

**UNIVERSIDAD PRIVADA DE TACNA**

**FACULTAD DE INGENIERÍA**

**Escuela Profesional de Ingeniería de Sistemas**

**Mejoramiento de la Aplicación**

**Proyecto de implementación de una agenda virtual para la I.E.P. Steve Jobs**

Curso: Calidad y Pruebas de Software

Docente: Ing. *Patrick Cuadros Quiroga*

**Integrantes:**

***Edward Hernan Apaza Mamani (2018060915)***

***Ronal Daniel Lupaca Mamani (2020067146)***

***Carlos Andrés Escobar Rejas (2021070016)***

***Aarón Pedro Paco Ramos (2018000654)***

**Tacna – Perú**

***2024***

**Descripción**

Descripción del Proyecto: "Implementación de una agenda virtual para la I.E.P. Steve Jobs"

Este proyecto, que durará 86 días a partir del 5 de abril hasta el 30 de junio, se centra en la implementación de una agenda virtual con Chatbot en la Institución Educativa Privada Steve Jobs. El objetivo principal es mejorar la comunicación interna, proporcionando a estudiantes y padres acceso inmediato a comunicados institucionales y seguimiento conductual de los alumnos. Entre los objetivos específicos se incluyen la confirmación de recepción de comunicados, registro de asistencias, y fomento de la confianza con los padres. El proyecto enfrenta desafíos como la adaptación a la tecnología por parte de los padres y limitaciones de recursos tecnológicos. La factibilidad técnica, económica, operativa, legal y social ha sido demostrada, asegurando la viabilidad del sistema en términos de infraestructura y costos. La inversión proyectada promete retornos positivos según análisis financieros, como el Valor Actual Neto y la Tasa Interna de Retorno, garantizando beneficios tanto tangibles como intangibles para la institución.

**Abstract**

Project Description: "Implementation of a Virtual Agenda for the I.E.P. Steve Jobs"

This project, scheduled from April 5 to June 30, aims to implement a virtual agenda with a Chatbot at the Private Educational Institution Steve Jobs. The primary objective is to enhance internal communication by providing students and parents with immediate access to institutional announcements and behavioral monitoring of students. Specific goals include confirming the reception of communications, recording attendances, and building trust with parents. The project addresses challenges such as parental technology adaptation and limited technological resources. Technical, economic, operational, legal, and social feasibility has been established, ensuring the system's viability in terms of infrastructure and costs. The projected investment is expected to yield positive returns, as indicated by financial analyses such as Net Present Value and Internal Rate of Return, ensuring tangible and intangible benefits for the institution.

**Antecedentes o introducción**

El presente proyecto trata sobre la implementación de una agenda virtual con Chatbot, incorporando diferentes funcionalidades útiles, que puede interactuar con el usuario, y puede ofrecer una amplia variedad de servicios. El chatbot puede ayudar a los estudiantes y a los padres de familia para tener el conocimiento de comunicados institucionales o conductuales de los estudiantes. Teniendo como objetivo principal mejorar la comunicación interna del Colegio Steve Jobs mediante datos e informe de los alumnos y docentes logrando de esta manera que la información sea más fluida, ordenada y automatizada, teniendo como fin, mejorar el control de toda la gestión académica y conductual de los estudiantes.

**Título**

Implementación de una agenda virtual para la I.E.P. Steve Jobs

**Autores**

Edward Hernan Apaza Mamani 2018060915

Ronal Daniel Lupaca Mamani 2020067146

Carlos Andrés Escobar Rejas 2021070016

Aarón Pedro Paco Ramos 2018000654

**Planteamiento del problema**

**Problema**

El principal problema identificado es la baja efectividad de la comunicación directa con los padres de familia mediante la agenda escolar física, que se utiliza actualmente en la institución. Esto resulta en confusión y falta de recepción de comunicados importantes debido a la falta de flexibilidad del medio físico y a errores humanos por parte de los docentes.

**Justificación**

La justificación del proyecto se centra en la necesidad de mejorar la calidad educativa y la comunicación entre estudiantes, padres y docentes. La implementación de una agenda virtual optimizará los procesos de comunicación y gestión de información, aumentando la eficiencia en la administración de la institución y mejorando la experiencia educativa para toda la comunidad.

**Alcance**

El alcance del proyecto abarca la implementación de la agenda virtual en la Institución Educativa Privada "Steve Jobs", dirigida a mejorar la comunicación entre docentes, padres de familia y alumnos. Esto incluirá la sistematización de asistencias, comunicados y actividades escolares para informar de manera rápida y controlada sobre la situación académica y conductual de los alumnos​

