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

**Zafiro** **Versión 1.0**

**Perito:**

**Nombre: Ericka Julieth Sora Quintero**

**Cedula: 1007226350**

**Email: ericka.sora@usantoto.edu.co**

foto

**Contenido del informe**

[1. Propósito de la evaluación 2](#_heading=h.gjdgxs)

[2. Producto a evaluar 2](#_heading=h.30j0zll)

[3. Especificación de la(s) herramientas usadas para medición 2](#_heading=h.1fob9te)

[4. Especificación de la Norma de calidad 2](#_heading=h.3znysh7)

[5. Requerimientos específicos de calidad funcionales y técnicos. 2](#_heading=h.2et92p0)

[6. Atributos de calidad. 3](#_heading=h.3dy6vkm)

[6.1. Asignación de puntajes para atributos de calidad. 3](#_heading=h.1t3h5sf)

[6.2. Atributos internos. 3](#_heading=h.4d34og8)

[6.2.1. Tamaño de sistemas y código fuente 3](#_heading=h.2s8eyo1)

[6.2.2. Complejidad del software 3](#_heading=h.17dp8vu)

[6.2.3. Deuda técnica 3](#_heading=h.3rdcrjn)

[6.2.4. Seguridad 3](#_heading=h.26in1rg)

[6.3. Atributos Externos. 3](#_heading=h.lnxbz9)

[6.3.1. Usabilidad 3](#_heading=h.35nkun2)

[6.3.2. Fiabilidad 4](#_heading=h.1ksv4uv)

[6.3.3. Mantenibilidad 4](#_heading=h.44sinio)

[7. Recomendaciones y conclusiones 4](#_heading=h.2jxsxqh)

[7.1. Seguridad 4](#_heading=h.z337ya)

[7.2. Confiabilidad 4](#_heading=h.3j2qqm3)

[7.3. Usabilidad 4](#_heading=h.1y810tw)

[8. Bibliografía 4](#_heading=h.4i7ojhp)

[9. Firmas de evaluadores. 4](#_heading=h.2xcytpi)

# Propósito de la evaluación

*Este documento se realiza con el objetivo principal de evidenciar falencias encontradas en el proyecto Zafiro, y para posteriormente, llevar a cabo una actualización y mejora de errores en futuras versiones. Igualmente, en el documento se plasma con la mayor claridad posible los ítems evaluados, especificaciones de la herramienta que se usó para la medición, atributos de calidad entre muchos otros aspectos. Se les recomienda a los elaboradores recibir las observaciones hechas hacia el codigo que respetuosamente se generaron a través del proceso de dicha evaluación y donde se observan claras fallas con respeto de aplicar buenas prácticas de programación.*

# Producto a evaluar

*El producto que se evaluará a continuación es una aplicación (SCIREBOX) que tiene como propósito suministrar soluciones eficientes a nivel tecnológico en cuanto a sistemas de facturación e inventario; se desea prestar un servicio que sea totalmente preciso e intuitivo y que además cumpla los estándares de calidad. Este software está diseñado sobre la tecnología JavaFX y utilizando la arquitectura de software MVC, además está compuesto de varios módulos que permiten su funcionamiento (facturación e inventario), y entre ellos: generación de reportes, sistema de login, ventas, productos, créditos, impuestos entre otros.*

# Especificación de la(s) herramientas usadas para medición

*Para la evaluación de este producto se utilizó la herramienta SonarQube; es una plataforma de evaluación hacia la calidad del codigo fuente, donde se realiza un análisis estático para el software y muy probablemente sin ejecutarlo. Se utilizó la versión Community de descarga la cual abraca un total de 15 lenguajes dentro de su soporte. El objetivo de esta plataforma radica en evidenciar y advertir acerca de diferentes aspectos que deben mejorarse en el producto final para obtener la menor falencia posible en el codigo. Nos ayuda en aspectos como codigo duplicado, codigo muerto, estándares de codificación, bugs, complejidad ciclomatica, comentarios entre otros. Una vez que este ya instalado el SonarQube se procede a instalar y configurar un escáner que sea apropiado para sus necesidades. Sonar-Scanner posee integración SCM con la cual se crea asignación automática de problemas, anotación de codigo en el visor de codigo y detección de codigo nuevo. Git y SVN son compatibles de forma predeterminada. SonarQube también nos brinda una configuración avanzada del motor de seguridad el cual detecta cuando los datos son manipulados por un usuario de forma malintencionada que también se denominan datos contaminados, se le brinda al usuario la oportunidad de agregar elementos a su configuración personalizada como la fuente, para personalizar el motor de seguridad SonarQube, necesita alimentar los datos de configuración de seguridad a través de los parámetros dados a los SonarScanners.*

# Especificación de la Norma de calidad

Primeramente, se reseña la palabra modelo como un punto de referencia o ejemplar que se debe seguir o imitar por su precisión, y calidad como una apreciación que se le hace a un producto respecto al nivel de satisfacción de un usuario. Por tanto, un modelo de calidad es un conjunto de prácticas que están vinculadas a procesos de gestión y desarrollo de proyectos. Modelo de calidad de un software es un conjunto de buenas prácticas para el ciclo de vida del software. En relación con la calidad del software aparece las normas ISO/IEC 25000, que proporciona una guía para el uso de estándares internacionales SQuaRE. Esta Norma ISO/IEC 25000 se toma como base o guía para medir la calidad de un producto puesto que, está compuesta por 5 divisiones: gestión de calidad, modelo de calidad, mediciones de calidad, requisitos de calidad y evaluación de calidad, donde por cada división se evalúan minuciosamente aspectos puntuales e importantes para al final obtener un producto de la mejor calidad.

