	<b>COMERCIALIZADORA RÁPIDO S.A. DE C.V.</b>	
	Tipo de documento:	<b>Procedimiento específico</b>
	Título:	<b>Análisis estático</b>
	Código:	<b>PECRSI06</b>

#### CONTROL DE CAMBIOS

Cambio en Formato a partir del PGCRC02 Elaboración de información Documentada  
Organización de información

### 1. OBJETIVO

Implantar dentro del ciclo de vida de desarrollo de aplicaciones y programas el análisis de código estático para detectar y mitigar vulnerabilidades de la seguridad del código

### 2. ALCANCE

El análisis de código estático de las aplicaciones y proyectos desarrollados en Comercializadora Rápido S.A. de C.V.

Elaboró:	Vo. Bo.	Revisó:	Aprobó:
Fructuoso Rodríguez Joaquín Elías Programador/desarrollador de Software	Pitol Pimentel Carlos Adrián Gerente de Sistemas	Martínez Ponce Janely Gestión de Calidad	Montes Barrera Elliioth Abdel Gerente General

### 3. REFERENCIAS

ISO/IEC 27001:2022 Sistemas de gestión de la seguridad de la información (SGSI)

### 4. DEFINICIONES Y ABREVIATURAS

#### 4.1 Análisis de código estático.

Es un análisis realizado de forma automatizada por una herramienta cuyo objetivo es encontrar, defectos de codificación en el ciclo de vida del desarrollo, generalmente después de escribir el código fuente de la aplicación.

#### 4.2 Bugs.

Error o defecto en el software que hace que un programa funcione de forma incorrecta.

#### 4.3 Vulnerabilidad.

Es una debilidad en el software que permite a un atacante reducir la seguridad en sistemas críticos.

#### 4.4 Sonar Qube.

Plataforma de código abierto usada para controlar la calidad del código; desarrollado con el principal objetivo de hacer accesible la administración de la calidad del código con un mínimo esfuerzo. Como tal, contiene en su núcleo de funcionalidades un analizador de código, una herramienta de reportes, un módulo que detecta defectos y una función para regresar los cambios realizados en el código.


### 5. RESPONSABILIDADES

#### 5.1 Gerente General:

Aprobar la información documentada del SGC, asegurando que los recursos necesarios estén disponibles para lograr sin problema la implementación efectiva del documento.

Vigente a partir de: <b>29-ABR-2024</b>	Revisión: <b>3</b>	Página: <b>1 de 5</b>
--	-----------------------	--------------------------

"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"

	<b>COMERCIALIZADORA RÁPIDO S.A. DE C.V.</b>	
	Tipo de documento:	<b>Procedimiento específico</b>
	Título:	<b>Análisis estático</b>
	Código:	<b>PECRSI06</b>

## 5.2 Gerente Sistemas IT

Es responsable de validar los resultados del análisis de código estático durante la etapa del desarrollo de las aplicaciones, verifica el cumplimiento de las pruebas y registros en la matriz.

## 5.3 Programador-Desarrollador de software

Es responsable de llevar a cabo el proceso para el análisis de código estático con la finalidad de detectar errores y verificar que cumple con los criterios de calidad y seguridad, documenta los errores detectados durante la ejecución del analizador.

## 5.1 Gestión de Calidad:

Gestionar el cumplimiento documental según lo establecido en el SGC, asegura su adecuada implementación, manteniendo la eficacia, así como la mejora continua de estas, resguardando y emitiendo la documentación controlada.

## 6. DESARROLLO

### 6.1 Selección del programa para pruebas de código estático

Todos los integrantes del equipo de desarrollo deben definir los programas, aplicaciones y/o plataformas que requieren ser probados y garantizar la seguridad del código estático, así mismo anunciar los resultados obtenidos.

Para el análisis de código estático que se realiza en los proyectos de desarrollo se utiliza: Sonar Qube, versión más reciente de la herramienta aprobada y utilizada con la finalidad de sujetarse a los nuevos lineamientos de protección y funciones de análisis de la seguridad.

