**Introducción**

La seguridad en los sistemas de información es fundamental para proteger los datos y garantizar el funcionamiento confiable de las operaciones comerciales. En el caso de un sistema de gestión de inventarios y punto de venta, es crucial implementar medidas de seguridad que resguarden la información sobre productos, existencias y transacciones de ventas. Este documento establece los requisitos básicos de seguridad que deben cumplirse para asegurar la confidencialidad, integridad y disponibilidad del sistema, protegiendo tanto los datos de la empresa como la experiencia de sus usuarios.

**Requisitos básicos de seguridad**

1. **Autenticación de usuarios**

* Uso de credenciales únicas por usuario: Cada usuario debe tener su propio acceso para asegurar que todas las acciones sean trazables y atribuibles a una persona específica.
* Implementación de autenticación en dos pasos: Añade una capa extra de seguridad para roles críticos como administradores y supervisores, reduciendo el riesgo de accesos no autorizados.

1. **Control de acceso y gestión de roles**

* Definir permisos basados en el puesto del usuario: Permite que cada usuario solo acceda a la información y funciones necesarias para su trabajo.
* Aplicar el principio de mínimo privilegio: Limita los permisos al mínimo indispensable para evitar que un error o un ataque comprometa funciones críticas.
* Revisar periódicamente los accesos: Garantiza que antiguos empleados o cambios de puesto no tengan permisos que ya no requieren.

1. **Cifrado de datos**

* Uso de algoritmos seguros: Protege contraseñas y datos sensibles frente a accesos no autorizados o robo de información.
* Cifrado en tránsito mediante HTTPS y SSL/TLS: Asegura que la información transmitida entre el usuario y el servidor no pueda ser interceptada ni modificada.

1. **Respaldo de información**

* Copias de seguridad automáticas: Permite recuperar la información en caso de errores humanos, fallos técnicos o ataques cibernéticos.
* Políticas de restauración de datos: Define cómo recuperar datos de manera eficiente para minimizar interrupciones del negocio.

1. **Integridad y trazabilidad de la información**

* Registro de auditoría de todas las operaciones: Permite detectar errores o irregularidades en ventas, devoluciones y ajustes de inventario.
* Identificación de usuario, fecha, hora y dispositivo: Facilita el seguimiento preciso de cada acción realizada en el sistema.

1. **Monitoreo y registro de actividad**

* Detección de comportamientos inusuales: Ayuda a prevenir fraudes internos o errores que puedan afectar el inventario o las ventas.
* Alertas en tiempo real: Permite reaccionar rápidamente ante situaciones sospechosas o intentos de acceso indebido.

1. **Protección contra amenazas externas**

* Implementación de antivirus y firewalls: Bloquea software malicioso y accesos no autorizados desde Internet.
* Segmentación y cifrado de la red local: Protege la comunicación interna de la empresa y evita accesos indebidos a datos sensibles.

1. **Disponibilidad y continuidad del servicio**

* Plan de contingencia para caídas del servidor o fallos de red: Garantiza que las operaciones puedan continuar incluso ante incidentes técnicos.
* Alta disponibilidad en procesos de venta: Evita interrupciones que puedan afectar la experiencia del cliente y la operación del negocio.

1. **Concientización del personal**

* Capacitación en buenas prácticas de seguridad digital: Incrementa la protección mediante el conocimiento y prevención de riesgos por parte de los empleados.
* Uso responsable de contraseñas y detección de phishing: Reduce la probabilidad de que ataques de ingeniería social comprometan el sistema.

Diagrama

Descripción generada automáticamente

**Conclusión**

La implementación de estos requisitos de seguridad es esencial para asegurar el correcto funcionamiento del sistema de gestión de inventarios y punto de venta. Un sistema protegido garantiza que la información sobre productos, stock y ventas esté segura frente a accesos no autorizados o errores internos, además de respaldar la continuidad operativa del negocio. La seguridad debe considerarse un proceso continuo, donde tanto las medidas tecnológicas como la capacitación del personal juegan un papel clave. La combinación de controles técnicos, organizativos y formativos permite que el sistema funcione de manera confiable, eficiente y resistente frente a riesgos internos y externos.