Texto, Logotipo

Descripción generada automáticamente

**UNIVERSIDAD PRIVADA DE TACNA**

**FACULTAD DE INGENIERIA**

**Escuela Profesional de Ingeniería de Sistemas**

**PWASP SCANNER – Sistema de Detección de Vulnerabilidades Web**

Curso: *Patrones de Software*

Docente: Ing. Patrick Jose Cuadros Quiroga

|  |  |
| --- | --- |
| Integrantes: |  |
| ***Ccalli Chata, Joel Robert*** | ***(2017057528)*** |
| ***Jarro Cachi, Jose Luis*** | ***(2020067148)*** |

**Tacna – Perú**

***2025***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CONTROL DE VERSIONES | | | | | |
| Versión | Hecha por | Revisada por | Aprobada por | Fecha | Motivo |
| 1.0 | JRCC | JRCC | JCC | 19/04/2025 | Versión Original |

**PWASP SCANNER – Sistema de Detección de Vulnerabilidades Web**

**FD03 - Documento de Especificación de Requerimientos de Software**

# Versión 1.0

ÍNDICE GENERAL

[**UNIVERSIDAD PRIVADA DE TACNA** 1](#_Toc202001508)

[Versión 1.0 2](#_Toc202001509)

[**1. Introducción** 4](#_Toc202001510)

[**2. Generalidades de la Empresa** 4](#_Toc202001511)

[**2.1 Nombre de la Empresa** 4](#_Toc202001512)

[**2.2 Visión** 5](#_Toc202001513)

[**2.3 Misión** 5](#_Toc202001514)

[**2.4 Organigrama Organizacional** 5](#_Toc202001515)

[**3. Visionamiento del Proyecto** 5](#_Toc202001516)

[**3.1 Descripción del Problema** 5](#_Toc202001517)

[**3.2 Objetivos del Proyecto** 6](#_Toc202001518)

[**3.3 Alcance del Proyecto** 6](#_Toc202001519)

[**4. Viabilidad del Proyecto** 6](#_Toc202001520)

[**4.1 Viabilidad Técnica** 6](#_Toc202001521)

[**4.2 Viabilidad Operativa** 6](#_Toc202001522)

[**4.3 Viabilidad Económica** 7](#_Toc202001523)

[**5. Recolección y Análisis de Información** 7](#_Toc202001524)

[**5.1 Estudio Cuantitativo** 7](#_Toc202001525)

[**5.2 Estudio Cualitativo** 7](#_Toc202001526)

[**5.3 Benchmarking** 7](#_Toc202001527)

[**6. Especificación de Requisitos de Software** 7](#_Toc202001528)

[**6.1 Requerimientos Funcionales** 7](#_Toc202001529)

[**🔷 CASOS DE USO EN PLANTUML (10)** 8](#_Toc202001530)

[**✅ 1. Autenticación de Usuario** 8](#_Toc202001531)

[**✅ 2. Registro de Nueva Cuenta** 9](#_Toc202001532)

[**✅ 3. Escaneo de un Sitio Web** 10](#_Toc202001533)

[**✅ 4. Visualizar Reportes de Vulnerabilidades** 11](#_Toc202001534)

[**✅ 5. Configuración del Perfil de Usuario** 12](#_Toc202001535)

[**✅ 6. Gestión de Permisos (Admin)** 13](#_Toc202001536)

[**✅ 7. Programar Escaneo Automático** 14](#_Toc202001537)

[**✅ 8. Generar Informe Personalizado** 15](#_Toc202001538)

[**✅ 9. Recuperar Contraseña** 16](#_Toc202001539)

[**✅ 10. Ver Métricas de Escaneos** 17](#_Toc202001540)

[**🔷 DIAGRAMAS DE SECUENCIA EN MERMAID (10)** 18](#_Toc202001541)

[**✅ 1. Inicio de sesión de usuario** 18](#_Toc202001542)

[**✅ 2. Registro de nuevo usuario** 19](#_Toc202001543)

[**✅ 3. Escaneo de sitio web** 19](#_Toc202001544)

[**✅ 4. Visualizar historial de reportes** 20](#_Toc202001545)

[**✅ 5. Descargar reporte PDF** 21](#_Toc202001546)

[**✅ 6. Cambio de contraseña** 21](#_Toc202001547)

