WHITEPAPER · SECTOR FINANCIERO POPULAR Y NO BANCARIO

Gestión Integral de Riesgos y Cumplimiento en SOFIPOs y SOFOMEs de México

La oportunidad de un modelo GRC unificado para el cumplimiento, el riesgo, la seguridad de la información, la continuidad del negocio y la auditoría

NovaSec GRC

Governance · Risk · Compliance

Edición México · 2026

Índice

1. Resumen ejecutivo

El sector financiero popular y el crédito no bancario en México atraviesan un punto de inflexión. Las Sociedades Financieras Populares (SOFIPO) se han convertido en el vehículo preferido de los neobancos y las fintech para captar ahorro del público —la mayor SOFIPO del país administraba cerca de 120 mil millones de pesos en activos al cierre de octubre de 2025—, mientras que las Sociedades Financieras de Objeto Múltiple (SOFOME) suman más de 2,150 entidades registradas que sostienen buena parte del crédito al consumo, el factoraje y el arrendamiento. Este crecimiento acelerado convive con una supervisión regulatoria cada vez más estricta y con capacidades de gestión de riesgos que, en muchas entidades, no han evolucionado al mismo ritmo.

La intervención y posterior revocación de una de las SOFIPOs más grandes del sector durante 2025, que afectó a más de 1.3 millones de ahorradores, dejó una lección clara: la debilidad en el gobierno corporativo, la administración de riesgos y el control interno no es un problema teórico, sino un riesgo material para el patrimonio de los usuarios y para la continuidad del negocio.

Mensajes clave para la alta dirección

- **Presión regulatoria creciente y verificable:** en julio de 2025 la CNBV publicó y puso en vigor reformas a las Disposiciones de carácter general del sector de ahorro y crédito popular que refuerzan la administración de riesgos, la diversificación de riesgos, los criterios contables y la continuidad operativa de las SOFIPOs.
- **Cumplimiento transversal:** SOFIPOs y SOFOMEs comparten obligaciones en prevención de lavado de dinero (LFPIORPI, Art. 95 Bis LGOAAC y Art. 124 LACP) y en la nueva Ley Federal de Protección de Datos Personales en Posesión de los Particulares, vigente desde el 21 de marzo de 2025.
- **Brechas estructurales de gestión:** hojas de cálculo, procesos manuales, silos entre cumplimiento, riesgos, TI y auditoría, y ausencia de monitoreo continuo son aún la norma en gran parte del sector.
- **La oportunidad GRC:** un modelo de Gobierno, Riesgo y Cumplimiento (GRC) unificado integra en una sola plataforma la gestión del cumplimiento, los riesgos, la seguridad de la información, la continuidad del negocio y la auditoría, elevando la trazabilidad y reduciendo la carga operativa.
- **El rol de NovaSec GRC:** con trece módulos organizados en los tres pilares del GRC, NovaSec ofrece a SOFIPOs y SOFOMEs un camino para pasar de la gestión reactiva en Excel a un sistema auditable, con implementación en semanas y presencia regional que incluye a México.

Fuentes: CNBV; DOF (23–25 jul 2025); El Financiero / Moody's Local (jun 2025); LGOAAC; LACP; DOF (20 mar 2025); novasec.co.

2. Introducción: por qué el GRC importa en SOFIPOs y SOFOMEs

Durante la última década, México ha vivido una expansión notable de la inclusión financiera impulsada por entidades que operan fuera de la banca múltiple tradicional. Las SOFIPOs, nacidas al amparo de la Ley de Ahorro y Crédito Popular (LACP) de 2001, fueron concebidas para acercar servicios de ahorro y crédito a segmentos históricamente desatendidos. Hoy, esa misma figura es la puerta de entrada regulatoria de los neobancos y las fintech que buscan captar depósitos del público mexicano.

En paralelo, las SOFOMEs —creadas mediante las reformas de 2006 a la Ley General de Organizaciones y Actividades Auxiliares del Crédito (LGOAAC)— se convirtieron en el motor del crédito no bancario: otorgamiento de crédito, arrendamiento financiero y factoraje financiero. Su modelo, más ligero en autorización que el bancario, permitió una proliferación de entidades, pero también generó una enorme heterogeneidad en las capacidades de control interno y gestión de riesgos.

Este crecimiento no ha estado exento de sobresaltos. Las tasas de rendimiento agresivas ofrecidas por algunas SOFIPOs para competir por el ahorro, la dependencia de proveedores tecnológicos externos y la debilidad en el gobierno corporativo se combinaron en 2025 en un episodio que puso a prueba la confianza del sector. La pregunta para cada consejo de administración y dirección general es directa:

> ***¿Está su entidad preparada para demostrar, ante el regulador y ante sus usuarios, que gestiona de forma integral y trazable el cumplimiento, el riesgo, la seguridad de la información, la continuidad y la auditoría?***

Este documento analiza el contexto regulatorio verificado de SOFIPOs y SOFOMEs, identifica las brechas más frecuentes en su gestión de riesgos y cumplimiento, y explica cómo un modelo GRC unificado —ejemplificado con la plataforma NovaSec GRC— puede convertir esas obligaciones en un sistema operativo, auditable y sostenible.

