Modelado de amenazas en aplicación web de gestión PyME

Versión 1.0
01/2026

Proyecto: Mini SSDLC aplicado a sistemas web

Autor: Pedro Garvich

1. Resumen ejecutivo

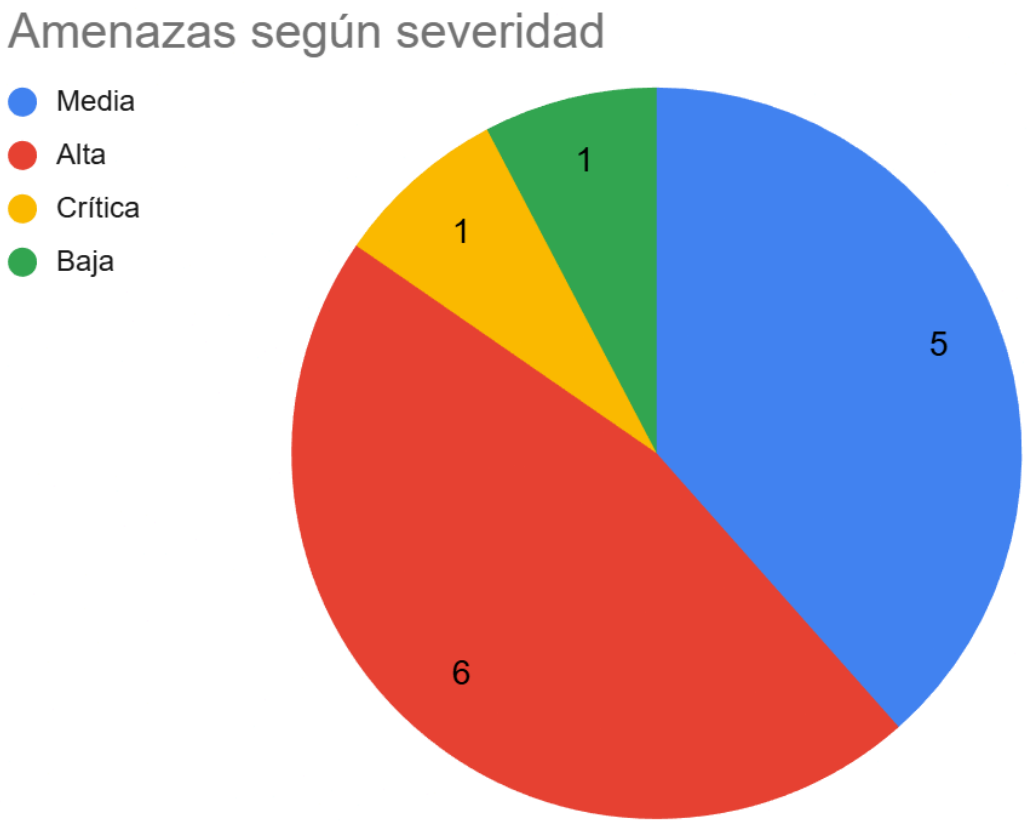
El sistema analizado es una aplicación web de gestión interna destinada a una empresa dedicada a la fabricación e instalación domiciliaria de estructuras metálicas recreativas para exteriores.

Su objetivo principal es centralizar la información operativa y financiera del negocio, actualmente dispersa en planillas y comunicaciones informales, permitiendo una gestión más confiable, trazable y escalable.

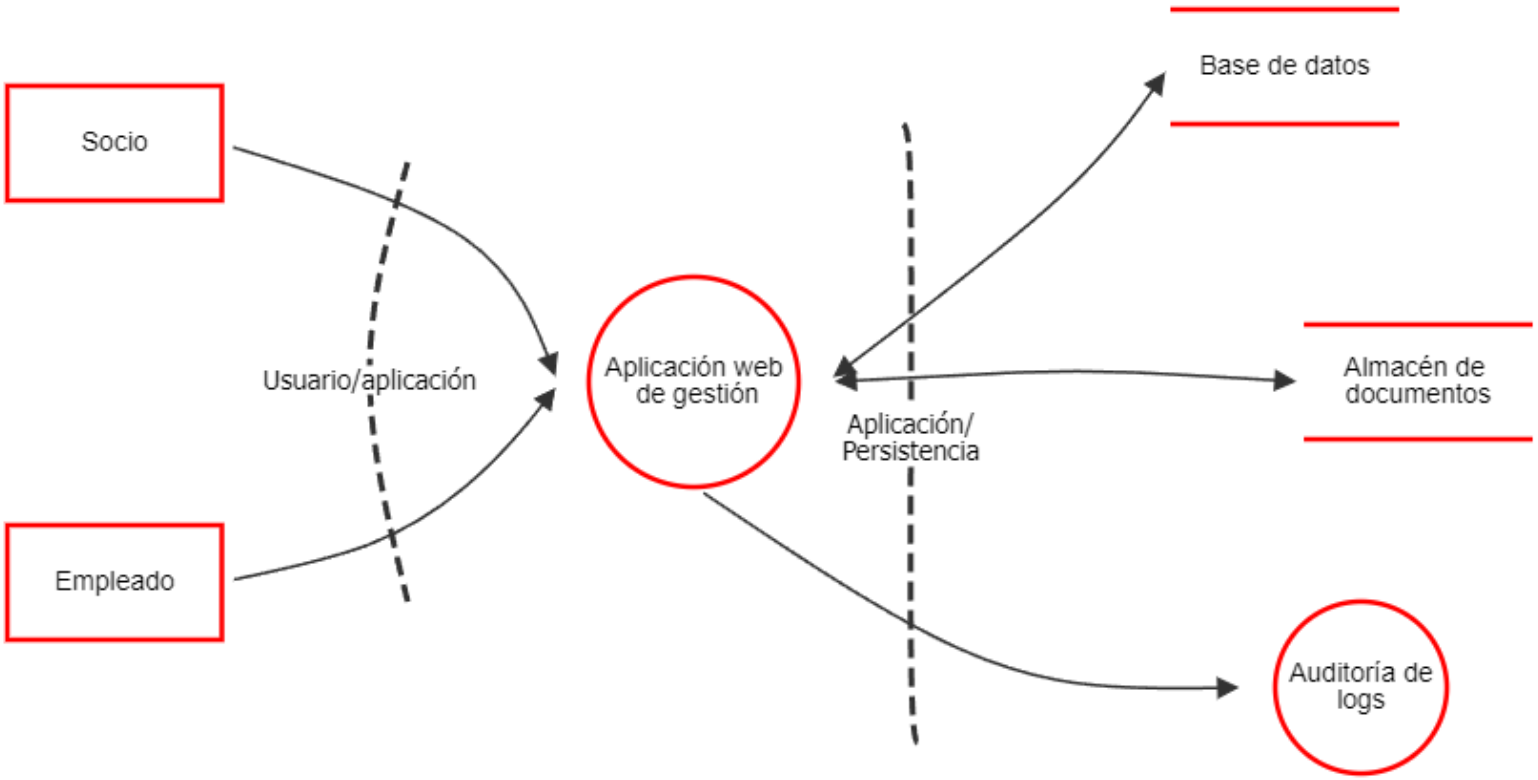
El modelado de amenazas se realizó siguiendo la metodología STRIDE, partiendo del documento de contexto del sistema y con el objetivo de identificar riesgos relevantes para el diseño seguro de la aplicación. El foco se puso en amenazas vinculadas a autenticación, autorización, lógica de negocio y trazabilidad, dado que el sistema gestiona información financiera sensible y operaciones críticas para el negocio.