### 6.2 Revisión de la compatibilidad con el tipo de lenguaje

Para realizar una prueba de código estático, el equipo desarrollador tiene como prioridad asegurar que la herramienta utilizada tenga los criterios y reglas a fines del lenguaje del programa desarrollado. Por mencionar algunos: Java, JavaScript, PHP, Python, Ruby, C++, C#, Perl, etc


#### 6.2.1 Ejecución del análisis de código estático

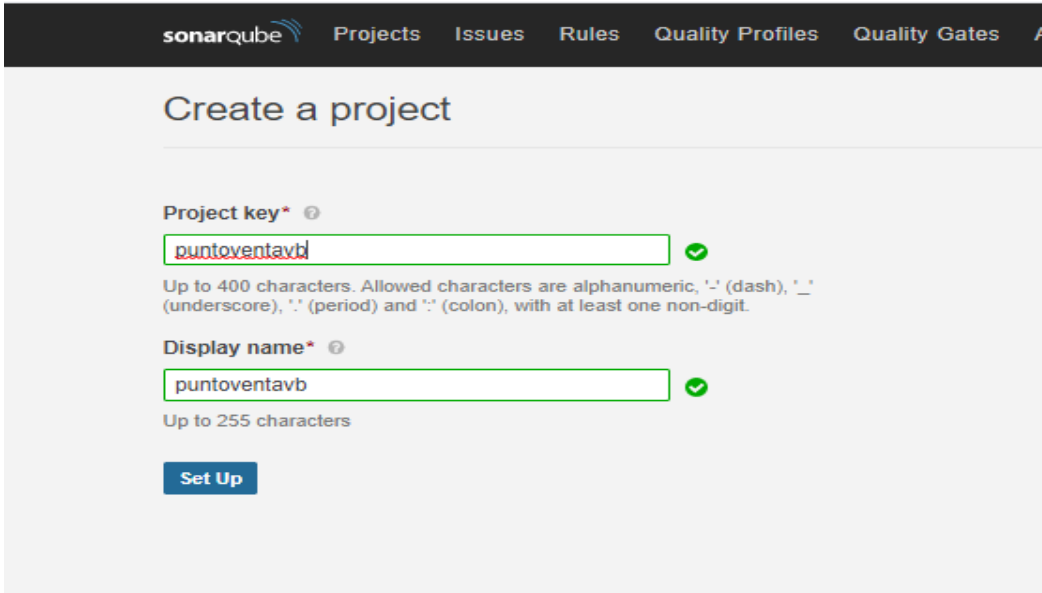
Se realiza la creación de un nuevo proyecto dentro del servidor local de la aplicación.

**Ejemplo:** ingresos de nuevo proyecto

Vigente a partir de: <b>29-ABR-2024</b>	Revisión: <b>3</b>	Página: <b>2 de 5</b>
--	-----------------------	--------------------------

*"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"*

	<b>COMERCIALIZADORA RÁPIDO S.A. DE C.V.</b>	
	Tipo de documento:	Procedimiento específico
	Título:	Análisis estático
	Código:	PECRSI06



sonarqube Projects Issues Rules Quality Profiles Quality Gates A

## Create a project

**Project key\*** ⓘ

puntoventavb ✓

Up to 400 characters. Allowed characters are alphanumeric, '-' (dash), '\_' (underscore), '.' (period) and ':' (colon), with at least one non-digit.

**Display name\*** ⓘ

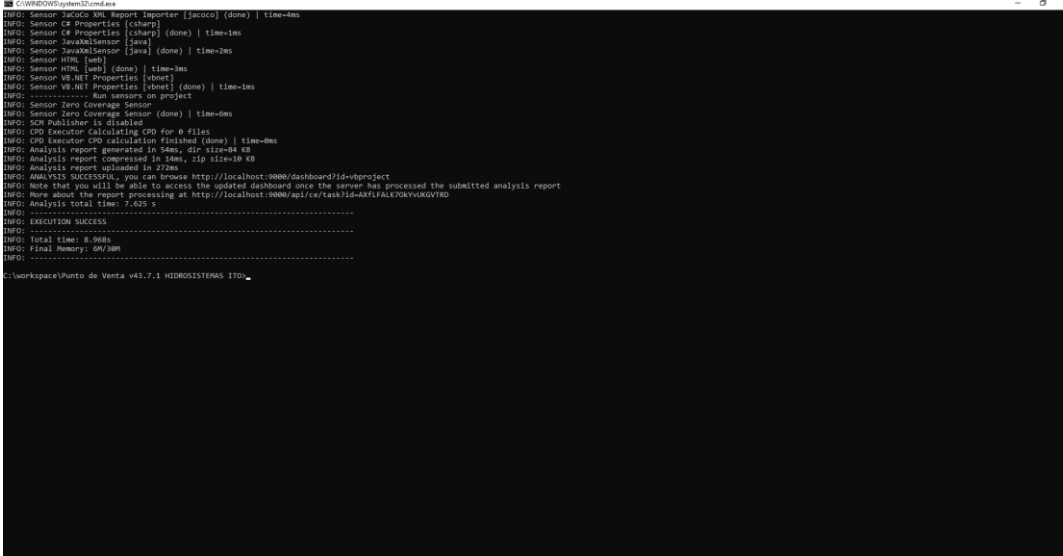
puntoventavb ✓

Up to 255 characters

**Set Up**

Se ingresa la información del proyecto Punto de Venta para ejecutar el análisis.

