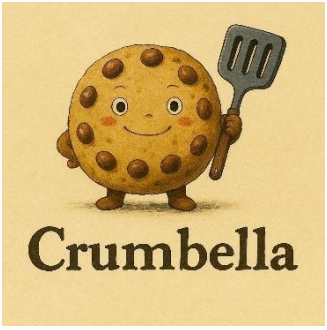
Proyecto CRUMBELLA

Desarrollo e implementación de un sistema integral para la administración del punto de venta, la gestión de pedidos en línea y la automatización de procesos internos de la empresa:

CRUMBELLA



Colaboradores

22001039 RAFAEL GERARDO CAMACHO HERNÁNDEZ

22001494 ALONSO DANIEL LÓPEZ SILVA

18002133 MIGUEL ÁNGEL RODRÍGUEZ PADILLA

21000017 JONATHAN MORENO MUÑOZ

21000407 CARLOS GABRIEL VALDIVIA LÓPEZ

LEÓN, GTO

07 Abril de 2025

Contenido

Introducción

CRUMBELLA es una empresa emergente en el mercado Leones. Nuestro giro principal es producción y venta de galletas artesanales, al intentar llegar al objetivo de ventas mensuales se detectaron varios inconvenientes durante el proceso de producción de las galletas, como el ineficiente registro de mermas, la discordancia continua del corte en la caja, los insumos son susceptibles a pasar su fecha de expiración sin que el personal se de cuenta de ello.

Para eso se trabajo en la idea de implementar u sistema que nos permitiera manejar estos inconvenientes de una forma más segura y un tanto automatizada, así fue como nación el proyecto SWEETRACK una solución digital integral diseñada para gestionar de forma eficiente los procesos clave de una panadería artesanal o industrial. Este sistema busca centralizar el control de inventarios, recetas, producción, ventas, pedidos, proveedores y usuarios, permitiendo a los administradores y trabajadores acceder a herramientas intuitivas que optimicen su operación diaria.

Propuesta de Proyecto

Objetivo General

Desarrollar un sistema web de gestión para galleteria que automatice y digitalice los procesos operativos, administrativos y comerciales de forma segura, escalable y fácil de usar.

Objetivos Específicos

- Controlar de manera precisa el inventario de insumos y productos.
- Facilitar el registro y seguimiento de recetas, pedidos y procesos de producción.
- Llevar un historial confiable de ventas, compras y mermas.
- Permitir la interacción con clientes y proveedores desde una misma plataforma.
- Garantizar la seguridad de los datos mediante roles de usuario, validaciones y logs de auditoría.

Alcance del Sistema

Al llegar al final de la primera versión de nuestro sistema este podra ser capaz de realizar las siguientes acciones:

- Autenticación y gestión de usuarios con niveles de acceso.
- Módulo de inventario con control de stock, pedidos y proveedores.
- Gestión de producción y recetas de productos como galletas.
- Control y registro de ventas, incluyendo reportes y estadísticas.
- Seguimiento de pedidos de clientes con historial y notificaciones.
- Gestión documental e informes de rendimiento.

Acerca del sistema

Módulos del Sistema

Por la naturaleza del proyecto este tiene que estar dividido en distintos módulos para garantizar una correcta funcionalidad del sistema. A continuación, listaremos aquellos que tenemos contemplados para la primera versión funcional:

- **Auth:** Login, registro, perfiles, seguridad con captcha y CSRF
- **Inventario:** Insumos, stock, mermas, proveedores, pedidos
- **Producción:** Pedidos de producción, control de lotes, mermas
- **Ventas:** Registro de ventas, historial, control post-venta
- **Cliente:** Pedidos, historial, perfil de cliente
- **Proveedores:** Gestión de proveedores y sus insumos
- **Recetas:** Crear/editar recetas, costos e ingredientes
- **Pedidos:** Estado de pedidos, notificaciones, historial
- **Informe:** Reportes de ventas, producción, inventario
- **Principal:** Página de inicio, pedidos de clientes, intranet y redirección segura

Tecnologías Utilizadas

Para el desarrollo de Don Galleto se seleccionaron tecnologías modernas y ampliamente adoptadas que permiten garantizar un sistema robusto, seguro y escalable. Estas herramientas facilitan tanto el desarrollo ágil como el mantenimiento a largo plazo, asegurando una experiencia fluida para el usuario final y una estructura sólida para el equipo técnico.

- **Backend:** Flask (Python), SQLAlchemy
- **Frontend:** Bootstrap 5, HTML/CSS/JS
- **Base de Datos:** MySQL (local), adaptable a PostgreSQL o MySQL (en la nube)
- **Seguridad:** Flask-Login, Werkzeug, CSRF Tokens, Captchas

Procesos Internos

Proceso de compra de materia prima

La compra de materia prima será realizada por el encargado de mostrador. El sistema de gestión notificará al usuario mediante una alerta cuando los insumos estén por agotarse, indicando que es necesario reponerlos para continuar con la producción. Al recibir la alerta, el encargado se comunicará con los proveedores, quienes habrán sido seleccionados previamente en función de la relación calidad-precio de sus productos. Además, se priorizará la adquisición de materias primas de producción local siempre que sea posible.

Proceso de venta

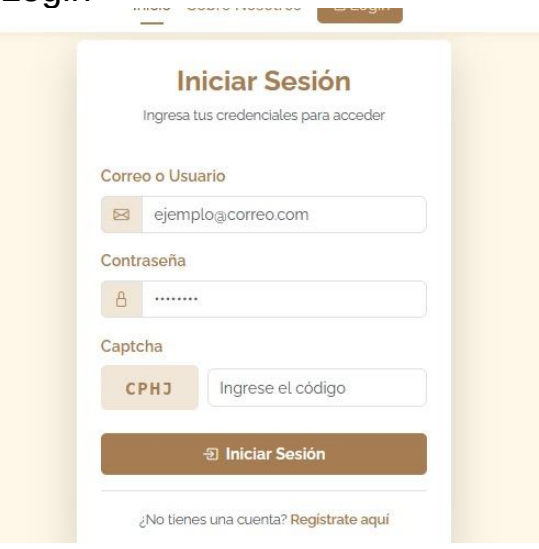
La venta será gestionada por el encargado de mostrador, quien podrá vender las galletas por kilo, por cantidad monetaria o por pieza. El sistema contará con una interfaz gráfica que le permitirá seleccionar el tipo de galleta, consultar el inventario disponible, verificar el precio según la unidad de venta y calcular el precio total. Una vez realizada la venta, el sistema generará un ticket de compra que podrá imprimirse. Además, la transacción quedará registrada en una base de datos para su posterior consulta en caso de ser necesario.

Procesos internos

Para garantizar la calidad del servicio, se implementará un sistema de gestión integral para el negocio. Este sistema permitirá gestionar el proceso de producción, manteniendo informado al encargado de mostrador sobre el estado de cada lote de galletas en producción. Asimismo, facilitará el control de inventarios, tanto de insumos como de productos terminados.
Para asegurar la calidad del producto, solo se permitirá la elaboración de recetas completas, lo que garantizará una consistencia en el sabor entre los diferentes lotes de producción. Finalmente, el sistema también permitirá registrar las mermas generadas durante todo el proceso de producción, lo que contribuirá a un mejor control de costos y eficiencia.

Módulos de Aplicación (Maquetado)

Login

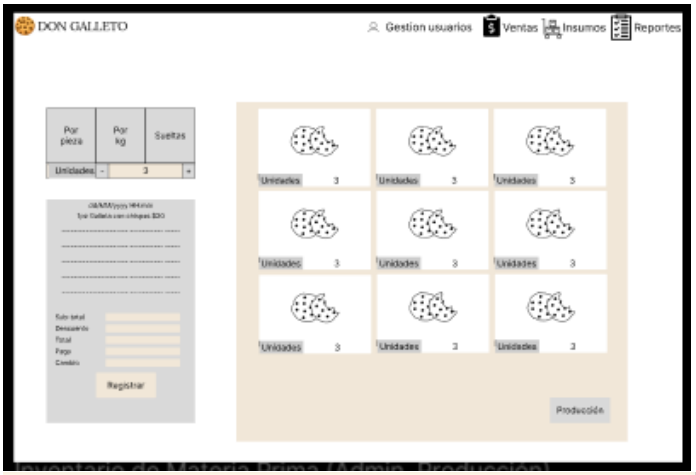


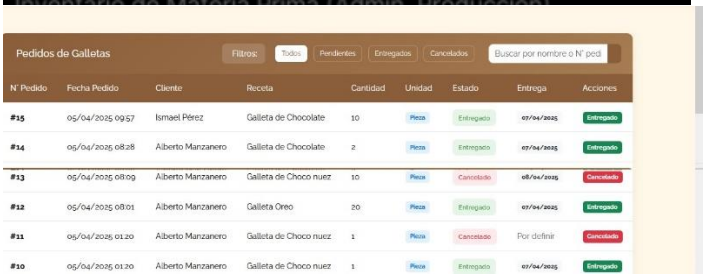
Para poder realizar un pedido en línea o usar el sistema de gestión se tiene que iniciar sesión con un usuario y una contraseña, en caso de que alguien de los clientes no este registrado se tiene una opción para resgitrarse

Pantalla principal

Al iniciar sesión como administrador, mostrador o cocina este es la pantalla de bienvenida, se podrá visualizar un pequeño historial de ventas además saber cuáles son las galletas más vendidas por cada presentación, también este te facilitará en viajar entre los distintos módulos de la aplicación.

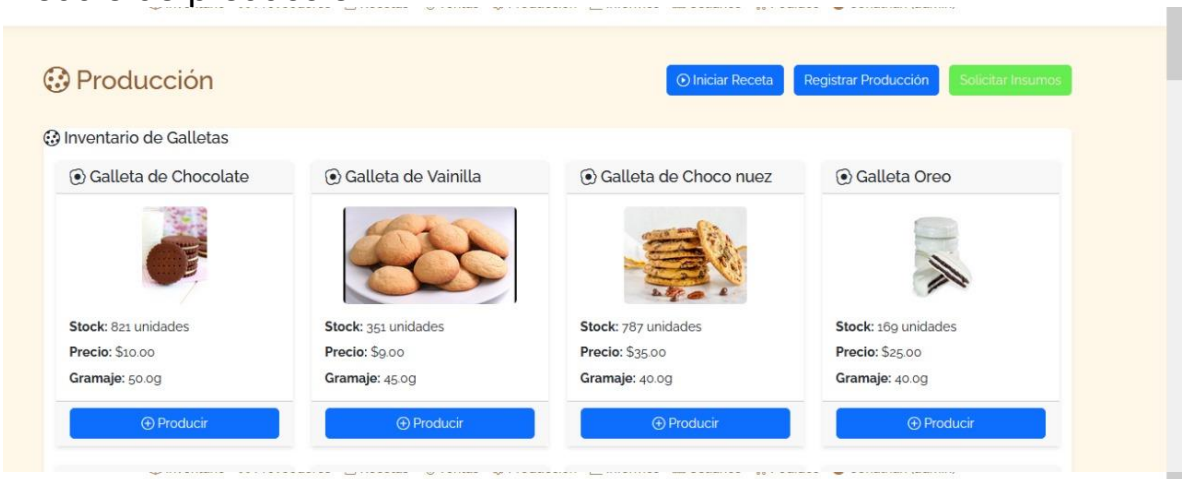
Modulo de ventas

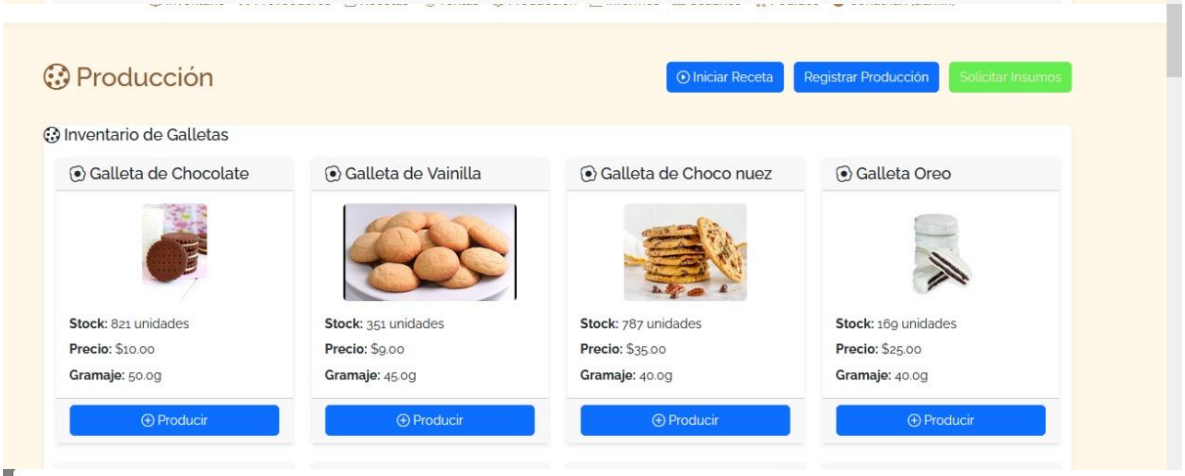




En este modulo se podra realizar la venta desde mostrador de algun producto en exitencia, en este se podra escoger la receta de galleta a vende, la unidad de venta y el precio unitario y el precio total, ademas de un boton para poder guardar la venta en la base de datos para poder ser cunsultada a su posterioridad.

