RF-001: Gestión de productos (CRUD)

Nombre: Gestión de productos

Identificador:	RF–001	**Tipo:**	Funcional	**Requerimientos que lo utiliza:**	RF–01 a RF–0012	**¿Crítico?**	Sí
Prioridad de desarrollo:	Alta	**Documentos de visualización asociados:**		admin.html, agregar_producto.html, editar_producto_admin.html, modificar_producto.html			

Entrada:

- Datos del producto (nombre, descripción, precio, stock, imágenes)
- Acciones CRUD (Crear, Leer, Actualizar, Eliminar).

Salida:

- Productos registrados en la base de datos.
- Listado actualizado de productos en la interfaz.

Precondición:

- Usuario debe tener rol de administrador o inventario.
- Sesión activa.

Descripción: El sistema debe permitir a los usuarios autorizados realizar operaciones CRUD sobre los productos, incluyendo gestión de imágenes y stock.

Postcondición:

- Base de datos actualizada.
- Cambios reflejados en la interfaz.

Situaciones anormales:

- Error al subir imágenes.
- Intento de eliminar producto con pedidos asociados.
- Datos inválidos en formulario.

Criterios de aceptación:

- Todos los campos obligatorios deben ser validados.
- Las imágenes deben almacenarse correctamente.
- Los cambios deben persistir después de recargar.

Reglas de negocio:

- Solo administradores pueden eliminar productos.
- El precio debe ser mayor a 0.

RF-002 : Gestión de usuarios y roles.

Nombre: Gestión de usuarios y roles.

Identificador:	RF–002	**Tipo:**	Funcional	**Requerimientos que lo utiliza:** RF–001, RF–004, RF–005, RNF–001**,** RNF–002	**¿Crítico?**	Sí	
Prioridad de desarrollo:	Alta	**Documentos de visualización asociados:**		usuarios_admin.html, editar_usuario.html, registro.html, login.html			

Entrada:

- Datos del usuario (nombre, contraseña, rol).
- Acciones CRUD (Crear, Leer, Actualizar, Eliminar).
- Cambios en roles y permisos.

Salida:

- Usuarios registrados en la base de datos.
- Listado actualizado de usuarios en el panel de administración.
- Confirmación de operaciones (éxito/error).

Precondición:

- Solo usuarios con rol admin pueden gestionar usuarios y roles.
- La sesión debe estar activa.
- No se puede eliminar el último administrador del sistema.

Descripción: El sistema debe permitir a los administradores gestionar usuarios (crear, editar, eliminar) y asignar roles (admin, inventario, cliente). Además, debe validar que no se generen conflictos de permisos.

Postcondición:

- Base de datos actualizada con los cambios en usuarios.
- Los cambios en roles afectan inmediatamente los permisos del usuario.

Situaciones anormales:

- Intento de eliminar un usuario con pedidos activos.
- Asignación de un rol inválido.
- Intento de registro con un nombre de usuario ya existente.
- Pérdida de conexión durante la edición.

Criterios de aceptación:

- Creación de usuario:
  - El formulario debe validar campos obligatorios.
  - La contraseña debe almacenarse de forma segura (hash).

- Edición de usuario:
  - Permitir cambio de contraseña (opcional).
  - No permitir asignar roles superiores al del administrador que realiza el cambio.
- Eliminación de usuario:
  - Confirmación requerida antes de eliminar.
  - No permitir eliminar el último administrador.
- Control de acceso:
  - Solo admin puede gestionar usuarios.
  - Usuarios con rol cliente no deben ver opciones de administración.

Reglas de negocio:

- Roles definidos:
  - Admin. Acceso total (usuarios, productos, pedidos, reportes).
  - Inventario. Solo gestión de productos y stock.
  - Cliente. Solo compras y perfil personal.
- Restricciones:
  - Un usuario no puede auto-eliminarse.
  - No puede haber usuarios sin rol asignado.

RF-003: Proceso de compra y carrito.