No se incluyeron aspectos de infraestructura productiva ni configuraciones específicas de hosting, ya que exceden el alcance de este mini SSDLC y corresponderían a una etapa posterior del proyecto real. Los resultados del modelado sirven como insumo directo para la etapa de diseño, permitiendo definir controles de seguridad alineados con OWASP y CWE desde etapas tempranas del desarrollo.

El sistema no tiene exposición pública y está pensado para uso exclusivo de personal interno autorizado.



2. Diagrama de flujo de datos



2.1 Supuestos de Seguridad y Alcance

Para el presente modelado, se han definido los siguientes supuestos como precondiciones de seguridad del entorno, los cuales son requisitos indispensables para la efectividad de los controles de aplicación propuestos:

- **Protección de la Información en Tránsito:** Se asume la implementación obligatoria de protocolos de comunicación cifrada (**TLS 1.2 o superior**) en todos los flujos de datos. Esto incluye la interacción entre el cliente (Socio/Empleado) y la Aplicación Web, así como las comunicaciones internas entre la Aplicación, la Base de Datos y el Almacén de Documentos.
- **Integridad del Entorno de Ejecución:** Se asume que el servidor de aplicaciones y la base de datos operan en un entorno controlado donde el acceso físico y administrativo a la infraestructura está restringido.
- **Aislamiento de Red:** Las bases de datos y almacenes de logs no están expuestos directamente a internet, sino que solo aceptan conexiones provenientes del proceso de la aplicación.

3. Matriz Consolidada de Amenazas

ID	Componente / Flujo	Amenaza	Categoría	Severidad	Mitigación Propuesta
1	Socio / Empleado	Negación de acciones (repudio de gastos o presupuestos)	Repudiation	Medium	Logs de acciones críticas, asociación usuario-timestamp e inmutabilidad lógica.
2	Socio	Suplantación de identidad para acceso financiero	Spoofing	High	Autenticación robusta y uso de MFA (TOTP) para roles sensibles.
3	Aplicación Web	Manipulación de datos (montos, estados) desde el cliente	Tampering	Medium	Validación estricta en backend y control de integridad lógica.
4	Aplicación Web	Acceso de empleados a reportes consolidados o márgenes	Info Disclosure	High	Control de acceso basado en roles (RBAC) y separación de endpoints.
5	Aplicación Web	Elevación de privilegios (empleado a socio/admin)	Elevation of Privilege	Critical	Autorización centralizada en backend (no confiar en el frontend).
6	Aplicación Web	Secuestro de sesión o robo de tokens	Spoofing	High	Gestión segura de sesiones, expiración y cookies seguras (HttpOnly, Secure).
7	Aplicación Web	Salto de reglas de negocio (estados de trabajos/versiones)	Tampering	High	Validaciones de estado y transiciones controladas en la lógica de negocio.
8	Auditoría de Logs	Falta de registro de acciones a nivel aplicación	Repudiation	Medium	Implementación de logging centralizado de eventos de negocio.
9	Base de Datos	Inyección SQL para alteración de registros	Tampering	High	Uso exclusivo de consultas parametrizadas y ORM.
10	Base de Datos	Acceso no autorizado a tablas sensibles por compromiso de BD	Info Disclosure	High	Cifrado lógico, control de acceso a nivel red y gestión de secretos.
11	Almacén de Docs	Alteración de documentos históricos (PDFs)	Tampering	Medium	Almacenamiento con versionado inmutable y prohibición de sobreescritura.
12	Almacén de Docs	Acceso a PDFs mediante manipulación de URLs predecibles	Info Disclosure	Low	Validación de propiedad del recurso y uso de rutas no públicas.
13	Auditoría de Logs	Borrado o alteración de registros de auditoría	Tampering	Medium	Implementación de logs de tipo append-only y acceso restringido.