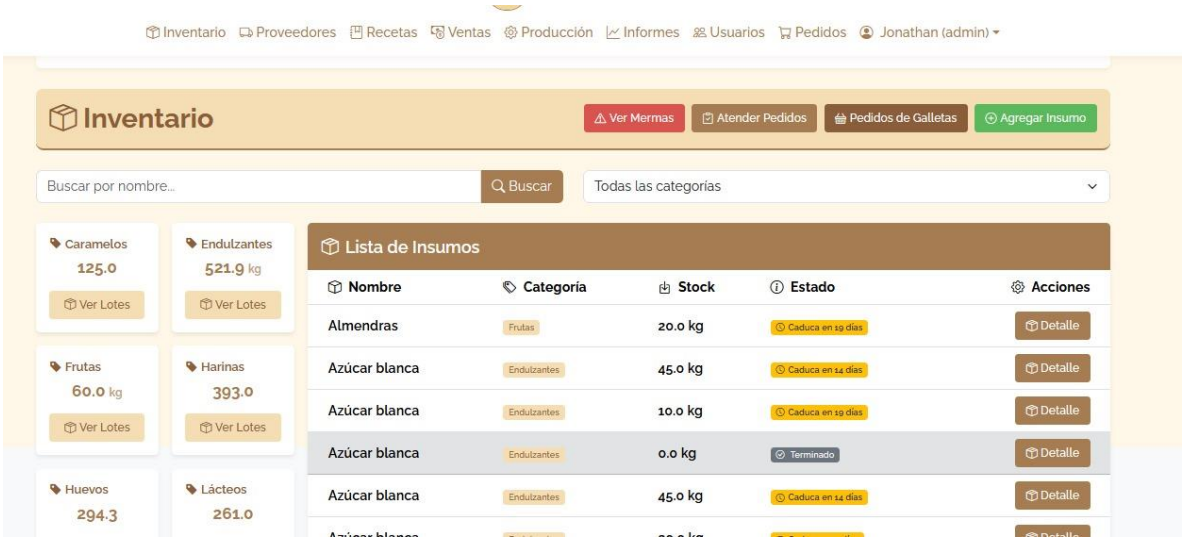
Modulo de produccíon





En este modulo el personal en mostrador podra mandar a pedir alguna receta cuando esta se este terminando en el inventario de galletas, se guardara el pedido y se mostarar en la tabla, desde la cocina el personal podra actualizar el estatus de los pedidos de produccion entre recibido, en preparacion y terminado

Modulo de insumos

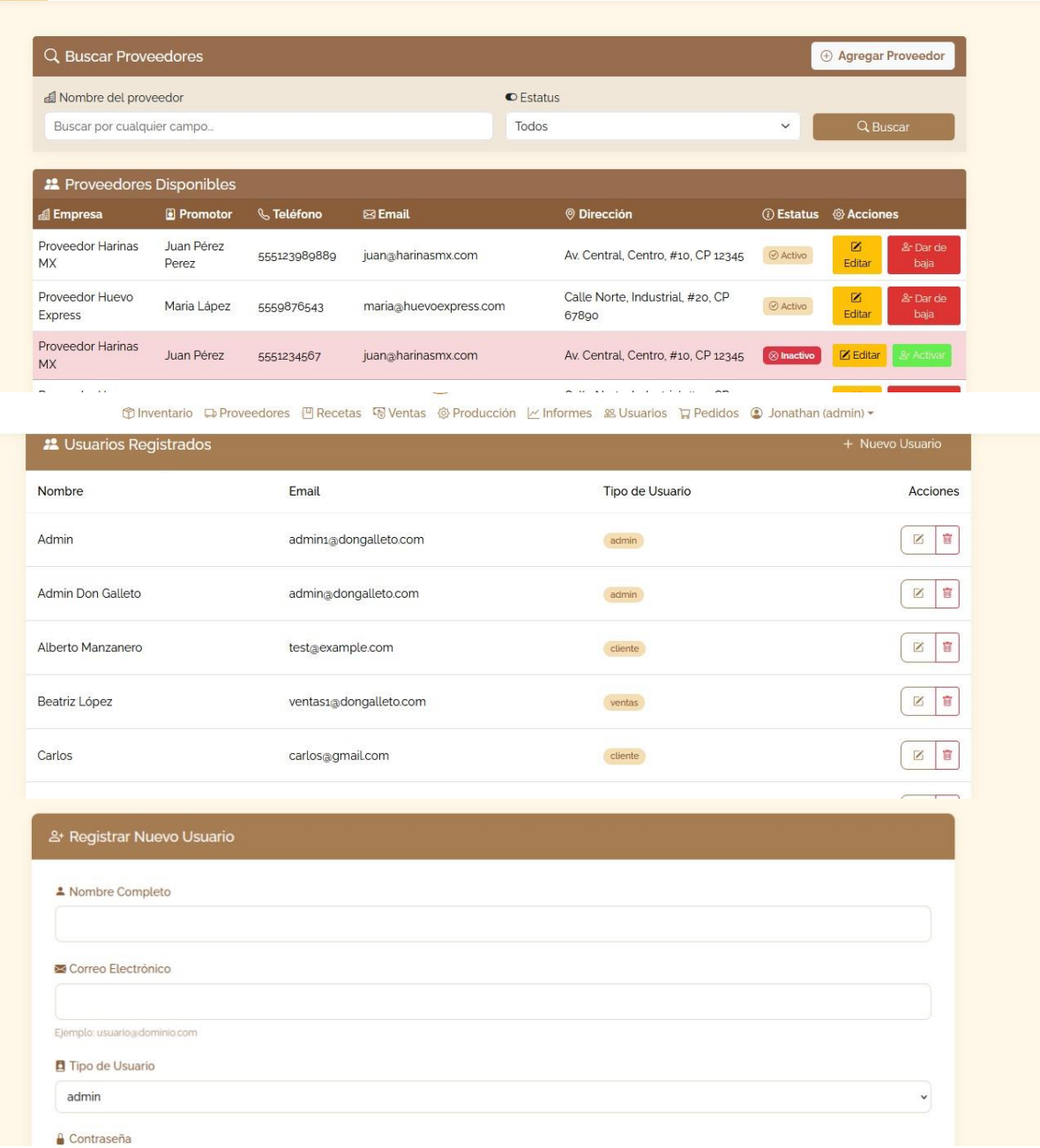


En este módulo podrás visualizar todos los insumos que tienes hasta la fecha, este se dividirá en tres, del lado izquierdo de la pantalla te mostrada los productos existentes, en el centro se podrá ver una tabla con todo el inventario de ese producto separado por lotes, aquí se podrá ver su fecha de vencimiento, la cantidad que se tiene, quien provee ese producto y el total gastado al comprar el producto. Y por último al lado derecho se encuentra un formulario para registrar un nuevo lote de producto entrante.

Reporte de ventas

En este aparatado el personal en casa y el administrador podrán visualizar el total de ventas diario por día, del lado derecho de la pantalla se puede visualizar un calendario, en este podrás escoger una fecha para consultar el total de ventas ese día, y del lado izquierdo se realizará un desglose de la venta.

Módulos de Gestión

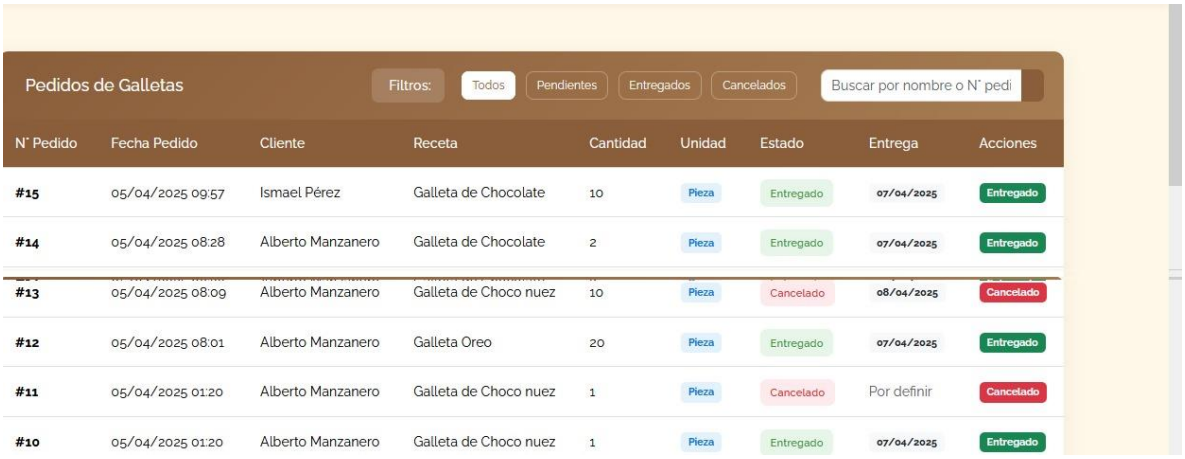


Estos modulos en escencia tiene una funcion similar y es llevar el control de los usuarios, proveedores y galletas, aquí podras visualizar la informacion de cada uno de ellos podras, buscarlos, editarlos o agregar nuevos elementos a cada una de las distintas gestiones.

Pedido online

En este modulo un usuario podra realizar pedidos desde la tienda online para poder recojerlos en caja, podra elegir el sabor de la galleta y su precentacion, ademas se vusalizaran uan imagen del producto, su nombre y su precio.

Carrito



Aquí podrás visualizar el pedido completo de galletas, en este se incluye todos los productos comprados, la cantidad, el precio unitario el precio total de cada uno, además se te presentara la fecha del pedido que funcionara como un historial de las compras online

Casos de Uso

ID	Nombre	Descripción
Requerimientos Funcionales		
RF-01	Registro de Usuarios	El sistema permitirá registrar usuarios con distintos roles (administrador,ciente, ventas, produccion), validando campos como correo, nombre, contraseña y captcha para prevenir automatización.
RF-01-0	Edición de Usuarios	Los usuarios podrán editar su información personal desde su perfil, incluyendo datos de contacto y contraseña, siempre que cumplan con las reglas de seguridad definidas.
RF-03	Eliminación de Cuenta	Los usuarios tendrán la opción de solicitar la eliminación de su cuenta. El sistema aplicará una eliminación lógica para preservar la integridad de los datos históricos.
RF-04	Inicio de Sesión Seguro	Se permitirá el inicio de sesión mediante correo y contraseña, con verificación de captcha para prevenir intentos automatizados. Las sesiones serán gestionadas de forma segura.
RF-05	Gestión de Roles	El sistema contará con roles definidos que determinan el nivel de acceso de cada usuario. Solo administradores podrán modificar roles de otros usuarios.
RF-06	Control de Stock de Insumos	El sistema permitirá llevar un control detallado del stock de insumos, indicando cantidades disponibles, fecha de ingreso, vencimiento y unidad de medida.
RF-07	Registro de Mermas	Se podrá registrar las mermas derivadas de caducidad o errores de producción, afectando automáticamente el inventario correspondiente.
RF-08	Pedidos de Insumos	Los usuarios con permisos podrán registrar pedidos de insumos a proveedores, con seguimiento de estado y notificación de recepción.
RF-09	Gestión de Proveedores	El sistema permitirá registrar y consultar proveedores con información clave como contacto, insumos disponibles y condiciones de entrega.
RF-10	Registro de Producción	El personal podrá registrar lotes de producción con insumos utilizados, fecha de elaboración y cantidad producida.
RF-11	Control de Lotes	El sistema gestionará los lotes de producción para su posterior trazabilidad en ventas o mermas.
RF-12	Registro de Mermas de Producción	Se podrán registrar pérdidas específicas durante el proceso productivo, separadas de las mermas de insumo.
RF-13	Registro de Ventas	Se podrá registrar cada venta realizada, asociándola con productos, cantidades, precios y fecha de la transacción.
RF-14	Historial de Ventas	Los usuarios autorizados podrán consultar un historial detallado de ventas con filtros por fecha, producto o cliente.

RF-15	Pedidos de Clientes	Los clientes podrán realizar pedidos desde el sistema, visualizar su estado en tiempo real y consultar su historial.
RF-16	Notificaciones de Pedido	El sistema generará notificaciones internas que informen al usuario sobre el estado del pedido (recibido, en producción, entregado).
RF-17	Gestión de Recetas	Se podrá crear, editar y eliminar recetas de productos, especificando los ingredientes, cantidades y costos asociados.
RF-18	Cálculo de Costos	El sistema calculará automáticamente el costo de una receta en función del valor actualizado de los insumos utilizados.
RF-19	Informes de Producción	Se podrán generar informes con estadísticas de producción por fecha, producto o lote.
RF-20	Informes de Ventas	Se podrán visualizar reportes gráficos y tabulares con datos de ventas, productos más vendidos y comparación mensual.
RF-21	Informes de Inventario	El sistema ofrecerá reportes que muestren el estado del inventario, entradas, salidas y mermas por periodo.
Requerimientos no funcionales		
RN-01	Seguridad de Datos	Todas las contraseñas se almacenarán en forma encriptada. El sistema protegerá las sesiones mediante tokens y limitará intentos de login.
RN-02	Respuesta y Rendimiento	Las funciones del sistema deberán ejecutarse en un tiempo menor a 2 segundos en promedio, para garantizar una experiencia fluida.
RN-03	Interfaz Amigable	El sistema debe contar con una interfaz clara y responsiva, accesible desde computadoras y dispositivos móviles.
RN-04	Escalabilidad	La arquitectura del sistema debe permitir futuras integraciones y crecimiento hacia soluciones en la nube.
RN-05	Trazabilidad y Logs	Todas las acciones críticas serán registradas en un sistema de logs que facilite la auditoría y el seguimiento del comportamiento del sistema.
Requerimientos de seguridad		
RS-01	Autenticación Segura	El sistema implementará mecanismos de autenticación que incluyan validación por contraseña encriptada, captcha al inicio de sesión y bloqueo por múltiples intentos fallidos.
RS-02	Control de Accesos por Rol	Cada usuario tendrá un rol asignado que limitará o permitirá ciertas funcionalidades dentro del sistema. El sistema mostrará solo las opciones disponibles según el perfil del usuario.
RS-03	Protección contra CSRF y XSS	Las peticiones del sistema incluirán tokens de seguridad CSRF para prevenir ataques de falsificación, y se validará la entrada de datos para evitar inyecciones de código malicioso.
RS-04	Encriptación de Contraseñas	Todas las contraseñas serán almacenadas utilizando algoritmos de hash seguro (como bcrypt), sin posibilidad de desencriptado.