### Ejemplo: Ejecucion de análisis



```

C:\WINDOWS\system32\cmd.exe
INFO: Sensor JavaCC XML Report Importer [jacocc] (done) | time=4ms
INFO: Sensor C# Properties [csharp]
INFO: Sensor C# Properties [csharp] (done) | time=1ms
INFO: Sensor JavaKotlinSensor [java]
INFO: Sensor JavaKotlinSensor [java] (done) | time=2ms
INFO: Sensor HTML [web] (done) | time=1ms
INFO: Sensor VB.NET Properties [vbnet]
INFO: Sensor VB.NET Properties [vbnet] (done) | time=1ms
INFO: ----- Run sensors on project
INFO: Sensor Zero Coverage Sensor
INFO: Sensor Zero Coverage Sensor (done) | time=0ms
INFO: SCM Publisher is disabled
INFO: C# Executor Calculating CPO for 0 files
INFO: CPO Executor CPO calculation finished (done) | time=0ms
INFO: Analysis report generated in 5ms, dir size=10 KB
INFO: Analysis report compressed in 5ms, zip size=10 KB
INFO: Analysis report uploaded in 272ms
INFO: ANALYSIS SUCCESSFUL, you can browse http://localhost:9000/dashboard?id=vpproject
INFO: Note that you will be able to access the updated dashboard once the server has processed the submitted analysis report
INFO: More about the report processing at http://localhost:9000/api/ci/task?id=AXFLFKTKYVURGVTRD
INFO: Analysis total time: 7.625 s
INFO: EXECUTION SUCCESS
INFO: Total time: 8.060s
INFO: Final Memory: 4M/30M
INFO:
C:\workspace\Punto de Venta v03.7.1\HIDROSISTEMAS LTD\

```


### 6.2.2 Validación del análisis

Desde la página principal de Sonarqube, dar click encima del nombre del proyecto deseado para entrar en su detalle. Por defecto aparecerá en la sección “Dashboard” que incluye información sobre:

- Valores totales de número de líneas de código, métodos, clases y paquetes.
- Porcentaje de código comentario y porcentaje de código duplicado.

Vigente a partir de: <b>29-ABR-2024</b>	Revisión: <b>3</b>	Página: <b>3 de 5</b>
--	-----------------------	--------------------------

“Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada”

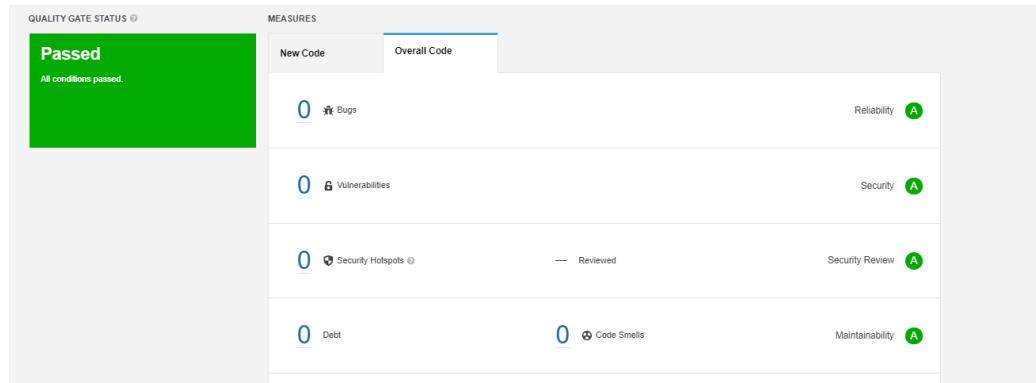
	<b>COMERCIALIZADORA RÁPIDO S.A. DE C.V.</b>	
	Tipo de documento:	<b>Procedimiento específico</b>
	Título:	<b>Análisis estático</b>
	Código:	<b>PECRSI06</b>

- Resultados de las pruebas ejecutadas y porcentaje de cobertura del código conseguido con las pruebas.
- Eventos de versiones etiquetadas sobre el código.
- Métricas cuyos valores sobrepasan el umbral de alerta definido en el perfil de calidad del proyecto.