# Requerimientos específicos de calidad funcionales y técnicos.

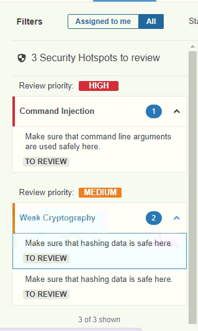
La empresa requiere que se evalué los siguientes requerimientos funcionales y técnicos específicos

|  |  |  |
| --- | --- | --- |
| 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). | Media |
| 3 | Que tenga soporte multiidiomas, especialmente inglés y español | Baja |
| 4 | Que permita adecuar su estilo de visualización para adecuarse a personas con limitaciones visuales (Ley 1680 de 20 de noviembre de 2013) | Media |
| 5 | Implementación de Ley 1581 del 2012 – Protección de datos (HABEAS DATA) | Alta |
| 6 | Permita generar reportes en EXCEL Y PDF. | media |
| 7 | Funcionalidad/modulo para reportar errores técnicos o funcionales desde el software. | Alta |
| 8 | Permitir acceso a 100 usuarios simultáneos | baja |
| 9 | Tolerancia a fallos (caída de red, apagones eléctricos frecuentes). | Alta |
| 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. | media |
| 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. El software cumple con compatibilidad en todos los sistemas operativos ya que su plataforma principal es web. se puede acceder a él mediante cualquier navegador de internet.
2. Obtuvo calificación Alta, no se logró explorar el frontEnd del programa a profundidad, pero basada en archivos fxml y estilos Css cuenta con ayudas visibles e intuitivas
3. No se encontró en un archivo que permita determinar si cuenta con soporte multi idioma. En este caso se recomienda crear ficheros .properties con los nombres de las etiquetas de nuestro vocabulario y sus traducciones a mostrar en el software, o bien incluirlas en un fichero ya existente.
4. Se encuentra con tamaño de letra adecuado y además contiene varias señalizaciones intuitivas que pueden servir de ayuda para personas con limitaciones visuales (Ley 1680 de 20 de noviembre de 2013)
5. Existe un archivo que especifica a los usuarios la políticas términos y condiciones de privacidad;

además, se nota un claro proceso de encriptación de datos en la base de datos.

1. Si permite generar reportes PDF
2. Primeramente, en caso de no haber conexión a la base de datos el software se lo informa al usuario, en el proceso de login, en caso de no poder crear, eliminar, imprimir, cerrar etc.
3. No se encontró archivos que permitan comprobar acceso a 100 usuarios simultáneos
4. Los datos se encuentran en la nueve, en caso de fallos o apagones no se afectará de mayor manera.
5. se encuentran archivos que comprueban integración con office
6. Existe una alerta de seguridad por command injection, criptografía débil y otras 15 vulnerabilidades en los controllers.



1. El software basa su información en la base de datos, esta cuenta con el respaldo directo desde la nube

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| mÍte | Requerimiento de calidad | % de implementacion | Costo $ | Tiempo de implementación |
| 1 | Que el software pueda funcionar en sistemas operativos Android, MACOs, Windows XP, Windows 7 y Windows 10 (en 32 y 64 bits) | 100% | --------- | ------ |
| 2 | Que permita trabajar en forma rápida e intuitiva (cuente con ayudas visuales y auditivas interactivas en el software). | 90% | $100000 | 5 días |
| 3 | Que tenga soporte multi idiomas, especialmente inglés y español | 0% | $150.000 | 1 días |
| 4 | Que permita adecuar su estilo de visualización para adecuarse a personas con limitaciones visuales (Ley 1680 de 20 de noviembre de 2013) | 30% | $480.000 | 3 días |
| 5 | Implementación de Ley 1581 del 2012 – Protección de datos (HABEAS DATA) | 100% | ------------ | ------- |
| 6 | Permita generar reportes en EXCEL Y PDF. | 50% | $300000 | 3 días |
| 7 | Funcionalidad/módulo para reportar errores técnicos o funcionales desde el software. | 100% | -------------- | -------- |
| 8 | Permitir acceso a 100 usuarios simultáneos | 20% | $480.000 | 4 días |
| 9 | Tolerancia a fallos (caída de red, apagones eléctricos frecuentes). | 100% | ------------- | -------- |
| 10 | Integración con office | 100% |  | n/a |
| 11 | Cumplimiento del 80% con el estándar OWASP, priorizando en las vulnerabilidades de robo de información, XSS, SQL injection y ransomware. | 50% | $300.000 | 3 días |
| 12 | Capacidad de respaldo y recuperación de información desde el software. | 100% | ------------- | ------- |
|  | | **Total:** | **$1.810.000** | **16**  **días** |

Atributos de calidad.

