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

**Factura Scripts**

**Versión 1.0**

**Perito:**



**Nombre: Andres Felipe Medina Lozano**

**Cedula: 1.002.725.524**

**Email: andres.medina@usantoto.edu.co**

**Contenido del informe**

[1. Propósito de la evaluación 2](#_Toc43387663)

[2. Producto a evaluar 2](#_Toc43387664)

[3. Especificación de la(s) herramientas usadas para medición 2](#_Toc43387665)

[4. Especificación de la Norma de calidad 3](#_Toc43387666)

[5. Requerimientos específicos de calidad funcionales y técnicos. 4](#_Toc43387667)

[6. Atributos de calidad. 5](#_Toc43387668)

[6.1. Asignación de puntajes para atributos de calidad. 5](#_Toc43387669)

[6.2. Atributos internos. 5](#_Toc43387670)

[6.2.1. Tamaño de sistemas y código fuente (20%) 5](#_Toc43387671)

[6.2.2. Complejidad del software(20%) 6](#_Toc43387672)

[6.2.3. Deuda técnica (20%) 6](#_Toc43387673)

[6.2.4. Seguridad (20%) 8](#_Toc43387674)

[6.2.5. 3d code metrics (20%) 9](#_Toc43387675)

[6.3. Atributos Externos. 10](#_Toc43387676)

[6.3.1. Usabilidad (20%) 10](#_Toc43387677)

[6.3.2. Fiabilidad (30%) 10](#_Toc43387678)

[6.3.3. Mantenibilidad (50%) 10](#_Toc43387679)

[7. Recomendaciones y conclusiones 10](#_Toc43387680)

[7.1. Seguridad 10](#_Toc43387681)

[7.2. Confiabilidad 11](#_Toc43387682)

[7.3. Usabilidad 11](#_Toc43387683)

[8. Bibliografía 11](#_Toc43387684)

[9. Firma del perito. 11](#_Toc43387685)

# Propósito de la evaluación

El propósito de realizar un control o evaluación de calidad del software es mantener bajo control por medio de la medición de calidad de la serie de procesos de desarrollo que cumpla con normas y parámetros con el fin que fue diseñado, además revisa que los requisitos levantados para el software cumplan su propósito, sean técnicos y funcionales y cómo se comporta la aplicación con el usuario (Rendimiento). Se verifica que cumplan con la norma ISO 25000, la evaluación se basa en tres atributos de calidad.

* Internos
* Externos
* En uso

Para los cuales se asignan puntajes o calificación con los que se concluye el porcentaje de calidad del software, junto con recomendaciones especiales respecto a seguridad, confiabilidad y usabilidad de dicho código.

# Producto a evaluar

FacturaScripts es un programa de contabilidad y facturación con el fin de ayudar a las empresas con todo el tema de sus finanzas y así tener un mayor control. Con él podrá gestionar el día a día de su empresa (Abierto a muchas Empresas): pedidos, facturas, factura electrónica, recibos, contabilidad, contactos, tienda online y un largo etcétera. La versión a evaluar es la versión 1.0

# Especificación de la(s) herramientas usadas para medición

La herramienta utilizada para la evaluación es SonarQube versión 8.3.1, la cual fue instalada en mi equipo por medio de Docker y a su vez sonar-scanner junto con el plugin 3D Code Metrics y SoftVis 3D Viewer para visualizar el software como una ciudad. SonarQube se eligió para esta práctica debido a que es una herramienta de revisión automática de código para detectar errores, vulnerabilidades y código maloliente. Esta herramienta se puede integrar a un flujo de trabajo existente para permitir la inspección continua de código en todas las ramas de un proyecto y solicitudes de extracción. [1]

SonarQube es la herramienta líder para inspeccionar continuamente la calidad y seguridad del código, debido que cubre 27 lenguajes de programación, al mismo tiempo que se empareja con nuestro canal de software existente, SonarQube proporciona una guía de remediación clara para que los desarrolladores entiendan y solucionen problemas y para los equipos en general para ofrecer un software mejor y más seguro.