### 6.2.3 Resultados

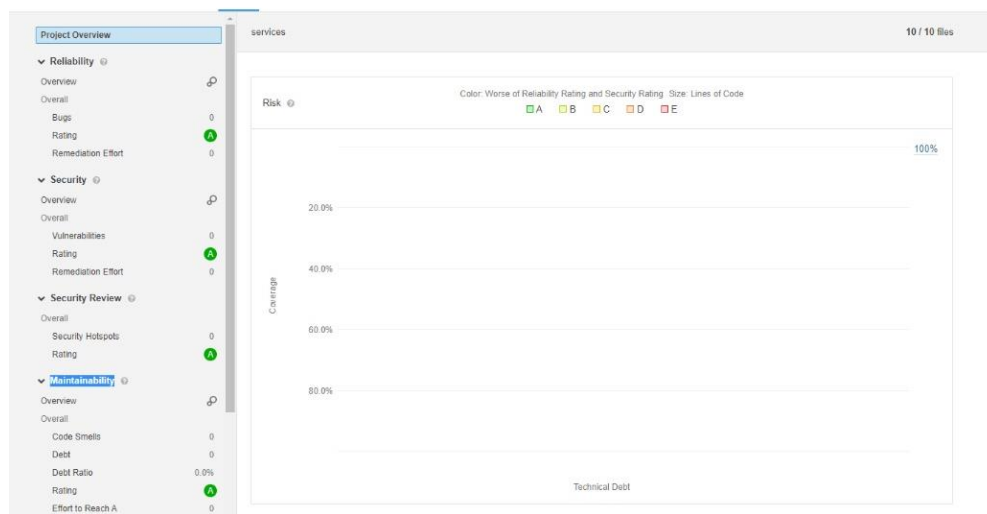
Los resultados de las pruebas y del análisis estático se muestran en la siguiente figura.

**Ejemplo: Resultados de análisis**




Para obtener una mayor información de las métricas y medidas del análisis que sonarqube realiza sobre el código que se analizó de punto de venta, el evaluador con apoyo del equipo desarrollador ingresa al host local de la herramienta analizadora en localhost:9000 y se hace la validación de los resultados al proyecto en cuestión. Cualquiera en la misma red puede realizar un análisis sobre su código entrando a la IP del servidor que verificamos ejecutando el comando ifconfig.

**Ejemplo: Métricas y medidas**



Vigente a partir de: <b>29-ABR-2024</b>	Revisión: <b>3</b>	Página: <b>4 de 5</b>
--	-----------------------	--------------------------

*"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"*

	<b>COMERCIALIZADORA RÁPIDO S.A. DE C.V.</b>		
	Tipo de documento:	<b>Procedimiento específico</b>	
	Título:	<b>Análisis estático</b>	
	Código:	<b>PECRSI06</b>	

### 6.3 Mejora.

Con la finalidad de revisión de los informes dada por la herramienta de análisis de código estático, se determina que para dar continuidad en la identificación de vulnerabilidades en el ciclo de desarrollo seguro, el evaluador interno deberá validar los resultados obtenidos por la aplicación que se ha utilizado. El periodo de revisión deberá ser anual y con fines de registro se deberán almacenar los resultados obtenidos por cada análisis realizado en el formato de **Matriz de pruebas PECRSI06\_F01(2)**

### 6.4 Parámetros de análisis

Los parámetros del análisis de proyectos se pueden configurar de acuerdo a las necesidades y objetivo de las pruebas realizadas, a continuación, se mencionan las siguientes:

- Las propiedades globales, definidas en la interfaz de usuario, se aplican a todos los proyectos (Desde la barra superior, vaya a Administración > Configuración > Configuración general)
- Las propiedades del proyecto, definidas en la interfaz de usuario, invalidan los valores de propiedad globales (en un nivel de proyecto, vaya a Configuración del proyecto > Configuración general)
- Los parámetros de análisis de proyectos, definidos en un archivo de configuración de análisis de proyecto o un archivo de configuración del analizador, invalidan los definidos en la interfaz de usuario
- Parámetros de análisis / línea de comandos, definidos al iniciar un análisis (con en la línea de comandos), invalidar los parámetros de análisis de proyecto-D.

### 7. DIAGRAMA DE FLUJO

Puesto involucrado	Puesto involucrado	Puesto involucrado	Puesto involucrado
NA	NA	NA	NA

### 8. ANEXOS

TIPO	CODIGO	TITULO
Formato	PECRSI06_F01(2)	Matriz de Prueba
Ayuda visual	NA	NA
Políticas	NA	NA
Otros (documento externo)	NA	NA

Vigente a partir de: <b>29-ABR-2024</b>	Revisión: <b>3</b>	Página: <b>5 de 5</b>
--	-----------------------	--------------------------

*"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"*