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

*Tabla 1 Atributos de calidad*

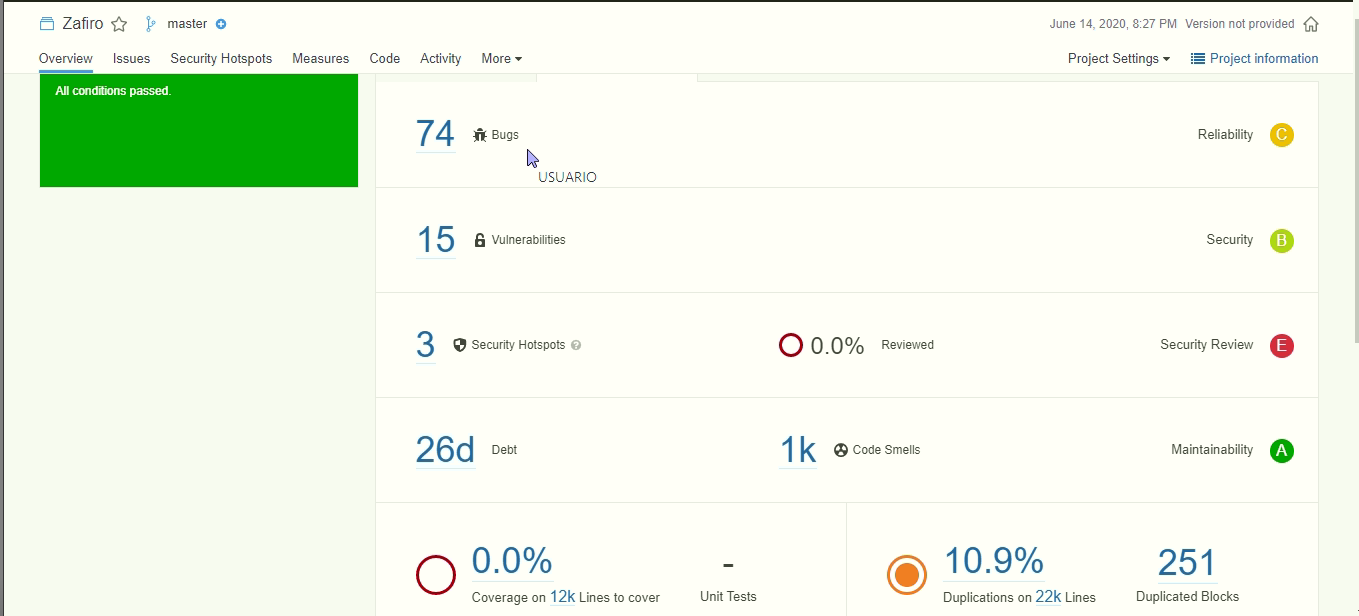
|  |  |
| --- | --- |
| ATRIBUTOS INTERNOS | Características del software que determinan su habilidad para satisfacer las necesidades propias e implícitas. |
| ATRIBUTOS EXTERNOS | Características del software que determinan su habilidad para satisfacer las necesidades explicitas e implícitas. |
| ATRIBUTOS 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.*

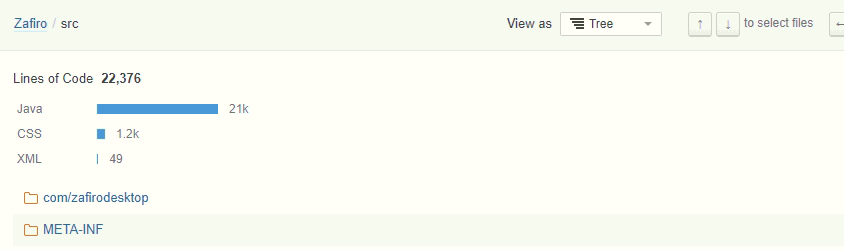
|  |  |
| --- | --- |
| Tipo de atributo | Puntaje |
| Atributos internos | 65 |
| Atributos externos | 35 |
| Total | 100 |



## Atributos internos.

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

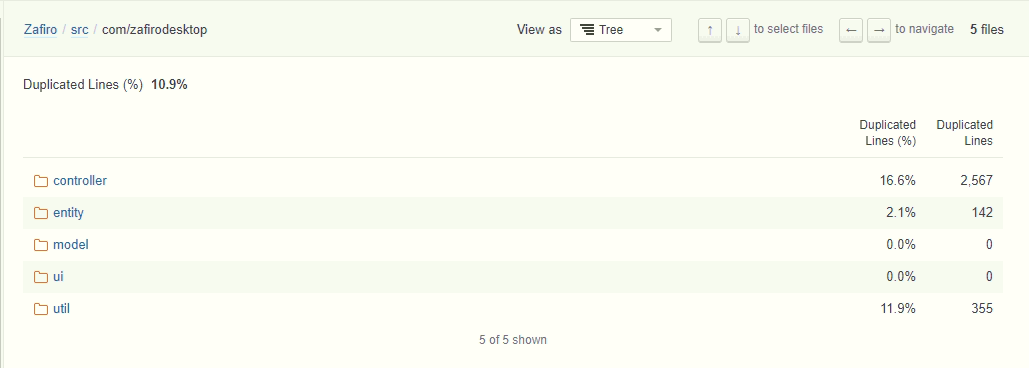
* Tenemos 22376 lineas de codigo



* Tenemos 1.570 lineas de codigo donde entity es el modulo que tiene mas funciones