Nombre: Proceso de compra

Identificador:	RF–003	**Tipo:**	Funcional	**Requerimientos que lo utiliza:** RF–001, RF–002, RF–004, RF–010, RNF–003, RNF–005	**¿Crítico?**	Sí
Prioridad de desarrollo:	Alta	**Documentos de visualización asociados:**		carrito.html, comprador.html, pago_exitoso.html		

Entrada:

- Productos seleccionados.
- Datos de envío y pago.

Salida:

- Pedido registrado.
- Confirmación de compra.

Precondición:

- Usuario autenticado como cliente.
- Productos disponibles en stock.

Descripción: El sistema debe permitir a los clientes agregar productos al carrito, gestionar su contenido y completar el proceso de compra con opciones de pago.

Postcondición:

- Stock actualizado.
- Pedido registrado en el sistema.

Situaciones anormales:

- Producto agotado durante el proceso.
- Pago rechazado.
- Datos de envío incompletos.

Criterios de aceptación:

- El total debe calcularse correctamente.
- El stock debe disminuir al confirmar compra.
- Debe generarse confirmación por pantalla y correo.

Reglas de negocio:

- Mínimo de compra: $1.
- Stock no puede ser negativo.

RF-004 : Gestión de pedidos.

Nombre: Gestión de pedidos.

				Requerimientos que lo utiliza:			
Identificador:	RF–004	**Tipo:**	Funcional	RF–003, RF–006, RF–008, RF–009, RF–010	**¿Crítico?**	Sí	
Prioridad de desarrollo:	Alta	**Documentos de visualización asociados:**		admin_pedidos.html, ventas.html, pago_exitoso.html			

Entrada:

- Datos del carrito (productos, cantidades).
- Información del cliente (ID, dirección, método de pago).
- Acciones de seguimiento (cambiar estado: *"En proceso"*, *"Enviado"*, *"Entregado"*).

Salida:

- Pedido registrado en la base de datos.
- Confirmación al cliente (página de éxito o correo electrónico).
- Actualización de inventario.

Precondición:

- El usuario debe estar autenticado.
- El carrito no debe estar vacío.
- Debe existir al menos una dirección de envío registrada.

Descripción: El sistema debe permitir: registrar pedidos generados desde el carrito, asignar estados a los pedidos (*"En proceso"*, *"Pagado"*, *"Enviado"*, etc.), notificar al cliente y actualizar el inventario automáticamente.

Postcondición:

- Base de datos actualizada con el nuevo pedido.
- Stock de productos ajustado.
- Historial de compras disponible para el cliente.

Situaciones anormales:

- Producto agotado durante el procesamiento del pedido.
- Error en el método de pago (ej: tarjeta rechazada).
- Dirección de envío inválida (no registrada o incompleta).

Criterios de aceptación:

- Registro correcto:
  - Todos los campos obligatorios deben completarse.
  - El sistema debe generar un ID único para cada pedido.
- Actualización de estados:

- Solo usuarios autorizados (admin/inventario) pueden cambiar estados.
- Los clientes deben recibir notificaciones al cambiar el estado.

- Integridad de datos:
  - Los pedidos deben reflejar con precisión los productos comprados.
  - No se permiten pedidos sin dirección de envío válida.

Reglas de negocio:

- Estados permitidos:
  - *En proceso → Pagado → Enviado → Entregado*.
  - No se puede retroceder estados (ej: de *"Enviado"* a *"En proceso"*).
- Mínimo de compra. No se registran pedidos con total ≤ $0.
- Tiempo de respuesta. Los pedidos deben procesarse en ≤ 24 horas.

RF-005 : Sistema de autenticación.

Nombre: Sistema de autenticación.

Identificador:	RF–005	**Tipo:**	Funcional	**Requerimientos que lo utiliza:** RF–001 a RF–012, RNF–001, RNF–002	**¿Crítico?**	Sí	
Prioridad de desarrollo:	Máxima	**Documentos de visualización asociados:**		login.html, registro.html, base.html			

Entrada:

- Credenciales de usuario (nombre de usuario y contraseña).
- Datos de registro (usuario, contraseña, rol).
- Solicitudes de cierre de sesión.

Salida:

- Sesión iniciada/denegada.
- Token de sesión válido.
- Redirección a interfaz según rol.