**Objetivos**

**General**

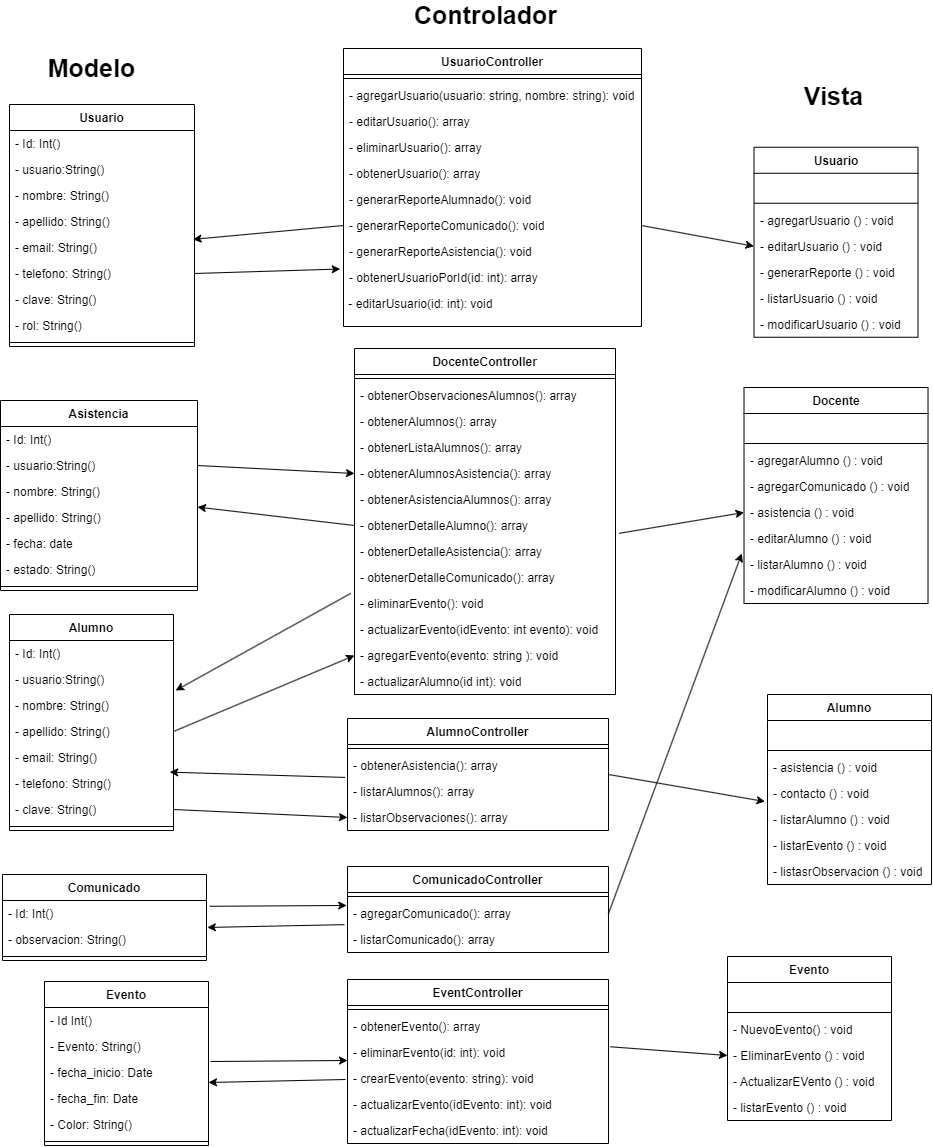
Implementar una agenda virtual que permite notificar de manera controlada la asistencia, comunicados, situación académica y conductual de los alumnos a los padres de familia para mejorar la comunicación en la Institución Educativa Privada “Steve Jobs” y facilitar el acceso a la información relevante para estudiantes, docentes y padres de familia

**Específicos**

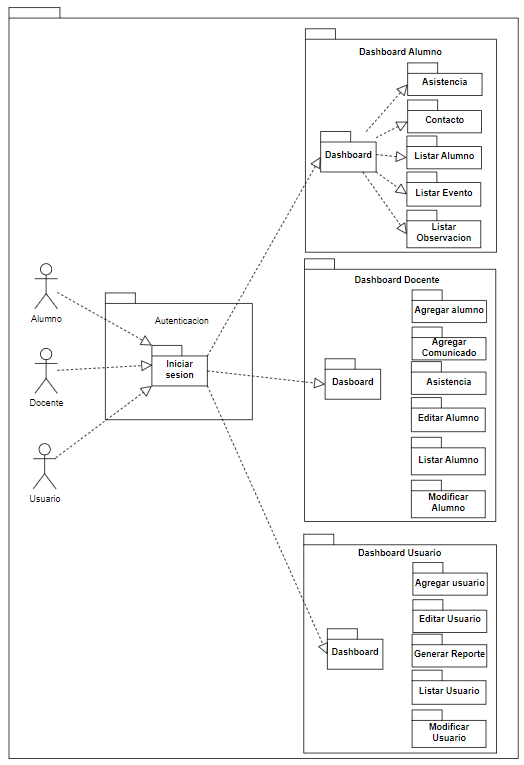
* Confirmar la recepción de comunicados por parte de los padres de familia.
* Confirmar la asistencia de los alumnos a los padres de familia.
* Generar una mejor comunicación y confianza con los padres de familia.
* Controlar el registro de asistencias de alumnos de la Institución Educativa Steve Jobs​