* Codigo duplicado 10.9% (3064 Líneas). En controller se encuentra el mayor número de duplicidad

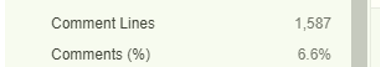


* La densidad de comentarios es de 66%(1587)

*DoC* = *CLoC /* (*LoC* + *CLoC*)

DoC = 1587/(22376+1587) =0,066

DoC=6,6%

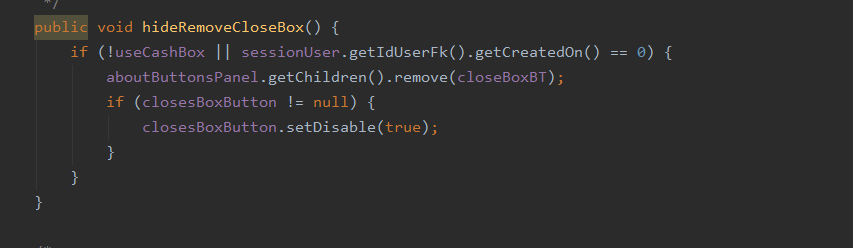


### Complejidad del software(20%)

* COMPLEJIDAD SIMCLOMATICA: Se puede notar que se tiene una complejidad ciclomatica de 3.373 donde



* Ejemplo sacado del controller:



El cual tiene:

***v*(*g*) = *e - n* + 2**

**n =6**

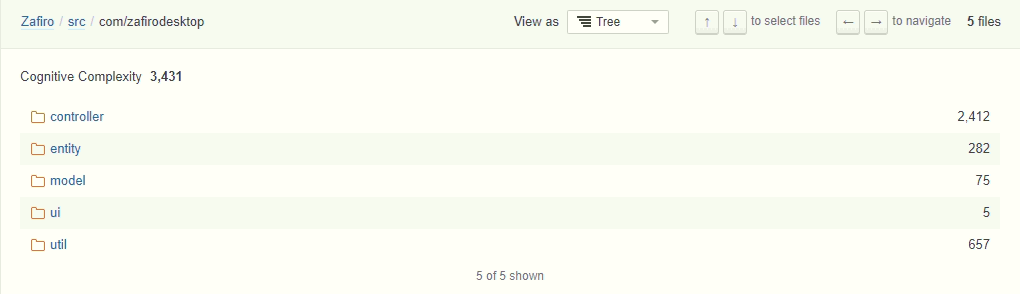
**e =6**

**v(g)= 6-6+2**

**=2**

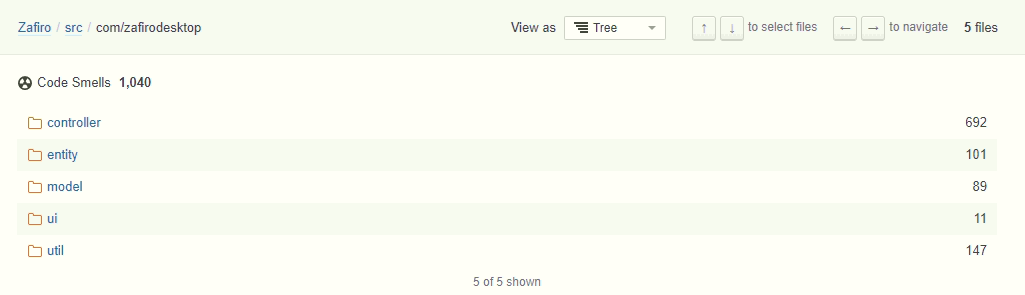
Y quiere decir que es un programa simple sin mucho riesgo

* COMPLEJIDAD COGNITIVA: se puede notar que se tiene una complejidad cognitiva de 3471 donde el 2.412 pertenece al módulo de controladores

