

ETERNA DIGITALCOM MÉXICO, S.A. DE C.V.

POLÍTICA DE SEGURIDAD EN PAGOS

Controles y responsabilidades para el procesamiento seguro de pagos electrónicos

Código documental	EDM-CMP-004
Versión	1.0
Fecha de emisión	Julio de 2026
Última revisión	Julio de 2026
Próxima revisión	Julio de 2027
Clasificación	Documento corporativo de consulta pública

Este documento establece lineamientos generales aplicables a los servicios digitales de Eterna Digitalcom México. No constituye certificación técnica ni sustituye obligaciones contractuales o legales específicas de proveedores externos.

Índice

1. Objeto
2. Alcance
3. Modelo de procesamiento
4. Marco de referencia
5. Datos de pago
6. Métodos de pago
7. Autenticación y validación
8. Entrega digital
9. Conciliación y registros
10. Contracargos y reembolsos
11. Prevención de fraude
12. Proveedores de pago
13. Responsabilidades del usuario
14. Incidentes de pago
15. Limitaciones, contacto y vigencia

1. Objeto

Describir las medidas generales aplicables a la recepción, procesamiento, confirmación, conciliación y gestión de pagos realizados para adquirir servicios digitales, membresías, publicidad, automatizaciones, herramientas de plataforma y otros productos ofrecidos por Eterna.

2. Alcance

Aplica a pagos con tarjeta, transferencias, SPEI, referencias de efectivo como OXXO Pay y otros métodos habilitados por proveedores autorizados. La disponibilidad depende del país, moneda, riesgo, servicio y procesador.

3. Modelo de procesamiento

Eterna utiliza proveedores especializados para capturar y procesar pagos. La información sensible de tarjeta se introduce normalmente en interfaces o componentes del proveedor. Eterna procura no almacenar números completos de tarjeta, códigos de seguridad ni datos de autenticación sensibles.

4. Marco de referencia

Los proveedores de tarjetas pueden operar bajo estándares de la industria como PCI DSS. PCI DSS establece una base de requisitos técnicos y operativos para proteger datos de cuentas de pago. La referencia a PCI DSS no significa que Eterna afirme una certificación propia; la obligación y alcance dependen de la arquitectura y de los proveedores utilizados.

También resultan aplicables, según el caso, la legislación mexicana de protección de datos, comercio electrónico, protección al consumidor, contratos, comprobantes y prevención de fraude.

5. Datos de pago

Eterna puede recibir del procesador datos limitados como marca, últimos dígitos, estado, fecha, monto, identificador, resultado de validación y motivo de rechazo. Estos datos se utilizan para conciliación, soporte, prevención de fraude y defensa de disputas.

6. Métodos de pago

6.1 Tarjetas

La autorización depende del emisor y procesador. Pueden aplicarse autenticación reforzada, 3-D Secure u otros mecanismos cuando estén disponibles.

6.2 SPEI y transferencias

La confirmación depende de la recepción e identificación de fondos. El usuario deberá usar la referencia y monto correctos.

6.3 OXXO Pay y efectivo referenciado

La orden permanecerá pendiente hasta que el proveedor confirme el pago. La acreditación puede no ser inmediata y está sujeta a horarios, vigencia y reglas del comercio receptor.

6.4 Otros métodos

Podrán habilitarse wallets o medios alternativos conforme a disponibilidad y condiciones del proveedor.

7. Autenticación y validación

- Validación del estado de la transacción.
- Controles del procesador, emisor o banco.
- Autenticación adicional cuando aplique.
- Revisión de señales de riesgo.
- Verificación de coincidencia entre orden y pago.
- Posible solicitud de información adicional en operaciones de mayor riesgo.

8. Entrega digital

La entrega se realiza después de que el pago aparezca confirmado o liquidado conforme al método. Una autorización pendiente no equivale necesariamente a pago definitivo. En caso de reversión, fraude o error, Eterna podrá suspender accesos o servicios conforme a los términos aplicables.

9. Conciliación y registros

Eterna conservará registros razonables de órdenes, confirmaciones, identificadores, estados, facturación y entrega. La conciliación puede incluir comparación entre plataforma, procesador y banco. Las diferencias se investigarán y documentarán.

10. Contracargos y reembolsos

Los reembolsos se procesarán conforme a la Política de Reembolsos y a las reglas del proveedor. Los tiempos de reflejo dependen del banco y método. Los contracargos serán atendidos mediante evidencia disponible, respetando derechos del consumidor y procedimientos del procesador.

11. Prevención de fraude

Podrán aplicarse límites, validaciones, retenciones temporales o revisiones de acuerdo con la Política de Prevención de Fraude. Eterna no revelará configuraciones cuya divulgación pueda facilitar evasión de controles.

12. Proveedores de pago

Cada proveedor conserva control sobre su infraestructura, autorizaciones, disponibilidad, reglas y cumplimiento. Eterna seleccionará proveedores razonablemente adecuados, pero no garantiza la operación ininterrumpida de redes bancarias, tiendas de conveniencia o terceros.

13. Responsabilidades del usuario

- Utilizar medios de pago propios o autorizados.
- Proporcionar datos correctos.
- Conservar comprobantes y referencias.
- No compartir códigos de autenticación.
- Revisar el monto antes de confirmar.
- Reportar cargos no reconocidos sin demora.

14. Incidentes de pago

Si se detecta un posible incidente, Eterna coordinará con el proveedor para contenerlo y determinar su alcance. Los usuarios deberán seguir instrucciones oficiales y evitar compartir datos sensibles por canales no autorizados. Cuando exista afectación legalmente relevante, se realizarán comunicaciones conforme a la normativa aplicable.

15. Limitaciones, contacto y vigencia

Esta política no constituye certificación PCI propia ni garantía de que un pago será autorizado. Facturación: facturacion@eternadigitalcom.mx. Soporte: soporte@eternadigitalcom.mx. Seguridad: seguridad@eternadigitalcom.mx. Vigente desde julio de 2026.

Control de cambios

Versión	Fecha	Descripción	Responsable
1.0	Julio 2026	Emisión inicial	Dirección General