RS-05	Registro de Actividades (Logs)	Se mantendrá un registro detallado de las acciones relevantes realizadas por los usuarios, como inicio de sesión, creación o eliminación de registros, y cambios críticos.
RS-06	Verificación de Captcha en Formularios	Se utilizará CAPTCHA en formularios sensibles como login, recuperación de cuenta y registro, para prevenir acciones automatizadas por bots.
RS-07	Validación de Sesiones	Las sesiones de usuario estarán protegidas por tokens únicos y se invalidarán después de cierto tiempo de inactividad o al cerrar sesión.

Modelado De Amenazas

Riesgo: Control de acceso insuficiente

Probabilidad								
Factores de agente de amenaza					Factores de vulnerabilidad.			
Nivel de habilidad	**Motivo**	**Oportunidad**	**Tamaño**		**Facilidad para Descubrir**	**Facilidad para la Explotación**	**Conciencia**	**Detección de Intrusión**
5 - Uso Avanzado de computadoras	4 - Posible recompensa	4 - Acceso especial o recursos requeridos	4 - Usuarios de intranet		2 - Muy Dificil	3 - Dificil	1 - Desconocido	3 - Registrado y revisado
Probabilidad general:				**3.250**	**MEDIO**			

Impacto técnico					Impacto de negocio			
Pérdida de la Confidencialidad	**Pérdida de Integridad**	**Pérdida en Disponibilidad**	**Pérdida en Responsabilidad**		**Daño Financiero**	**Daño en Reputación**	**No cumplimiento**	**Violación de Privacidad**
4 - Datos críticos mínimos revelados, datos no sensibles extensos revelados	5 - Amplios datos ligeramente corruptos	1 - Servicios secundarios mínimos interrumpidos	7 - Posiblemente rastreable		7 - Efecto significativo en la ganancia anual	5 - Pérdida de buena voluntad	5 - Clara violación	7 - Miles Personas
Impacto técnico general:		**4.250**	**MEDIO**		**Impacto comercial general:**		**6.000**	**ALTO**
Impacto general:				**5.125**	**MEDIO**			

Gravedad general del riesgo = Probabilidad x Impacto				
Impacto	ALTO	Medium	High	CRITICO
	MEDIO	Low	**Medium**	ALTO
	BAJO	Note	Low	MEDIO
		BAJO	MEDIO	ALTO
	Probabilidad			

Niveles de probabilidad e impacto	
0 to <3	BAJO
3 to <6	MEDIO
6 to 9	ALTO

Riesgo: Autenticación débil

Probabilidad								
Factores de agente de amenaza					**Factores de vulnerabilidad.**			
Nivel de habilidad	**Motivo**	**Oportunidad**	**Tamaño**		**Facilidad para Descubrir**	**Facilidad para la Explotación**	**Conciencia**	**Detección de Intrusión**
3 - Algunas Habilidades tecnicas	3 - un poco de posible recompensa	4 - Acceso especial o recursos requeridos	5 - Partners		3 - Dificil	3 - Dificil	6 - Ovio	3 - Registrado y revisado
Probabilidad general:				**3.750**	**MEDIO**			

Impacto técnico					**Impacto de negocio**			
Pérdida de la Confidencialidad	**Pérdida de Integridad**	**Pérdida en Disponibilidad**	**Pérdida en Responsabilidad**		**Daño Financiero**	**Daño en Reputación**	**No cumplimiento**	**Violación de Privacidad**
5 - Extensos datos críticos revelados	3 - Mínimo datos seriamente corruptos	7 - Amplios servicios primarios interrumpidos	1 - totalmente rastreable		7 - Efecto significativo en la ganancia anual	5 - Pérdida de buena voluntad	2 - violación menor	5 - cientos personas
Impacto técnico general:		**4.000**	**MEDIO**		**Impacto comercial general:**		**4.750**	**MEDIO**
Impacto general:				**4.375**	**MEDIO**			

Gravedad general del riesgo = Probabilidad x Impacto				
Impacto	ALTO	Medium	High	CRITICO
	MEDIO	Low	**Medium**	ALTO
	BAJO	Note	Low	MEDIO
		BAJO	MEDIO	ALTO
	Probabilidad			

Niveles de probabilidad e impacto	
0 to <3	BAJO
3 to <6	MEDIO
6 to 9	ALTO

Riesgo: Configuraciones de seguridad incorrectas

Probabilidad								
Factores de agente de amenaza					Factores de vulnerabilidad.			
Nivel de habilidad	**Motivo**	**Oportunidad**	**Tamaño**		**Facilidad para Descubrir**	**Facilidad para la Explotación**	**Conciencia**	**Detección de Intrusión**
2 - No require mas que una computadora	4 - Posible recompensa	9 - No se requiere acceso ni recursos	4 - Usuarios de intranet		2 - Muy Dificil	1 - Teoricamente	4 - Oculto	8 - Registrado sin revisión
Probabilidad general:				**4.250**	**MEDIO**			

Impacto técnico					Impacto de negocio			
Pérdida de la Confidencialidad	**Pérdida de Integridad**	**Pérdida en Disponibilidad**	**Pérdida en Responsabilidad**		**Daño Financiero**	**Daño en Reputación**	**No cumplimiento**	**Violación de Privacidad**
5 - Extensos datos críticos revelados	3 - Mínimo datos seriamente corruptos	1 - Servicios secundarios mínimos interrumpidos	9 - Completamente anónimo		7 - Efecto significativo en la ganancia anual	4 - Pérdida de cuentas importantes	2 - violación menor	5 - cientos personas
Impacto técnico general:		**4.500**	**MEDIO**		**Impacto comercial general:**		**4.500**	**MEDIO**
Impacto general:				**4.500**	**MEDIO**			

Gravedad general del riesgo = Probabilidad x Impacto				
Impacto	ALTO	Medium	High	CRITICO
	MEDIO	Low	**Medium**	ALTO
	BAJO	Note	Low	MEDIO
		BAJO	MEDIO	ALTO
		Probabilidad		

Niveles de probabilidad e impacto	
0 to <3	BAJO
3 to <6	MEDIO
6 to 9	ALTO

Riesgo: Exposición de datos sensibles

Probabilidad								
Factores de agente de amenaza					**Factores de vulnerabilidad.**			
Nivel de habilidad	**Motivo**	**Oportunidad**	**Tamaño**		**Facilidad para Descubrir**	**Facilidad para la Explotación**	**Conciencia**	**Detección de Intrusión**
2 - No require mas que una computadora	3 - un poco de posible recompensa	4 - Acceso especial o recursos requeridos	2 - Desarrolladores, administradores de sistemas		1 - Practicamente Imposible	6 - muy facil	4 - Oculto	3 - Registrado y revisado
Probabilidad general:				**3.125**	**MEDIO**			

Impacto técnico					**Impacto de negocio**			
Pérdida de la Confidencialidad	**Pérdida de Integridad**	**Pérdida en Disponibilidad**	**Pérdida en Responsabilidad**		**Daño Financiero**	**Daño en Reputación**	**No cumplimiento**	**Violación de Privacidad**
4 - Datos críticos mínimos revelados, datos no sensibles extensos revelados	3 - Mínimo datos seriamente corruptos	1 - Servicios secundarios mínimos interrumpidos	7 - Posiblemente rastreable		3 - Efecto menor en la ganancia anual.	5 - Pérdida de buena voluntad	7 - Violación de alto nivel	5 - cientos personas
Impacto técnico general:		**3.750**	**MEDIO**		**Impacto comercial general:**		**5.000**	**MEDIO**
Impacto general:				**4.375**	**MEDIO**			

Gravedad general del riesgo = Probabilidad x Impacto				
Impacto	ALTO	Medium	High	CRITICO
	MEDIO	Low	**Medium**	ALTO
	BAJO	Note	Low	MEDIO
		BAJO	MEDIO	ALTO
	Probabilidad			

Niveles de probabilidad e impacto	
0 to <3	BAJO
3 to <6	MEDIO
6 to 9	ALTO

Riesgo: Subida de archivos sin restricciones

Probabilidad								
Factores de agente de amenaza					**Factores de vulnerabilidad.**			
Nivel de habilidad	**Motivo**	**Oportunidad**	**Tamaño**		**Facilidad para Descubrir**	**Facilidad para la Explotación**	**Conciencia**	**Detección de Intrusión**
7 - mucha habilidad en informatica	9 - Alta recompensa	4 - Acceso especial o recursos requeridos	6 - Usuarios autenticados		7 - Facil	5 - Facil	6 - Ovio	8 - Registrado sin revisión
Probabilidad general:				**6.500**	**ALTO**			

Impacto técnico					**Impacto de negocio**			
Pérdida de la Confidencialidad	**Pérdida de Integridad**	**Pérdida en Disponibilidad**	**Pérdida en Responsabilidad**		**Daño Financiero**	**Daño en Reputación**	**No cumplimiento**	**Violación de Privacidad**
5 - Extensos datos críticos revelados	7 - Amplios datos seriamente corruptos	5 - Servicios primarios mínimos interrumpidos, servicios secundarios extensivos interrumpidos	7 - Posiblemente rastreable		7 - Efecto significativo en la ganancia anual	4 - Pérdida de cuentas importantes	5 - Clara violación	5 - cientos personas
Impacto técnico general:		**6.000**	**ALTO**		**Impacto comercial general:**		**5.250**	**MEDIO**
Impacto general:				**5.625**	**MEDIO**			

Gravedad general del riesgo = Probabilidad x Impacto				
Impacto	ALTO	Medium	High	CRITICO
	MEDIO	Low	**Medium**	ALTO
	BAJO	Note	Low	MEDIO
		BAJO	MEDIO	ALTO
	Probabilidad			

Niveles de probabilidad e impacto	
0 to <3	BAJO
3 to <6	MEDIO
6 to 9	ALTO

Riesgo: Falta de validación en formularios

Probabilidad								
Factores de agente de amenaza					Factores de vulnerabilidad.			
Nivel de habilidad	**Motivo**	**Oportunidad**	**Tamaño**		**Facilidad para Descubrir**	**Facilidad para la Explotación**	**Conciencia**	**Detección de Intrusión**
5 - Uso Avanzado de computadoras	7 - Dañar la reputacion de la empresa	4 - Acceso especial o recursos requeridos	4 - Usuarios de intranet		7 - Facil	5 - Facil	6 - Ovio	1 - Detección activa en aplicación
Probabilidad general:				**4.875**	**MEDIO**			

Impacto técnico					Impacto de negocio			
Pérdida de la Confidencialidad	**Pérdida de Integridad**	**Pérdida en Disponibilidad**	**Pérdida en Responsabilidad**		**Daño Financiero**	**Daño en Reputación**	**No cumplimiento**	**Violación de Privacidad**
2 - Datos mínimos no sensibles divulgados	7 - Amplios datos seriamente corruptos	7 - Amplios servicios primarios interrumpidos	7 - Posiblemente rastreable		7 - Efecto significativo en la ganancia anual	9 - Daño de marca	7 - Violación de alto nivel	7 - Miles Personas
Impacto técnico general:		**5.750**	**MEDIO**		**Impacto comercial general:**		**7.500**	**ALTO**
Impacto general:				**6.625**	**ALTO**			

Gravedad general del riesgo = Probabilidad x Impacto				
Impacto	ALTO	Medium	High	CRITICO
	MEDIO	Low	**Medium**	ALTO
	BAJO	Note	Low	MEDIO
		BAJO	MEDIO	ALTO
	Probabilidad			

Niveles de probabilidad e impacto	
0 to <3	BAJO
3 to <6	MEDIO
6 to 9	ALTO

Riesgo: Falta de monitoreo y registros

Probabilidad								
Factores de agente de amenaza					**Factores de vulnerabilidad.**			
Nivel de habilidad	**Motivo**	**Oportunidad**	**Tamaño**		**Facilidad para Descubrir**	**Facilidad para la Explotación**	**Conciencia**	**Detección de Intrusión**
2 - No require mas que una computadora	4 - Posible recompensa	4 - Acceso especial o recursos requeridos	5 - Partners		4 - medio dificil	4 - medio	6 - Ovio	3 - Registrado y revisado
Probabilidad general:				**4.000**	**MEDIO**			

Impacto técnico					**Impacto de negocio**			
Pérdida de la Confidencialidad	**Pérdida de Integridad**	**Pérdida en Disponibilidad**	**Pérdida en Responsabilidad**		**Daño Financiero**	**Daño en Reputación**	**No cumplimiento**	**Violación de Privacidad**
9 - Todos los datos divulgados	7 - Amplios datos seriamente corruptos	1 - Servicios secundarios mínimos interrumpidos	1 - totalmente rastreable		1 - Menos del costo para arreglar la vulnerabilidad	9 - Daño de marca	2 - violación menor	4 - 20 personas
Impacto técnico general:		**4.500**	**MEDIO**		**Impacto comercial general:**		**4.000**	**MEDIO**
Impacto general:				**4.250**	**MEDIO**			

Gravedad general del riesgo = Probabilidad x Impacto				
Impacto	ALTO	Medium	High	CRITICO
	MEDIO	Low	**Medium**	ALTO
	BAJO	Note	Low	MEDIO
		BAJO	MEDIO	ALTO
	Probabilidad			