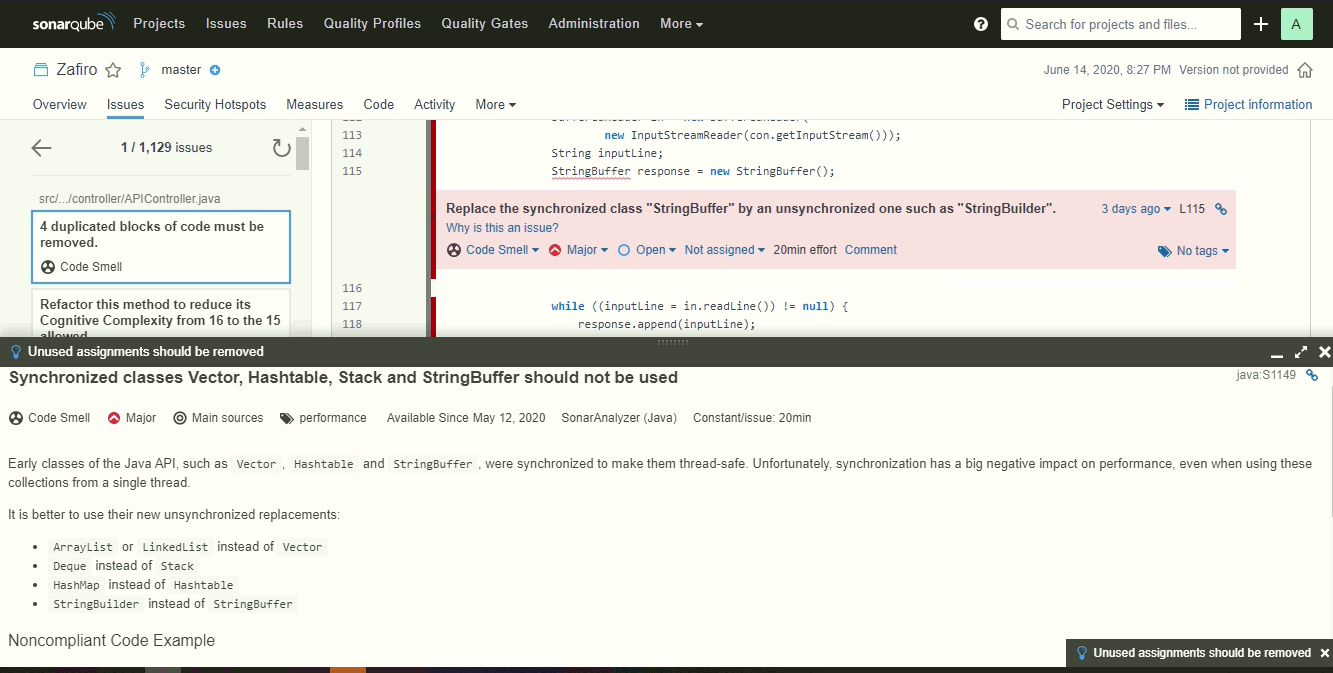


### Deuda técnica (20%)

* Code smell tiene un total de 1.040 distribuido en todos los módulos. Controller contiene mayor cantidad de code Smell



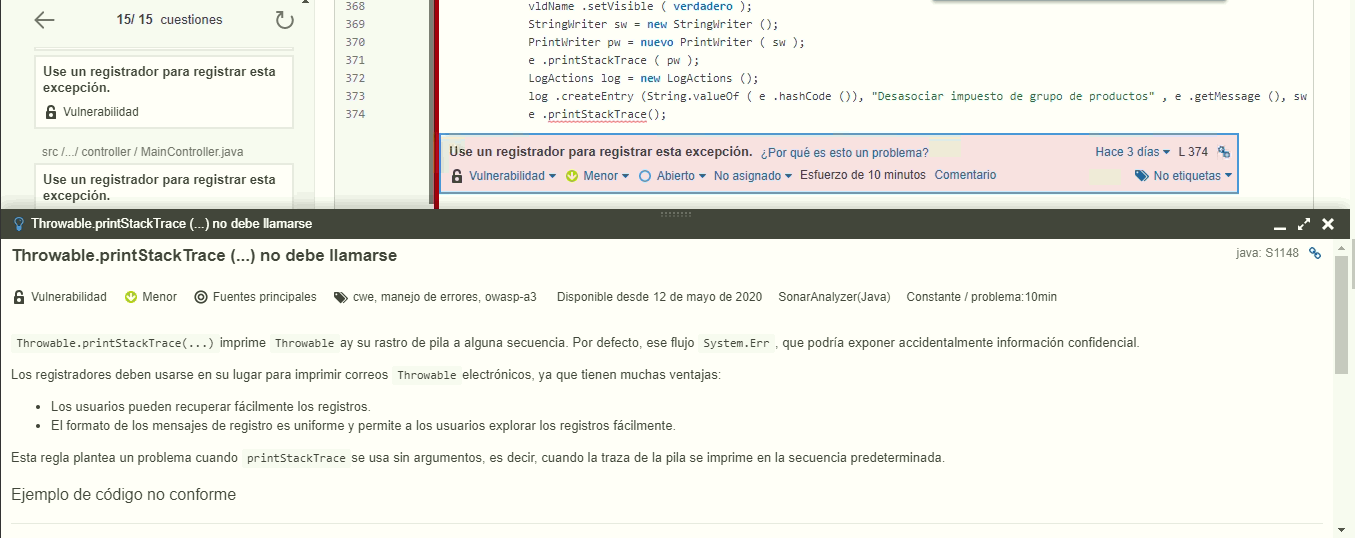
* Este es un ejemplo de Code Smell encontrado