3. Contexto regulatorio de SOFIPOs y SOFOMEs en México

Comprender la diferencia regulatoria entre ambas figuras es esencial para dimensionar la oportunidad GRC, porque el alcance de la supervisión y de las obligaciones difiere de forma importante.

3.1 Sociedades Financieras Populares (SOFIPO)

Las SOFIPOs son sociedades anónimas de capital variable autorizadas por la Comisión Nacional Bancaria y de Valores (CNBV) para captar recursos del público y canalizarlos al crédito, con la finalidad de fomentar la inclusión financiera. Se rigen por la LACP y por las Disposiciones de carácter general que emite la CNBV, y son supervisadas por la propia CNBV y, en materia de protección al usuario, por la CONDUSEF.

Los ahorradores cuentan con la protección del Fondo de Protección de Sociedades Financieras Populares (Prosofipo), que cubre depósitos hasta por 25,000 Unidades de Inversión (UDIS) por persona —del orden de 212 mil pesos—. Esta cobertura es sustancialmente menor a la de la banca múltiple, cuyos depositantes están protegidos por el IPAB hasta 400,000 UDIS, un contraste que eleva la importancia de la solidez de cada entidad.

Reformas de 2025: refuerzo de la gestión de riesgos

El 23 y 25 de julio de 2025 se publicaron en el DOF modificaciones a las Disposiciones de carácter general aplicables a las entidades de ahorro y crédito popular, con entrada en vigor el 24 de julio de 2025. Estas reformas fortalecen el marco prudencial de las SOFIPOs en aspectos como:

- Diversificación de riesgos y revisión del concepto de “riesgo común”, alineado con estándares internacionales, para analizar exposiciones agrupadas por vínculos familiares o patrimoniales.
- Evaluación documentada de la capacidad de pago de cada acreditado y consulta obligatoria de historial en sociedades de información crediticia.
- Nuevos criterios y registros contables especiales que la CNBV puede autorizar de forma temporal en situaciones críticas, orientados a la estabilidad, continuidad y solidez del sistema.

Fuentes: CNBV — Sector de Ahorro y Crédito Popular; DOF, 23 y 25 de julio de 2025; Nader, Hayaux & Goebel; Basham.

3.2 Sociedades Financieras de Objeto Múltiple (SOFOME)

La SOFOME se define en el artículo 87-B de la LGOAAC: el otorgamiento de crédito, el arrendamiento financiero y el factoraje financiero pueden realizarse de forma habitual y profesional sin necesidad de autorización del Gobierno Federal. Toda SOFOME debe añadir a su denominación la expresión “sociedad financiera de objeto múltiple” y precisar si es Entidad Regulada (E.R.) o Entidad No Regulada (E.N.R.). La distinción es decisiva:

- **SOFOME E.R. (Entidad Regulada):** mantiene vínculos patrimoniales (participación del 20% o más) con instituciones de crédito, SOCAPs o SOFIPOs, o emite deuda bursátil. Está sujeta a supervisión prudencial de la CNBV y a Disposiciones de carácter general específicas.

- **SOFOME E.N.R. (Entidad No Regulada):** no tiene esos vínculos. No está sujeta a supervisión prudencial de la CNBV; su registro y la supervisión en protección al usuario corresponden a la CONDUSEF, y la CNBV la supervisa únicamente para efectos de prevención de lavado de dinero.

Al mes de octubre de 2025 existían más de 2,155 SOFOMEs registradas en México, de las cuales cerca del 98% eran E.N.R. y el 2% E.R. Esta enorme población de entidades no reguladas prudencialmente concentra un reto particular: obligaciones de cumplimiento reales (PLD, protección al usuario, protección de datos) sin la infraestructura de control que la regulación prudencial suele imponer.

Fuentes: LGOAAC (arts. 87-B y 95 Bis); CNBV — SOFOMES; CONDUSEF; análisis de mercado (octubre 2025).

Cuadro comparativo: SOFIPO vs. SOFOME E.R. vs. SOFOME E.N.R.

Dimensión	SOFIPO	SOFOME E.R.	SOFOME E.N.R.
Ley marco	LACP	LGOAAC	LGOAAC
Autorización	CNBV (autoriza)	Por vínculo / deuda bursátil	Sin autorización federal
Supervisión prudencial	CNBV — sí	CNBV — sí	No aplica
Capta ahorro público	Sí	No	No
Protección al usuario	CONDUSEF	CONDUSEF	CONDUSEF
PLD / AML	Art. 124 LACP + CNBV	LGOAAC + CNBV	Art. 95 Bis LGOAAC
Seguro de depósito	Prosofipo (25,000 UDIS)	No aplica	No aplica

Elaboración propia con base en LACP, LGOAAC y publicaciones de la CNBV y la CONDUSEF.