Niveles de probabilidad e impacto	
0 to <3	BAJO
3 to <6	MEDIO
6 to 9	ALTO

Riesgo: Falta de protección contra CSRF

Probabilidad								
Factores de agente de amenaza					**Factores de vulnerabilidad.**			
Nivel de habilidad	**Motivo**	**Oportunidad**	**Tamaño**		**Facilidad para Descubrir**	**Facilidad para la Explotación**	**Conciencia**	**Detección de Intrusión**
6 - Habilidades en Redes y Programación	4 - Posible recompensa	7 - Se requiere cierto acceso o recursos	4 - Usuarios de intranet		4 - medio dificil	3 - Dificil	1 - Desconocido	1 - Detección activa en aplicación
Probabilidad general:			**3.750**	**MEDIO**				

Impacto técnico					**Impacto de negocio**			
Pérdida de la Confidencialidad	**Pérdida de Integridad**	**Pérdida en Disponibilidad**	**Pérdida en Responsabilidad**		**Daño Financiero**	**Daño en Reputación**	**No cumplimiento**	**Violación de Privacidad**
9 - Todos los datos divulgados	7 - Amplios datos seriamente corruptos	7 - Amplios servicios primarios interrumpidos	9 - Completamente anónimo		7 - Efecto significativo en la ganancia anual	5 - Pérdida de buena voluntad	7 - Violación de alto nivel	7 - Miles Personas
Impacto técnico general:		**8.000**	**ALTO**		**Impacto comercial general:**		**6.500**	**ALTO**
Impacto general:			**7.250**	**ALTO**				

Gravedad general del riesgo = Probabilidad x Impacto				
Impacto	ALTO	Medium	High	CRITICO
	MEDIO	Low	**Medium**	ALTO
	BAJO	Note	Low	MEDIO
		BAJO	MEDIO	ALTO
	Probabilidad			

Niveles de probabilidad e impacto	
0 to <3	BAJO
3 to <6	MEDIO
6 to 9	ALTO

Riesgo: Inyección SQL

Probabilidad								
Factores de agente de amenaza					**Factores de vulnerabilidad.**			
Nivel de habilidad	**Motivo**	**Oportunidad**	**Tamaño**		**Facilidad para Descubrir**	**Facilidad para la Explotación**	**Conciencia**	**Detección de Intrusión**
3 - Algunas Habilidades tecnicas	5 - mucha recompensa	5 - se requiere masomenos acceso	9 - Usuarios de internet anónimos		5 - medio dificil	3 - Dificil	4 - Oculto	3 - Registrado y revisado
Probabilidad general:				**4.625**	**MEDIO**			

Impacto técnico					**Impacto de negocio**			
Pérdida de la Confidencialidad	**Pérdida de Integridad**	**Pérdida en Disponibilidad**	**Pérdida en Responsabilidad**		**Daño Financiero**	**Daño en Reputación**	**No cumplimiento**	**Violación de Privacidad**
9 - Todos los datos divulgados	7 - Amplios datos seriamente corruptos	9 - Todos los servicios completamente perdidos	9 - Completamente anónimo		7 - Efecto significativo en la ganancia anual	9 - Daño de marca	7 - Violación de alto nivel	7 - Miles Personas
Impacto técnico general:		**8.500**	**ALTO**		**Impacto comercial general:**		**7.500**	**ALTO**
Impacto general:				**8.000**	**ALTO**			

Gravedad general del riesgo = Probabilidad x Impacto				
Impacto	ALTO	Medium	High	CRITICO
	MEDIO	Low	**Medium**	ALTO
	BAJO	Note	Low	MEDIO
		BAJO	MEDIO	ALTO
	Probabilidad			

Niveles de probabilidad e impacto	
0 to <3	BAJO
3 to <6	MEDIO
6 to 9	ALTO

Riesgo: Componentes desactualizados o vulnerables

Probabilidad								
Factores de agente de amenaza					Factores de vulnerabilidad.			
Nivel de habilidad	**Motivo**	**Oportunidad**	**Tamaño**		**Facilidad para Descubrir**	**Facilidad para la Explotación**	**Conciencia**	**Detección de Intrusión**
9 - Habilidades en Ciberseguridad	5 - mucha recompensa	7 - Se requiere cierto acceso o recursos	5 - Partners		2 - Muy Dificil	3 - Dificil	1 - Desconocido	3 - Registrado y revisado
Probabilidad general:				**4.375**	**MEDIO**			

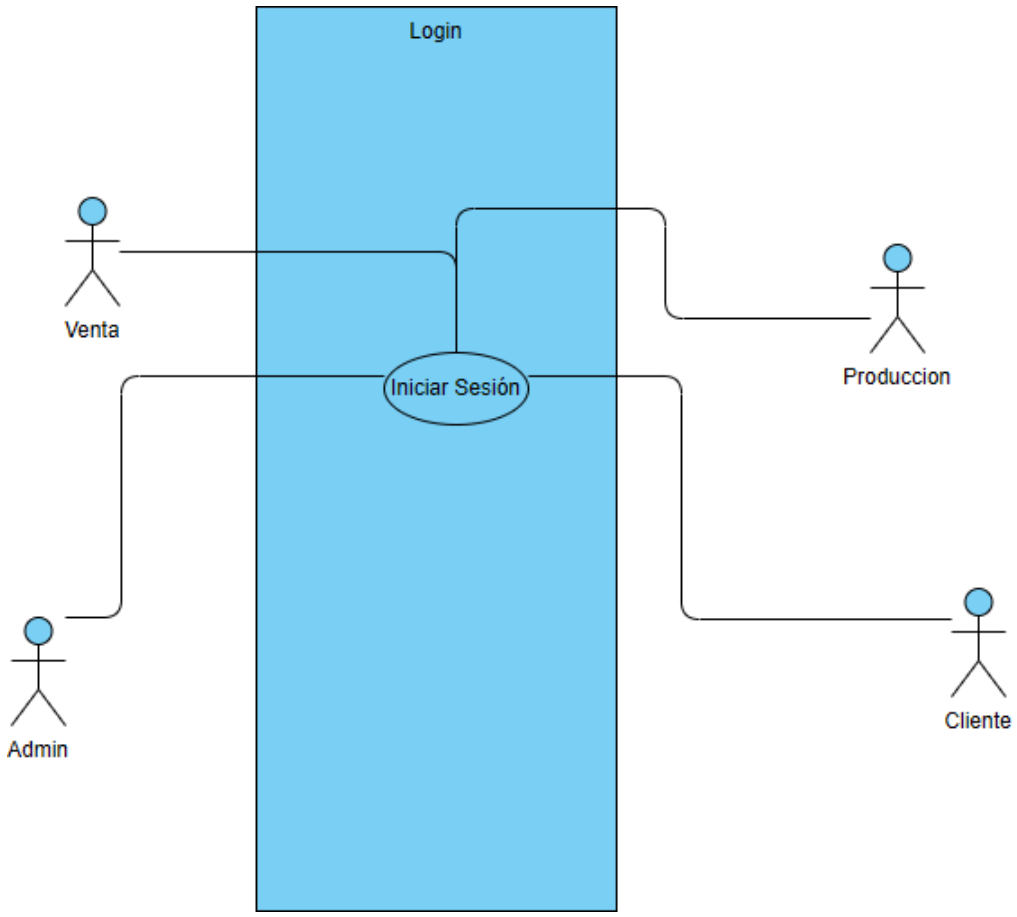
Impacto técnico					Impacto de negocio			
Pérdida de la Confidencialidad	**Pérdida de Integridad**	**Pérdida en Disponibilidad**	**Pérdida en Responsabilidad**		**Daño Financiero**	**Daño en Reputación**	**No cumplimiento**	**Violación de Privacidad**
5 - Extensos datos críticos revelados	7 - Amplios datos seriamente corruptos	1 - Servicios secundarios mínimos interrumpidos	7 - Posiblemente rastreable		7 - Efecto significativo en la ganancia anual	9 - Daño de marca	5 - Clara violación	7 - Miles Personas
Impacto técnico general:		**5.000**	**MEDIO**		**Impacto comercial general:**		**7.000**	**ALTO**
Impacto general:				**6.000**	**ALTO**			

Gravedad general del riesgo = Probabilidad x Impacto				
Impacto	ALTO	Medium	High	CRITICO
	MEDIO	Low	**Medium**	ALTO
	BAJO	Note	Low	MEDIO
		BAJO	MEDIO	ALTO
	Probabilidad			

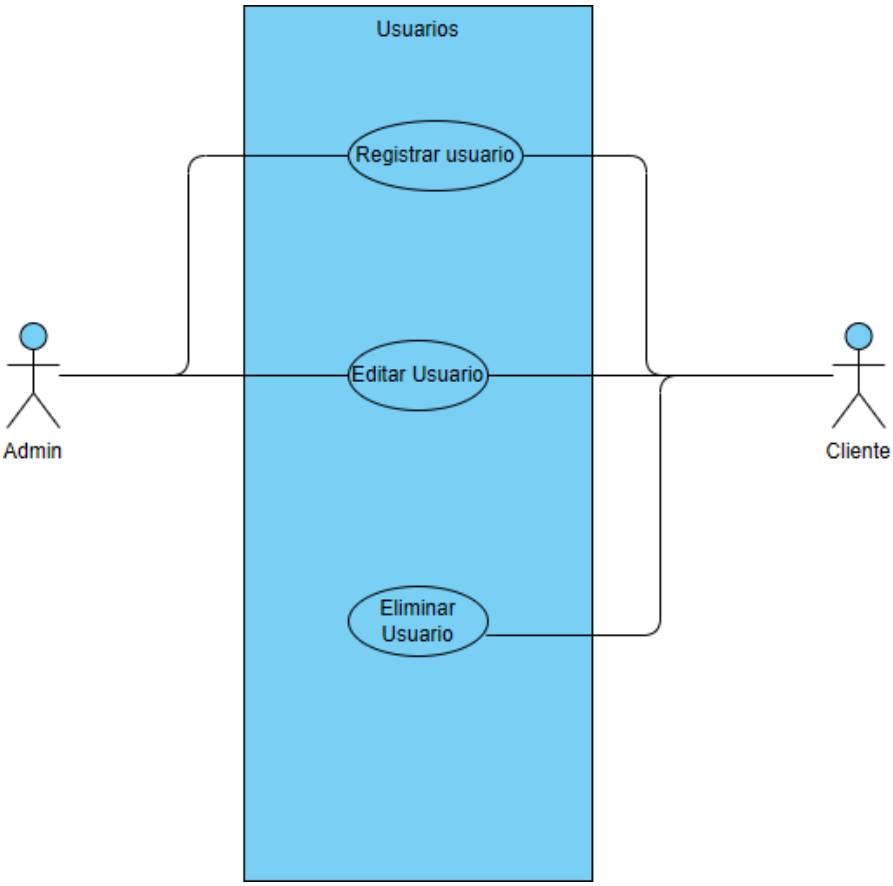
Niveles de probabilidad e impacto	
0 to <3	BAJO
3 to <6	MEDIO
6 to 9	ALTO

Casos de Uso

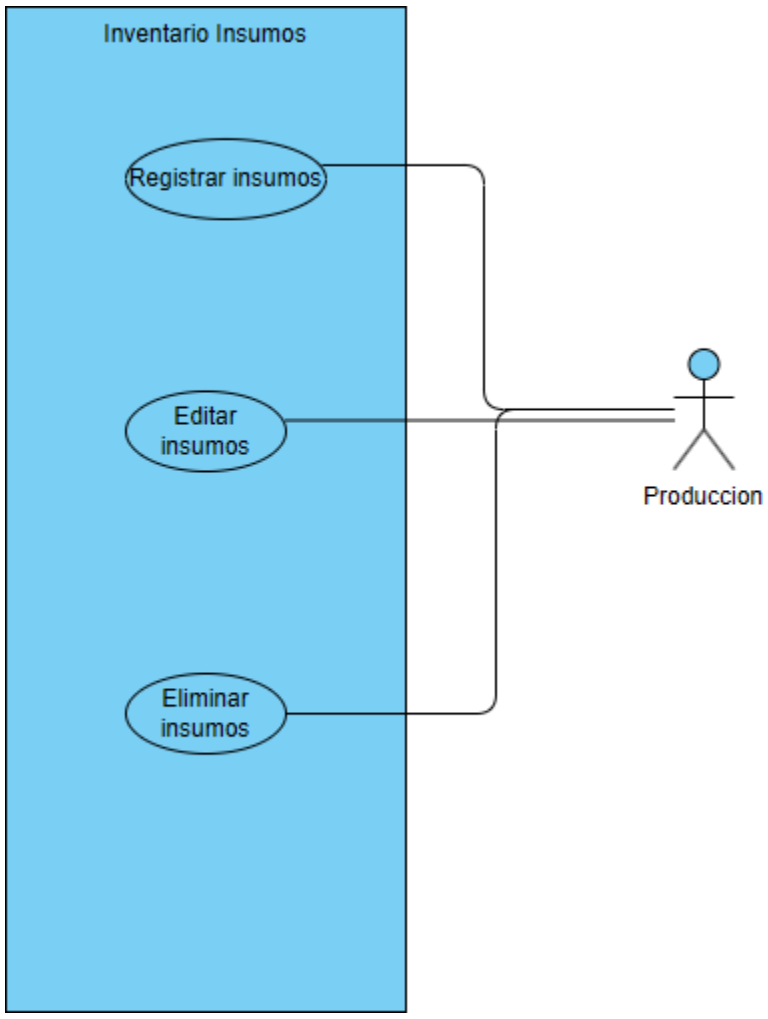
Login:



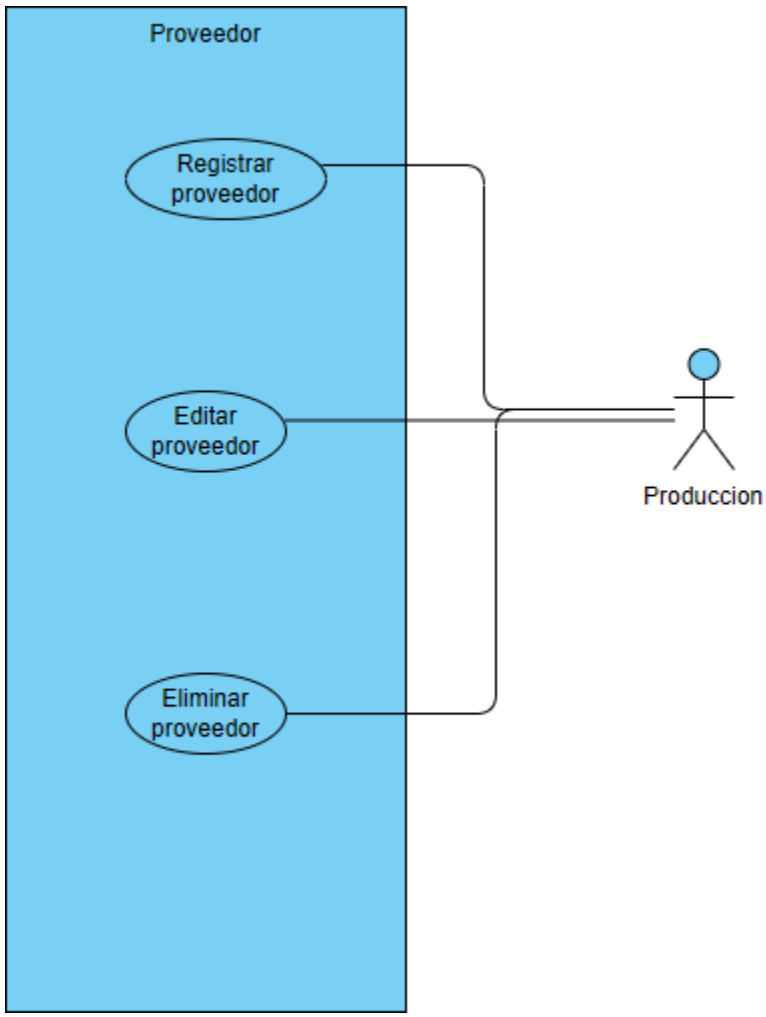
Usuarios


Usuarios
Registrar usuario
Editar Usuario
Eliminar Usuario
Admin
Cliente

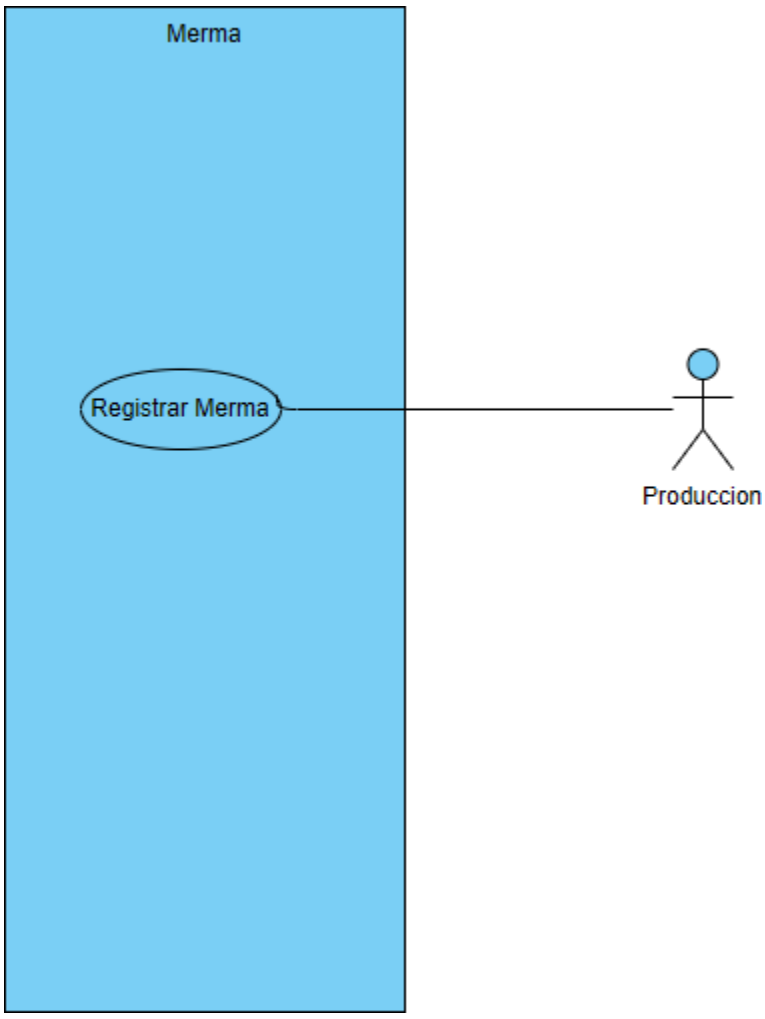
Insumos:


Inventario Insumos
Registrar insumos
Editar insumos
Eliminar insumos
Produccion

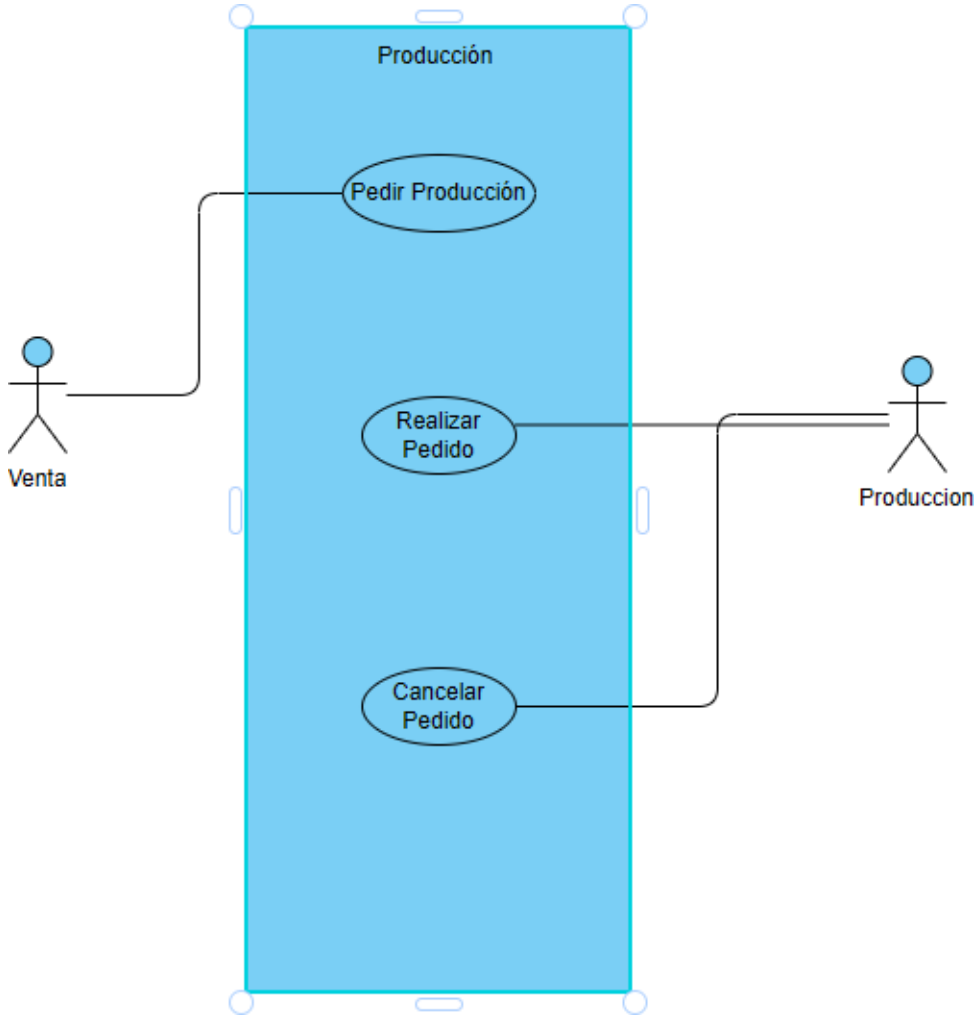
Proveedor


Proveedor
Registrar proveedor
Editar proveedor
Eliminar proveedor
Produccion

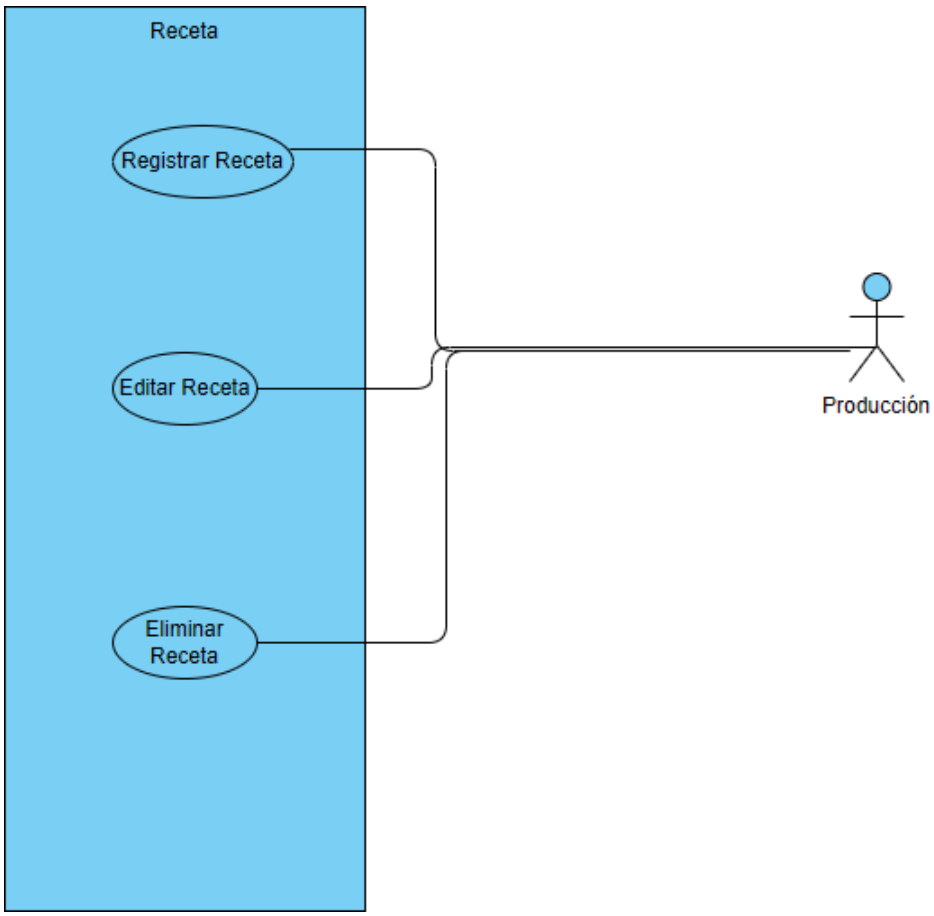
Merma



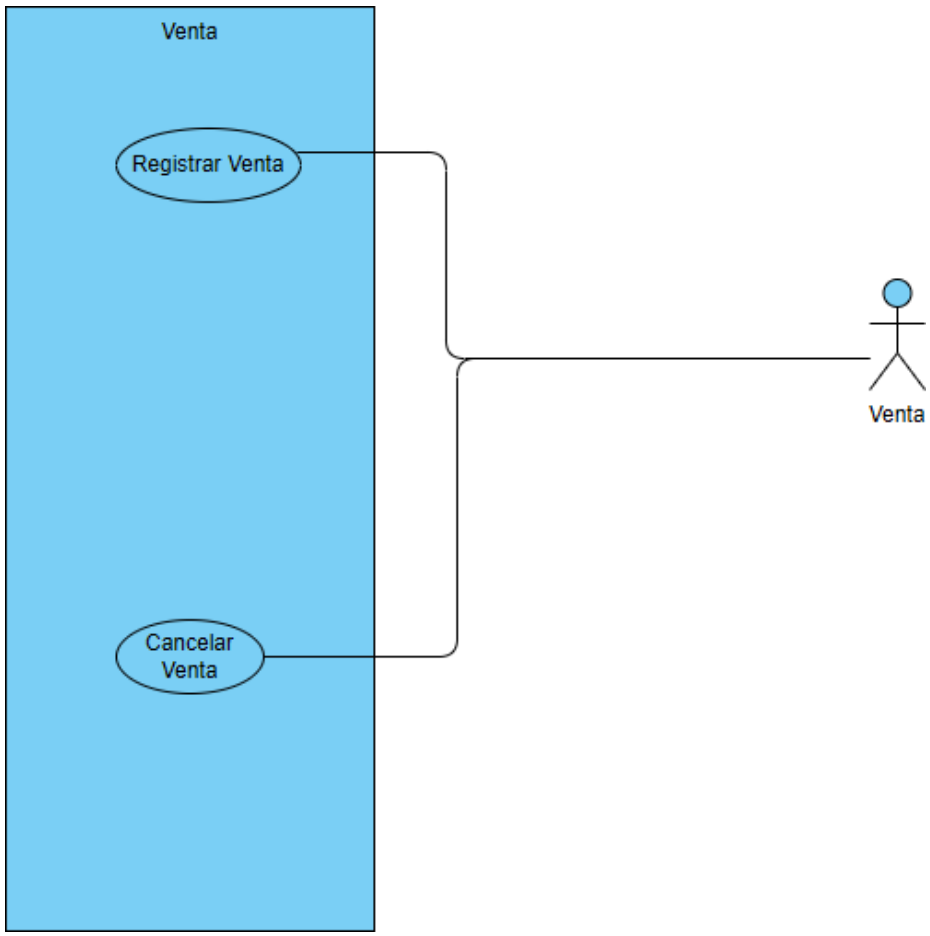
Producción


Producción
Pedir Producción
Realizar Pedido
Cancelar Pedido
Venta
Produccion

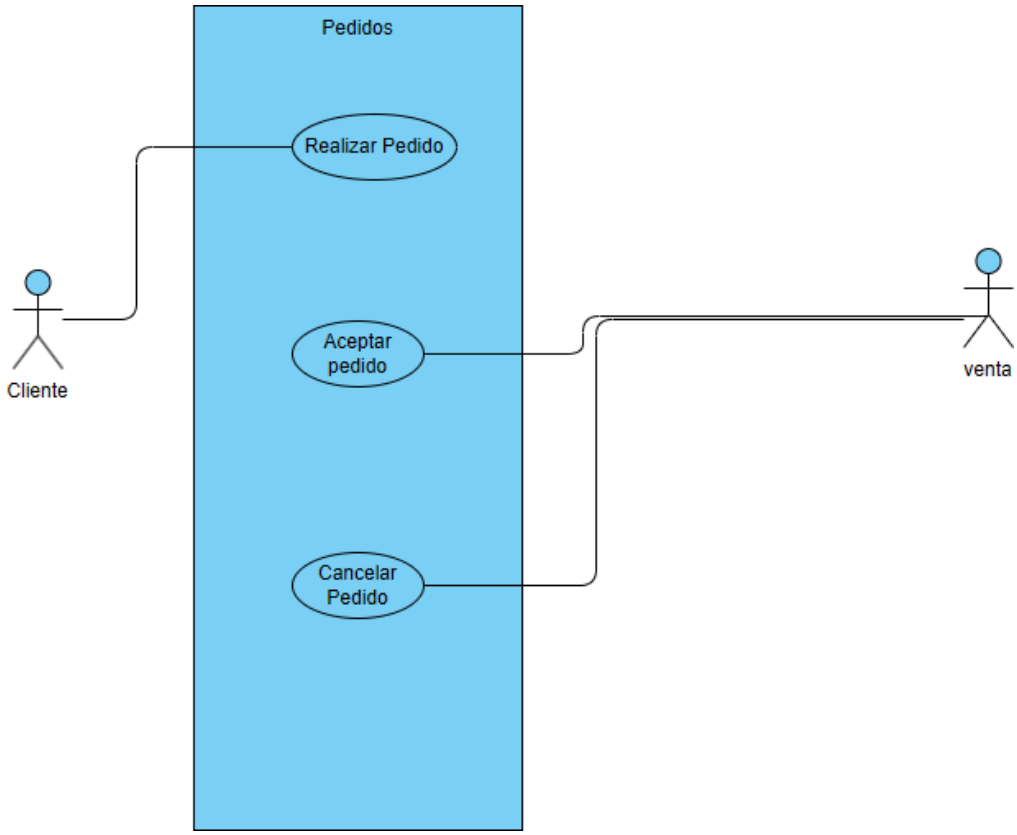
Receta


Receta
Registrar Receta
Editar Receta
Eliminar Receta
Producción

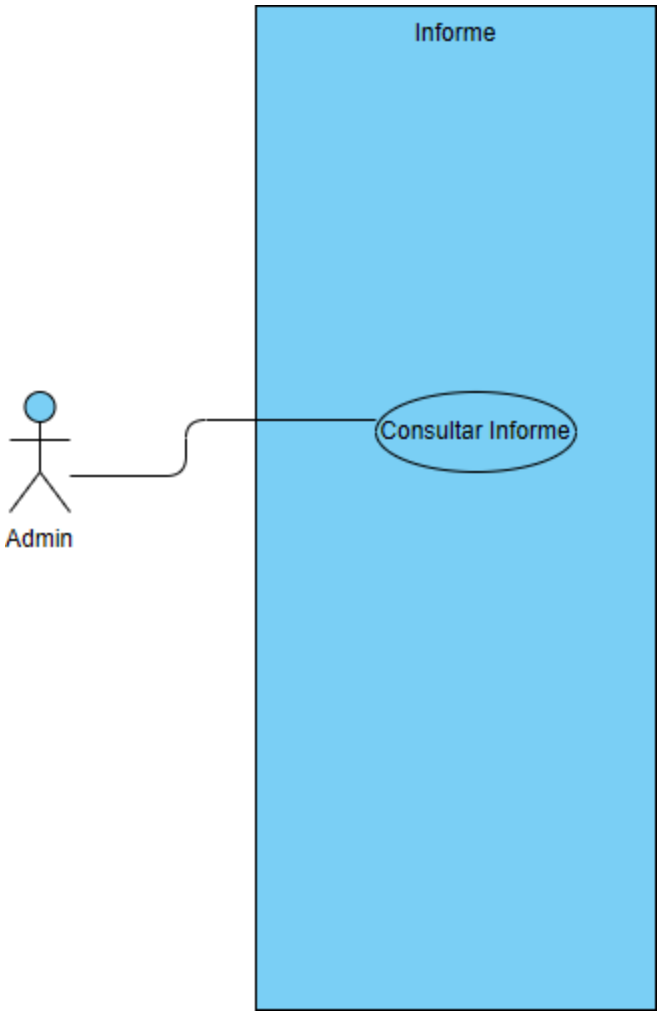
Ventas



Pedidos


Pedidos
Realizar Pedido
Aceptar pedido
Cancelar Pedido
Cliente
venta

Informe



Casos de Abuso

CONTROL DE ACCESO INSUFICIENTE

El daño:
El sistema de gestión para panaderías almacena información clave del negocio, incluyendo recetas, costos, ventas, inventario y datos de clientes. Un control de acceso insuficiente puede permitir que usuarios con permisos limitados accedan a módulos reservados para administradores o encargados, lo que les permitiría visualizar, modificar o eliminar datos sensibles del negocio, como precios, ingredientes de recetas, reportes de ventas o historial de compras.
Esto puede ocasionar alteraciones en los registros contables, manipulación de inventarios, fraudes, eliminación de evidencias de mermas o robos, e incluso pérdida de confianza por parte de clientes y proveedores.

Rango de Privilegios:
Un atacante con acceso a una cuenta de usuario básico (cliente, produccion o empleado común) podría:

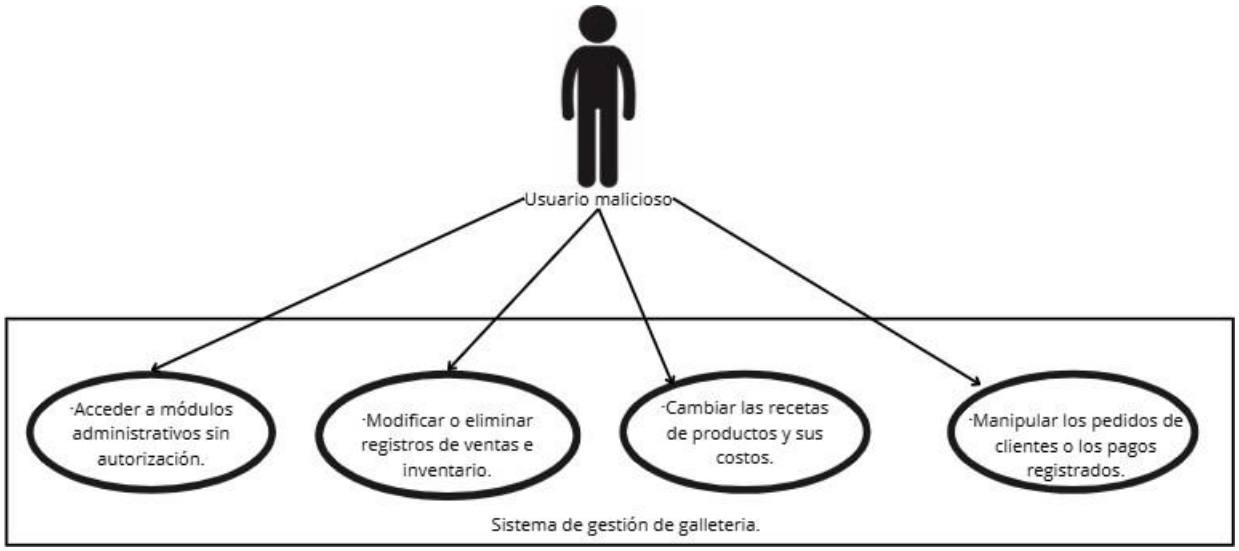
- Acceder a módulos administrativos sin autorización.
- Modificar o eliminar registros de ventas e inventario.
- Cambiar las recetas de productos y sus costos.
- Escalar privilegios de su cuenta o de otros usuarios.
- Visualizar reportes de ventas, compras y mermas confidenciales.
- Manipular los pedidos de clientes o los pagos registrados.

Interacción de Abuso:
Un usuario autenticado con permisos restringidos manipula las direcciones URL o parámetros del sistema para intentar acceder a funcionalidades fuera de su alcance. Al no existir una validación robusta de roles o permisos en las rutas del sistema, este le permite ingresar a secciones administrativas como:

- /admin/inventario
- /admin/ventas
- /admin/usuarios

- /recetas/editar
- /reportes/ventas

Una vez dentro, el atacante puede alterar los registros de inventario, eliminar pedidos, modificar los datos de los productos o visualizar reportes de rendimiento, aprovechando la falta de control de acceso adecuado en las validaciones del backend.



AUTENTIFICACION DEBIL

El daño:
El sistema de gestión permite el acceso a usuarios registrados que manejan información crítica como inventarios, ventas, recetas, y datos de clientes y proveedores. Un mecanismo de autenticación débil puede permitir que atacantes accedan a cuentas legítimas sin autorización, ya sea mediante ataques de fuerza bruta, credenciales predeterminadas, contraseñas fáciles de adivinar o la falta de mecanismos de bloqueo de cuenta tras varios intentos fallidos.
Esto puede resultar en robo de información, manipulación de datos importantes del negocio, generación de ventas falsas, eliminación de registros, o incluso la total toma de control del sistema por parte del atacante.

Rango de Privilegios:
Un atacante externo o interno sin privilegios inicialmente podría:

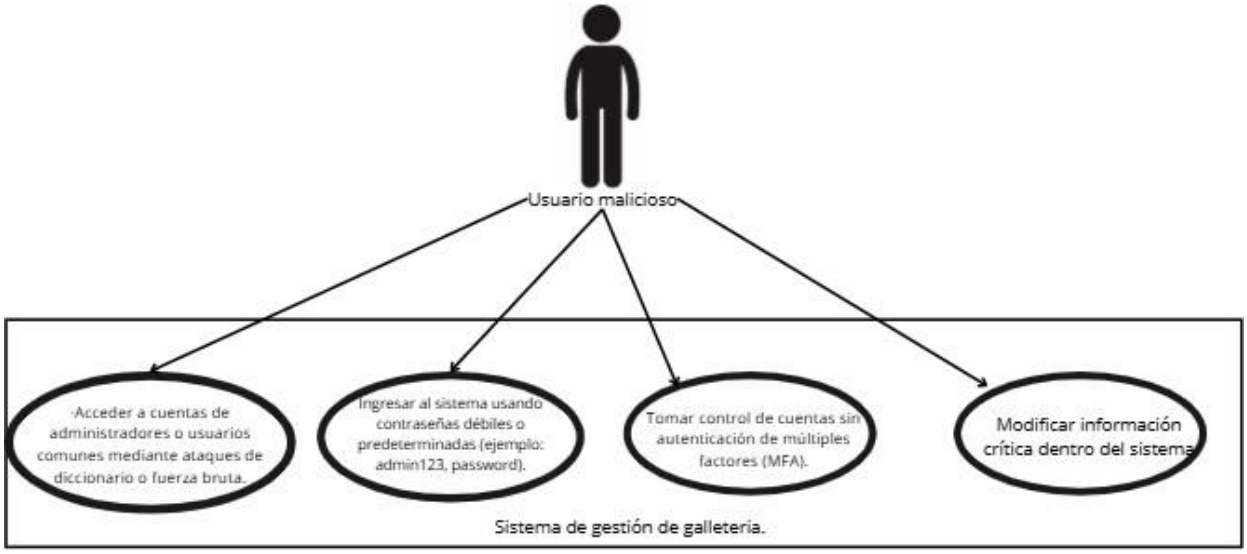
- Acceder a cuentas de administradores o usuarios comunes mediante ataques de diccionario o fuerza bruta.
- Ingresar al sistema usando contraseñas débiles o predeterminadas (ejemplo: admin123, password).
- Tomar control de cuentas sin autenticación de múltiples factores (MFA).
- Obtener acceso completo a los módulos del sistema con solo conocer un correo y adivinar la contraseña.
- Modificar información crítica dentro del sistema.

Interacción de Abuso
Un atacante externo o interno realiza múltiples intentos de acceso a cuentas existentes probando combinaciones de usuario y contraseña utilizando herramientas automatizadas (fuerza bruta o diccionario).

Al no existir mecanismos de defensa robustos como:

- Políticas de contraseñas fuertes,
- Captcha en el login,
- Bloqueo de cuenta tras intentos fallidos,
- Notificaciones de inicio de sesión sospechoso,
- autenticación en dos pasos,

el atacante logra adivinar la contraseña de un usuario legítimo y accede al sistema con los permisos de esa cuenta. Desde ahí puede visualizar, modificar o eliminar datos de ventas, inventarios, recetas, o incluso escalar sus privilegios si accede a un usuario con más permisos.


Usuario malicioso
·Acceder a cuentas de administradores o usuarios comunes mediante ataques de diccionario o fuerza bruta.
Ingresar al sistema usando contraseñas débiles o predeterminadas (ejemplo: admin123, password).
Tomar control de cuentas sin autenticación de múltiples factores (MFA).
Modificar información crítica dentro del sistema
Sistema de gestión de galleteria.

.