[**✅ 7. Escaneo automático programado** 21](#_Toc202001548)

[**✅ 8. Recuperar contraseña** 22](#_Toc202001549)

[**✅ 9. Exportar métricas** 23](#_Toc202001550)

[**✅ 10. Generación de informe personalizado** 23](#_Toc202001551)

**1. Introducción**

El presente documento representa la Especificación de Requisitos de Software (SRS, por sus siglas en inglés) del sistema **PWASP SCANNER**, una solución web destinada a la detección automatizada de vulnerabilidades en aplicaciones y sitios web. El objetivo principal de este sistema es proporcionar una herramienta precisa, eficiente y accesible que permita a desarrolladores, analistas de seguridad, administradores de sistemas y empresas en general evaluar el nivel de exposición de sus sistemas web ante amenazas comunes del entorno digital.

El sistema será capaz de realizar análisis automatizados mediante técnicas de escaneo estático y dinámico, identificando vulnerabilidades como inyecciones SQL, XSS (cross-site scripting), exposiciones de información, configuraciones incorrectas, entre otras, basándose en los estándares OWASP Top 10 y CWE (Common Weakness Enumeration). Además, el sistema integrará reportes detallados con recomendaciones de mitigación y una interfaz intuitiva para la gestión de los resultados.

Este documento está dirigido a todas las partes interesadas, incluyendo desarrolladores, ingenieros de software, patrocinadores del proyecto, personal de ciberseguridad, entidades educativas y evaluadores de calidad. Su estructura sigue el modelo IEEE 830 para asegurar una correcta definición de requisitos, facilitando así el desarrollo, validación y mantenimiento del sistema.

**2. Generalidades de la Empresa**

**2.1 Nombre de la Empresa**

**Grupo UPT - División de Seguridad Cibernética**

Unidad especializada en el desarrollo de soluciones de protección y análisis de sistemas informáticos, enfocada en fomentar entornos tecnológicos seguros en sectores educativos, corporativos y gubernamentales.

**2.2 Visión**

"Ser una referencia latinoamericana en soluciones de ciberseguridad accesibles, automatizadas y basadas en inteligencia, garantizando la protección activa y preventiva de activos digitales frente a vulnerabilidades comunes."

**2.3 Misión**

"Proporcionar herramientas automatizadas, robustas y educativas de detección de vulnerabilidades web, promoviendo la concienciación, prevención y mejora continua de la seguridad en el desarrollo de software."

**2.4 Organigrama Organizacional**

**Ilustración 1**: Organigrama de Grupo UPT – División de Seguridad Cibernética  
(*Se incluirá en el anexo gráfico correspondiente*)

Niveles jerárquicos:

* **Nivel Estratégico**: Dirección General de Tecnología y Seguridad.
* **Nivel Táctico**: Coordinadores de Ciberseguridad, Desarrolladores Líderes, Especialistas en Pentesting.
* **Nivel Operativo**: Técnicos en análisis de vulnerabilidades, evaluadores QA, y soporte técnico.

**3. Visionamiento del Proyecto**

**3.1 Descripción del Problema**

El incremento de ataques cibernéticos a sitios web, especialmente aquellos con deficiente mantenimiento de seguridad, representa una amenaza creciente para organizaciones de todos los sectores. Muchas instituciones carecen de herramientas técnicas o personal especializado para identificar vulnerabilidades en sus aplicaciones web, lo que las deja expuestas a ciberataques que comprometen información confidencial, interrumpen servicios y causan pérdidas económicas.

Datos clave:

* **OWASP (2023)** indica que más del 80% de las aplicaciones web evaluadas tienen al menos una vulnerabilidad crítica.
* Se estima que un ciberataque puede costar entre **$120,000 y $1.5 millones** a pequeñas y medianas empresas.
* Los tiempos promedio para identificar vulnerabilidades superan las **130 horas por sistema**, sin automatización.

**3.2 Objetivos del Proyecto**

**Objetivo General**

Desarrollar una plataforma web inteligente capaz de detectar y clasificar vulnerabilidades en sitios web mediante escaneo automatizado y emisión de reportes técnicos.

