# Riesgos de Seguridad – Sistema de Gestión de Inventario y Punto de Venta

## Lista de Riesgos de Seguridad

### Inyección SQL

Descripción: Entrada de datos maliciosa en campos como login, búsqueda de productos o gestión de clientes que manipule consultas SQL.

Impacto: Acceso no autorizado a datos sensibles (inventario, ventas, clientes), alteración o eliminación de información crítica.

Mitigación: Uso de queries parametrizadas/preparadas, validación estricta de entradas y principio de mínimo privilegio en la base de datos.

### Fuga de Datos Sensibles

Descripción: Exposición de información de clientes (NIT/RFC, correos, teléfonos) o empleados mediante APIs inseguras o fallas de configuración.

Impacto: Robo de identidad, incumplimiento de normativas fiscales y de privacidad, sanciones legales.

Mitigación: Cifrado en tránsito (TLS 1.3) y en reposo (AES-256), control estricto de acceso y logs sin datos sensibles.

### Acceso No Autorizado (Escalada de Privilegios)

Descripción: Un usuario con rol limitado (ej. cajero) podría obtener privilegios de supervisor o propietario debido a fallas en la validación de roles.

Impacto: Manipulación de ventas, facturación falsa, eliminación de registros, fraude interno.

Mitigación: Middleware robusto de autorización, pruebas de control de acceso y auditoría de cambios críticos.

### Gestión Insegura de Sesiones

Descripción: Tokens de sesión o cookies sin protección podrían ser robados (session hijacking) en terminales POS compartidas.

Impacto: Suplantación de identidad de usuarios y acceso a operaciones críticas.

Mitigación: Tokens con expiración corta y refresh tokens, cookies con HttpOnly/Secure/SameSite, cierre automático de sesión por inactividad.

### Contraseñas Débiles y Recuperación Insegura

Descripción: Almacenamiento de contraseñas con hash débil o mecanismos inseguros de recuperación (tokens sin expiración).

Impacto: Compromiso de múltiples cuentas, ataques de fuerza bruta y reutilización de credenciales.

Mitigación: Hashing con bcrypt/Argon2 + salt, política de contraseñas robusta, tokens de recuperación con caducidad y notificación al gerente.

### Ataques de Cross-Site Scripting (XSS)

Descripción: Inyección de scripts en campos como descripciones de productos, notas de ventas o direcciones de clientes.

Impacto: Robo de sesiones de usuarios, manipulación de interfaz POS, alteración de reportes.

Mitigación: Escapar correctamente entradas en frontend, sanitización en formularios y uso de Content Security Policy (CSP).

### Fraude en Transacciones y Manipulación del POS

Descripción: Alteración de precios, descuentos o métodos de pago desde el frontend (ej. manipulación de requests HTTP).

Impacto: Pérdida financiera, ventas falsas, reportes contables incorrectos.

Mitigación: Validación de reglas de negocio en backend, auditoría de cambios de precios y alertas automáticas de transacciones anómalas.

### Denegación de Servicio (DoS/DDoS)

Descripción: Saturación del sistema de inventario o panel de ventas con múltiples solicitudes concurrentes.

Impacto: Caída del sistema POS en horas críticas de venta.

Mitigación: Rate limiting, balanceadores de carga y monitoreo de tráfico inusual.

### Integraciones Externas Inseguras

Descripción: APIs de pagos o hardware POS mal configurados que expongan llaves o credenciales.

Impacto: Robo de datos financieros, transacciones fraudulentas.

Mitigación: Uso de llaves API en servidores seguros, rotación periódica de credenciales y certificación PCI DSS.

### Backups y Logs sin Protección

Descripción: Archivos de respaldo o logs con datos sensibles almacenados en texto plano o accesibles públicamente.

Impacto: Pérdida masiva de datos en caso de fuga, incumplimiento legal.

Mitigación: Cifrado de backups y acceso restringido, rotación y purga de logs antiguos, plan de continuidad de negocio probado.

## Tabla Comparativa de Riesgos de Seguridad

|  |  |  |  |
| --- | --- | --- | --- |
| Riesgo | Descripción | Impacto | Mitigación |
| Inyección SQL | Entrada de datos maliciosa en campos como login, búsqueda de productos o gestión de clientes que manipule consultas SQL. | Acceso no autorizado a datos sensibles (inventario, ventas, clientes), alteración o eliminación de información crítica. | Uso de queries parametrizadas/preparadas, validación estricta de entradas y principio de mínimo privilegio en la base de datos. |
| Fuga de Datos Sensibles | Exposición de información de clientes (NIT/RFC, correos, teléfonos) o empleados mediante APIs inseguras o fallas de configuración. | Robo de identidad, incumplimiento de normativas fiscales y de privacidad, sanciones legales. | Cifrado en tránsito (TLS 1.3) y en reposo (AES-256), control estricto de acceso y logs sin datos sensibles. |
| Acceso No Autorizado (Escalada de Privilegios) | Un usuario con rol limitado (ej. cajero) podría obtener privilegios de supervisor o propietario debido a fallas en la validación de roles. | Manipulación de ventas, facturación falsa, eliminación de registros, fraude interno. | Middleware robusto de autorización, pruebas de control de acceso y auditoría de cambios críticos. |
| Gestión Insegura de Sesiones | Tokens de sesión o cookies sin protección podrían ser robados (session hijacking) en terminales POS compartidas. | Suplantación de identidad de usuarios y acceso a operaciones críticas. | Tokens con expiración corta y refresh tokens, cookies con HttpOnly/Secure/SameSite, cierre automático de sesión por inactividad. |
| Contraseñas Débiles y Recuperación Insegura | Almacenamiento de contraseñas con hash débil o mecanismos inseguros de recuperación (tokens sin expiración). | Compromiso de múltiples cuentas, ataques de fuerza bruta y reutilización de credenciales. | Hashing con bcrypt/Argon2 + salt, política de contraseñas robusta, tokens de recuperación con caducidad y notificación al gerente. |
| Ataques de Cross-Site Scripting (XSS) | Inyección de scripts en campos como descripciones de productos, notas de ventas o direcciones de clientes. | Robo de sesiones de usuarios, manipulación de interfaz POS, alteración de reportes. | Escapar correctamente entradas en frontend, sanitización en formularios y uso de Content Security Policy (CSP). |
| Fraude en Transacciones y Manipulación del POS | Alteración de precios, descuentos o métodos de pago desde el frontend (ej. manipulación de requests HTTP). | Pérdida financiera, ventas falsas, reportes contables incorrectos. | Validación de reglas de negocio en backend, auditoría de cambios de precios y alertas automáticas de transacciones anómalas. |
| Denegación de Servicio (DoS/DDoS) | Saturación del sistema de inventario o panel de ventas con múltiples solicitudes concurrentes. | Caída del sistema POS en horas críticas de venta. | Rate limiting, balanceadores de carga y monitoreo de tráfico inusual. |
| Integraciones Externas Inseguras | APIs de pagos o hardware POS mal configurados que expongan llaves o credenciales. | Robo de datos financieros, transacciones fraudulentas. | Uso de llaves API en servidores seguros, rotación periódica de credenciales y certificación PCI DSS. |
| Backups y Logs sin Protección | Archivos de respaldo o logs con datos sensibles almacenados en texto plano o accesibles públicamente. | Pérdida masiva de datos en caso de fuga, incumplimiento legal. | Cifrado de backups y acceso restringido, rotación y purga de logs antiguos, plan de continuidad de negocio probado. |