SonarQube admite una práctica de inspección continua. Por lo tanto, viene con todo lo necesario para respaldar la práctica, una puerta de calidad, gestión de fugas, análisis de sucursales, procesamiento de informes paralelos, funciones de gobierno, alta disponibilidad, un ciclo de retroalimentación corto y más. [2]

* Un servidor SonarQube que inicia 3 procesos principales:
* Servidor web para desarrolladores y gerentes, para explorar imágenes de calidad y configurar la instancia de SonarQube.
* Servidor de búsqueda, basado en búsqueda elástica para realizar búsquedas posteriores desde la interfaz de usuario.
* Servidor de motor de cómputo, a cargo de procesar informes de análisis de código y guardarlos en la base de datos SonarQube.
* Una base de datos SonarQube para almacenar:
* La configuración de la instancia de SonarQube (seguridad, configuración de complementos, etc.)
* Las imágenes de calidad de proyectos, vistas, etc.
* Múltiples complementos SonarQube instalados en el servidor, que posiblemente incluyan complementos de idioma, SCM, integración, autenticación y gobierno.
* Uno o más Sonar Scanners que se ejecutan en sus Servidores de Integración Compuesta / Continua para analizar proyectos. [2]

SonarQube proporciona una puerta GO/NO-GO para la promoción de aplicaciones. La puerta de calidad es una característica importante ya que proporciona la capacidad de saber en cada análisis si una aplicación aprueba o no los criterios de lanzamiento. En otras palabras, en cada análisis nos indica si una aplicación está lista para la producción "en términos de calidad".

Asimismo, la experiencia de SonarQube se puede aumentar con complementos, esta herramienta tiene disponibles más de 60 complementos comerciales y comunitarios, lo que facilita mejorar la experiencia con idiomas, métricas y páginas adicionales. Los complementos también se pueden desarrollar para satisfacer necesidades específicas dentro de una organización. [2]



**Imagen 1**. Biblioteca de complementos. [2]

# Especificación de la Norma de calidad

La norma ISO/IEC 25000 Se le conoce como SQuaRE (System and Software Quality Requirements and Evaluation, esta es una familia de normas cuyo objetivo principal es evaluación de la calidad de un producto.

Esta ISO ha sido un proceso evolutivo de otras normas anterior como los es ISO/IEC 9126 la cual nos describe las características de un modelo de calidad de software también es familiar de la ISO/IEC 14598, la cual nos habla de los procesos de evaluación del software la ISO 2500 se encuentra compuesta por 5 divisiones

Una ventaja que encontramos en dicha norma, facilita delimitar la definición del software a evaluar, así como mejora la calidad del software, ya que la evaluación se realiza en todos los aspectos de dicho producto



**Imagen 2**. Biblioteca de complementos.

# 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). | Media |
| 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) | Alta |
| 5 | Implementación de Ley 1581 del 2012 – Protección de datos (HABEAS DATA) | Alta |
| 6 | Permita generar reportes en EXCEL Y PDF. | Baja |
| 7 | Funcionalidad/modulo para reportar errores técnicos o funcionales desde el software. | Media |
| 8 | Permitir acceso a 100 usuarios simultáneos | Alta |
| 9 | Tolerancia a fallos (caída de red, apagones eléctricos frecuentes). | Media |
| 10 | Integración con office | Baja |
| 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) | Media |

