POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Para la Prestación de los Servicios que el Usuario contrate, el Prestador del Servicio observará en todo momento las políticas que a continuación se detallan:

1. Origen

- Integramos con Interfaces de Programación de Aplicaciones oficiales de centros comerciales electrónicos para sincronizar pedidos.
- Utilizamos conexiones seguras con autenticación estándar de la industria e identificadores digitales encriptados con expiración limitada.
- Validamos todas las solicitudes mediante firewalls de aplicación web y listas de direcciones IP autorizadas.
- Implementamos controles de entrada que verifican la integridad de datos antes del procesamiento.

2. Procesamiento

- Procesamos datos exclusivamente para gestión de pedidos y logística siguiendo metodologías ágiles con revisiones de código obligatorias.
- Generamos reportes operativos para optimizar procesos, registrando solo información técnica sin datos personales en registros del sistema.
- No realizamos perfilamiento ni análisis de comportamiento sin autorización explícita.
- Aplicamos análisis de código automatizado para detectar vulnerabilidades antes de cada actualización.
- Mantenemos entornos de prueba con datos sintéticos, prohibiendo el uso de datos reales en desarrollo.

3. Resguardo

- Base de datos en la nube con cifrado AES-256 en reposo y rotación automática de claves cada 90 días.
- Infraestructura en la nube con segmentación de red en tres capas: Web, Aplicación y Base de Datos.
- Respaldos automatizados con el mismo nivel de encriptación.
- Política de retención de 31 a 90 días después del envío del pedido.
- Control de acceso a base de datos mediante roles diferenciados y conexiones seguras.

4. Protección

- TLS 1.2 y 1.3 para todas las comunicaciones.
- Conexión segura obligatoria para accesos remotos con autenticación mediante llaves criptográficas.
- Autenticación multifactor (MFA) obligatoria para todos los usuarios con accesos críticos.
- Firewalls perimetrales y protección contra las 10 principales vulnerabilidades web.
- Escaneos de vulnerabilidades automatizados cada 180 días y pruebas de penetración anuales con soporte externo.
- Sistema de detección de intrusos implementado con alertas en tiempo real.
- Herramientas de auditoría para registro completo de actividades.

5. Puesta a Disposición

- Interfaces de programación seguras con paqueterías para coordinar envíos usando HTTPS exclusivamente.
- Integración controlada con pasarelas de pago (sin almacenar datos sensibles de tarjetas).
- Control de acceso basado en gestión de identidades y accesos con matriz de roles diferenciados y principio de privilegio mínimo.
- Bitácoras completas de todos los accesos a información con retención de registros de seguridad por 365 días.
- Revisión trimestral de permisos con documentación de justificación para cada acceso otorgado.
- Proceso formal de aprobación por personal autorizado para cambios en producción.

6. Eliminación

- Procesos automatizados mediante rutinas programadas eliminan datos de clientes después de 60 días.
- Depuración de registros operativos cada 90 días, registros de aplicación cada 90 días, y registros de base de datos cada 180 días.
- Eliminación segura mediante sobrescritura múltiple siguiendo estándares internacionales para borrado seguro.
- Mecanismo de eliminación manual para solicitudes específicas con verificación y certificación del proceso.
- Destrucción física de dispositivos con documentación y certificación cuando corresponde.
- Proceso monitoreado con verificación automática del conteo de registros eliminados.

El Prestador del Servicio tiene la facultad de actualizar en cualquier momento, este documento y publicarlo en su sitio web para efectos de conocimiento del Usuario.