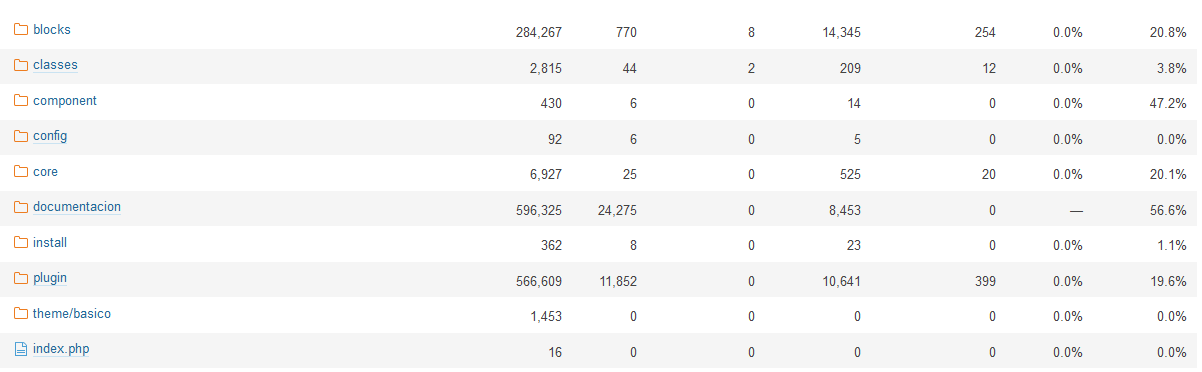
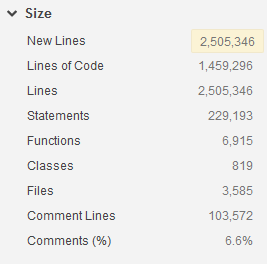
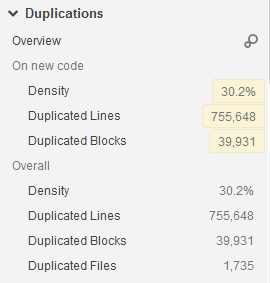
Figura 2. Información General de Código Fuente.