Precondición:

- Para login: usuario debe estar registrado previamente.
- Para registro: nombre de usuario debe ser único.
- Para acceder a funciones: sesión debe estar activa.

Descripción: El sistema debe: permitir registro de nuevos usuarios con roles definidos, validar credenciales durante el login, mantener sesiones seguras, restringir acceso según roles (admin, inventario, cliente), y permitir cierre de sesión seguro.

Postcondición:

- Usuario autenticado obtiene acceso a funciones según su rol.
- Base de datos actualizada con nuevos registros.
- Sesión activa con tiempo de expiración definido.

Situaciones anormales:

- Credenciales incorrectas (usuario/contraseña inválidos).
- Intento de registro con usuario ya existente.
- Sesión expirada durante operaciones críticas.
- Ataques por fuerza bruta (múltiples intentos fallidos).

Criterios de aceptación:

- Seguridad:
  - Contraseñas deben almacenarse con hash (no texto plano).
  - Mínimo 3 intentos fallidos antes de bloqueo temporal.

- Funcionalidad:
  - Tiempo de respuesta < 2 segundos para autenticación.
  - Sesiones expiran después de 30 minutos de inactividad.
- Usabilidad:
  - Mensajes de error claros (sin revelar información sensible).
  - Redirección correcta según rol al autenticarse.

Reglas de negocio:

- Roles predefinidos: admin, inventario, cliente
- Contraseñas:
  - Mínimo 8 caracteres.
  - Requiere al menos 1 número y 1 carácter especial.
- Administradores. Solo pueden ser creados por otros administradores
- Bloqueos. 5 intentos fallidos bloquean la cuenta por 15 minutos

RF-006 : Gestión de inventario.

Nombre: Gestión y control de inventario.

Identificador:	RF–006	**Tipo:**	Funcional	**Requerimientos que lo utiliza:** RF–001, RF–003, RF–004, RF–008, RNF–005	**¿Crítico?** Sí
Prioridad de desarrollo:	Alta	**Documentos de visualización asociados:**		inventario.html, modificar_producto.html, admin.html	

Entrada:

- Movimientos de inventario (compras, devoluciones, ajustes).
- Nuevos productos con stock inicial.
- Actualizaciones manuales de existencias.

Salida:

- Stock actualizado en base de datos.
- Alertas de bajo inventario.
- Registro histórico de movimientos.

Precondición:

- Usuario debe tener rol admin o inventario.
- Producto debe existir en el sistema.
- Sesión activa.

Descripción:

El sistema debe: actualizar automáticamente el stock al procesar compras, permitir ajustes manuales de inventario, generar alertas cuando stock ≤ mínimo configurado y mantener histórico de movimientos.

Postcondición:

- Base de datos con valores actualizados.
- Consistencia entre stock físico y digital.
- Registro auditado de cambios.

Situaciones anormales:

- Stock negativo: Intento de vender más unidades de las disponibles.
- Producto no encontrado: ID inválido al actualizar.
- Concurrencia: Múltiples actualizaciones simultáneas.

Criterios de aceptación:

- Actualización en tiempo real. Cambios deben reflejarse inmediatamente en todo el sistema.
- Validación de datos:
  - Stock no puede ser negativo.

- Solo números enteros positivos.

- Alertas automáticas. Notificar cuando stock < 5 unidades.

Reglas de negocio:

- Mínimo de stock. No permitir ventas si stock = 0.
- Responsables. Solo personal autorizado (inventario/admin) puede hacer ajustes manuales.
- Histórico. Conservar registros por 2 años.

RF-007 : Sistema de calificaciones y comentarios.

Nombre: Sistema de valoración y comentario de productos.

Identificador:	RF–007	**Tipo:**	Funcional	**Requerimientos que lo utiliza:** RG–001, RG–003, RG–005, RG–011, RNF–005		**¿Crítico?**	Medio
Prioridad de desarrollo:	Media	**Documentos de visualización asociados:**		calificar.html, comprador.html, admin.html			

Entrada:

- Calificación (1-5 estrellas).
- Comentario textual (opcional).
- ID de producto y usuario

Salida:

- Promedio de valoraciones actualizado.
- Comentario publicado en ficha de producto.
- Actualización en sistema de recomendaciones.