3.3 Obligaciones transversales que aplican a ambas figuras

Prevención de lavado de dinero (PLD/FT)

Tanto SOFIPOs como SOFOMEs están sujetas a un régimen de prevención e identificación de operaciones con recursos de procedencia ilícita. El marco general es la LFPIORPI, complementada por el Art. 95 Bis de la LGOAAC para las SOFOMEs E.N.R. y por el Art. 124 de la LACP para las SOFIPOs. En la práctica, las entidades deben implementar un programa institucional de PLD, designar un oficial de cumplimiento, aplicar políticas de conocimiento del cliente (KYC), monitorear operaciones, consultar listas de personas bloqueadas y presentar reportes de operaciones (relevantes, inusuales e internas preocupantes) ante la Unidad de Inteligencia Financiera (UIF). El incumplimiento puede derivar en multas que alcanzan decenas de millones de pesos y, para las SOFOMEs, la cancelación del registro ante la CONDUSEF.

Fuentes: LFPIORPI; LGOAAC art. 95 Bis; LACP art. 124; UIF-SHCP.

Protección de datos personales (nueva ley 2025)

El 20 de marzo de 2025 se publicó en el DOF la nueva Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), en vigor desde el 21 de marzo de 2025, que abroga la ley de 2010. Como consecuencia de la desaparición del INAI, la autoridad en materia de protección de datos

pasó a la Secretaría Anticorrupción y Buen Gobierno. Para SOFIPOs y SOFOMEs, que manejan datos financieros y de identidad sensibles de millones de usuarios, esto implica revisar avisos de privacidad, contratos con encargados y terceros, y las medidas de seguridad conforme al nuevo marco.

Fuentes: DOF, 20 de marzo de 2025; Basham; EY México; KPMG México.

Estándares internacionales de referencia

Más allá de la norma local, el sector adopta como buenas prácticas estándares internacionales que estructuran un programa GRC: ISO 31000 (gestión de riesgos), ISO/IEC 27001 (seguridad de la información), ISO 22301 (continuidad del negocio), el NIST Cybersecurity Framework y COSO ERM para el control interno. Estos marcos son, precisamente, los que sustentan la arquitectura modular de una plataforma GRC moderna.

4. El papel estratégico del GRC: cinco dominios, un solo sistema

GRC (Gobierno, Riesgo y Cumplimiento) es el marco que unifica la forma en que una organización dirige, controla y demuestra su gestión. En una SOFIPO o SOFOME, su valor consiste en romper los silos entre las áreas de cumplimiento, riesgos, tecnología, continuidad y auditoría, para que trabajen sobre una misma fuente de verdad. Los tres pilares clásicos del GRC se traducen, en la operación cotidiana de una entidad financiera popular, en cinco dominios de gestión que la dirección debe integrar:

Dominio	Qué exige el sector	Consecuencia de gestionarlo en silos
Cumplimiento	PLD/FT, protección al usuario, protección de datos, reportes a CNBV/CONDUSEF/UIF.	Multas, cancelación de registro y reprocesos por evidencia dispersa.
Riesgos	Administración integral de riesgos (crédito, operativo, liquidez, riesgo común).	Pérdidas no detectadas y decisiones sin apetito de riesgo definido.
Seguridad de la información	Protección de datos financieros, gestión de activos e incidentes (ISO 27001).	Brechas de datos, exposición regulatoria y daño reputacional.
Continuidad del negocio	BIA, planes de continuidad y pruebas (ISO 22301) ante interrupciones.	Indisponibilidad de servicios críticos y pérdida de confianza.
Auditoría	Auditoría interna basada en riesgos, hallazgos y seguimiento al cierre.	Hallazgos sin trazabilidad y observaciones recurrentes del supervisor.

Las organizaciones con un GRC maduro conectan las decisiones de negocio con su apetito de riesgo, elevan los riesgos relevantes al nivel del consejo y generan reportes integrados y auditables. NovaSec GRC ejemplifica este enfoque: en lugar de trece herramientas aisladas, ofrece trece módulos que comparten datos, flujos y evidencias dentro de una misma plataforma.

5. Estadísticas y datos del sector (2025)

5.1 Un sector en expansión acelerada

La figura SOFIPO se ha convertido en la vía de entrada de los neobancos al ahorro mexicano. El regulador contabiliza más de 50 jugadores digitales en el ecosistema financiero, muchos de los cuales operan como SOFIPO o como Institución de Fondos de Pago Electrónico (IFPE) al amparo de la Ley Fintech. Algunas cifras verificables al cierre de octubre de 2025 ilustran la magnitud:

≈ $120,201 M	+2,155	10%–15%
Activos de la mayor SOFIPO del país (Nu México), oct. 2025.	SOFOMEs registradas; ~98% E.N.R. y ~2% E.R. (oct. 2025).	Rendimientos anuales ofrecidos por SOFIPOs y neobancos para captar ahorro.

