Cemefi Hace bien. ESR Empresa Socialmente Responsable® Cemefi

Ficha de indicadores

Criterio: *Social- Comercio electrónico*

Indicador: *Plataforma segura de transacciones electrónicas*

Índice.

1. Introducción

El indicador de Plataforma segura de transacciones electrónicas evalúa la seguridad, privacidad y confiabilidad de los canales digitales de la empresa para transacciones comerciales. Con la aceleración del e-commerce y los pagos digitales en México post-pandemia, la ciberseguridad se ha convertido en un requisito estratégico y regulatorio.

El Código de Comercio (comercio electrónico), la LGPDPPP (protección de datos en transacciones), la Ley Fintech (cuando aplique) y las regulaciones del sistema financiero configuran el marco legal. A nivel internacional, PCI DSS es el estándar de seguridad en pagos con tarjeta, e ISO 27001 el marco de referencia para seguridad de la información.

2. Indicadores relacionados del Distintivo ESR®.

Indicadores	Ámbito	Descripción
Protección de datos personales	Consumidores	La seguridad de las transacciones requiere la protección integral de datos personales y financieros del consumidor.
Información transparente al consumidor	Consumidores	La transparencia sobre políticas de seguridad y devoluciones genera confianza en las transacciones digitales.
Atención y servicio al cliente	Consumidores	Un servicio al cliente eficiente es clave para resolver incidentes de seguridad en transacciones electrónicas.
Gestión de riesgos	Gobernanza	Los fraudes electrónicos y las vulneraciones de datos financieros son riesgos críticos que requieren gestión sistemática.
Ética e integridad	Gobernanza	La seguridad en transacciones electrónicas refleja el compromiso ético de la empresa con sus consumidores.

3. Industrias más relevantes

Industria	Relevancia específica
E-commerce y retail digital	Pagos en línea, datos de tarjeta, cuentas de usuario, historial de compras
Banca y fintech	Banca digital, transferencias, pagos, datos financieros sensibles
Telecomunicaciones	Recargas, pagos de servicios, datos de facturación en plataformas digitales
Seguros	Contratación en línea, pagos de primas, datos sensibles de salud
Turismo y aerolíneas	Reservas, pagos internacionales, datos de pasajeros
Delivery y plataformas	Pagos recurrentes, datos de ubicación, tarjetas guardadas

4. Normas, leyes, estándares y certificaciones aplicables

Marco	Tipo	Aplicación
Código de Comercio (e-commerce)	Obligatorio	Marco legal de comercio electrónico en México
LGPDPPP	Obligatorio	Protección de datos personales en transacciones
Ley Fintech	Obligatorio	Regulación de instituciones de tecnología financiera
NOM-151-SCFI-2002	Obligatorio	Conservación de mensajes de datos y firma electrónica
PCI DSS v4.0	Voluntario	Estándar de seguridad de datos de la industria de tarjetas de pago
ISO/IEC 27001:2022	Voluntario	Sistema de gestión de seguridad de la información
GRI 418	Referencia	Privacidad del cliente en transacciones
ODS 9	Referencia	Infraestructura resiliente e innovación
ODS 16	Referencia	Instituciones sólidas y seguridad
NIST Cybersecurity Framework	Referencia	Marco de ciberseguridad del gobierno de EE.UU.

5. Factores que influyen en la implementación

5.1 Factores internos

- Madurez de la infraestructura tecnológica y de ciberseguridad
- Equipo de seguridad informática con competencias actualizadas
- Presupuesto de ciberseguridad como inversión, no como gasto
- Cultura de seguridad digital en toda la organización
- Integración de seguridad desde el diseño de plataformas (security by design)

5.2 Factores externos

- Ciberataques cada vez más sofisticados (ransomware, phishing, fraude)
- Regulación creciente de seguridad de pagos y datos
- Expectativas del consumidor sobre seguridad en e-commerce
- Procesadores de pago que exigen cumplimiento PCI DSS
- Competencia por la confianza digital del consumidor

6. Creación de un programa de RSE para este indicador

6.1 Elementos esenciales

- Política de seguridad de la información con alcance a plataformas transaccionales
- Evaluación de vulnerabilidades y pruebas de penetración periódicas
- Cumplimiento PCI DSS para procesamiento de pagos con tarjeta
- Plan de respuesta a incidentes de ciberseguridad probado
- Monitoreo continuo de amenazas y anomalías transaccionales
- Cifrado de datos en tránsito (TLS) y en reposo

6.2 Pasos de implementación

- Evaluar la seguridad actual de todas las plataformas transaccionales
- Implementar controles de seguridad conforme a PCI DSS e ISO 27001
- Realizar pruebas de penetración y corregir vulnerabilidades
- Establecer monitoreo continuo de transacciones y alertas de fraude
- Capacitar al personal en ciberseguridad y respuesta a incidentes
- Realizar simulacros de incidentes de ciberseguridad al menos anualmente

7. Beneficios empresariales

7.1 Beneficios tangibles

- Prevención de pérdidas financieras por fraude electrónico
- Cumplimiento de requisitos de procesadores de pago (PCI DSS)
- Prevención de sanciones regulatorias por vulneraciones de datos financieros
- Reducción de contracargos y disputas de transacciones