CONFIGURACION DE SEGURIDAD INCORRECTA

El daño:

El sistema de gestión depende de una correcta configuración de seguridad tanto en su infraestructura como en su aplicación. Una configuración deficiente o insegura puede exponer el sistema a ataques externos o internos, permitiendo el acceso no autorizado, robo de información, manipulación de datos, o incluso la caída completa del sistema.
Estas malas configuraciones pueden incluir: credenciales por defecto no cambiadas, puertos abiertos innecesarios, información sensible expuesta (como claves API o credenciales en el código), versiones desactualizadas con vulnerabilidades conocidas, o permisos mal asignados en archivos o carpetas del sistema.
Esto podría comprometer la disponibilidad, integridad y confidencialidad de la información crítica del negocio.

Rango de Privilegios:

Un atacante externo o interno podría:

- Acceder a paneles de administración con credenciales por defecto (admin/admin).
- Obtener información sensible desde archivos públicos (como .env o config.js).
- Explotar versiones desactualizadas del sistema o librerías con fallos de seguridad conocidos.
- Manipular configuraciones del servidor expuestas públicamente.
- Acceder a base de datos, reportes o backups mal protegidos.
- Ver información de errores detallados que revelan estructura interna del sistema.

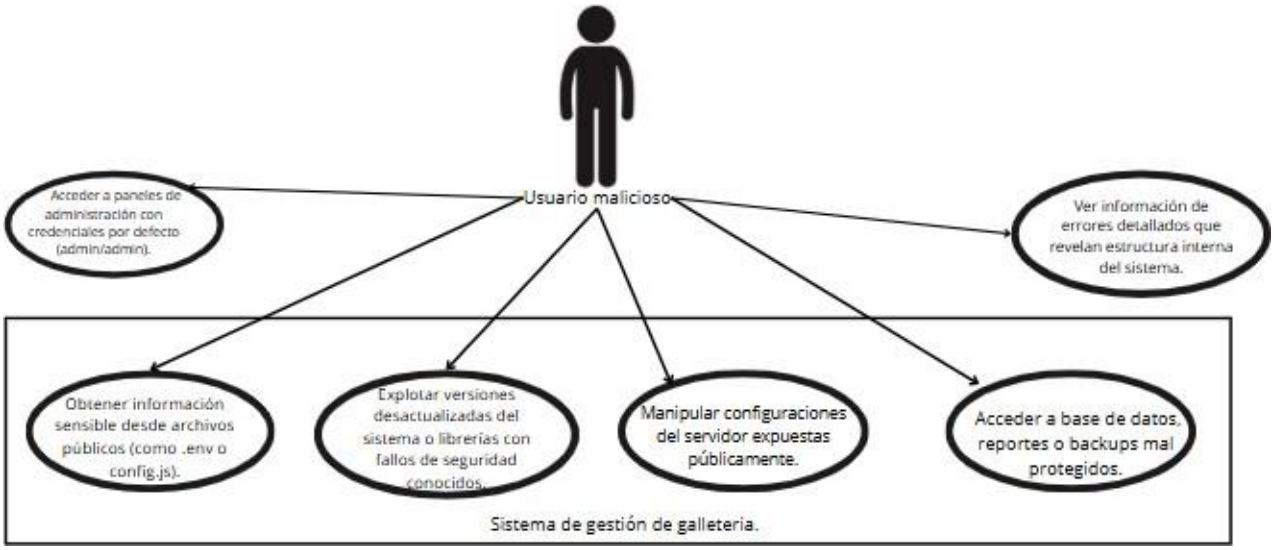
Interacción de Abuso:

Un atacante realiza un escaneo básico del sistema utilizando herramientas automáticas (como Nmap, Dirbuster o Shodan) y detecta configuraciones débiles, por ejemplo:

- Directorios públicos expuestos como /backups/ o /config/.
- Mensajes de error del sistema que muestran queries SQL, rutas internas o estructuras de tablas.
- Consolas administrativas sin protección adecuada accesibles desde /app/ o /admin/.
- Credenciales por defecto sin modificar (admin / 1234).
- Archivos de configuración visibles en el servidor con datos sensibles: env, backup.sql.

Aprovechando estas configuraciones incorrectas, el atacante obtiene acceso a

información confidencial, manipula datos, o incluso compromete totalmente la infraestructura del sistema.



EXPOSICION DE DATOS SENSIBLES

El daño:

El sistema de gestión, desarrollado en Python utilizando el framework Flask, almacena y procesa información confidencial como datos de usuarios, contraseñas, información de ventas, pedidos, proveedores, recetas y costos de producción.

La exposición de datos sensibles ocurre cuando esta información no se encuentra correctamente protegida en su almacenamiento o transmisión, permitiendo que un atacante pueda interceptarla o visualizarla.

Esto puede causar robo de identidad, fraude, espionaje comercial, pérdida de confianza de los clientes, multas por incumplimiento de normativas de protección de datos y daños reputacionales dentro de nuestra galleteria.

Rango de Privilegios:

Un atacante con acceso no privilegiado o incluso externo podría:

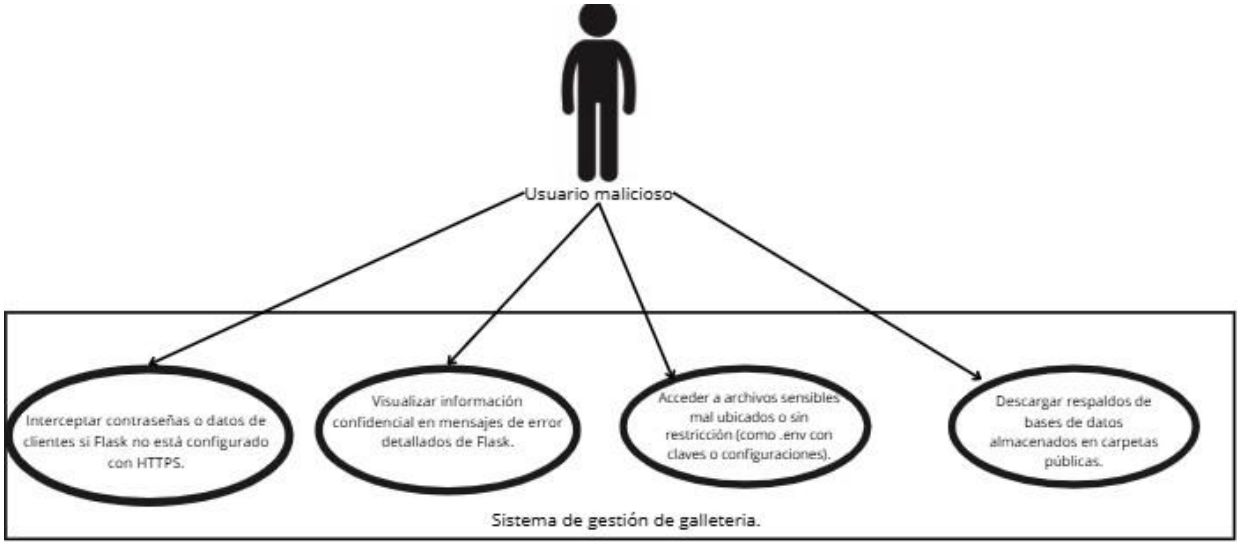
- Interceptar contraseñas o datos de clientes si Flask no está configurado con HTTPS.
- Visualizar información confidencial en mensajes de error detallados de Flask.
- Acceder a archivos sensibles mal ubicados o sin restricción (como .env con claves o configuraciones).
- Descargar respaldos de bases de datos almacenados en carpetas públicas.
- Encontrar tokens o contraseñas hardcodeadas en archivos de código expuestos.

Interacción de Abuso:

Un atacante accede al sistema web desarrollado en Flask y realiza un análisis básico de seguridad. Detecta múltiples fallos:

- El sistema no utiliza HTTPS, permitiendo capturar tráfico con herramientas como Wireshark.
- Durante un error de programación, Flask muestra un Traceback completo con rutas internas, contraseñas de base de datos o configuraciones.
- El archivo .env con credenciales de producción es accesible desde el navegador.
- Las cookies de sesión generadas por Flask no están configuradas como Secure o HttpOnly, permitiendo su robo.

Con estos fallos, el atacante logra extraer datos de clientes, información de ventas, recetas confidenciales y potencialmente tomar control del sistema..


Usuario malicioso
Interceptar contraseñas o datos de clientes si Flask no está configurado con HTTPS.
Visualizar información confidencial en mensajes de error detallados de Flask.
Acceder a archivos sensibles mal ubicados o sin restricción (como .env con claves o configuraciones).
Descargar respaldos de bases de datos almacenados en carpetas públicas.
Sistema de gestión de galleteria.

SUBIDA DE ARCHIVOS SIN RESTRICCIONES

El daño:

Aunque el sistema web de gestión para panaderías no permite que los clientes suban archivos, dentro de la intranet (accesible solo por usuarios con roles admin, ventas o producción) podrían existir funcionalidades internas como subida de imágenes de productos, documentación interna o reportes.

Si en estas secciones no existen restricciones adecuadas para controlar los archivos que se suben, un atacante interno o un usuario malintencionado podría:

- Subir archivos maliciosos que comprometan el servidor Flask.
- Ejecutar código arbitrario.
- Obtener acceso a información confidencial.
- Desfigurar la interfaz del sistema.
- Escalar privilegios dentro de la intranet.

Rango de Privilegios:

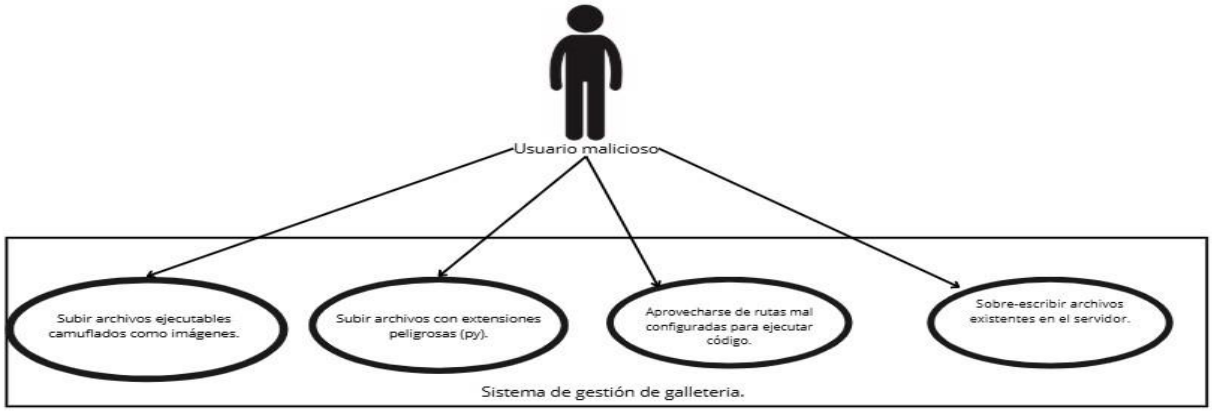
Un atacante con acceso básico al sistema (usuario cliente o proveedor) podría:

- Subir archivos ejecutables camuflados como imágenes.
- Subir archivos con extensiones peligrosas (py).
- Aprovecharse de rutas mal configuradas para ejecutar código.
- Sobre-escribir archivos existentes en el servidor.
- Escalar privilegios dentro del sistema.

Interacción de Abuso:

Un atacante autenticado en el sistema podría explorar el sitio en busca de puntos de carga de archivos. Al identificar una vulnerabilidad en la validación, intentaría subir un archivo con una extensión permitida, pero cuyo contenido sea un script malicioso (por ejemplo, un archivo .php disfrazado de imagen).

Si el servidor permite la ejecución de archivos subidos en un directorio accesible, el atacante podría ejecutar el código directamente visitando la URL correspondiente. Desde ahí, tendría la capacidad de ejecutar comandos en el servidor, exfiltrar información o escalar privilegios, comprometiendo completamente la seguridad del sistema.



FALTA DE VALIDACION EN FORMULARIOS

El daño:

La falta de validación en los formularios del sistema puede provocar que los atacantes o usuarios malintencionados envíen datos manipulados o maliciosos, afectando el correcto funcionamiento de la aplicación y comprometiendo la integridad de la información.

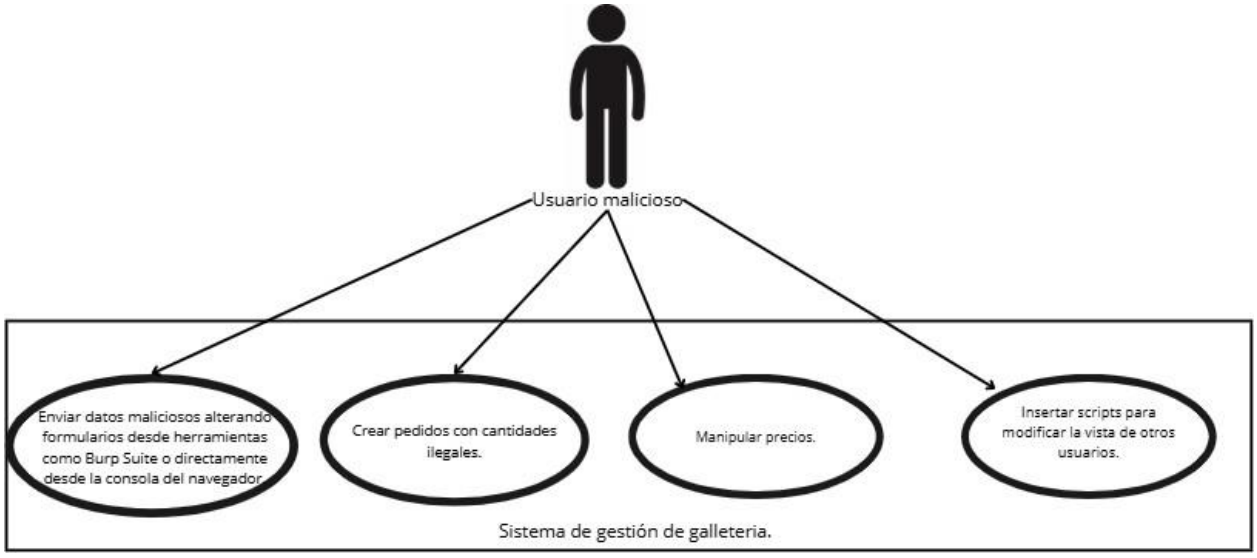
Rango de Privilegios:

Un atacante con acceso básico como cliente (desde la web) o cualquier usuario dentro de la intranet (admin, ventas o producción) podría:

- Enviar datos maliciosos alterando formularios desde herramientas como Burp Suite o directamente desde la consola del navegador.
- Crear pedidos con cantidades ilegales.
- Manipular precios.
- Insertar scripts para modificar la vista de otros usuarios.
- Afectar el registro de ventas, inventarios o datos de producción.

