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***

# PWASP SCANNER – Sistema de Detección de Vulnerabilidades Web

# Documento - Diccionario de Datos

**Versión *1.0***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CONTROL DE VERSIONES | | | | | |
| Versión | Hecha por | Revisada por | Aprobada por | Fecha | Motivo |
| 1.0 | JCC | JCC | JCC | 26/06/2025 | Versión Original |

ÍNDICE GENERAL

[UNIVERSIDAD PRIVADA DE TACNA 1](#_Toc202369671)

[PWASP SCANNER – Sistema de Detección de Vulnerabilidades Web 2](#_Toc202369672)

[Documento - Diccionario de Datos 2](#_Toc202369673)

[**Introducción** 4](#_Toc202369674)

[**Estructura del Diccionario** 4](#_Toc202369675)

[**Diccionario de Tablas** 4](#_Toc202369676)

[**Tabla: Usuarios** 4](#_Toc202369677)

[**Tabla: Escaneos** 5](#_Toc202369678)

[**Tabla: Vulnerabilidades** 5](#_Toc202369679)

[**Tabla: Reportes** 6](#_Toc202369680)

[**Tabla: LogEventos** 6](#_Toc202369681)

[**Observaciones Generales** 7](#_Toc202369682)

[**Conclusión** 7](#_Toc202369683)

**Introducción**

El presente documento corresponde al **Diccionario de Datos** del sistema *PWASP SCANNER*, cuyo propósito es describir detalladamente **todas las estructuras de datos utilizadas en el sistema**, incluyendo nombres de tablas, campos, tipos de datos, claves primarias y foráneas, y reglas de validación.

Este diccionario es esencial para garantizar la **integridad y comprensión del modelo de datos**, facilitando el desarrollo, mantenimiento y escalabilidad del sistema.

**Estructura del Diccionario**

Cada entidad o tabla del sistema se presenta en una tabla con los siguientes campos:

* **Nombre del Campo:** Nombre técnico del atributo.
* **Tipo de Dato:** Tipo de dato definido en SQL Server (o sistema equivalente).
* **Tamaño:** Longitud máxima (si aplica).
* **Descripción:** Breve explicación del campo.
* **Clave Primaria (PK):** Si el campo es clave primaria.
* **Clave Foránea (FK):** Si el campo referencia a otra tabla.
* **Restricciones/Validaciones:** Reglas especiales (único, no nulo, formato, etc.)

**Diccionario de Tablas**

**Tabla: Usuarios**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nombre del Campo | Tipo de Dato | Tamaño | Descripción | PK | FK | Restricciones/Validaciones |
| id\_usuario | INT | — | Identificador único del usuario | Sí | No | AUTO\_INCREMENT, NOT NULL |
| nombre\_usuario | VARCHAR | 100 | Nombre completo del usuario | No | No | NOT NULL |
| correo | VARCHAR | 150 | Correo electrónico del usuario | No | No | NOT NULL, UNIQUE, formato email |
| contraseña | VARCHAR | 255 | Contraseña encriptada del usuario | No | No | NOT NULL |
| rol | VARCHAR | 50 | Rol del usuario (admin, básico) | No | No | DEFAULT: 'básico' |
| fecha\_registro | DATETIME | — | Fecha de creación del usuario | No | No | DEFAULT CURRENT\_TIMESTAMP |

**Tabla: Escaneos**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nombre del Campo | Tipo de Dato | Tamaño | Descripción | PK | FK | Restricciones/Validaciones |
| id\_escaneo | INT | — | Identificador único del escaneo | Sí | No | AUTO\_INCREMENT |
| id\_usuario | INT | — | Usuario que realizó el escaneo | No | Sí (Usuarios) | NOT NULL |
| url\_analizada | TEXT | — | URL objetivo del escaneo | No | No | NOT NULL |
| fecha\_escaneo | DATETIME | — | Fecha en que se realizó el escaneo | No | No | DEFAULT CURRENT\_TIMESTAMP |
| tipo\_escaneo | VARCHAR | 50 | Tipo de escaneo (rápido, completo, autenticado) | No | No | DEFAULT 'rápido' |

**Tabla: Vulnerabilidades**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nombre del Campo | Tipo de Dato | Tamaño | Descripción | PK | FK | Restricciones/Validaciones |
| id\_vulnerabilidad | INT | — | Identificador único | Sí | No | AUTO\_INCREMENT |
| id\_escaneo | INT | — | Escaneo asociado | No | Sí (Escaneos) | NOT NULL |
| tipo\_vulnerabilidad | VARCHAR | 100 | Tipo detectado (XSS, SQLi, CSRF, etc.) | No | No | NOT NULL |
| descripcion | TEXT | — | Detalle técnico de la vulnerabilidad | No | No | — |
| gravedad | VARCHAR | 20 | Nivel de gravedad (Alta, Media, Baja) | No | No | CHECK ('Alta','Media','Baja') |
| ruta\_afectada | TEXT | — | Ruta o parámetro afectado | No | No | — |

**Tabla: Reportes**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nombre del Campo | Tipo de Dato | Tamaño | Descripción | PK | FK | Restricciones/Validaciones |
| id\_reporte | INT | — | Identificador del reporte generado | Sí | No | AUTO\_INCREMENT |
| id\_escaneo | INT | — | Escaneo asociado al reporte | No | Sí (Escaneos) | NOT NULL |
| formato | VARCHAR | 10 | Formato generado (PDF, CSV, HTML) | No | No | NOT NULL |
| ruta\_archivo | TEXT | — | Ubicación del archivo en el sistema | No | No | NOT NULL |
| fecha\_generado | DATETIME | — | Fecha de creación del reporte | No | No | DEFAULT CURRENT\_TIMESTAMP |

**Tabla: LogEventos**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nombre del Campo | Tipo de Dato | Tamaño | Descripción | PK | FK | Restricciones/Validaciones |
| id\_evento | INT | — | Identificador único del evento | Sí | No | AUTO\_INCREMENT |
| id\_usuario | INT | — | Usuario que generó el evento | No | Sí (Usuarios) | — |
| tipo\_evento | VARCHAR | 100 | Tipo de actividad (login, escaneo, error, etc.) | No | No | NOT NULL |
| descripcion | TEXT | — | Detalle del evento ocurrido | No | No | — |
| fecha\_evento | DATETIME | — | Fecha y hora del evento | No | No | DEFAULT CURRENT\_TIMESTAMP |

**Observaciones Generales**

* Las relaciones entre tablas están correctamente normalizadas.
* Se aplican claves primarias en todas las entidades principales.
* Las claves foráneas aseguran la integridad referencial entre usuarios, escaneos y reportes.
* Se utilizan restricciones como NOT NULL, UNIQUE y CHECK para validar y proteger la consistencia de los datos.
* Las fechas de registro son manejadas automáticamente con valores por defecto del sistema.

**Conclusión**

Este diccionario de datos sirve como guía para desarrolladores, analistas, testers y cualquier profesional que necesite entender la estructura interna del sistema *PWASP SCANNER*. A través de este documento se busca garantizar la calidad, coherencia y mantenimiento del modelo de datos en todas las etapas del ciclo de vida del software.