Precondición:

- Usuario debe haber comprado el producto.
- Sesión activa.
- Producto debe existir.

Descripción:

El sistema debe permitir: valorar productos con estrellas (1-5), añadir comentarios opcionales, mostrar historial de valoraciones, calcular promedio automáticamente y filtrar contenido ofensivo.

Postcondición:

- Base de datos actualizada con nueva valoración.
- Promedio visible en ficha de producto.
- Recomendaciones ajustadas.

Situaciones anormales:

- Producto no comprado. Intento de valorar sin compra previa.
- Comentario vacío. Envío solo de estrellas sin texto.
- Contenido inapropiado. Detección de palabras prohibidas

Criterios de aceptación:

- Validación:
  - Solo 1 valoración por usuario por producto.
  - Rango estrictamente 1-5 estrellas.

- Moderación. Comentarios con palabras prohibidas se marcan como "pendientes de revisión".
- Actualización. Promedio se recalcula en tiempo real.

Reglas de negocio:

- Verificación de compra. Solo se puede valorar productos adquiridos en últimos 90 días.
- Anonimato. Los comentarios muestran solo iniciales del usuario (ej: "Carlos M." → "C.M.").
- Edición. Usuarios pueden editar sus comentarios dentro de las primeras 24 horas.

RF-008 : Gestión de reportes y estadísticas.

Nombre: Generación y visualización de reportes analíticos.

Identificador:	RF–008	**Tipo:**	Funcional	**Requerimientos que lo utiliza:** RF–001, RF–003, RF–004, RF–07, RNF–001	**¿Crítico?**	Medio	
Prioridad de desarrollo:	Media	**Documentos de visualización asociados:**		admin_reportes.html, ventas.html			

Entrada:

- Rango de fechas para filtrado.
- Tipos de reporte solicitados (ventas, inventario, etc.).
- Parámetros de agrupación (por producto, categoría, región).

Salida:

- Reportes en formato tabla/gráfico.
- Archivos exportables (CSV, PDF).
- Alertas de tendencias clave.

Precondición:

- Usuario con rol admin.
- Datos históricos existentes (mínimo 1 mes).
- Sesión activa.

Descripción:

El sistema debe generar: reportes diarios/semestrales/anuales de ventas, análisis de productos estrella y bajo desempeño, tendencias de satisfacción y proyecciones de inventario.

Postcondición:

- Datos consolidados para toma de decisiones.
- Registro de reportes generados.
- Base de datos no modificada (solo consulta).

Situaciones anormales:

- Sin datos: Período seleccionado sin registros.
- Rango inválido: Fecha inicial mayor a final.
- Carga pesada: Consultas sobre >1 millón de registros.

Criterios de aceptación:

- Rendimiento:
  - Generar reportes mensuales en <10 segundos.
  - Exportar CSV con 50k registros en <30 segundos.
- Precisión:

- Diferencias máx. del 0.1% vs datos crudos.
- Redondeo consistente en valores monetarios.

- Seguridad. Datos financieros visibles solo para administradores.

Reglas de negocio:

- Retención de datos. Reportes deben incluir datos hasta 36 meses atrás
- Confidencialidad. Ocultar montos específicos en vistas previas
- Automatización. Envío automático de reportes clave cada lunes a las 8:00 AM

RF-009 : Gestión de direcciones de envío.

Nombre: Administración de direcciones de entrega.

Identificador:	RF–009	**Tipo:**	Funcional	**Requerimientos que lo utiliza:** RF–003, RF–004, RF–005, RNF–002	**¿Crítico?**	Sí	
Prioridad de desarrollo:	Alta	**Documentos de visualización asociados:**		direcciones.html, carrito.html			

Entrada:

- Datos de dirección (calle, ciudad, CP, etc.).
- Acciones CRUD (crear/editar/eliminar).
- Selección para envío.

Salida:

- Direcciones almacenadas en perfil de usuario.
- Confirmación visual de operaciones.
- Dirección aplicada a nuevos pedidos.

Precondición:

- Usuario autenticado.
- Datos mínimos completos (calle, ciudad, CP).
- Límite máximo de 5 direcciones por usuario.

