Cemefi Hace bien. ESR Empresa Socialmente Responsable® Cemefi

Ficha de indicadores

Criterio: *Social- Protección y privacidad de los datos de consumidores*

Indicador: *Atención de clientes y consumidores*

Índice.

1. Introducción

La protección de datos personales constituye un pilar fundamental de la relación ética entre empresas y consumidores en la era digital. Con la creciente digitalización de procesos comerciales, las organizaciones recopilan, almacenan y procesan volúmenes crecientes de información personal de clientes, empleados y terceros.

En México, la Ley General de Protección de Datos Personales en Posesión de los Particulares (LGPDPPP) establece obligaciones claras para el tratamiento lícito de datos. El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) supervisa el cumplimiento y puede imponer sanciones millonarias ante vulneraciones.

El Distintivo ESR® evalúa la capacidad de la empresa para garantizar la protección, tratamiento lícito y seguridad de los datos personales, promoviendo una gobernanza de datos que genere confianza, cumpla con la regulación y se convierta en un activo estratégico para la competitividad empresarial.

Este indicador mide el grado en que la empresa implementa políticas, sistemas y controles para garantizar la protección, tratamiento lícito y seguridad de los datos personales de clientes, empleados y terceros, conforme a la legislación aplicable y las mejores prácticas internacionales de privacidad.

2. Indicadores relacionados del Distintivo ESR®

Indicadores	Ámbito	Descripción
Plataforma segura de transacciones electrónicas	Consumidores	La seguridad de las transacciones electrónicas requiere protección integral de datos financieros y personales del consumidor.
Información transparente al consumidor	Consumidores	La transparencia informativa incluye avisos de privacidad claros y consentimiento informado para el uso de datos.
Ética e integridad	Gobernanza	La protección de datos es una expresión concreta de los principios éticos en la relación con los grupos de interés.
Gestión de riesgos	Gobernanza	Las vulneraciones de datos representan riesgos operativos, legales y reputacionales que requieren gestión sistemática.
Derechos humanos en la cadena de valor	DDHH	El derecho a la privacidad es un derecho humano fundamental reconocido internacionalmente.

3. Industrias más relevantes

Industria	Relevancia específica
Banca y servicios financieros	Datos financieros sensibles; regulación CNBV; riesgo de fraude
Telecomunicaciones	Volumen masivo de datos; geolocalización; metadatos de comunicación
E-commerce y retail	Datos de compra, perfiles, historial; pagos electrónicos
Salud y farmacéutico	Datos de salud (sensibles); expedientes clínicos; regulación especial
Tecnología y plataformas	Big data, inteligencia artificial, perfilamiento, decisiones automatizadas
Educación	Datos de menores; historial académico; datos familiares
Seguros	Datos de salud y financieros; evaluación de riesgos con datos personales

4. Normas, leyes, estándares, certificaciones, ODS e ISO

Categoría	Nombre	Descripción	Relevancia para el indicador
Ley mexicana	LGPDPPP y su Reglamento	Ley General de Protección de Datos Personales en Posesión de los Particulares	Marco obligatorio que define principios, derechos ARCO y obligaciones para el tratamiento de datos personales.
Ley mexicana	Ley General de Protección de Datos en Posesión de Sujetos Obligados	Regulación para el sector público	Referencia normativa complementaria para empresas que interactúan con entidades gubernamentales.
NOM	NOM-151-SCFI-2002	Prácticas comerciales para conservación de mensajes de datos	Regula la conservación segura de mensajes de datos y registros electrónicos.
Organismo regulador	INAI	Instituto Nacional de Transparencia y Protección de Datos	Autoridad garante que supervisa el cumplimiento y puede imponer sanciones millonarias.
ISO	ISO/IEC 27001	Sistema de gestión de seguridad de la información	Estándar internacional para proteger la confidencialidad, integridad y disponibilidad de la información.
ISO	ISO/IEC 27701	Sistema de gestión de privacidad de la información	Extensión de ISO 27001 específica para la gestión de datos personales y privacidad.
Referencia internacional	RGPD (Unión Europea)	Reglamento General de Protección de Datos	Referencia internacional de mejores prácticas en protección de datos; relevante para empresas con operaciones globales.
Marco internacional	Marco de Privacidad APEC	Marco de cooperación en privacidad Asia-Pacífico	Referencia para empresas con operaciones en mercados Asia-Pacífico.
ODS	ODS 16	Paz, justicia e instituciones sólidas	Promueve instituciones responsables y transparentes que protejan los derechos fundamentales.

Categoría	Nombre	Descripción	Relevancia para el indicador
Estándar RSE	GRI 418	Privacidad del cliente	Estándar de reporte sobre reclamaciones por violación de privacidad y pérdida de datos de clientes.

5. Factores que influyen en la implementación

- Volumen y sensibilidad de los datos personales recopilados por la organización.
- Nivel de digitalización de procesos comerciales y canales de interacción con clientes.
- Infraestructura tecnológica de seguridad de la información disponible.
- Cultura organizacional respecto a la privacidad y el manejo responsable de información.
- Complejidad regulatoria por operaciones en múltiples jurisdicciones con legislaciones distintas.
- Capacitación del personal en materia de protección de datos y ciberseguridad.
- Presupuesto asignado a sistemas de gestión de seguridad de la información.

6. Cómo crear un programa de protección de datos personales

- Realizar un inventario completo de bases de datos personales y flujos de información.
- Designar un oficial de protección de datos o responsable de privacidad.
- Elaborar y publicar avisos de privacidad conformes a la LGPDPPP.
- Implementar un sistema de gestión de seguridad de la información basado en ISO 27001/27701.
- Establecer mecanismos para el ejercicio de derechos ARCO (Acceso, Rectificación, Cancelación, Oposición).
- Realizar evaluaciones de impacto en privacidad (PIA) para nuevos procesos o tecnologías.
- Desarrollar un plan de respuesta a incidentes de vulneración de datos.
- Capacitar periódicamente al personal en manejo seguro de información y privacidad.