Interacción de Abuso:

Un cliente que realiza un pedido desde la vista pública de la web inspecciona el formulario de pedido de galletas.
Al modificar el input de cantidad (que visualmente está limitado a un rango de 1 a 20), el atacante lo cambia manualmente en el navegador a un valor negativo o muy elevado o escalar privilegios, comprometiendo completamente la seguridad del sistema.



FALTA DE MONITOREO Y REGISTROS

El daño:

La falta de monitoreo y registros (logs) dentro del sistema de gestión para panaderías impide la detección temprana de actividades sospechosas, errores críticos o intentos de ataque.
Un sistema sin registros adecuados deja vulnerabilidades invisibles, lo cual afecta directamente la seguridad, auditoría y la capacidad de respuesta ante incidentes.

Rango de Privilegios:

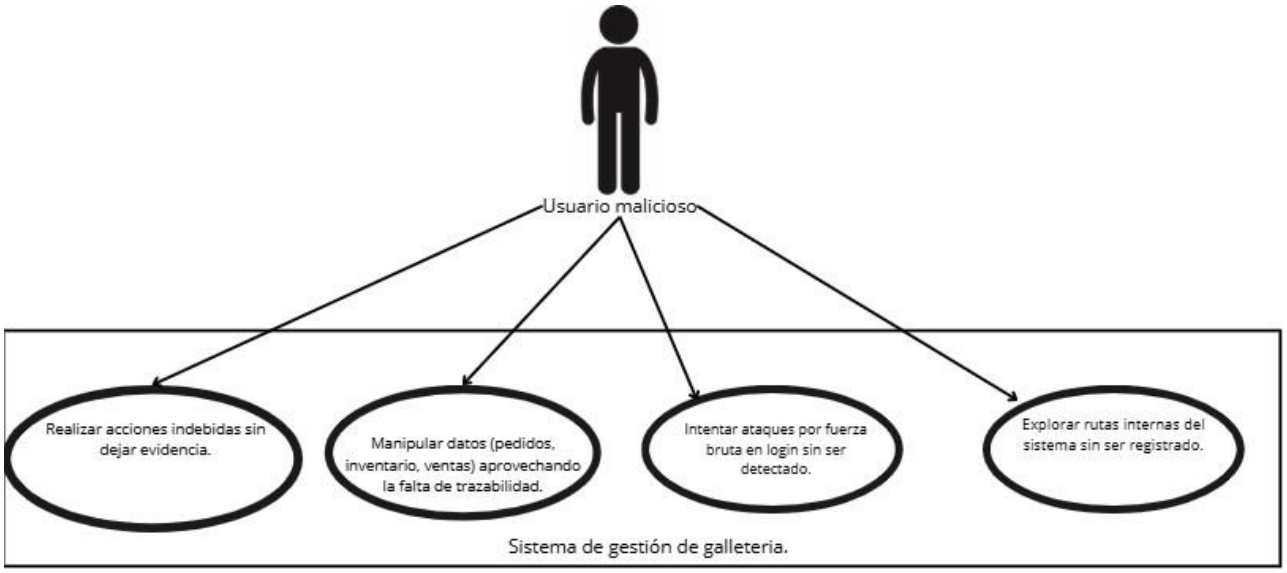
Cualquier usuario con acceso (cliente, ventas, producción o admin) podría:

- Realizar acciones indebidas sin dejar evidencia.
- Manipular datos (pedidos, inventario, ventas) aprovechando la falta de trazabilidad.
- Intentar ataques por fuerza bruta en login sin ser detectado.

Interacción de Abuso:

Un usuario cliente o interno accede a la plataforma y empieza a probar comportamientos no esperados como:

- Forzar inicios de sesión con múltiples contraseñas hasta adivinar alguna.
- Acceder a rutas que no le corresponden.
- Manipular parámetros de formularios o URLs.
- Eliminar o modificar registros sensibles.



FALLA DE PROTECCION CONTRA CSRF

Daño:

- La falta o mala implementación de protección CSRF en el sistema de gestión de panaderías desarrollado con Flask podría permitir que un atacante engañe a un usuario autenticado (cliente, ventas, producción o admin) para realizar acciones no autorizadas dentro del sistema.
  Dado que el sistema permite hacer pedidos, gestionar inventario y registrar ventas desde una intranet accesible vía web, un ataque CSRF exitoso podría ocasionar:
- Creación masiva de pedidos falsos de galletas.
- Modificación de información del perfil del cliente.
- Eliminación de registros de ventas o pedidos desde cuentas administrativas.
- Desconfiguración del inventario o asignación errónea de stock.

Rango de Privilegios

Un atacante externo necesita que la víctima esté autenticada en el sistema (cliente o usuario interno) y que visite un enlace malicioso o página controlada por el atacante.
Este ataque podría permitir:

- A un atacante externo crear pedidos falsos desde la cuenta de un cliente.
- Modificar datos de perfil, direcciones o contraseñas.
- Afectar inventarios, ventas o registros administrativos si el ataque es dirigido a usuarios de intranet.

Interacción de Abuso:

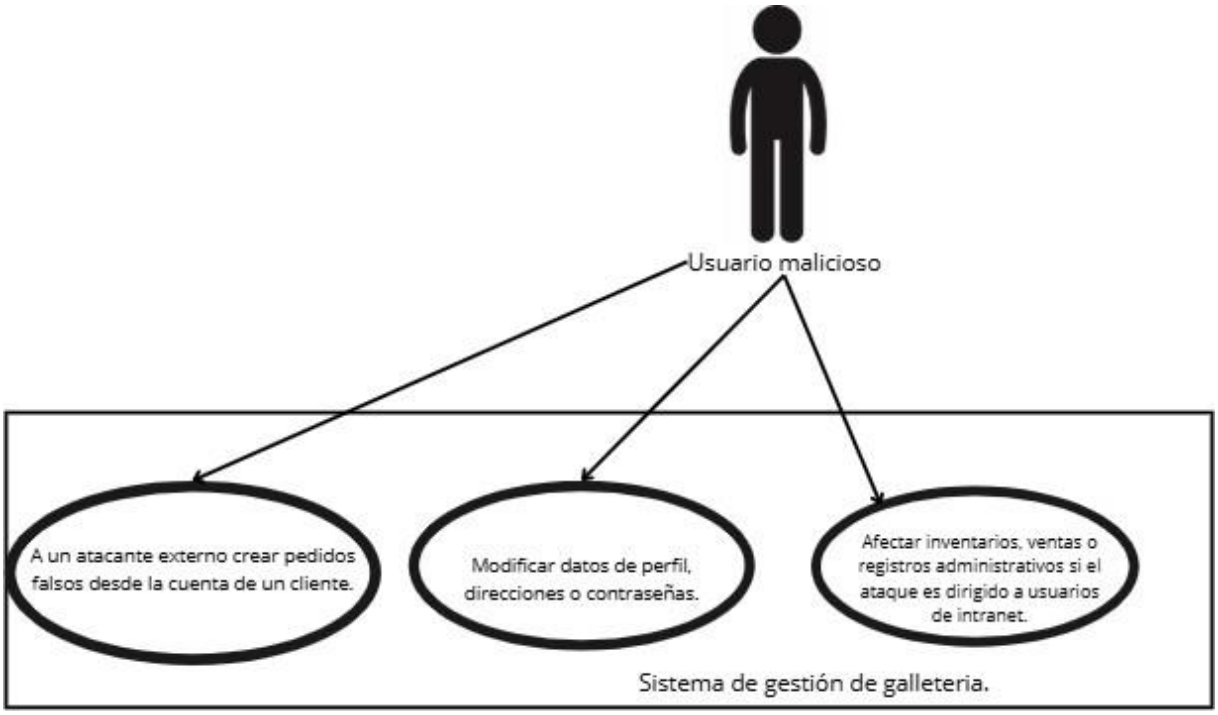
Un cliente o usuario interno (ventas, producción o admin) inicia sesión normalmente en la plataforma desde la web.

Luego, el atacante envía un enlace o página externa (correo, redes sociales, whatsapp) que ejecuta peticiones hacia las rutas internas del sistema Flask, como:

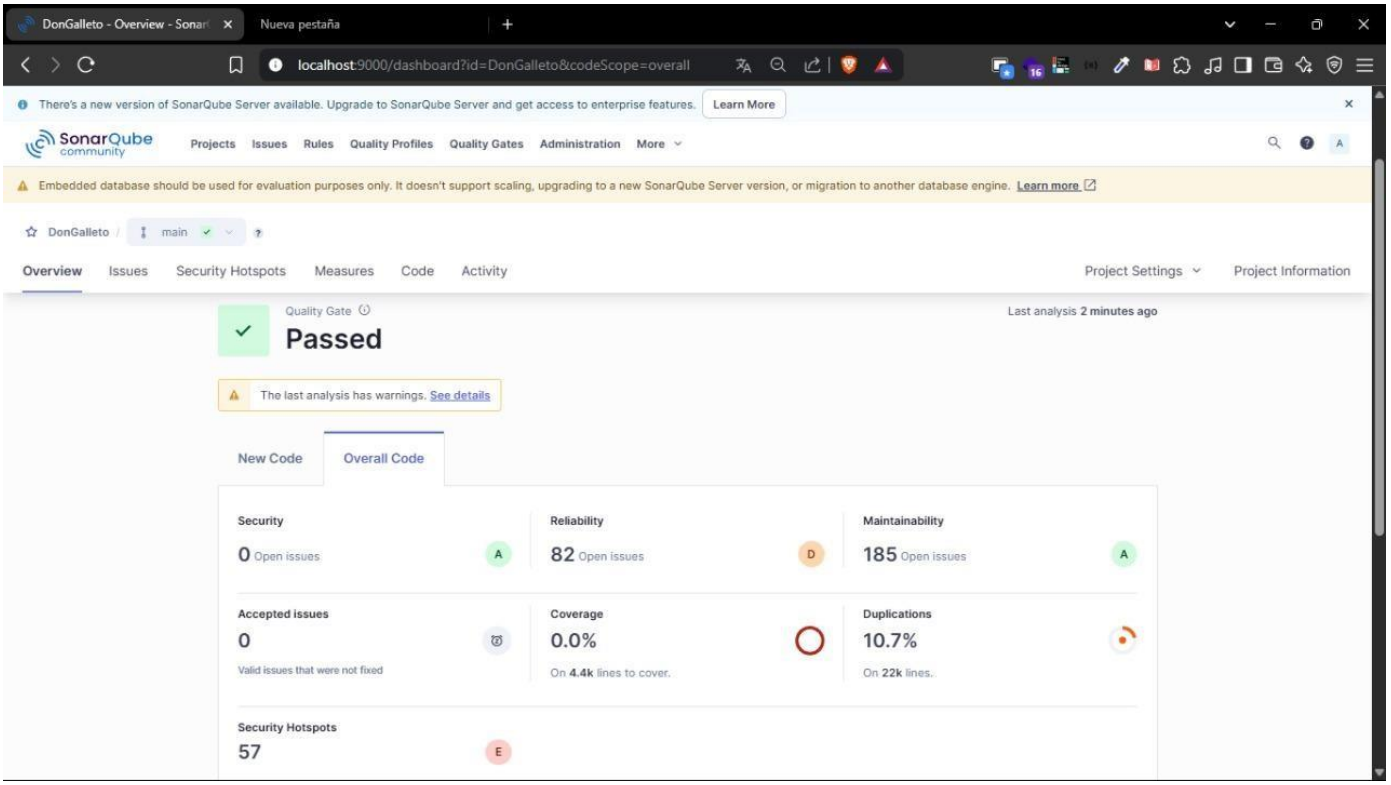
POST /cliente/pedido
POST /ventas/eliminar/registro
POST /inventario/actualizar

Debido a la falta de protección contra CSRF, estas peticiones se procesan sin validar si provienen del usuario real o de un sitio malicioso.
El atacante podría:

- Generar múltiples pedidos de galletas falsos.
- Modificar o eliminar datos importantes.
- Desconfigurar el sistema de inventarios o ventas.


Usuario malicioso
A un atacante externo crear pedidos falsos desde la cuenta de un cliente.
Modificar datos de perfil, direcciones o contraseñas.
Afectar inventarios, ventas o registros administrativos si el ataque es dirigido a usuarios de intranet.
Sistema de gestión de galleteria.

COMPROBACION DE SEGURIDAD



Después de realizar una serie de pruebas con sqlmap, no se encontraron vulnerabilidades en los parámetros proporcionados. El informe muestra que los parámetros que se probaron no son inyectables, lo que indica que no se encontraron puntos débiles en el sistema en cuanto a inyecciones SQL.

Además, hubo algunas advertencias sobre un posible mecanismo de protección como un CAPTCHA y un WAF (Web Application Firewall) que podrían haber interferido con las pruebas.

Proyecto CRUMBELLA