Contexto y Alcance de Seguridad en aplicación web de gestión PyME

Versión 1.0
01/2026

Proyecto: Mini SSDLC aplicado a sistemas web

Pedro Garvich

Pedro Garvich

Índice

Pedro Garvich

Propósito del documento

El presente documento tiene como objetivo definir el **contexto de seguridad**, el **alcance del análisis** y las **suposiciones iniciales** de un sistema de gestión web, sirviendo como base para:

- el modelado de amenazas
- el diseño seguro
- la planificación de pruebas de seguridad

Todo esto dentro de un enfoque de Secure Software Development Life Cycle (SSDLC).

Este artefacto se elabora **previo a la implementación del código**, siguiendo un enfoque *shift-left* de seguridad.

Descripción general del sistema

El sistema analizado es una **aplicación web de gestión interna** destinada a una empresa dedicada a la fabricación e instalación de estructuras metálicas recreativas en domicilios particulares.

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

Alcance funcional del sistema

El alcance funcional considerado para el análisis de seguridad incluye:

Caja

- Registro de ingresos por cliente y etapa de pago.
- Registro de egresos (compras, sueldos, alquiler, servicios, gastos variables).
- Clasificación de gastos.
- Visualización de caja mensual.

Clientes y trabajos

- Registro de clientes.
- Registro de trabajos asociados.
- Estado del trabajo (presupuestado, en curso, finalizado).
- Pagos parciales y saldo pendiente.

Presupuestos y contratos

- Uso de plantillas estandarizadas.
- Generación de documentos en formato PDF.
- Numeración única de documentos.
- Versionado (los documentos no se modifican; se generan nuevas versiones).

Stock básico

- Registro de insumos (aproximadamente 60 ítems).
- Cantidad disponible.
- Valor de referencia asociado (preferentemente en USD).

Reportes

- Caja mensual.
- Resumen de ingresos y egresos.
- Margen aproximado por trabajo.

Usuarios y roles

El sistema contempla los siguientes roles de usuario:

Socios

Usuarios con **acceso completo a todas las funcionalidades de negocio** del sistema, incluyendo:

- Gestión financiera.
- Gestión de clientes y trabajos.
- Emisión y versionado de documentos.
- Acceso a reportes.

Los socios **no poseen privilegios de administración técnica** del sistema subyacente (infraestructura, base de datos, configuración del entorno).

Empleados

Usuarios con **acceso limitado**, orientado exclusivamente a la carga de gastos operativos (por ejemplo: gastos de obra, cargas de combustible).

No pueden acceder a información financiera consolidada ni modificar datos críticos del negocio.

Administrador del sistema

Rol excepcional, con acceso a operaciones técnicas de alto impacto (por ejemplo, tareas administrativas globales).

Este rol no forma parte del uso cotidiano del sistema y se considera **fuera del alcance funcional normal**, pero relevante a efectos de análisis de riesgos.

Pedro Garvich

Activos críticos

Los principales activos protegidos por el sistema son:

- Información financiera (ingresos, egresos, caja).
- Presupuestos y contratos enviados a clientes.
- Datos personales y comerciales de clientes.
- Reportes.
- Historial de operaciones y registros de auditoría.

La alteración, pérdida o divulgación no autorizada de estos activos puede generar impactos significativos en la operación y en la toma de decisiones del negocio.

Alcance del análisis de seguridad

El análisis de seguridad incluye:

- Autenticación y gestión de sesiones.
- Autorización y control de acceso por roles.
- Gestión de datos financieros y documentos.
- Registro de operaciones y trazabilidad (logs).
- Operaciones de alto impacto sobre datos críticos.

Quedan explícitamente fuera de alcance:

- Configuración y operación del entorno de despliegue productivo
- Integraciones con sistemas externos.
- Firma digital avanzada.
- Automatización CI/CD completa.
- Cumplimiento normativo formal.

Suposiciones y restricciones

Para este análisis se asumen las siguientes condiciones:

- Aplicación web accesible desde navegador (PC o móvil).
- Autenticación basada en usuario y contraseña.
- Sin integraciones externas en la fase inicial.
- Uso por personal no técnico.
- Base de datos centralizada como única fuente de información.

Referencias y marcos considerados

El análisis se apoya conceptualmente en los siguientes marcos y buenas prácticas:

- **OWASP Top 10** (seguridad web).
- **OWASP ASVS**, aplicado a **nivel básico** como guía de controles fundamentales.

- **OWASP Proactive Controls**, como referencia de diseño seguro.
- **ISO/IEC 27001**, considerado a **nivel conceptual**, sin implementación de un ISMS formal.

Estos marcos se utilizan como **referencias técnicas**, no como requisitos contractuales ni de certificación.

Nota sobre el carácter del proyecto

Este documento forma parte de un **proyecto educativo y demostrativo**, orientado a mostrar competencias en análisis de seguridad, modelado de amenazas y diseño seguro en etapas tempranas del ciclo de desarrollo.

No corresponde a un sistema productivo actualmente en operación.