**Referentes teóricos**

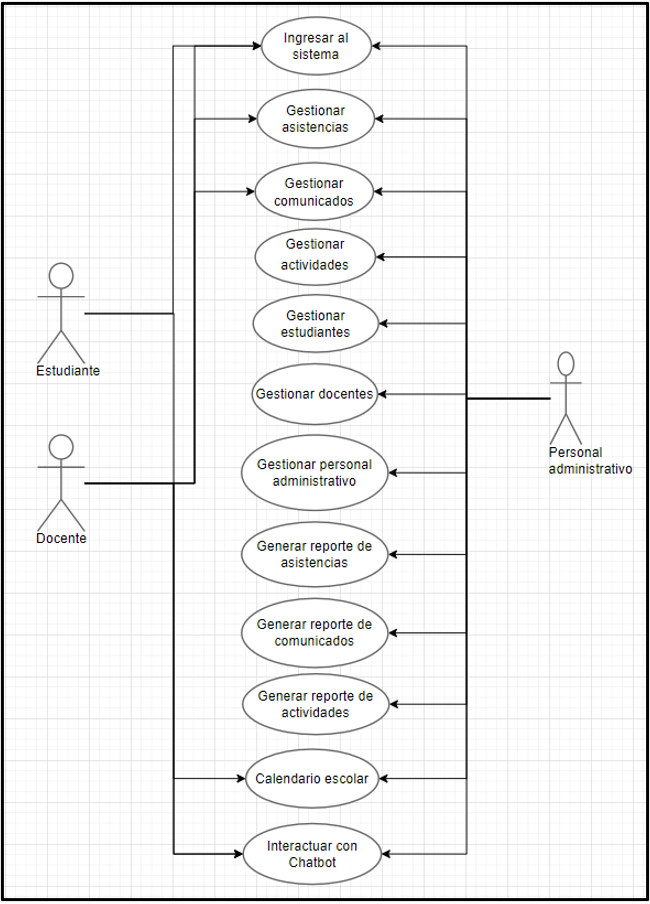
**Diagrama de Clases**



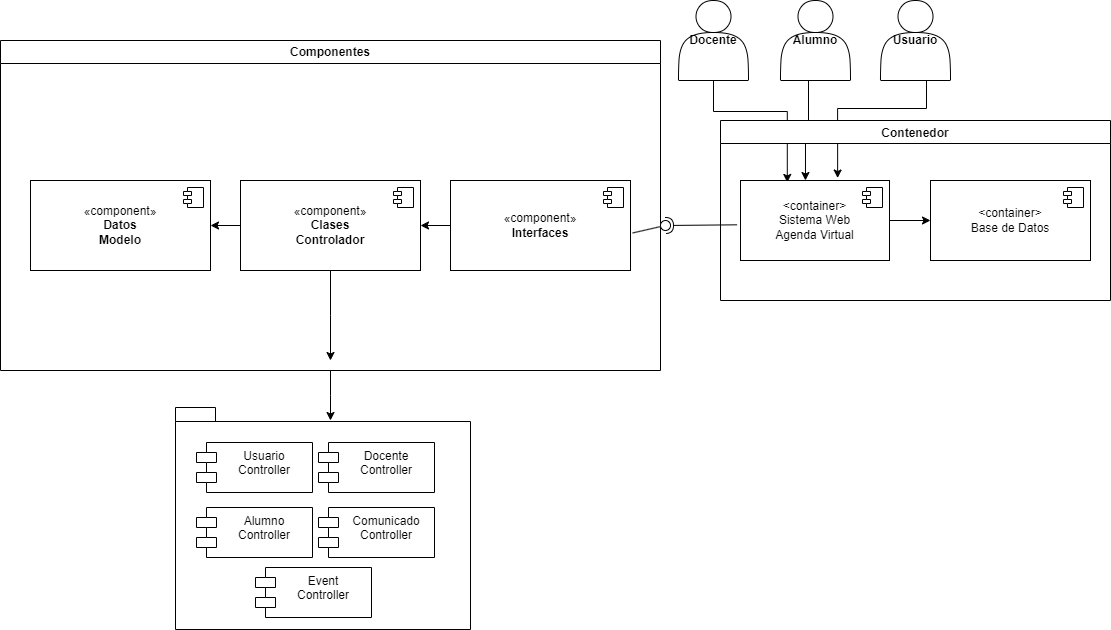
**Diagrama de paquetes**



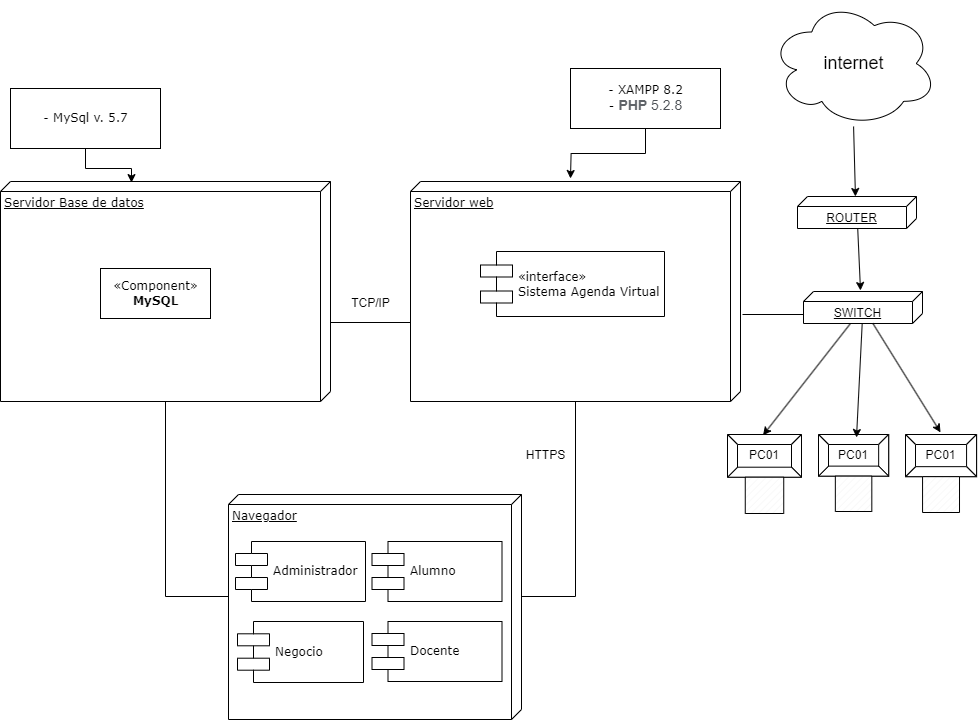
**Diagrama de Casos de Uso**

****

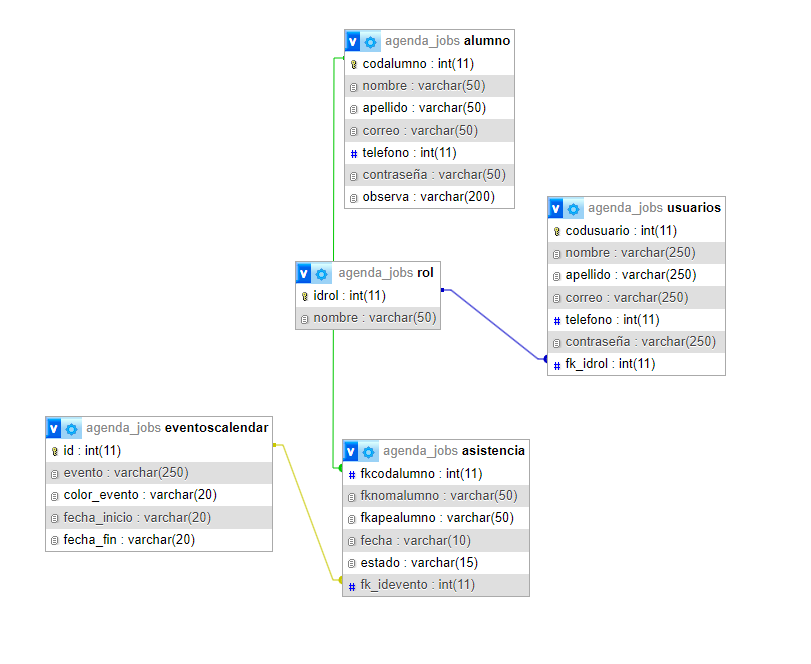
**Diagrama de componentes**



**Diagrama de despliegue**



**Diagrama de base de datos**



**Desarrollo de la propuesta**

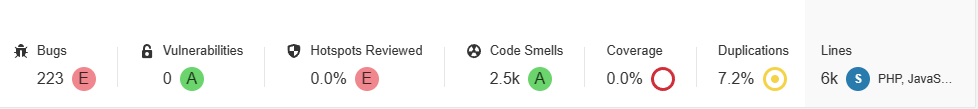
Para el desarrollo de la propuesta, se llevarán a cabo pruebas utilizando herramientas de análisis estático de código, tales como Snyk, SonarQube y SonarCloud. Estas herramientas nos permitirán identificar posibles vulnerabilidades, errores y problemas de calidad en el código, asegurando así un desarrollo más robusto y seguro. Además, facilitarán la implementación de buenas prácticas de programación y la mejora continua del software.

Pruebas realizadas en SonarQube

Antes:

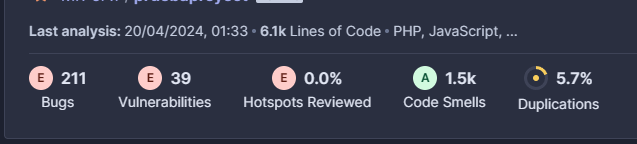


Después:

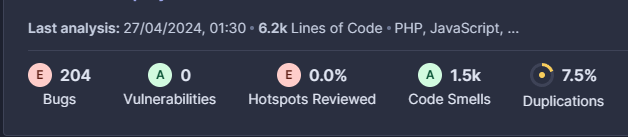


Pruebas realizadas en SonarCloud:

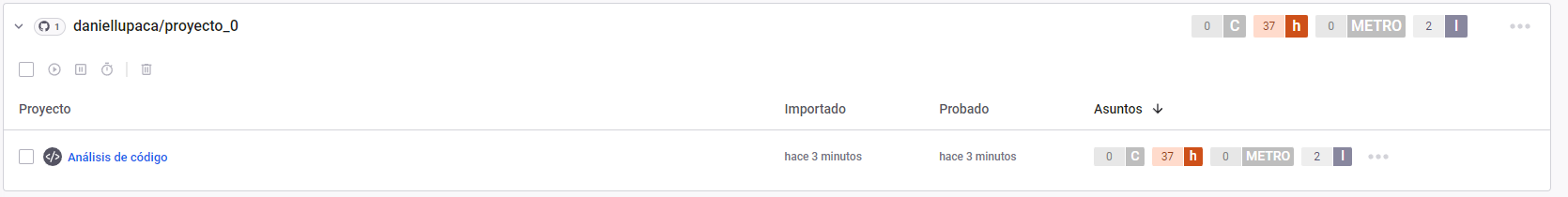
Antes:

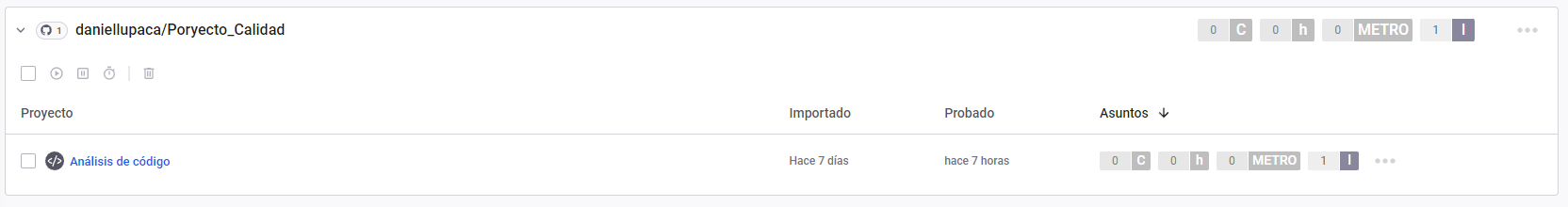


Después:

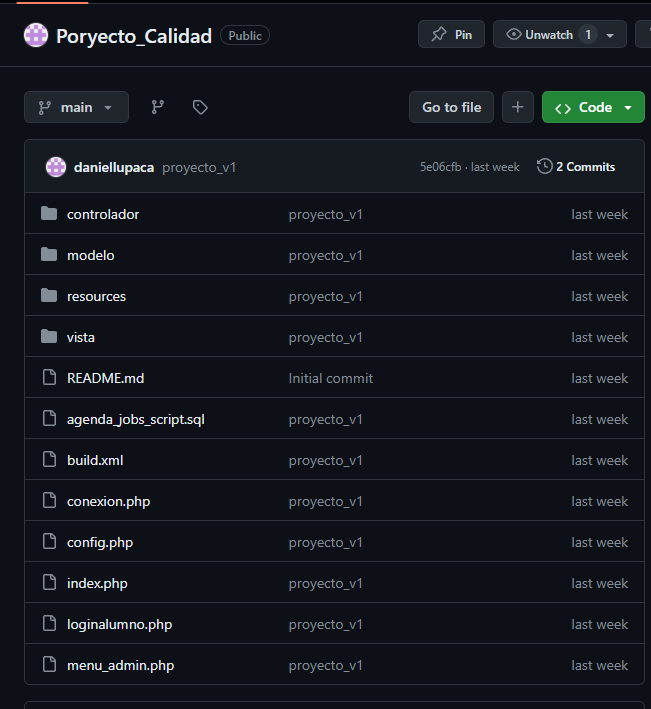


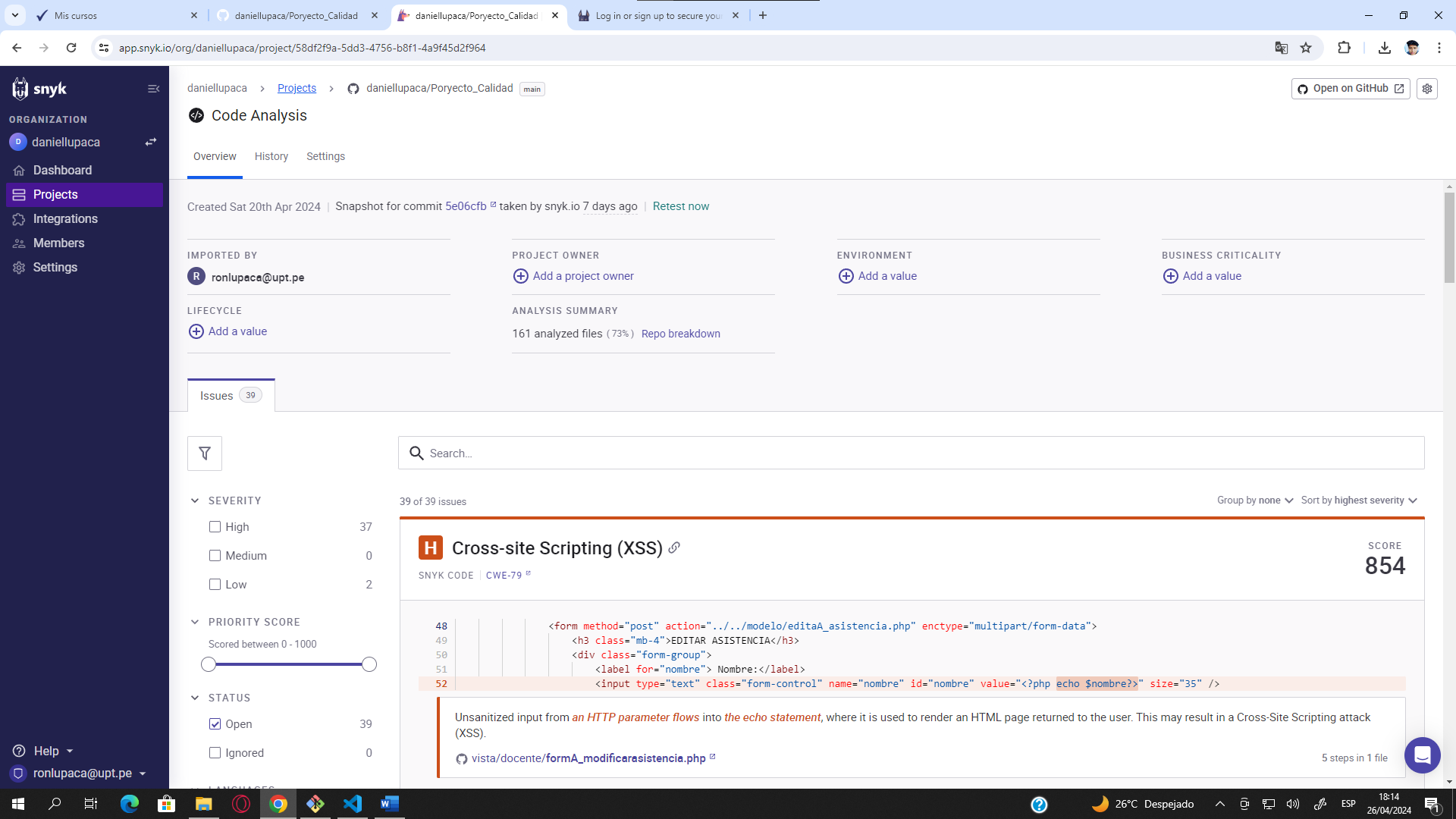
Pruebas realizadas en Snyk:

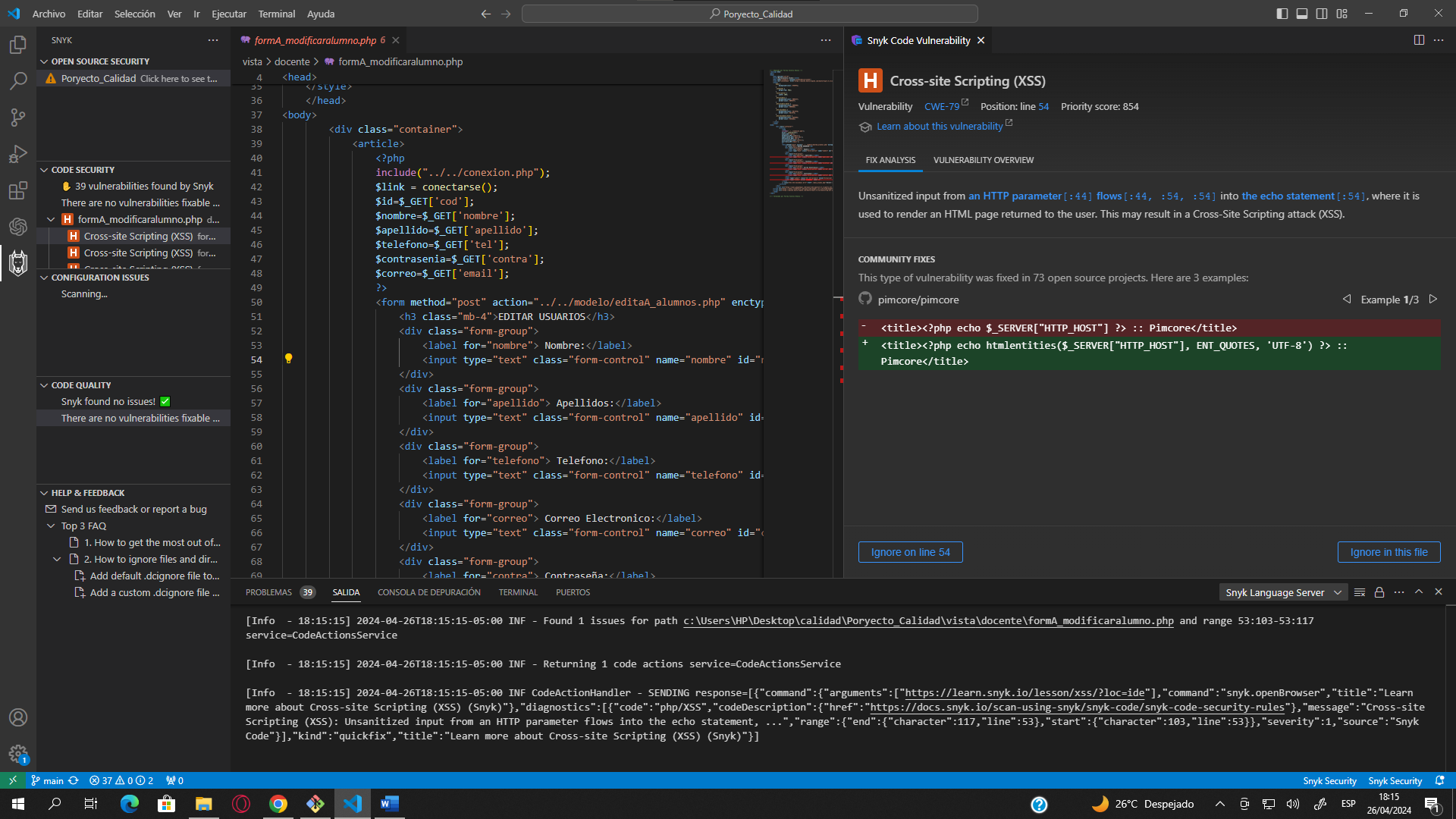
Antes:

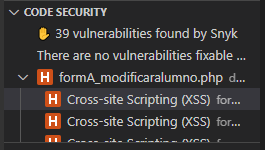
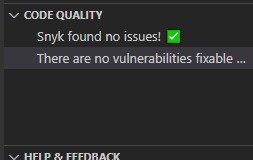
Después:









### Vulnerabilidad: Cross-site Scripting (XSS) - CWE-79

Descripción del Problema:

* Antes: La entrada del usuario proveniente de un parámetro HTTP no era saneada antes de ser incorporada en la salida HTML. Esto podría permitir que un atacante inyectara scripts maliciosos en la página, lo que podría resultar en ataques de tipo Cross-Site Scripting (XSS).
* Riesgo Asociado: Un atacante podría ejecutar scripts en el navegador del usuario final, lo que puede llevar a robo de cookies, sesiones de secuestro, defacement de sitios web, y otros ataques que comprometen la seguridad del usuario y la confianza en la aplicación web.

Solución Implementada:

* Después: Se sanitiza la entrada del usuario usando la función htmlspecialchars, la cual convierte caracteres especiales en entidades HTML. Esto previene la ejecución de scripts inyectados en el contexto HTML.
* Impacto de la Solución: La solución protege contra ataques XSS al asegurarse de que cualquier entrada del usuario que se incluya en la salida HTML sea segura y no pueda ser interpretada como código HTML/JavaScript.

Código Afectado:

* Ubicación en el Código: Archivo editaA\_asistencia.php, línea 71.
* Fragmento del Código Antes de la Corrección:
* php
* Copy code

<title><?php echo $\_SERVER["HTTP\_HOST"]; ?> :: Pimcore</title>

* Fragmento del Código Después de la Corrección:
* php
* Copy code

<title><?php echo htmlspecialchars($\_SERVER["HTTP\_HOST"], ENT\_QUOTES, 'UTF-8'); ?> :: Pimcore</title>

Referencias Adicionales:

* OWASP XSS Prevention Cheat Sheet
* CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

### Vulnerabilidad: SQL Injection - CWE-89

Descripción del Problema:

* Antes: La aplicación usaba concatenación directa de los valores ingresados por el usuario en las consultas SQL, lo que podría permitir a un atacante manipular la consulta para realizar acciones no autorizadas en la base de datos.
* Riesgo Asociado: Un atacante podría ejecutar consultas arbitrarias en la base de datos, lo que puede llevar a la exposición de datos sensibles, corrupción de datos, o incluso la eliminación completa de la base de datos.

Solución Implementada:

* Después: Se implementó el uso de sentencias preparadas y parámetros vinculados. Esto asegura que los valores ingresados por el usuario sean tratados como datos y no como parte de la consulta SQL, previniendo la inyección de SQL.
* Impacto de la Solución: La solución protege contra la inyección de SQL, garantizando que las operaciones sobre la base de datos sean ejecutadas usando valores seguros y evitando la ejecución de consultas maliciosas.

Código Afectado:

* Ubicación en el Código: Archivo editaU\_usuarios.php, líneas 13-14.
* Fragmento del Código Antes de la Corrección:
* php
* Copy code

$sql = "SELECT \* FROM usuarios WHERE codusuario = '$usuario' AND contraseña = '$password'";

* Fragmento del Código Después de la Corrección:
* php
* Copy code

$sth = $dbh->prepare("SELECT \* FROM usuarios WHERE codusuario = ? AND contraseña = ?");

$sth->execute(array($usuario, $password));

Referencias Adicionales:

* OWASP SQL Injection Prevention Cheat Sheet
* CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

### Vulnerabilidad: Use of Hardcoded Credentials - CWE-798

Descripción del Problema:

* Antes: Las credenciales para la conexión a la base de datos estaban codificadas directamente en el código, lo que representa un riesgo de seguridad si el código se expone.
* Riesgo Asociado: La exposición del código fuente podría revelar las credenciales de la base de datos, lo que podría ser utilizado para obtener un acceso no autorizado.