1. La aplicación es multi plataforma por que permite ser instalada en un hosting o almacenamientos propios, puede ser virtualizada en Docker y lanzarse como contenedor lo que permite que pueda funcionar en cualquier Sistema operativo y hasta en la nube 100%.
2. El software es entendible, debido a que tiene una interfaz sencilla muy amigable con el usuario. El porcentaje de cumplimiento es del 100%.
3. El software cuenta con una configuración regional predeterminada para el idioma español (Según la Zona horaria), aunque también tiene una configuración regional (Para otros idiomas) en este caso se tiene el idioma inglés. El porcentaje de cumplimiento es del 100%.
4. El software no se adecua a diferentes estilos de visualización ni tampoco a limitaciones visuales, por lo cual no cumple con la Ley 1680 del 20 de noviembre de 2013. Siendo así, el porcentaje de cumplimiento es del 0%. Realizar implementación, debe agregarse una configuración que permita que los usuarios adecuen los colores de visualización según sea pertinente para cada una de sus limitantes visuales; además, añadir un módulo lector (sintetizador de voz), el cual proporcionaría una versión hablada del software y permita que los usuarios puedan interactuar con el mismo por medio de escucha. El tiempo estimado para su puesta en marcha es de cuatro meses y en costos de $15.000.000.
5. El software en cuanto a la Ley 1581 del 2012, no pide autorización del tratamiento de datos ya que realiza facturas, pedidos, tiendas en ningún apartado del software vi que hiciera o le informara al usuario sobre el tratamiento de datos personales (Pero para este caso no es necesario según la ley colombiana) Sin embargo, no informan al usuario sobre cuál es el tratamiento que utilizarán para tratar sus datos, ni tampoco la identificación del responsable del tratamiento. El porcentaje de cumplimiento es del 0%. Recomiendo informar al usuario o sus clientes que se debe informar el cómo se van a tratar sus datos y si la empresa se hace responsable de los mismos para evitar líos jurídicos a futuro.
6. El software permite mostrar reportes que son generados por el mismo, pero no permite generarlos como documentos, pero si muestra un XML (Para facturación electrónica) lo que permite generar archivos en pdf y Excel. Siendo así, el porcentaje de cumplimiento es del 50%. El estimado en tiempo para implementarlo es de a semana y en costo es de $1.100.000.
7. El software no reporta cuales fueros los errores técnicos ni funcionales. El porcentaje de cumplimiento es del 10%. Para agregar el módulo se necesita de 1 mes y tiene un costo de $10.000.000.
8. El software permite alrededor de 102 usuarios simultáneos depende también de la cantidad de recursos para la maquina o el hosting donde se almacena, por lo que el porcentaje de cumplimiento es del 100%.
9. El software tiene una alta tolerancia a fallos, puesto que tiene un controlador en la nube predeterminado vinculado a la implementación del disco en la nube lo que permite que el fallo como apagones eléctricos y falta de internet no afecte el sistema ya que su almacenamiento está en un servidor. El porcentaje de cumplimiento es del 100%.
10. El software permite mostrar reportes mediante XML, pero no tiene ninguna integración con office. El porcentaje de cumplimiento es del 0%. El tiempo estimado de integración es de 2 semanas y un valor de $2.300.000.
11. Todos los componentes del software tienen su razón de ser, asimismo, el software verifica la identidad del usuario así que sólo los que están autorizados pueden iniciar sesión y sus datos son enviados en forma segura debido a que todos los datos de sesión se cifran antes de almacenarse, Laravel ejecuta automáticamente todo el cifrado, además transforma las consultas SQL a un sistema MVC lo que no permite procesar consultas SQL directamente y así proteger el software de la inyección SQL. También tiene una especificación de la cantidad de minutos para que la sesión permanezca activa antes de que caduque el cual es 120 y tiene la configuración si se desea que caduque inmediatamente al cerrar el navegador. El software no tiene puertas traseras. El porcentaje de cumplimiento es del 75%. El tiempo estimado para la implementación es de 2 meses y tendría un costo de $18.000.000.
12. La capacidad de respaldo y recuperación de información del software es buena, porque cuenta con varias tecnologías lo que permite hasta un respaldo en nube. Por lo tanto, el porcentaje de cumplimiento es del 100%.
13. El software no necesita una gran cantidad de recursos de hardware para funcionar de manera nativa en un equipo ni en la nube ni en un contenedor Docker. El porcentaje de cumplimiento es del 100%.

# Atributos de calidad.

Los atributos de calidad que se utilizaran para la evaluación del Software Facturas Script, de acuerdo a lo especificado en el siguiente cuadrado:

*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:

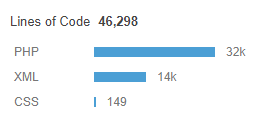
*Tabla 2, Asignación de pesos sobre la medición de atributos.*

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

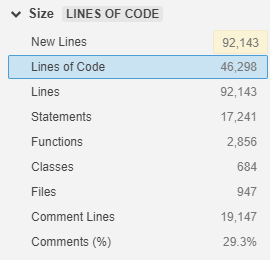
## Atributos internos.

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

Este software cuenta con 92.143 líneas, de las cuales son: 46.298 líneas de código (LoC), 19.147 líneas de código con comentarios (CLoC); 17.241 líneas de código de declaraciones;2.856 líneas de código de funciones; 684 líneas de código de clases



**Imagen 3**. Líneas de código

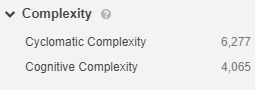


**Imagen 4**. Elementos Líneas de código

### Complejidad del software(20%)

Dentro de esta sección se evalúan los elementos correspondientes a la complejidad ciclomática y cognitiva de la siguiente manera:

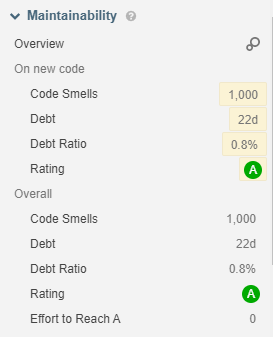
* Complejidad celomática: Es calculada por SonarQube en función del número de rutas a través del código. Siempre que el flujo de control de una función se divide, el contador de complejidad se incrementa en uno. Este cálculo varía ligeramente según el idioma porque las palabras clave y las funcionalidades lo hacen. [5]
* Complejidad cognitiva: es una nueva métrica formulada para medir con mayor precisión la comprensibilidad relativa de los métodos. Al hacerlo, aborda las deficiencias de la complejidad ciclomática en esta área. [6]



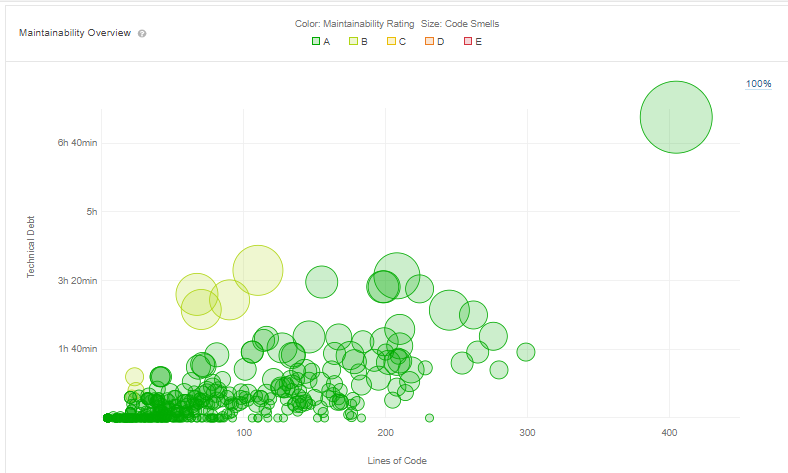
**Imagen 5**. Complejidad Ciclomatica y Cognitiva

### Deuda técnica (20%)

* 1000 líneas de código mal oliente (Code Smells, un problema de mantenimiento que hace que el código sea confuso y difícil de mantener),
* 1.099 bugs (un error de codificación que romperá el código y debe corregirse de inmediato) y una deuda técnica de 5 días y 4 horas.
* La categoría de mantenibilidad es A, debido a que el radio de deuda técnica es 0%, siendo este menor al 10% recordemos que se considera un proyecto sano.



**Imagen 5**. Mantenibilidad



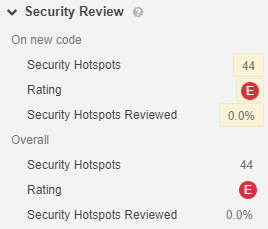
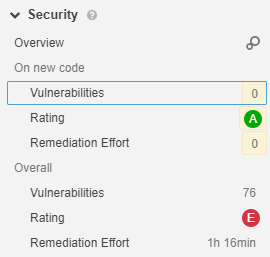
**Imagen 6**. Grafica de mantenibilidad

**Imagen 6**. Grafica de rentabilidad.

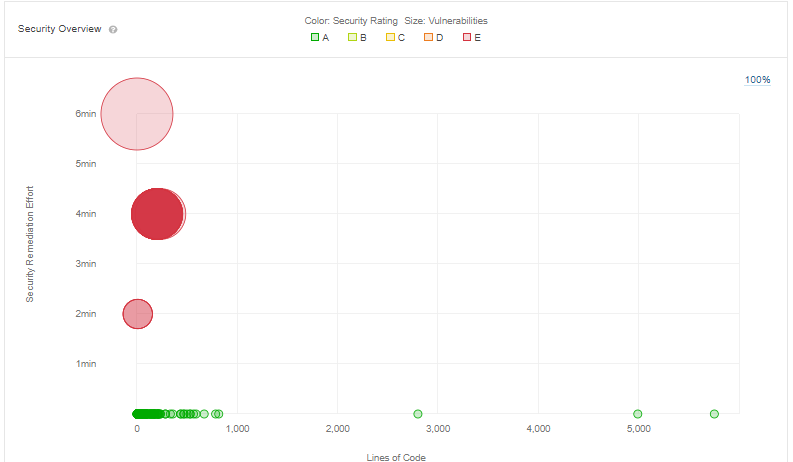
### Seguridad (20%)

Partiendo de que los puntos de accesos encontrados fueron cero podemos decir que el software es sensible en ciertos fragmentos de código, pero en general no se encuentra comprometida la aplicación, es robusta, pero con cosas por corregir, el auditor verifica si se deben realizar correcciones en esta parte si es necesarias, pero se debe hacer por alguien experto, en cuanto a la vulnerabilidades son las falla descubiertas al momento del test lo que nos muestra las brechas de seguridad que tiene la aplicación estas correcciones deben hacerse de inmediato ya que no es óptimo entregar una aplicación con problemas de seguridad, dentro de estas vulnerabilidades se encontraron inyección de código con un nivel alto lo que quiere decir que es grande esta vulnerabilidad, denegación de servicio con un nivel medio entre otras.