Descripción:

El sistema debe permitir: registrar múltiples direcciones por usuario, marcar dirección principal, validar formato de código postal, integrarse con proceso de compra y proteger datos personales.

Postcondición:

- Base de datos actualizada.
- Disponible para selección en futuras compras.
- Histórico conservado en pedidos completados.

Situaciones anormales:

- CP inválido. No coincide con ciudad/estado.
- Límite excedido. Intento de añadir > 5 direcciones.
- Eliminación en uso. Dirección asociada a pedido pendiente.

Criterios de aceptación:

- Validación:
  - Formato CP según país (ej: 5 dígitos para México).
  - Campos obligatorios completos.
- Integración:

- Selección obligatoria en checkout.
- Visualización correcta en detalles de pedido.

- Seguridad. Nunca mostrar dirección completa en listados públicos.

Reglas de negocio:

- Geolocalización. Solo direcciones nacionales (no internacionales).
- Actualizaciones. Pedidos en proceso mantienen dirección original aunque el usuario la modifique después.
- Privacidad. Opción de "eliminar" solo oculta la dirección (borrado lógico).

RF-010 : Gestión de tarjetas de crédito.

Nombre: Administración de métodos de pago con tarjetas.

Identificador:	RF–010	**Tipo:**	Funcional	**Requerimientos que lo utiliza:** RF–003, RF–004, RF–005, RF–012, RNF–003	**¿Crítico?**	Sí	
Prioridad de desarrollo:	Crítica	**Documentos de visualización asociados:**		tarjetas.html, carrito.html			

Entrada:

- Datos de tarjeta (número, titular, vencimiento, CVV).
- Acciones CRUD (agregar/eliminar).
- Selección para transacción.

Salida:

- Token seguro almacenado (no datos completos).
- Confirmación visual de operaciones.
- Método disponible para futuras compras.

Precondición:

- Usuario autenticado.
- Campos válidos según estándares PCI.
- Límite máximo de 3 tarjetas por usuario.

Descripción:

El sistema debe: almacenar tarjetas de forma segura, validar datos según emisor (Visa/MC/Amex), permitir marcado como "predeterminada", integrarse con pasarela de pagos e implementar autenticación 3D Secure cuando aplique.

Postcondición:

- Datos tokenizados en base de datos.
- Disponible para selección en futuras compras.
- Histórico conservado en transacciones.

Situaciones anormales:

- Tarjeta rechazada. Validación inicial fallida.
- Expirada. Fecha vencida al intentar usar.
- Límite excedido. Intento de añadir >3 tarjetas.

Criterios de aceptación:

- Seguridad:
  - Cumplimiento PCI DSS Nivel 4.
  - Nunca almacenar CVV completo.

- Validación:
  - Algoritmo de Luhn para números de tarjeta.
  - Formatos específicos por tipo (Amex 15 dígitos, etc.).
- Experiencia. Carga de tarjeta predeterminada automáticamente.

Reglas de negocio:

- Tokenización. Solo últimos 4 dígitos visibles en interfaz.
- Actualizaciones. Edición no permitida (eliminar y crear nueva).
- Internacionalización. Aceptar tarjetas internacionales con recargo del 3%.

RF-011 : Sistema de recomendaciones.

Nombre: Motor de recomendaciones personalizadas.

Identificador:	RF–011	**Tipo:**	Funcional	**Requerimientos que lo utiliza:** RF–01, RF–03, RF–07, RF–08, RNF–005	**¿Crítico?**	Medio	
Prioridad de desarrollo:	Media	**Documentos de visualización asociados:**		comprador.html, recomendaciones.html			

Entrada:

- Historial de compras del usuario.
- Valoraciones propias y de otros usuarios.
- Productos frecuentemente comprados juntos.

Salida:

- Listado personalizado de 3-5 productos recomendados.
- Sección "Productos similares" en fichas.
- Sugerencias basadas en tendencias.

Precondición:

- Usuario autenticado.
- Mínimo 3 productos en catálogo.
- Al menos 1 interacción previa (compra/valoración).