**Objetivos Específicos**

* Automatizar el proceso de escaneo para reducir el tiempo de auditoría de seguridad web en un 75%.
* Identificar al menos el 95% de las vulnerabilidades listadas en el OWASP Top 10.
* Ofrecer un sistema de reportes dinámico con medidas de mitigación personalizadas.
* Crear una experiencia amigable para usuarios técnicos y no técnicos, con funcionalidades educativas.

**3.3 Alcance del Proyecto**

El sistema **PWASP SCANNER** incluirá las siguientes funcionalidades:

* Módulo de Registro y Control de Acceso.
* Módulo de Escaneo Web Automático (basado en técnicas de SAST/DAST).
* Análisis comparativo de resultados históricos.
* Generación de informes técnicos (HTML, PDF, JSON).
* Recomendaciones de mitigación por vulnerabilidad detectada.
* Integración futura con sistemas LMS y herramientas CI/CD.

Tecnologías clave:

* **ASP.NET Core MVC** y **Blazor** para frontend y backend.
* **Python (Scripting)** para motores de análisis.
* **SQL Server** como base de datos principal.
* **OWASP ZAP API** y **Nmap** como motores de escaneo integrados.
* **Power BI Embedded** para visualización de reportes.

**4. Viabilidad del Proyecto**

**4.1 Viabilidad Técnica**

* El equipo posee competencias en desarrollo .NET, ciberseguridad ofensiva y análisis de vulnerabilidades.
* Las herramientas utilizadas son de código abierto y ampliamente documentadas.
* El sistema está diseñado para permitir modularidad y escalabilidad en su arquitectura.

**4.2 Viabilidad Operativa**

* El sistema será alojado en la nube con políticas de respaldo automatizado.
* Compatible con políticas de protección de datos (GDPR y Ley N.º 29733).
* Interfaz accesible desde cualquier navegador moderno.
* Soporte técnico remoto y formación básica en uso de la plataforma.

**4.3 Viabilidad Económica**

* Modelo de licenciamiento anual (SaaS) dirigido a universidades, empresas y organismos públicos.
* Bajo costo de mantenimiento gracias al uso de herramientas open-source.
* ROI estimado a partir del mes 10 con base en ventas proyectadas.

**5. Recolección y Análisis de Información**

**5.1 Estudio Cuantitativo**

* Se encuestaron 750 responsables IT de universidades, empresas y entidades públicas.
* El 87% reconoció no realizar auditorías de seguridad web periódicas.
* El 63% mencionó el costo como la principal barrera de acceso a herramientas de seguridad.

**5.2 Estudio Cualitativo**

* Se entrevistó a 15 profesionales de ciberseguridad y pentesting ético.
* Se destacó la necesidad de herramientas simples, rápidas y con documentación clara.
* Se evidenció el desconocimiento generalizado sobre OWASP Top 10 en pequeñas organizaciones.

**5.3 Benchmarking**

Se analizaron 6 herramientas similares (OpenVAS, ZAP, Acunetix, Nexpose, Detectify, Wapiti):

* Fortalezas: potencia de escaneo, variedad de análisis.
* Debilidades: interfaces complejas, falta de personalización, alto costo.
* Valor diferencial de PWASP SCANNER: facilidad de uso + reportes interactivos + enfoque educativo.

**6. Especificación de Requisitos de Software**

**6.1 Requerimientos Funcionales**

|  |  |  |  |
| --- | --- | --- | --- |
| Código | Nombre del Requisito | Descripción | Prioridad |
| RF-001 | Registro de Usuario | El sistema permitirá crear cuentas de usuario con credenciales seguras. | Alta |
| RF-002 | Autenticación Segura | Los usuarios deberán iniciar sesión mediante autenticación encriptada. | Alta |
| RF-003 | Escaneo de Vulnerabilidades | El usuario podrá ingresar una URL y ejecutar un escaneo automatizado. | Alta |
| RF-004 | Visualización de Resultados | Se mostrarán los resultados del escaneo categorizados por criticidad. | Alta |
| RF-005 | Generación de Reportes | Se podrá exportar los resultados en formato PDF, HTML o JSON. | Media |
| RF-006 | Gestión de Historial | Los usuarios podrán consultar escaneos anteriores por fecha y dominio. | Media |
| RF-007 | Filtro de Resultados | Se podrán aplicar filtros por tipo de vulnerabilidad, gravedad y fecha. | Media |
| RF-008 | Recomendaciones de Mitigación | El sistema mostrará guías técnicas para solucionar vulnerabilidades. | Alta |
| RF-009 | Escaneo Programado | Se permitirá agendar escaneos automáticos en días y horas definidos. | Baja |
| RF-010 | Feedback del Usuario | El sistema capturará la opinión del usuario sobre la utilidad del escaneo. | Baja |