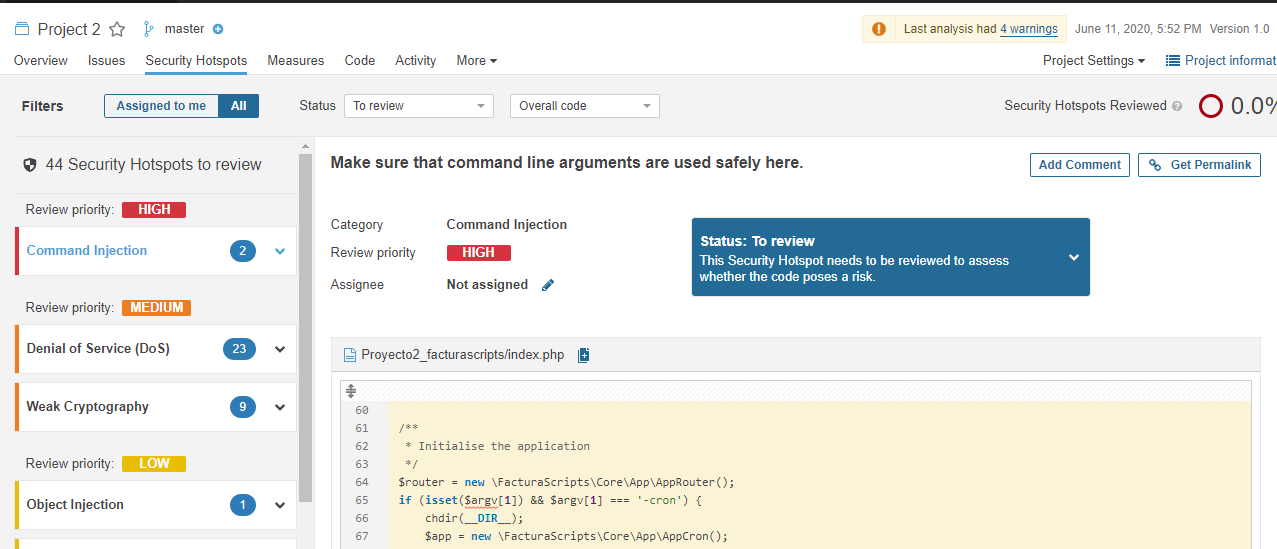
En cuanto el apartado de seguridad de la evaluación se encontraron en general 76 vulnerabilidades y nos muestra que eso hace que se posicione en la categoría E.



**Imagen 7**. Vulnerabilidades y puntos de acceso.



**Imagen 8**. Grafica de seguridad en la visión general.

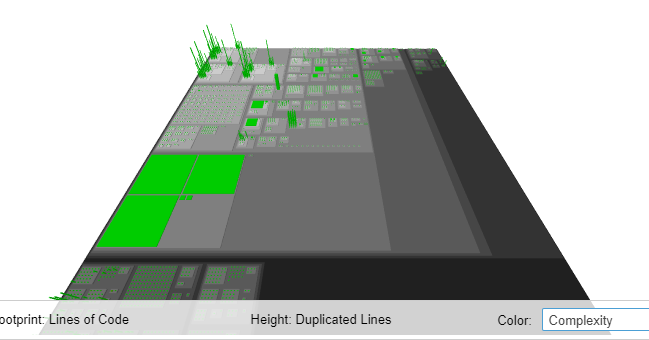


**Imagen 9**. Tipos de vulnerabilidades y nivel de prioridad

### 3d code metrics (20%)



**Imagen 10**. Complejidad ciclomatica vs líneas de codigo.



**Imagen 11**. Líneas de código vs líneas dupolicadas.

## Atributos Externos.

### Usabilidad (20%)

● En cuanto a la efectividad podemos decir que cuenta con botones fáciles de identificar y visualmente agradable, es un software desarrollado muy bien por que cuenta con cada módulo y los separa de manera que hace que sea intuitiva, a mi parecer hace falta una descripción de por que ha fallado el programa en algunas partes.

