**ANÁLISIS STRIDE – SISTEMA DE GESTIÓN DE INVENTARIO Y VENTAS**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Módulo** | **S (Suplantación)** | **T (Repudio)** | **R (Robo de info)** | **I (Integridad)** | **D (Denegación)** | **E (Elevación)** |
| **Usuarios** | Riesgo de login falso si no hay autenticación fuerte. | Podría negar haber hecho cambios si no hay logs. | Datos personales expuestos si no se cifran. | Cambiar contraseñas u otros perfiles sin permiso. | Ataques de fuerza bruta al login. | Riesgo de obtener rol de administrador sin autorización. |
| **Inventario** | Suplantar usuario para registrar movimientos falsos. | Negar movimientos de productos (ej. salida de stock). | Robo de datos de productos, costos o proveedores. | Alterar cantidades para simular faltantes o excesos. | Bloquear consultas de inventario con sobrecarga. | Dar permisos de edición a usuarios que solo deberían ver. |
| **Ventas** | Suplantar cajero para registrar o cancelar ventas. | Negar que se realizó una venta o devolución. | Exposición de datos de clientes y tickets. | Modificar precios o descuentos sin permiso. | Generar múltiples ventas falsas que saturen el sistema. | Pasar de vendedor normal a administrador. |
| **Reportes** | Suplantar usuario para acceder a reportes confidenciales. | Negar que se generó o compartió un reporte. | Fuga de datos sensibles (ej. ventas totales, ganancias). | Alterar reportes para mostrar información incorrecta. | Peticiones masivas de reportes que saturen el sistema. | Acceder a reportes restringidos (ej. solo gerencia). |

**EXPLICACIÓN BREVE**

- Suplantación (S): Si alguien roba credenciales, puede entrar como otro usuario y registrar ventas falsas.  
- Repudio (T): Si no hay bitácoras (logs), un usuario puede negar que cambió datos del inventario o eliminó un reporte.  
- Robo de información (R): Datos sensibles como clientes, precios, inventario o reportes de ventas podrían filtrarse.  
- Integridad (I): Existe riesgo de que alguien cambie datos de inventario, modifique ventas o edite reportes sin permiso.  
- Denegación de servicio (D): Ataques que saturen el login, inventario o reportes pueden dejar el sistema fuera de uso.  
- Elevación de privilegios (E): Un usuario con rol básico (ej. vendedor) podría intentar obtener permisos de administrador para controlar todo el sistema.