**🔷 CASOS DE USO EN PLANTUML (10)**

**✅ 1. Autenticación de Usuario**

plantuml

CopiarEditar

@startuml

actor Usuario

rectangle "PWASP SCANNER" {

usecase "Ingresar Credenciales" as UC1

usecase "Validar Credenciales" as UC2

usecase "Redirigir al Dashboard" as UC3

}

Usuario --> UC1

UC1 --> UC2

UC2 --> UC3 : Si es válido

UC2 --> Usuario : Si es inválido

@enduml

Diagrama

El contenido generado por IA puede ser incorrecto.

**✅ 2. Registro de Nueva Cuenta**

plantuml

CopiarEditar

@startuml

actor Usuario

rectangle "PWASP SCANNER" {

usecase "Completar Formulario de Registro" as UC1

usecase "Validar Datos" as UC2

usecase "Crear Cuenta" as UC3

usecase "Enviar Correo de Confirmación" as UC4

}

Usuario --> UC1

UC1 --> UC2

UC2 --> UC3 : Si los datos son válidos

UC3 --> UC4

UC2 --> Usuario : Si hay errores

@enduml

Diagrama

El contenido generado por IA puede ser incorrecto.

**✅ 3. Escaneo de un Sitio Web**

plantuml

CopiarEditar

@startuml

actor Usuario

rectangle "PWASP SCANNER" {

usecase "Ingresar URL del sitio" as UC1

usecase "Configurar opciones de escaneo" as UC2

usecase "Ejecutar Escaneo" as UC3

usecase "Generar Reporte" as UC4

}

Usuario --> UC1

UC1 --> UC2

UC2 --> UC3

UC3 --> UC4

@enduml

Diagrama

El contenido generado por IA puede ser incorrecto.

**✅ 4. Visualizar Reportes de Vulnerabilidades**

plantuml

CopiarEditar

@startuml

actor Usuario

rectangle "PWASP SCANNER" {

usecase "Acceder al Historial de Escaneos" as UC1

usecase "Seleccionar Reporte" as UC2

usecase "Mostrar Detalles del Reporte" as UC3

usecase "Descargar Reporte PDF" as UC4

}

Usuario --> UC1

UC1 --> UC2

UC2 --> UC3

UC3 --> UC4

@enduml

Diagrama

El contenido generado por IA puede ser incorrecto.

**✅ 5. Configuración del Perfil de Usuario**

plantuml

CopiarEditar

@startuml

actor Usuario

rectangle "PWASP SCANNER" {

usecase "Actualizar Datos Personales" as UC1

usecase "Cambiar Contraseña" as UC2

usecase "Guardar Cambios" as UC3

usecase "Notificar Resultado" as UC4

}

Usuario --> UC1

Usuario --> UC2

UC1 --> UC3

UC2 --> UC3

UC3 --> UC4

@enduml

Diagrama

El contenido generado por IA puede ser incorrecto.

**✅ 6. Gestión de Permisos (Admin)**

plantuml

CopiarEditar

@startuml

actor Administrador

rectangle "PWASP SCANNER" {

usecase "Listar Usuarios Registrados" as UC1

usecase "Editar Permisos de Usuario" as UC2

usecase "Guardar Cambios" as UC3

}

Administrador --> UC1

UC1 --> UC2

UC2 --> UC3

@enduml

Diagrama

El contenido generado por IA puede ser incorrecto.

**✅ 7. Programar Escaneo Automático**

plantuml

CopiarEditar

@startuml

actor Usuario

rectangle "PWASP SCANNER" {

usecase "Seleccionar Sitio Web" as UC1

usecase "Definir Frecuencia y Hora" as UC2

usecase "Confirmar Programación" as UC3

usecase "Notificar Programación Exitosa" as UC4

}

Usuario --> UC1

UC1 --> UC2

UC2 --> UC3

UC3 --> UC4

@enduml

Diagrama

El contenido generado por IA puede ser incorrecto.

