MINIMARKETPOS

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Código: MMP-SEG-001 | Versión: 3.2 | Fecha: 1 de noviembre de 2026

1. Objetivo

Establecer recomendaciones y responsabilidades para reducir riesgos de acceso no autorizado, pérdida, alteración o divulgación de la información utilizada en MiniMarketPOS.

2. Principio de almacenamiento local

La operación habitual de MiniMarketPOS está diseñada para ejecutarse localmente y sin conexión después de la activación. Esto reduce la dependencia de servicios en línea, pero no elimina riesgos asociados al computador, malware, accesos físicos, usuarios compartidos o daños del disco. Los servicios web de compra, activación, licenciamiento, promociones y soporte pueden requerir conexión.

3. Responsabilidades del comercio

- Mantener Windows y el software de seguridad actualizados.
- Usar contraseñas únicas y no compartir cuentas.
- Asignar permisos mínimos según las funciones de cada empleado.
- Bloquear la sesión o el equipo cuando no esté atendido.
- Restringir el acceso físico al computador y a los respaldos.
- No instalar versiones obtenidas de sitios no oficiales.
- No enviar bases de datos completas por canales inseguros.

4. Usuarios y contraseñas

El administrador debe crear y retirar usuarios cuando cambie el personal. Las credenciales no deben anotarse a la vista ni compartirse. Si se sospecha que una contraseña fue expuesta, debe cambiarse de inmediato. Las funciones administrativas deben limitarse a perfiles autorizados.

5. Protección del equipo

Se recomienda usar un sistema operativo con soporte vigente, protección antimalware, actualizaciones de seguridad, bloqueo de pantalla y una cuenta de Windows sin privilegios administrativos para el trabajo diario cuando sea viable.

6. Integridad de la base de datos

No edite, renombre ni reemplace manualmente archivos de datos mientras MiniMarketPOS esté abierto. Antes de actualizar, reinstalar o mover el programa, cree y verifique una copia de seguridad. Utilice únicamente paquetes oficiales.

7. Información de compra, licencia y promociones

Los datos de compra, referencias de pago, licencias, cupones, redenciones y huellas criptográficas de identificación deben protegerse mediante controles de acceso, secretos de servidor y permisos mínimos. No se deben incluir claves privadas, secretos de firma, claves de servicio ni credenciales administrativas en el HTML público o en el ejecutable distribuido. Los datos de identificación deben limitarse a la finalidad informada y no exponerse en registros o mensajes de error.

8. Envío de información a soporte

Comparta solo la información necesaria para resolver el caso. Oculte nombres, teléfonos, identificaciones, datos de clientes y valores sensibles cuando no sean necesarios. El usuario debe confirmar que está autorizado para compartir cualquier dato de terceros.

9. Incidentes

Ante pérdida del equipo, sospecha de malware, acceso no autorizado, corrupción de datos o envío accidental de información, el comercio debe desconectar el equipo de redes si es necesario para contener el incidente, preservar respaldos y evidencias, cambiar credenciales desde un dispositivo seguro y contactar soporte. Si hay datos personales comprometidos, el responsable del tratamiento deberá evaluar sus obligaciones legales de reporte y atención.

10. Alcance, límites y revisión

Esta política ofrece medidas recomendadas y no constituye una garantía de seguridad absoluta. La seguridad depende también del hardware, sistema operativo, configuración, conducta de usuarios y proveedores externos. No debe interpretarse como exoneración de obligaciones legales del desarrollador o del comercio. El responsable debe revisarla cuando cambien la arquitectura, las funciones de activación, los canales de soporte o los proveedores tecnológicos.

Datos del responsable

Titular y responsable del producto: MARIA CAMILA CAICEDO MINA. Identificación/NIT: 1111816206-7. Dirección para notificaciones: Av. 17 #7W-51, Piedecuesta, Santander, Colombia. Correo: soporte@minimarketpos.digital. Sitio web: https://minimarketpos.digital.