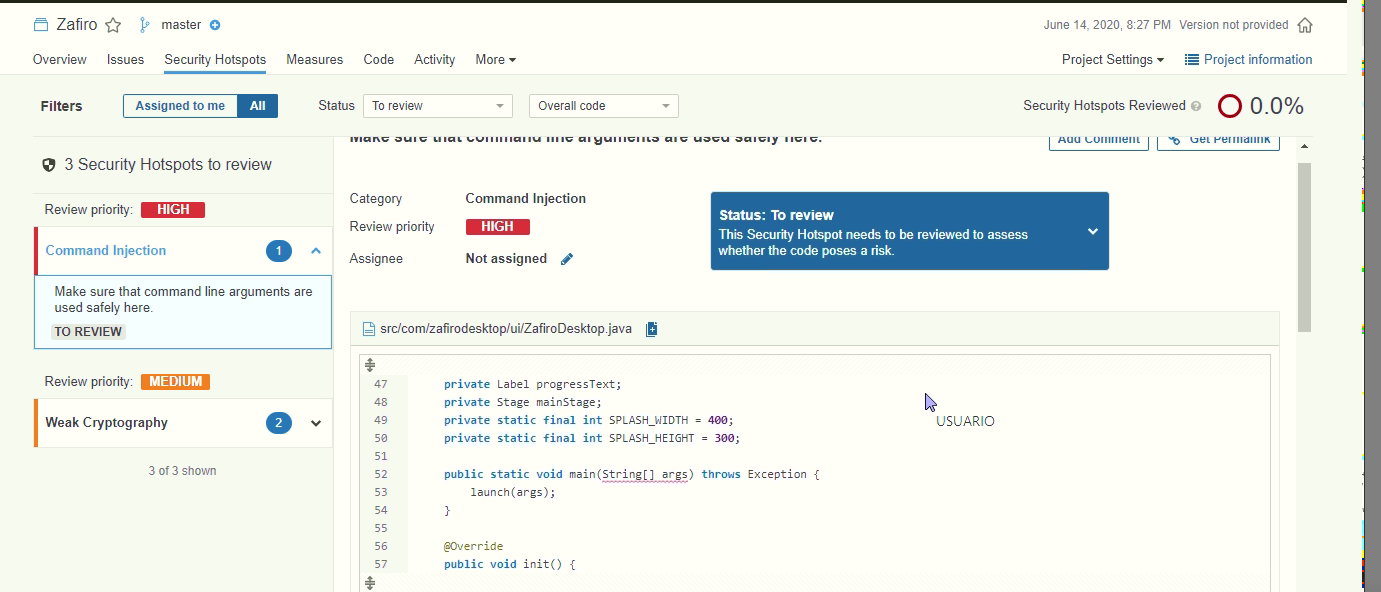
### Seguridad(20%)

* VULNERABILIDADES: Se encontraron 15 vulnerabilidades en el modulo de controllers

