

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

POLÍTICA DE PREVENCIÓN DE FRAUDE

Lineamientos para identificar, prevenir y gestionar operaciones abusivas o sospechosas

Código documental	EDM-CMP-003
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. Principios
4. Definiciones
5. Conductas de riesgo
6. Controles preventivos
7. Monitoreo y alertas
8. Revisión de operaciones
9. Contracargos y disputas
10. Cuentas y promociones
11. Investigación y evidencia
12. Medidas y consecuencias
13. Cooperación con terceros
14. Protección de datos
15. Canales de reporte y vigencia

1. Objeto

Establecer criterios generales para prevenir, detectar, revisar y responder a conductas fraudulentas, abusivas o engañosas relacionadas con cuentas, pagos, servicios digitales, suscripciones, publicidad, herramientas de plataforma y Fortucoins.

2. Alcance

Aplica a usuarios, clientes, proveedores, empleados, colaboradores, integraciones y operaciones efectuadas en sitios o plataformas de Eterna.

3. Principios

- Enfoque basado en riesgo.
- Proporcionalidad de medidas.
- Buena fe y trazabilidad.
- Protección del usuario legítimo.
- Conservación razonable de evidencia.
- Cooperación legal con procesadores y autoridades.

4. Definiciones

- Fraude: conducta intencional destinada a obtener beneficio indebido o causar perjuicio mediante engaño, manipulación o uso no autorizado.
- Contracargo: reversión iniciada por un emisor o medio de pago.
- Cuenta comprometida: cuenta utilizada por persona no autorizada.
- Abuso de promociones: uso artificioso o múltiple contrario a las condiciones publicadas.
- Ingeniería social: manipulación para obtener credenciales, pagos o información.
- Señal de riesgo: dato o patrón que justifica revisión adicional, sin implicar por sí mismo culpabilidad.

5. Conductas de riesgo

- Uso de identidad, tarjeta o cuenta ajena sin autorización.
- Información falsa, alterada o inconsistente.
- Múltiples cuentas para eludir límites.
- Contracargos abusivos o reiterados.
- Phishing, suplantación o ingeniería social.
- Bots, automatización no autorizada, scraping o manipulación técnica.
- Abuso de códigos, bonos, membresías o promociones.
- Intentos de convertir Fortucoins en efectivo o transferirlos fuera de las reglas.
- Uso del servicio para actividades ilícitas, engañosas o prohibidas.

6. Controles preventivos

- Validación de correo, cuenta y datos de operación.

- Controles de velocidad, frecuencia o límites cuando estén disponibles.
- Revisión de coincidencias e inconsistencias.
- Uso de herramientas antifraude del procesador.
- Autenticación adicional o comprobación documental en casos de mayor riesgo.
- Restricción de funciones hasta confirmar una operación.

7. Monitoreo y alertas

Eterna puede analizar patrones técnicos y operativos, tales como frecuencia, montos, dispositivo, IP, historial, disputas, intentos fallidos y comportamiento de cuenta. Las alertas se utilizan como apoyo y pueden requerir revisión humana.

8. Revisión de operaciones

Cuando existan señales razonables, Eterna podrá solicitar información adicional, suspender temporalmente la entrega, limitar funciones o cancelar una operación. La revisión buscará confirmar identidad, autorización y congruencia de la compra, sin obligación de revelar reglas internas que faciliten su evasión.

9. Contracargos y disputas

El usuario deberá contactar primero a soporte para intentar resolver cargos no reconocidos, errores de entrega o duplicidades. Eterna podrá aportar al procesador comprobantes de autorización, entrega electrónica, acceso, comunicaciones, términos aceptados y otros registros pertinentes. Los contracargos fraudulentos pueden dar lugar a suspensión o terminación.

10. Cuentas y promociones

Las promociones podrán sujetarse a límites por persona, cuenta, dispositivo, medio de pago o periodo. Eterna podrá retirar beneficios obtenidos mediante abuso, duplicidad, error manifiesto o incumplimiento, sin afectar derechos irrenunciables del consumidor.

11. Investigación y evidencia

- Registro cronológico del caso.
- Conservación de órdenes, comunicaciones y registros técnicos.
- Revisión de historial y patrones.
- Documentación de decisiones y medidas.
- Acceso restringido a la evidencia.
- Conservación durante el plazo legal u operativo aplicable.

12. Medidas y consecuencias

- Solicitud de verificación adicional.
- Retención temporal de entrega.
- Cancelación o reembolso cuando proceda.

- Revocación de beneficios obtenidos indebidamente.
- Limitación o suspensión de cuenta.
- Terminación de la relación.
- Reporte a procesadores o autoridades cuando exista fundamento.

13. Cooperación con terceros

Eterna podrá intercambiar información necesaria con procesadores, instituciones financieras, proveedores antifraude, asesores y autoridades, de acuerdo con la legislación, contratos y avisos de privacidad aplicables.

14. Protección de datos

Los datos de prevención de fraude se tratarán conforme a la Política de Protección de Datos Personales, limitando su uso a seguridad, investigación, defensa de derechos, cumplimiento contractual y obligaciones legales.

15. Canales de reporte y vigencia

Reportes: reportes@eternadigitalcom.mx. Soporte: soporte@eternadigitalcom.mx. Seguridad: seguridad@eternadigitalcom.mx. Esta política entra en vigor en julio de 2026 y podrá actualizarse conforme evolucionen riesgos, servicios o normas.

Control de cambios

Versión	Fecha	Descripción	Responsable
1.0	Julio 2026	Emisión inicial	Dirección General