Solución Implementada:

* Después: Las credenciales de la base de datos se obtienen ahora a través de variables de entorno, lo cual es una práctica más segura que protege las credenciales en caso de una exposición del código.
* Impacto de la Solución: El cambio a variables de entorno para manejar las credenciales protege la información sensible y cumple con las prácticas recomendadas de seguridad.

Código Afectado:

* Ubicación en el Código: Archivo conexion.php, línea 7.
* Fragmento del Código Antes de la Corrección:
* php
* Copy code

$usuario = "root";

$password = "";

* Fragmento del Código Después de la Corrección:
* php
* Copy code

$usuario = getenv("DB\_USUARIO") ?: 'root';

$password = getenv("DB\_PASSWORD") ?: '';

Referencias Adicionales:

* CWE-798: Use of Hard-coded Credentials

Cómo vistos al inicio se detectó 39 vulnerabilidades , 37 de grado Alto y dos de Bajo.



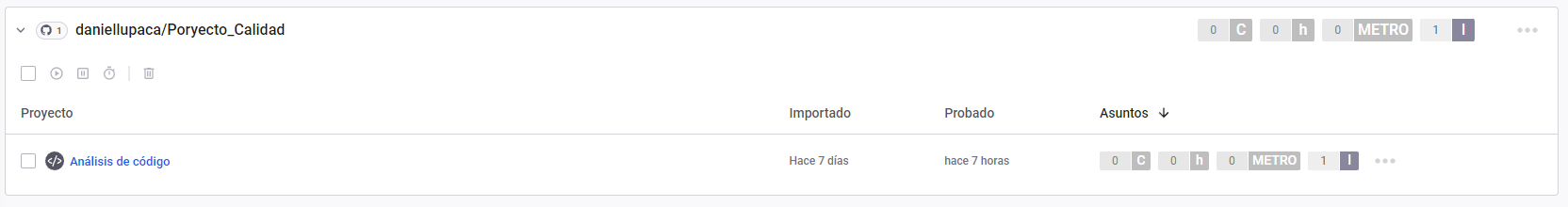
se trabajó en 4 tipos de vulnerabilidades :

1. Uso de Credenciales Codificadas (Hardcoded Credentials)
2. Cross-site Scripting (XSS)
3. Inyección SQL (SQL Injection)
4. Problemas de seguridad relacionados con la configuración del servidor (como la exposición del HTTP\_HOST)

Se trabajó en la visual code para corregir y hacer el commit en el repositorio público para que Snyk pueda volver a escanear el proyecto.

mostrando la eliminación de 38 vulnerabilidades.



Estas correcciones mejoran significativamente la seguridad de tu aplicación, protegiendo tanto los datos de los usuarios como la integridad de tu sistema.

**Tecnología de información**

Snyk: Utilizado para el escaneo de vulnerabilidades en las dependencias y para realizar análisis estático del código.

SonarQube: Implementado para la revisión continua del código, enfocado en la detección de bugs, vulnerabilidades y deuda técnica.

SonarCloud: Servicio en la nube que proporciona análisis automatizado para detectar y corregir fallas en el código.

Git: Sistema de control de versiones empleado para el seguimiento de cambios y colaboración en el desarrollo del proyecto.

GitHub: Plataforma de alojamiento para el repositorio del proyecto, integrada con Snyk para el análisis de seguridad tras cada push.

MySQL: Sistema de gestión de base de datos para almacenar, modificar y extraer la información utilizada en la aplicación.

PHP: Lenguaje de programación del lado del servidor para la implementación de la lógica de negocio de la aplicación.

**Metodología, técnicas usadas**

Desarrollo Ágil: Implementación iterativa e incremental para facilitar la flexibilidad y la entrega continua de valor.

Integración Continua/Despliegue Continuo (CI/CD): Prácticas que permiten la integración de cambios de forma automática y sistemática.

Revisión de Código: Práctica colaborativa en la que los cambios de código son revisados por pares antes de ser integrados al proyecto.

Análisis Estático de Código: Empleo de herramientas como Snyk y SonarQube para detectar problemas en el código sin ejecutarlo.

Seguridad de la Información: Aplicación de prácticas de codificación segura, tales como la sanitización de entradas y el uso de sentencias preparadas.

**Cronograma** (personas, tiempo, otros recursos) Basado en las observaciones que la herramienta SonarQube les informará sobre la aplicación, a fin de reducir la deuda técnica, vulnerabilidades, fallas, etc. a 0.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Actividades | Mes 1 | Mes 2 | Mes 3 | Mes 4 | Mes 5 |
| Vulnerabilidades Altas (Ronal Lupaca) | **X** | **X** |  |  |  |
| Vulnerabilidades Medias (Ronal Lupaca) | **X** | **X** |  |  |  |
| Vulnerabilidades Bajas (Ronal Lupaca y Carlos Escobar) | **X** | **X** | **X** |  |  |
| Redundancia de Código (Paco Ramos, Apaza Mamani) |  |  | **X** |  |  |
| Corrección de Bugs (Carlos Escobar, Ronal Lupaca) |  |  |  | **X** |  |
| Pruebas Finales (Ronal Lupaca , Carlos Escobar, Paco Ramos, Apaza Mamani ) |  |  |  |  | **X** |