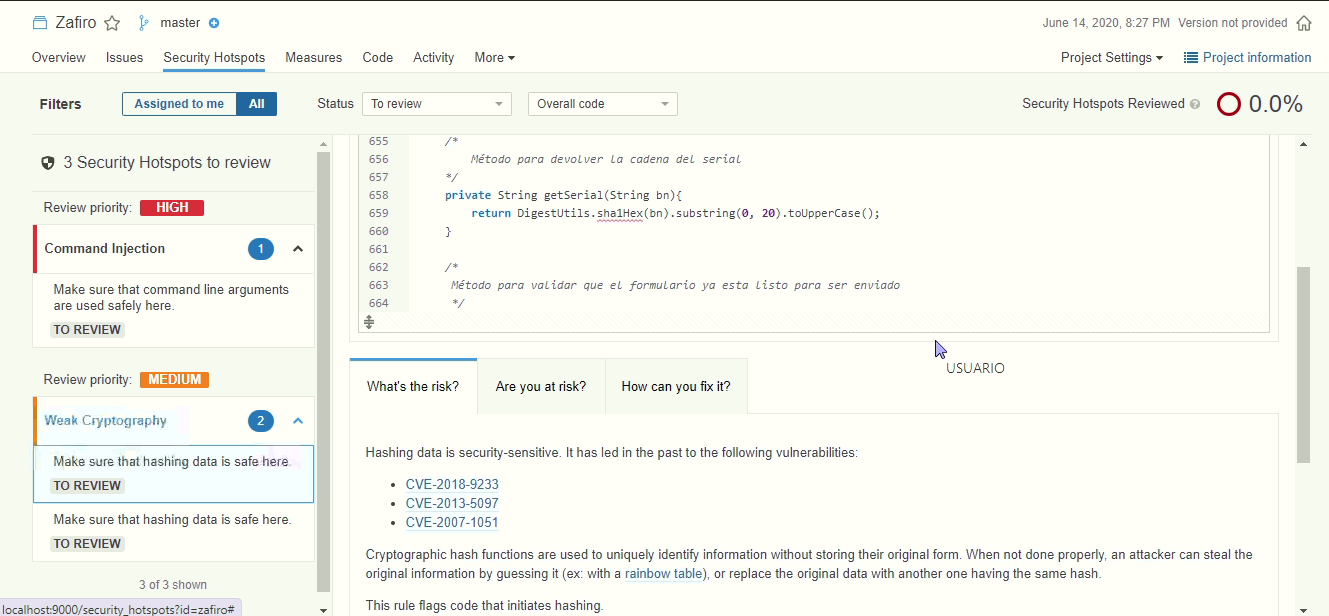




* injection



* cryptografia debil: Vulnerabilidad a la base de datos

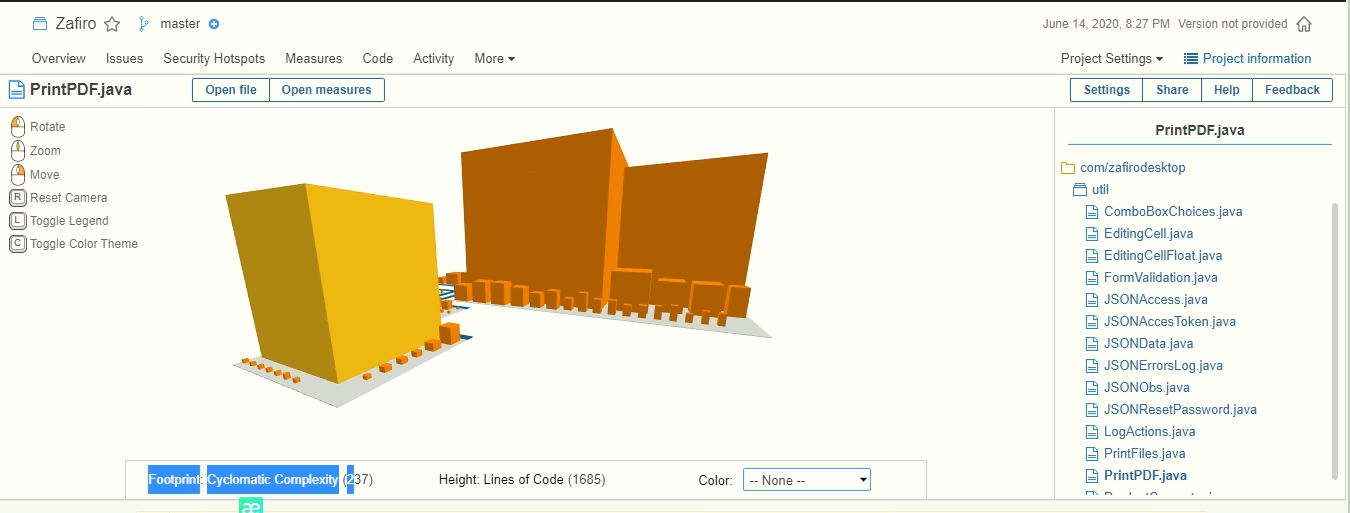


### 3d code metrics (20%)

* Ejemplo del archivo printPDF donde:

Complejidad ciclomatica:237

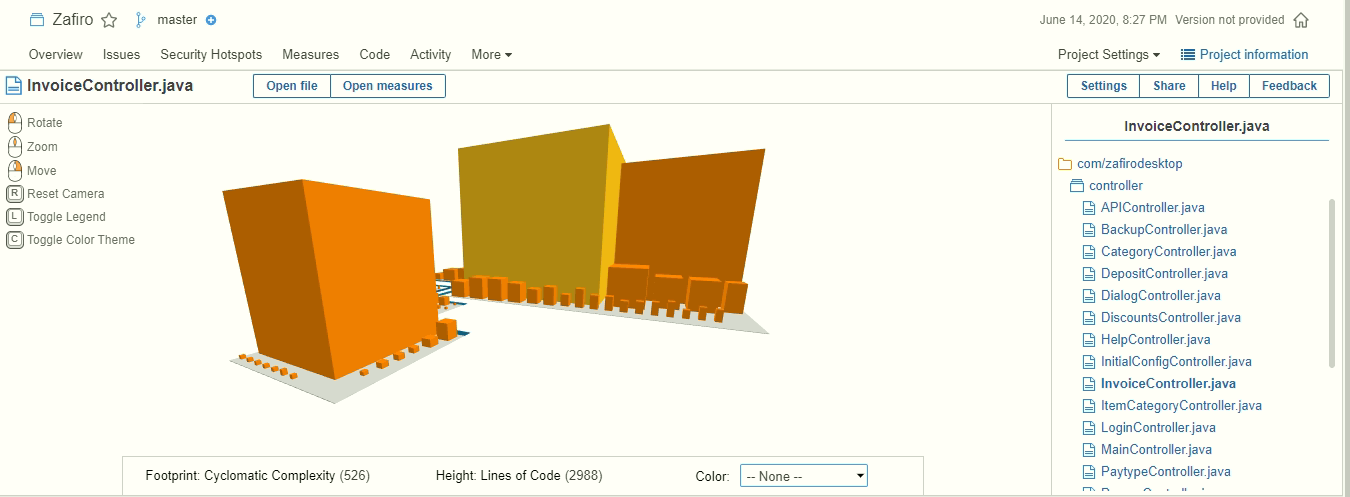
Líneas de codigo:1685



* Ejemplo del archivo InvoiceController.java donde:

Complejidad ciclomatica:526

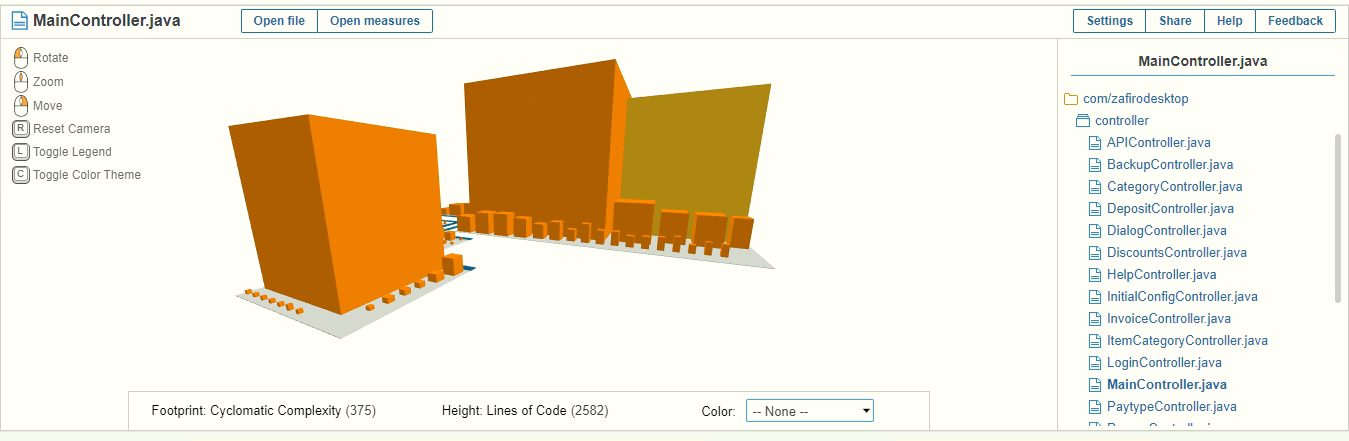
Líneas de codigo: 2988



* Ejemplo del archivo MainController.java donde:

Complejidad ciclomatica:375

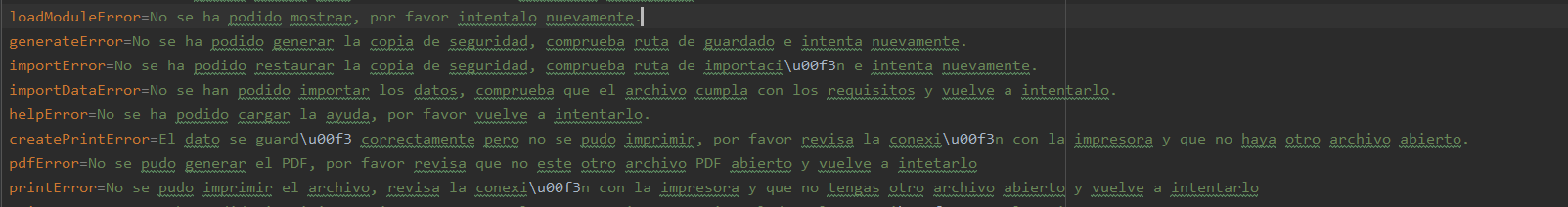
Líneas de codigo:2582



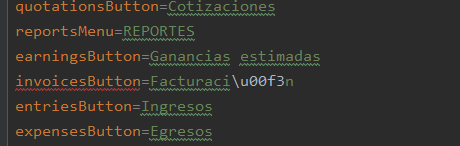
## Atributos Externos.

### Usabilidad (20%)

* EFECTIVIDAD: se denota un arduo trabajo por conseguir el menor margen de error posible asi como en temas de validaciones



* EFICIENCIA: Los nombres fueron muy bien colocados respecto a la funcionalidad a la que obedecen.



* SATISFACCION: Sería recomendable usar este software si se le corrige algunas mejoras importantes como las de seguridad.

### Fiabilidad (30%)

En este software existen algunas vulnerabilidades en temas relacionados con la base de datos que puede generar exposición indeseada de los datos que la misma contiene, así mismo contiene codigo que permite algún tipo de inyección de codigo malicioso. Lo corresponde con temas legales es igualmente importante mencionarlo en temas de fiabilidad.

### Mantenibilidad (50%)

Su mantenibilidad es considerable puesto que tiene un número significativo de fallos con respecto a leyes y vulnerabilidades, pero independientemente es un software interesante al que se le ha dedicado mucho esfuerzo y en futuras versiones sería muy rentable usarlo.

# Recomendaciones y conclusiones

## Seguridad

Se recomienda exponer la base de datos a la menor vulnerabilidad posible, puesto que es un tema supremamente delicado tanto en lo personal como en lo legal. La encriptación de datos fue una decisión asertiva que se tomó durante el proceso de la elaboración del producto.

## Confiabilidad

Se le recomienda manejar el tema de leyes durante la transición hacia la siguiente versión, así como seguir los estándares iso 25000 que aseguran un total cumplimento de las normas de calidad

## Usabilidad

En general este punto está completo, aunque siempre se debe estar abierto a buscar la mejor versión de nuestro software.

# Bibliografía

# Firma del perito.

|  |  |
| --- | --- |
| **Responsable de la evaluación** | **Firma** |
| Nombre:  Empresa:  Cargo:  GitHub: |  |