7.2 Beneficios intangibles

- Confianza del consumidor en la seguridad de la plataforma
- Ciberseguridad como ventaja competitiva en e-commerce
- Capacidad de respuesta ante incidentes que minimiza el daño
- Posicionamiento como plataforma segura ante inversionistas y socios

8. Riesgos empresariales de no implementar

8.1 Riesgos financieros y legales

- Pérdidas financieras directas por fraude electrónico
- Sanciones regulatorias por vulneraciones de datos financieros
- Responsabilidad civil por daños a consumidores afectados
- Pérdida de capacidad de procesar pagos por incumplimiento PCI DSS

8.2 Riesgos operativos y reputacionales

- Vulneraciones de datos financieros con impacto masivo en consumidores
- Interrupción del negocio por ciberataques (ransomware)
- Pérdida de confianza del consumidor en la plataforma
- Crisis reputacional amplificada por medios de comunicación

9. Herramientas y recursos

Herramienta	Descripción
PCI DSS v4.0	Estándar de seguridad de datos para la industria de pagos
ISO/IEC 27001:2022	Sistema de gestión de seguridad de la información
NIST Cybersecurity Framework	Marco de referencia para gestión de ciberseguridad
OWASP Top 10	Lista de las 10 principales vulnerabilidades de aplicaciones web
Pruebas de penetración	Evaluación proactiva de vulnerabilidades en plataformas
SIEM / SOC	Herramientas de monitoreo y respuesta a incidentes de seguridad

10. Mejores prácticas y casos de referencia

- Implementar autenticación multifactor (MFA) para todas las transacciones de alto valor
- Realizar pruebas de penetración al menos dos veces al año por terceros acreditados
- Implementar monitoreo en tiempo real de transacciones con alertas de anomalías
- Mantener un programa de bug bounty para detección proactiva de vulnerabilidades
- Cifrar todos los datos sensibles en tránsito y en reposo sin excepciones
- Publicar indicadores de ciberseguridad (sin revelar vulnerabilidades) en el reporte de sostenibilidad

11. Métricas e indicadores de desempeño

11.1 Métricas de prevención

Nombre de la métrica	Descripción	Fórmula	Periodicidad sugerida	Obligatoriedad normativa o marco de referencia
Evaluaciones de vulnerabilidades realizadas	Número de evaluaciones de seguridad de plataformas por año	Conteo de evaluaciones documentadas	Semestral	ISO 27001; PCI DSS
Cobertura de cifrado en transacciones	% de transacciones con cifrado end-to-end	(Transacciones cifradas / Total transacciones) × 100	Trimestral	PCI DSS (obligatorio para tarjetas); ISO 27001
Pruebas de penetración realizadas	Número de pruebas de penetración ejecutadas por año	Conteo de pentests documentados	Semestral	PCI DSS; ISO 27001
Capacitación en ciberseguridad	% de personal técnico capacitado en seguridad de plataformas	(Capacitados / Total personal técnico) × 100	Anual	ISO 27001; ODS 9

11.2 Métricas de corrección, control o mitigación

Nombre de la métrica	Descripción	Fórmula	Periodicidad sugerida	Obligatoriedad normativa o marco de referencia
Incidentes de seguridad en plataformas	Número de incidentes de seguridad en plataformas de transacción	Conteo de incidentes	Trimestral	LGPDPPP; PCI DSS; GRI 418
Tiempo de detección de incidentes	Horas promedio para detectar un incidente de seguridad	Suma horas detección / Número de incidentes	Por incidente	ISO 27001; PCI DSS
Tiempo de respuesta a incidentes	Horas promedio para contener un incidente de seguridad	Suma horas contención / Número de incidentes	Por incidente	ISO 27001; PCI DSS
Hallazgos críticos en pentests	Número de hallazgos críticos no resueltos de pruebas de penetración	Conteo de hallazgos críticos abiertos	Semestral	PCI DSS; ISO 27001

11.3 Métricas de transformación, resarcimiento o generación de bienestar

Nombre de la métrica	Descripción	Fórmula	Periodicidad sugerida	Obligatoriedad normativa o marco de referencia
Historial sin incidentes	Meses consecutivos sin incidentes de seguridad en plataformas	Conteo de meses sin incidente	Continuo	ISO 27001; PCI DSS
Certificaciones de seguridad vigentes	Número de certificaciones de ciberseguridad vigentes	Conteo (PCI DSS, ISO 27001, SOC2)	Anual	PCI DSS; ISO 27001
Confianza del consumidor en seguridad digital	% de consumidores que confían en la seguridad de las transacciones	(Respuestas positivas / Total encuestados) × 100	Anual	GRI 418; ODS 16
Inversión en ciberseguridad	% del presupuesto de TI destinado a seguridad de plataformas	(Presupuesto seguridad / Presupuesto TI) × 100	Anual	ISO 27001; ODS 9

12. Conclusión

La seguridad de las plataformas de transacciones electrónicas es un indicador de relevancia creciente en un entorno donde el e-commerce y los pagos digitales se expanden aceleradamente. Los ciberataques y las vulneraciones de datos financieros tienen impacto directo en la confianza del consumidor, la continuidad del negocio y la responsabilidad legal de la empresa.

El Distintivo ESR estructura el avance desde la evaluación de seguridad hasta la ciberseguridad como ventaja competitiva certificada.