Descripción:

El sistema debe: analizar patrones de compra/valoración; implementar 3 tipos de recomendaciones: basadas en usuario (similitud con otros compradores), basadas en ítem (productos relacionados) y tendencias (popularidad general); y excluir productos sin stock.

Postcondición:

- Recomendaciones actualizadas tras cada interacción.
- Registro de sugerencias mostradas.

Situaciones anormales:

- Usuario nuevo. Sin historial para personalización.
- Stock agotado. Producto recomendado no disponible.
- Sesión anónima. Mostrar solo tendencias generales.

Criterios de aceptación:

- Relevancia. 70% de productos recomendados deben coincidir con categorías previas del usuario.
- Rendimiento. Tiempo de generación < 2 segundos.
- Actualización. Incluir al menos 1 novedad semanal en sugerencias.

Reglas de negocio:

- Diversidad. Máximo 2 productos de misma categoría por lista.
- Priorización. Productos con rating > 4 estrellas tienen +20% de visibilidad.
- Ética. No recomendar productos con valoración promedio < 2 estrellas.

RF-012 : Integración con Stripe para pagos.

Nombre: Procesamiento de pagos mediante Stripe.

				Requerimientos que lo utiliza:			
Identificador:	RF–012	**Tipo:**	Funcional	RF–003, RF–004, RF–010, RNF–003	**¿Crítico?**	Sí	
Prioridad de desarrollo:	Crítica	**Documentos de visualización asociados:**		carrito.html (botón de pago Stripe), pago_exitoso.html			

Entrada:

- Token de pago generado por Stripe.
- Monto total y descripción de compra.
- Datos de envío.

Salida:

- Transacción aprobada/rechazada.
- Recibo electrónico generado.
- Pedido registrado.

Precondición:

- Carrito con total > $0.
- Usuario autenticado.
- Conexión activa a Internet.

Descripción:

El sistema debe: integrarse con API de Stripe v3; manejar 3 flujos de pago: Checkout embebido (para tarjetas guardadas), Checkout redirigido (nuevos métodos) y Pagos recurrentes (suscripciones); e implementar webhooks para confirmaciones asíncronas.

Postcondición:

- Registro de transacción en base de datos.
- Actualización de inventario.
- Notificación al cliente (email/app).

Situaciones anormales:

- Pago rechazado. Fondos insuficientes.
- Timeout. Sin respuesta de Stripe en 15 segundos.
- Doble cargo. Reintento fallido.

Criterios de aceptación:

- Seguridad:
  - No almacenar datos sensibles (cumple PCI DSS vía Stripe).
  - Validar firma webhooks.

- Experiencia:
  - Tiempo de procesamiento <8 segundos.
  - Soporte para 3DS2.
- Compatibilidad. Funcionar en navegadores modernos (Chrome, Safari, Edge).

Reglas de negocio:

- Comisiones. Absorber costo del 2.9% + $0.30 por transacción.
- Reintentos. Máximo 1 reintento automático por fallo.
- Divisas. Solo Mx inicialmente.

RNF-001 : Control de acceso basado en roles.

Nombre: Sistema de permisos por roles de usuarios.

Identificador:	RNF–001	**Tipo:**	No funcional	**Requerimientos que lo utiliza:** RF–001 a RF–012		**¿Crítico?**	Sí
Prioridad de desarrollo:	Máxima	**Documentos de visualización asociados:**		base.html, admin.html			

Entrada:

- Rol del usuario autenticado (admin/inventario/cliente).
- Solicitud de acceso a recurso/función.

Salida:

- Acceso concedido/denegado.
- Redirección a interfaz correspondiente.
- Registro de intentos no autorizados.

Precondición:

- Usuario autenticado.
- Roles definidos en sistema.

Descripción:

El sistema debe: implementar matriz RBAC (Role-Based Access Control); restringir funciones según 3 roles base: Admin (Acceso completo), Inventario (Solo gestión de productos/stock) y Cliente (Solo compras y perfil); y usar middlewares para verificación en cada endpoint.

Postcondición:

- Interfaz adaptada al rol.
- Auditoría de accesos en logs.
- Prevención de elevación de privilegios.