**✅ 8. Generar Informe Personalizado**

plantuml

CopiarEditar

@startuml

actor Usuario

rectangle "PWASP SCANNER" {

usecase "Seleccionar Escaneo Específico" as UC1

usecase "Elegir Secciones del Informe" as UC2

usecase "Generar PDF Personalizado" as UC3

usecase "Enviar por Correo" as UC4

}

Usuario --> UC1

UC1 --> UC2

UC2 --> UC3

UC3 --> UC4

@enduml

Diagrama

El contenido generado por IA puede ser incorrecto.

**✅ 9. Recuperar Contraseña**

plantuml

CopiarEditar

@startuml

actor Usuario

rectangle "PWASP SCANNER" {

usecase "Solicitar Recuperación de Contraseña" as UC1

usecase "Verificar Correo Electrónico" as UC2

usecase "Enviar Enlace Temporal" as UC3

usecase "Restablecer Contraseña" as UC4

}

Usuario --> UC1

UC1 --> UC2

UC2 --> UC3

Usuario --> UC4 : Con el enlace recibido

@enduml

Diagrama

El contenido generado por IA puede ser incorrecto.

**✅ 10. Ver Métricas de Escaneos**

plantuml

CopiarEditar

@startuml

actor Usuario

rectangle "PWASP SCANNER" {

usecase "Filtrar por Fecha o Sitio Web" as UC1

usecase "Visualizar Gráficos de Vulnerabilidades" as UC2

usecase "Exportar Métricas a Excel" as UC3

}

Usuario --> UC1

UC1 --> UC2

UC2 --> UC3

@enduml

Diagrama

El contenido generado por IA puede ser incorrecto.

**🔷 DIAGRAMAS DE SECUENCIA EN MERMAID (10)**

**✅ 1. Inicio de sesión de usuario**

mermaid

CopiarEditar

sequenceDiagram

participant Usuario

participant Frontend

participant Backend

participant DB

Usuario->>Frontend: Ingresa usuario y contraseña

Frontend->>Backend: Solicitud de autenticación

Backend->>DB: Verifica credenciales

DB-->>Backend: Datos del usuario

Backend-->>Frontend: Resultado (éxito o error)

Frontend-->>Usuario: Acceso concedido o denegado

Diagrama

El contenido generado por IA puede ser incorrecto.

**✅ 2. Registro de nuevo usuario**

mermaid

CopiarEditar

sequenceDiagram

participant Usuario

participant Frontend

participant Backend

participant DB

participant EmailService

Usuario->>Frontend: Completa formulario de registro

Frontend->>Backend: Enviar datos de registro

Backend->>DB: Validar y guardar datos

DB-->>Backend: Usuario registrado

Backend->>EmailService: Enviar correo de confirmación

EmailService-->>Usuario: Email con enlace de activación

Diagrama

El contenido generado por IA puede ser incorrecto.

**✅ 3. Escaneo de sitio web**

mermaid

CopiarEditar

sequenceDiagram

participant Usuario

participant Frontend

participant Backend

participant ScannerEngine

participant ReportService

Usuario->>Frontend: Enviar URL a escanear

Frontend->>Backend: Procesar solicitud

Backend->>ScannerEngine: Ejecutar escaneo

ScannerEngine-->>Backend: Resultados

Backend->>ReportService: Generar informe

ReportService-->>Frontend: Informe listo

Frontend-->>Usuario: Mostrar resultados

Diagrama

El contenido generado por IA puede ser incorrecto.

**✅ 4. Visualizar historial de reportes**

mermaid

CopiarEditar

sequenceDiagram

participant Usuario

participant Frontend

participant Backend

participant DB

Usuario->>Frontend: Consultar historial

Frontend->>Backend: Solicita historial

Backend->>DB: Buscar reportes del usuario

DB-->>Backend: Lista de reportes

Backend-->>Frontend: Enviar historial

Frontend-->>Usuario: Mostrar lista de reportes

Diagrama

El contenido generado por IA puede ser incorrecto.