Figura 2.1. Información General de Código Subdividido

* **Líneas de Código y Densidad de Comentarios - Duplicidad de Código**

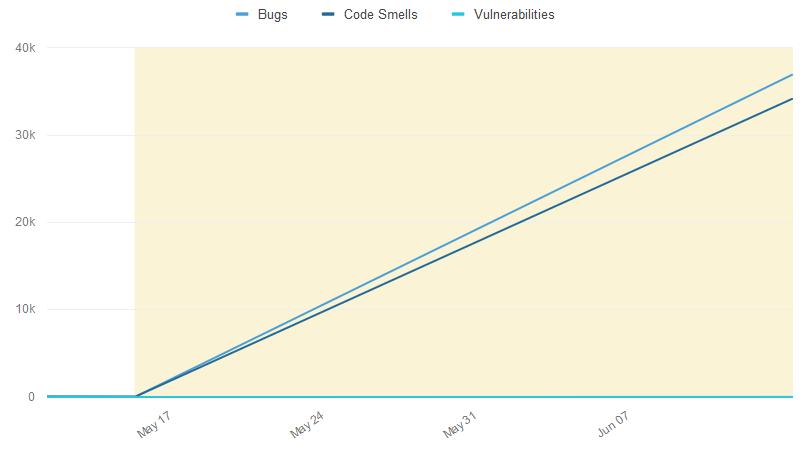
Figuras 3 y 4. Código

Figura 5. Bugs vs CodeSmells vs Vulnerabilities

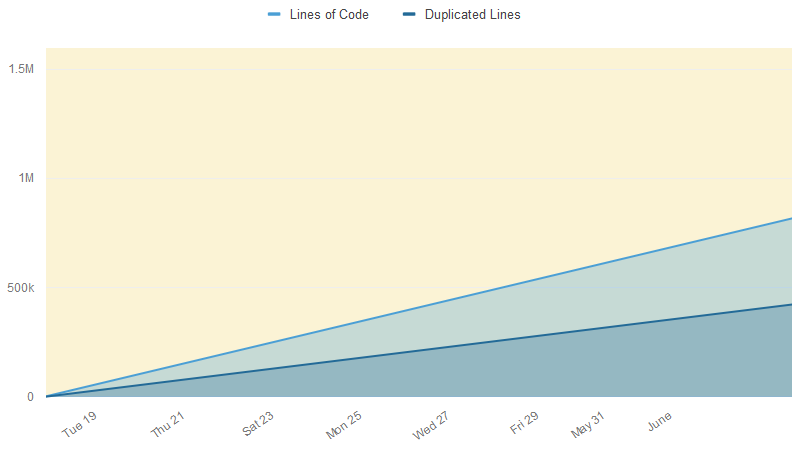
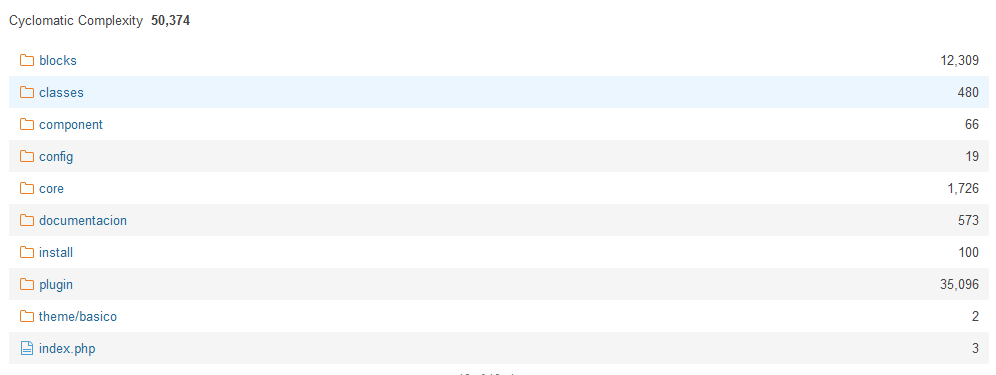


Figura 5.1. Líneas de Código vs Líneas duplicadas.

### Complejidad del software (20%)

Figura 6. Complejidad Ciclomática y Cognitiva

* **Complejidad Ciclomática:**



* **Complejidad Cognitiva**

### Deuda técnica (20%)

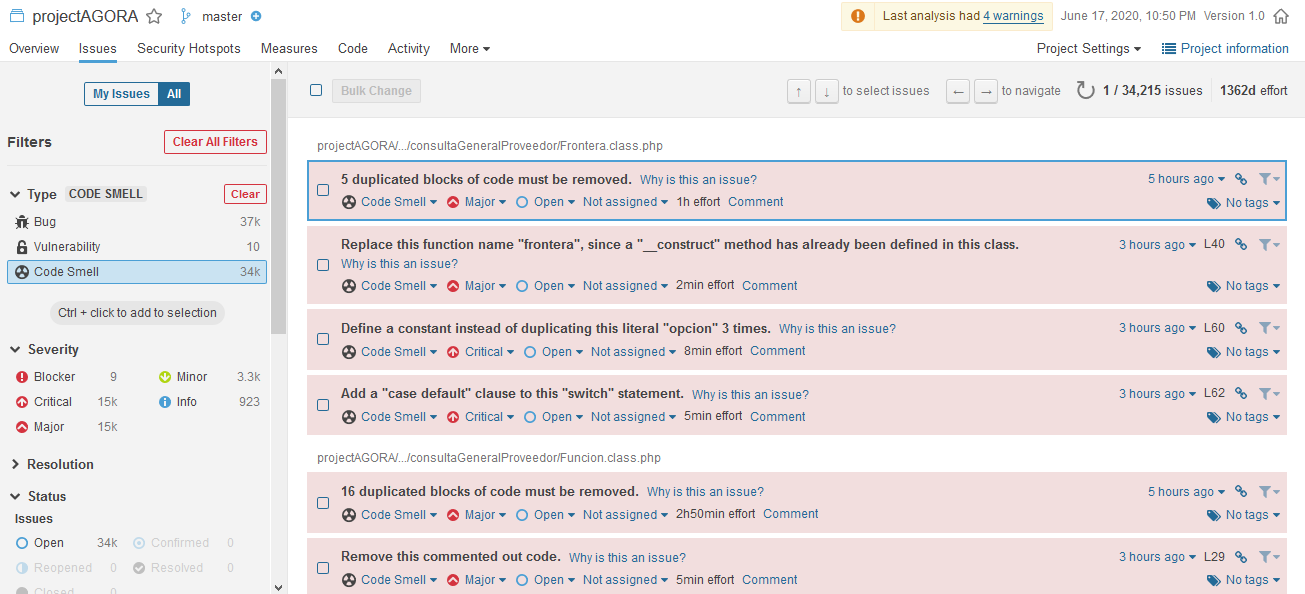
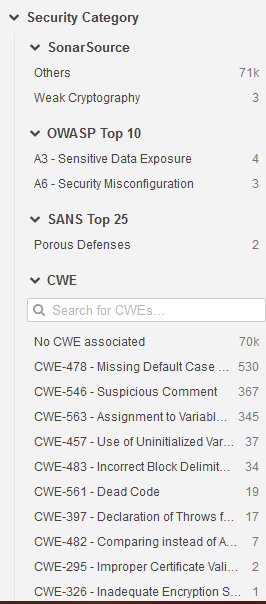
**Código Smell:** 34.215 issues