Situaciones anormales:

- Rol no reconocido. Usuario sin rol asignado.
- Token inválido. Sesión comprometida.
- Escalada de privilegios. Intento de acceder a funciones de admin.

Criterios de aceptación:

- Cobertura:
  - 100% de endpoints protegidos.
  - 0 accesos no autorizados en pruebas de penetración.
- Rendimiento. Verificación en <100ms por solicitud.
- Auditoría. Registro de todos los intentos fallidos con IP/timestamp.

Reglas de negocio:

- Mínimos privilegios. Los usuarios solo tienen lo estrictamente necesario.
- Herencia de roles. Admin hereda todos los permisos de inventario.
- Denegación por defecto. Acceso bloqueado si no hay regla explícita.

RNF-002 : Protección de datos sensibles.

Nombre: Protección de información confidencial.

Identificador:	RNF–S02	**Tipo:**	No funcional	**Requerimientos que lo utiliza:** RF–005, RF–009, RF–010, RF–012		**¿Crítico?**	Sí
Prioridad de desarrollo:	Máxima	**Documentos de visualización asociados:**		Política de privacidad del sistema, registro.html			

Entrada:

- Datos sensibles (contraseñas, tarjetas, direcciones).
- Solicitudes de acceso a información.

Salida:

- Datos cifrados almacenados.
- Información enmascarada en interfaces.
- Registros de auditoría.

Precondición:

- Identificación del tipo de dato (sensible/no sensible).
- Mecanismos de cifrado configurados.

Descripción:

El sistema debe: cifrar datos sensibles en tránsito (TLS 1.2+) y en reposo (AES-256), implementar enmascaramiento visual (ej: **** 4242), cumplir con GDPR/LGPD para datos personales y eliminar datos sensible de logs.

Postcondición:

- Datos almacenados de forma segura.
- Prevención de fugas de información.
- Cumplimiento normativo.

Situaciones anormales:

- Intento de acceso no autorizado.
- Fallo en cifrado/descifrado.
- Datos sensibles en logs.

Criterios de aceptación:

- Cifrado:
  - 100% de datos sensibles cifrados.
  - Claves rotadas cada 90 días.
- Enmascaramiento:

- Tarjetas: Solo últimos 4 dígitos visibles.
- Contraseñas: Nunca mostradas.

- Legal. Auditoría anual de cumplimiento GDPR.

Reglas de negocio:

- Retención. Datos financieros solo hasta completar transacción.
- Responsables. Solo personal autorizado puede acceder a datos crudos.
- Emergencias. Procedimiento para revocar accesos ante brechas.

RNF-003 : Seguridad en transacciones financieras.

Nombre: Protección de operaciones monetarias.

Identificador:	RNF–003	**Tipo:**	No funcional	**Requerimientos que lo utiliza:** RF–003, RF–004, RF–010, RF–012, RNF–002	**¿Crítico?**	Sí	
Prioridad de desarrollo:	Crítica	**Documentos de visualización asociados:**	carrito.html (formulario de pago), Política de seguridad financiera				

Entrada:

- Datos de transacción (monto, método de pago).
- Token de pago seguro.
- Datos de auditoría (IP, timestamp).

Salida:

- Transacción autorizada/rechazada.
- Comprobante digital.
- Registro cifrado en base de datos.

Precondición:

- Conexión HTTPS activa (TLS 1.2+).
- Integración con pasarela de pagos.
- Validación previa de datos.

Descripción:

El sistema debe garantizar: Cumplimiento PCI DSS Nivel 1, autenticación 3D Secure para transacciones >$100, no almacenamiento de datos sensibles post-transacción y verificación de montos contra órdenes de compra.

Postcondición:

- Transacción registrada y verificada.
- Reversión automática en fallos.
- Notificación a ambas partes.

Situaciones anormales:

- Discrepancia de montos. Diferencia >1% entre orden y cargo.
- Fallo de conexión. Interrupción durante transacción.
- Falsificación. Intento de modificar datos de pago.

Criterios de aceptación:

- Estándares:
  - 100% de transacciones PCI DSS compliant.

- Certificación anual QSA.