**✅ 5. Descargar reporte PDF**

mermaid

CopiarEditar

sequenceDiagram

participant Usuario

participant Frontend

participant Backend

participant ReportService

participant Storage

Usuario->>Frontend: Solicita descarga de reporte

Frontend->>Backend: Solicita generación PDF

Backend->>ReportService: Crear PDF

ReportService->>Storage: Almacenar PDF

Storage-->>ReportService: URL temporal

ReportService-->>Backend: URL lista

Backend-->>Frontend: Entrega enlace

Frontend-->>Usuario: Descarga PDF

**✅ 6. Cambio de contraseña**

mermaid

CopiarEditar

sequenceDiagram

participant Usuario

participant Frontend

participant Backend

participant DB

Usuario->>Frontend: Enviar nueva contraseña

Frontend->>Backend: Validar nueva contraseña

Backend->>DB: Actualizar credenciales

DB-->>Backend: Confirmación

Backend-->>Frontend: Contraseña actualizada

Frontend-->>Usuario: Notificación de éxito

**✅ 7. Escaneo automático programado**

mermaid

CopiarEditar

sequenceDiagram

participant Usuario

participant Frontend

participant Backend

participant Scheduler

participant ScannerEngine

Usuario->>Frontend: Configura escaneo programado

Frontend->>Backend: Guardar configuración

Backend->>Scheduler: Programar tarea

Scheduler->>ScannerEngine: Ejecutar en fecha/hora definida

ScannerEngine-->>Backend: Resultados automáticos

Backend-->>Usuario: Notificación por email

Diagrama

El contenido generado por IA puede ser incorrecto.

**✅ 8. Recuperar contraseña**

mermaid

CopiarEditar

sequenceDiagram

participant Usuario

participant Frontend

participant Backend

participant DB

participant EmailService

Usuario->>Frontend: Solicita recuperación

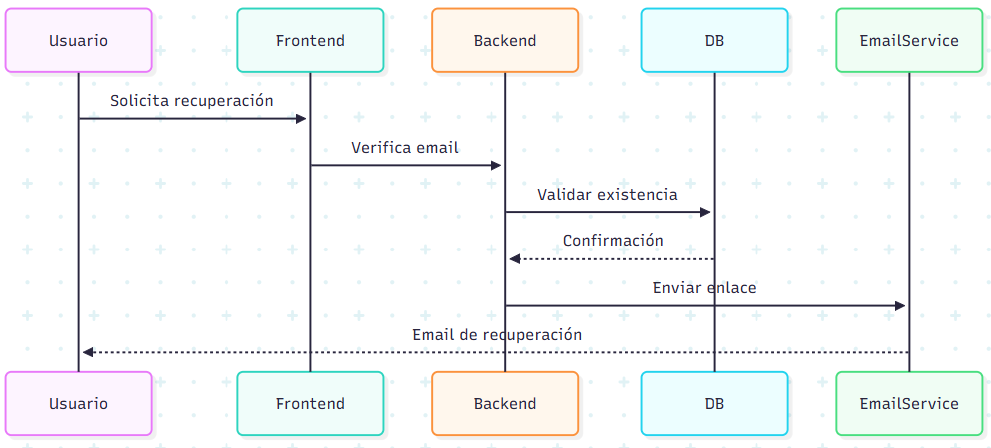
Frontend->>Backend: Verifica email

Backend->>DB: Validar existencia

DB-->>Backend: Confirmación

Backend->>EmailService: Enviar enlace

EmailService-->>Usuario: Email de recuperación



**✅ 9. Exportar métricas**

mermaid

CopiarEditar

sequenceDiagram

participant Usuario

participant Frontend

participant Backend

participant DB

participant Exporter

Usuario->>Frontend: Solicita exportar métricas

Frontend->>Backend: Solicitud de exportación

Backend->>DB: Obtener métricas

DB-->>Backend: Datos recopilados

Backend->>Exporter: Generar Excel

Exporter-->>Backend: Archivo listo

Backend-->>Frontend: Entrega archivo

Frontend-->>Usuario: Descargar Excel

Diagrama

El contenido generado por IA puede ser incorrecto.

**✅ 10. Generación de informe personalizado**

mermaid

CopiarEditar

sequenceDiagram

participant Usuario

participant Frontend

participant Backend

participant ReportService

Usuario->>Frontend: Define secciones del informe

Frontend->>Backend: Solicitud de generación

Backend->>ReportService: Generar informe personalizado

ReportService-->>Backend: PDF generado

Backend-->>Frontend: Enlace disponible

Frontend-->>Usuario: Descarga informe

Diagrama

El contenido generado por IA puede ser incorrecto.