● El software es eficiente, cumple el objetivo con el cual fue desarrollado y es ayudar en las fibnazas de la empresa, es practico la información que muestra es concreta, tiene tiempos de respuestas adecuados lo cual lo hace ser muy eficiente.

● Como usuario es cómodo al usarse es simple, pero sin dejar de ser una aplicación robusta, necesita muy poca capacitación.

### Fiabilidad (30%)

En este apartado se encontraron mucha falencia cuenta con algunos bugs lo cual lo posiciono en la categoría C, puede afectar su funcionamiento de cierta manera, pero nada que una actualización no corrige.

### Mantenibilidad (50%)

Mostro que es fácil para ser modificado, ya sea para hacer correcciones de bugs o vulnerabilidades como agregación de más módulos de la aplicación lo que quiere decir que lo hace escalable, tiene un poco de Code Smell, pero se puede enmendar.

# Recomendaciones y conclusiones

## Seguridad

Se encontraron algunas brechas en la seguridad, pero que pueden ser corregidas con algunas actualizaciones, no cuenta con la mejor seguridad, pero tampoco es la peor, podemos decir que se encuentra en una categoría media en seguridad, pero aún le falta mucho para que sea un poco mas robusta en cuanto a la seguridad. No cumple con algunos estándares de la OSWAP ya que encontramos Inyección de código y denegación de servicio en la evaluación.

## Confiabilidad

Podemos catalogar en una escala del uno al diez como un seis, ya que la aplicación necesita algunas mejoras si hablamos de los bugs vimos que tiene con algunas líneas de código, lo cual hace que la aplicación no tenga un nivel de confianza óptimo para el cliente

## Usabilidad

Podemos hablar que la usabilidad es buena pero aun le faltan algunas características necesarias que exige la ley colombiana como lo es adaptar el software para la persona que tiene discapacidades cognitivas, lo cual es un punto clave a tener en cuenta, mas por lo abierto a usarse en múltiples empresas que pueden contar con personal con discapacidad visual. Desde mi concepto el software cumple con su propósito que es mantener las finanzas de una empresa llevando a cabo facturas, factura electrónica, recibos, contabilidad, contactos, es practico, sencillo visualmente agradable ya que al ser desarrollado con laravel permite una interfaz agradable a nuestros usuarios.

# Conclusiones generales

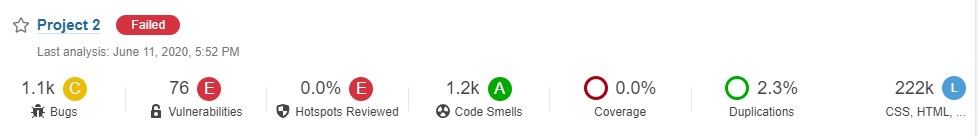
*Atributos internos 62%:*

* Tamaño de sistemas y código fuente: el valor se obtuvo debido a que la densidad de comentarios esta dentro de los rangos establecidos el cual es 20% y el 80% deberían ser líneas de código. Siendo así, 80 \* 0.2 = 16%.
* Complejidad del software: la complejidad media por clase mayor encentrada fue de 29, lo cual indica que está en el rango entre 21 y 50, para estar así en la categoría de un software complejo y de alto riesgo. 50 \* 0.2 = 10%.
* Deuda técnica: puedo decir que la deuda técnica es moderada debido a que no sobrepasa la semana, siendo así, 75 \* 0.2 = 15%.
* Seguridad: en este ámbito, encontramos múltiples vulnerabilidades las cuales son necesarias de corregir lo antes posible, 40 \* 0.2 = 8%.
* 3D code metrics = el plugin nos mostró el código de software para entenderlo con mayor facilidad, por tanto, 100 \* 0.2 = 20%.

*Atributos externos 75%:*

* Usabilidad: 65 \* 0.2 = 13%.
* Fiabilidad: 55 \* 0.3 = 16.5%.
* Mantenibilidad: 90 \* 0.5 = 45%

El porcentaje total de calidad del software de facturación es entonces:



# Bibliografía

[1] Documentación en el panel de control de SonarQube, http://localhost:9000/documentation

[2] Documentación SonarQube 8.3, https://docs.sonarqube.org/latest/

# Firma del perito.

|  |  |
| --- | --- |
| **Responsable de la evaluación** | **Firma** |
| Nombre: Andres Felipe Medina Lozano  Empresa: Nortic  Cargo: Auditor de calidad  GitHub: https://github.com/afml9954/dockerfile.git |  |