7. Beneficios empresariales

- Cumplimiento legal que evita sanciones millonarias del INAI.
- Fortalecimiento de la confianza del consumidor y fidelización de clientes.
- Competitividad en mercados internacionales con regulación estricta de datos.
- Reducción de riesgos operativos por vulneraciones de información.
- Protección de la reputación corporativa ante incidentes de ciberseguridad.
- Diferenciación como empresa responsable en el manejo de información personal.
- Facilitación de alianzas comerciales y acceso a cadenas de valor globales.

8. Riesgos de no implementar

- Sanciones económicas del INAI que pueden alcanzar millones de pesos.
- Vulneraciones masivas de datos con impacto directo en consumidores afectados.
- Pérdida irreversible de confianza y deserción de clientes.
- Litigios individuales y acciones colectivas por manejo indebido de información.
- Incumplimiento de requisitos internacionales para transferencia transfronteriza de datos.
- Daño reputacional amplificado por cobertura mediática de incidentes de privacidad.
- Exclusión de mercados y plataformas que exigen estándares de privacidad certificados.

9. Herramientas y recursos

- Plataformas de gestión de consentimiento y avisos de privacidad digitales.
- Herramientas de cifrado y anonimización de datos personales.
- Sistemas de detección y respuesta a incidentes de ciberseguridad (SIEM).
- Guías y lineamientos del INAI para el cumplimiento de la LGPDPPP.
- Marcos de certificación ISO 27001/27701 para sistemas de gestión de seguridad y privacidad.
- Herramientas de evaluación de impacto en privacidad (PIA).
- Programas de formación en ciberseguridad y protección de datos para empleados.

10. Mejores prácticas

- Adoptar el principio de privacidad por diseño en el desarrollo de productos y servicios.
- Implementar controles de acceso basados en roles para limitar la exposición de datos.
- Realizar auditorías periódicas de cumplimiento en protección de datos.
- Mantener un registro actualizado de actividades de tratamiento de datos.
- Establecer acuerdos de confidencialidad con proveedores que procesan datos personales.
- Implementar pruebas de penetración y evaluaciones de vulnerabilidad de forma regular.
- Comunicar de manera transparente las políticas de privacidad a todos los grupos de interés.

11. Métricas de impacto

11.1 Métricas de prevención

Nombre de la métrica	Descripción	Fórmula	Periodicidad sugerida	Obligatoriedad normativa o marco de referencia
Cobertura de avisos de privacidad	% de puntos de contacto con aviso de privacidad publicado	(Puntos con aviso / Total puntos) × 100	Anual	LGPDPPP (obligatorio)
Inventario de bases de datos	% de bases de datos personales inventariadas y documentadas	(Bases inventariadas / Total bases) × 100	Anual	LGPDPPP (obligatorio); ISO 27701
Capacitación en protección de datos	% de personal con acceso a datos capacitado en LGPDPPP	(Capacitados / Total con acceso a datos) × 100	Anual	LGPDPPP; ISO 27001
Evaluaciones de impacto en privacidad	Número de PIA (Privacy Impact Assessments) realizadas	Conteo de PIA documentadas	Anual	ISO 27701; RGPD

11.2 Métricas de corrección, control o mitigación

Nombre de la métrica	Descripción	Fórmula	Periodicidad sugerida	Obligatoriedad normativa o marco de referencia
Vulneraciones de datos reportadas	Número de vulneraciones de datos personales en el periodo	Conteo de vulneraciones	Trimestral	LGPDPPP (obligatorio); GRI 418-1
Solicitudes ARCO atendidas en plazo	% de solicitudes de derechos ARCO atendidas dentro del plazo legal	(Atendidas en plazo / Total solicitudes) × 100	Trimestral	LGPDPPP (obligatorio)
Hallazgos de auditoría de datos	Número de hallazgos en auditorías de protección de datos	Conteo de hallazgos por severidad	Anual	ISO 27001; LGPDPPP
Tiempo de respuesta a vulneraciones	Horas promedio para activar protocolo ante vulneración de datos	Suma horas activación / Número de vulneraciones	Por incidente	LGPDPPP; 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 vulneraciones	Meses consecutivos sin vulneraciones de datos reportadas	Conteo de meses sin vulneración	Continuo	LGPDPPP; GRI 418
Certificaciones de seguridad de información	Certificaciones ISO 27001/27701 vigentes	Conteo de certificaciones	Anual	ISO 27001; ISO 27701
Confianza del consumidor en manejo de datos	% de consumidores que confían en el manejo de sus datos	(Respuestas positivas / Total encuestados) × 100	Anual	GRI 418; LGPDPPP
Madurez del sistema de privacidad	Nivel de madurez del sistema de gestión de privacidad	Evaluación en escala 1–5 (CMM)	Anual	ISO 27701; RGPD

12. Conclusión

La protección de datos personales no es solo una obligación legal, sino un compromiso ético que define la calidad de la relación entre la empresa y sus grupos de interés. Las organizaciones que implementan sistemas robustos de gestión de privacidad no solo evitan sanciones del INAI, sino que construyen una ventaja competitiva basada en la confianza.

El Distintivo ESR® impulsa a las empresas a transitar desde el cumplimiento básico de la LGPDPPP hacia una gobernanza de datos que se convierta en activo estratégico, protegiendo derechos fundamentales y generando valor sostenible para consumidores, colaboradores y la sociedad.