Figura 7. Código Smell

### Seguridad (20%)

Figura 8. Vulnerabilidades



### 3d Code Metrics (20%)

## Atributos Externos.

* **Efectividad:** (90%) La parte gráfica de la plataforma es intuitiva y fácil de usar, pero pienso que podría ser más llamativa(bonita).
* **Eficiencia:** (100%) La funcionalidad de la plataforma en cuento a botones, ventanas emergentes, formularios es correcta y además es coherente con el nombre de los objetos.
* **Satisfacción:** (90%) La comodidad y aceptabilidad de la plataforma no es muy amigable, como ya había dicho antes, podría tener una apariencia estética diferente, más llamativa.

### Fiabilidad (30%)

Al ser un proyecto construido en base al framework SARA, creo que tiene todas las precauciones medidas y necesarias para evitar cualquier tipo de error o fallo, ya que, al hacer uso de este framework requiere datos y configuraciones como base, soporte e inicio para el uso del mismo.

### Mantenibilidad (50%)

Las posibles configuraciones que puedan requerir o existir en el sistema no son muy difíciles de llevar a cabo, ya que el sistema en su mayoría se basa en diligenciamiento de formularios y cargue de datos a una base de datos. En cuanto a documentación y comentarios del código sería importante que fueran más específicos.

# Recomendaciones y conclusiones

## Seguridad: Teniendo en cuenta los resultados que arrojó el SonarQube respecto a las vulnerabilidades del sistema, se pudo observar que encuentra un fallo en el protocolo SSL/TLS el cual se usa para el cifrado de mensajes de punto a punto(servidor-cliente), exposición y baja seguridad de datos, lo cual puede repercutir ante los responsables de la construcción de la plataforma por ello es importante superar estos fallos por bien del cliente como de la universidad.

## Confiabilidad: Basándonos en resultados del análisis de seguridad y vulnerabilidades el sistema Ágora podría sufrir algún robo de datos tanto del cliente como de su empresa.

## Usabilidad: La plataforma es intuitiva y fácil de usar, pero el aspecto gráfico podría ser mejorado y contener más mensajes de alerta, información o de error.

# Bibliografía

* <http://repository.udistrital.edu.co/bitstream/11349/3816/7/ANEXO%20F%20-%20FRAMEWORK%20SARA.pdf>
* <https://funcionarios.portaloas.udistrital.edu.co/agora/>

# Firma del perito.

|  |  |
| --- | --- |
| **Responsable de la evaluación** | **Firma** |
| Nombre: Laura Marcela Estévez Joya  Empresa: EC-Software  Cargo: Desarrolladora  GitHub: laura-zevetse |  |