- Trazabilidad:
  - Auditoría completa de cada transacción.
  - Tolerancia cero a transacciones no reconciliadas.
- Disponibilidad. SLA 99.99% para API de pagos.

Reglas de negocio:

- Límites. Transacciones >$500 requieren autenticación adicional.
- Reversiones. Reembolsos completos en <72 horas.
- Monitoreo. Alertas por patrones fraudulentos (≥3 intentos fallidos en 5 min).

RNF-004 : Protección contra CSRF.

Nombre: Prevención de falsificación de solicitudes entre sitios.

Identificador:	RNF–004	**Tipo:**	No funcional	**Requerimientos que lo utiliza:** RF–003, RF–004, RF–010, RF–012.		**¿Crítico?**	Si
Prioridad de desarrollo:	Alta	**Documentos de visualización asociados:**		Política de seguridad de formularios, Plantillas base del sistema			

Entrada:

- Solicitudes HTTP (POST/PUT/DELETE).
- Tokens CSRF generados por sesión.

Salida:

- Solicitudes validadas/rechazadas.
- Registros de intentos fallidos.

Precondición:

- Sesión de usuario activa.
- Formularios con campos ocultos para tokens.
- Cookies SameSite configuradas.

Descripción:

- El sistema debe implementar: Tokens CSRF únicos por sesión y formulario, validación en el servidor de cada solicitud crítica, cookies con atributos Secure y HttpOnly, y excepciones para APIs públicas/documentadas.

Postcondición:

- Transacciones seguras contra ataques CSRF.
- Tokens invalidados tras su uso o expiración.

Situaciones anormales:

- Token faltante. Solicitud sin token CSRF.
- Token inválido. No coincide con sesión.
- Token reutilizado. Intento de replay attack.

Criterios de aceptación:

- Cobertura:
  - 100% de formularios con acciones críticas protegidos.
  - 0 vulnerabilidades CSRF en pentests anuales.
- Rendimiento. Generación/validación en <50ms.
- Experiencia. Sin impacto visible para usuarios legítimos.

Reglas de negocio:

- Rotación. Tokens expiran tras 24h o cierre de sesión.
- Excepciones. APIs de solo lectura no requieren token.
- Monitoreo. Alerta tras >5 intentos fallidos consecutivos.

RNF-005 : Validación de entradas.

Nombre: Validación de datos de entrada.

Identificador:	RNF–005	**Tipo:**	No funcional	**Requerimientos que lo utiliza:** RF–001 a RF–012	**¿Crítico?** Si
Prioridad de desarrollo:	Alta	**Documentos de visualización asociados:**		Política de validación de datos, Especificación de formatos	

Entrada:

- Datos ingresados por usuarios/APIs.
- Parámetros de consulta.
- Archivos subidos

Salida:

- Datos normalizados y saneados.
- Mensajes de error descriptivos.
- Registros de intentos inválidos.

Precondición:

- Esquema de validación definido.
- Lista de patrones permitidos/denegados.

Descripción:

El sistema debe: validar en frontend y backend (defensa en profundidad); implementar: Estructura (Tipos de datos esperados), Contenido (Patrones regex (ej: emails)), Rango (Valores mínimos/máximos) y Contexto (Sanitización según destino (SQL/HTML)); y rechazar entradas maliciosas (XSS, SQLi).

Postcondición:

- Base de datos protegida contra inyecciones.
- Interfaces libres de código malicioso.
- Consistencia en datos almacenados.

Situaciones anormales:

- Datos inválidos. Fuera de formato/rango.
- Ataques. Inyección de código detectada.
- Corrupción. Caracteres extraños/bytes nulos.

Criterios de aceptación:

- Cobertura:
  - 100% de endpoints con validación.
  - 0 vulnerabilidades OWASP Top 10.

- Precisión. Falsos positivos <1% en pruebas.
- Experiencia. Mensajes de error sin detalles técnicos.

Reglas de negocio:

- Estandarización:
  - Formato fechas: ISO 8601 (YYYY-MM-DD).
  - Números: Puntos decimales, no comas.
- Seguridad. Bloqueo tras 5 intentos inválidos en 10 min.
- Registros. Auditoría de intentos fallidos con IP/datos.