Otros participantes relevantes reportaron, al cierre de octubre de 2025, activos por 9,793 millones de pesos (Klar) y 6,371 millones de pesos (Ualá), en un mercado donde la competencia por el ahorro empuja tasas muy por encima de las de la banca tradicional. La primera fintech en obtener licencia bancaria plena lo hizo en abril de 2025, señal de la madurez —y de las expectativas regulatorias— que alcanza el segmento.

Fuentes: CNBV; El CEO; ecollect; La Verdad (junio 2025).

5.2 La contracara: el riesgo se materializa

El apetito por captar ahorro a tasas elevadas y la debilidad de control en algunas entidades tuvieron consecuencias visibles en 2025. La cobertura de Prosofipo (25,000 UDIS por ahorrador) es limitada y, a diferencia del IPAB, el fondo no cuenta con respaldo presupuestal directo del Gobierno Federal: se financia con las aportaciones de las propias SOFIPOs. Al cierre de diciembre de 2024, Prosofipo reportaba activos líquidos por poco más de 594 millones de pesos, una cifra insuficiente para cubrir un evento de gran escala. Esta asimetría entre crecimiento y capacidad de respaldo es el argumento central de las reformas de julio de 2025.

Fuentes: Moody's Local (junio 2025); Proceso; El Financiero.

6. Principales falencias en la gestión de SOFIPOs y SOFOMEs

A partir del contexto regulatorio y del comportamiento observado del sector, se identifican debilidades recurrentes que un modelo GRC está diseñado para corregir:

Procesos manuales y dependencia de hojas de cálculo

Buena parte de las entidades gestiona su matriz de riesgos, sus controles PLD y sus hallazgos de auditoría en hojas de cálculo y correos, sin integración ni trazabilidad. Esto multiplica el error humano y dificulta demostrar evidencia ante la CNBV, la CONDUSEF o el auditor externo.

Silos entre cumplimiento, riesgos, TI y auditoría

Cuando cada área trabaja en su propio repositorio, un mismo hallazgo puede vivir en tres sistemas distintos y ninguno con el estatus real. La falta de una fuente única de verdad impide vincular un riesgo con su control, su prueba y su plan de acción.

Gobierno corporativo y patrocinio ejecutivo débiles

En especial en SOFOMEs E.N.R. y en entidades de rápido crecimiento, la gestión de riesgos se trata como un requisito formal más que como una función estratégica con respaldo del consejo. La ausencia de un apetito de riesgo formal y de roles claros deja decisiones críticas sin gobernanza.

Monitoreo insuficiente y ausencia de métricas

Sin indicadores de riesgo (KRIs) con umbrales y alertas, los cambios adversos —deterioro de cartera, incidentes de ciberseguridad, concentración— se detectan tarde. Pocos programas cuantifican probabilidad, impacto y tiempos de detección de forma sistemática.

Seguridad de la información y continuidad como puntos ciegos

La captación digital y la dependencia de proveedores cloud amplían la superficie de ataque. Muchas entidades carecen de un inventario clasificado de activos de información, de análisis de impacto al negocio (BIA) y de pruebas periódicas de sus planes de continuidad, exactamente las capacidades que la regulación de 2025 busca reforzar.

Gestión de terceros incipiente

El modelo fintech-SOFIPO descansa sobre proveedores tecnológicos críticos. La debida diligencia, el monitoreo continuo y las cláusulas de auditoría sobre esos terceros suelen ser superficiales, pese a que su falla puede interrumpir la operación completa.

7. Riesgos prioritarios

Los riesgos más relevantes para SOFIPOs y SOFOMEs pueden agruparse así:

Tipo de riesgo	Manifestación en el sector	Vínculo regulatorio
Crédito y riesgo común	Concentración, sobreendeudamiento del acreditado, deterioro de cartera.	Disposiciones CNBV (reforma jul. 2025), LACP.
Operativo	Fallas de procesos, fraude interno, errores en originación.	Administración integral de riesgos.
Tecnológico / ciber	Brechas de datos, indisponibilidad, ataques a canales digitales.	LFPDPPP (2025), ISO 27001, NIST.
Cumplimiento / PLD	Uso de la entidad para lavado, reportes tardíos a la UIF.	LFPIORPI, Art. 95 Bis LGOAAC, Art. 124 LACP.
Continuidad	Interrupción de servicios críticos de ahorro y crédito.	ISO 22301, continuidad operativa (reforma 2025).
Terceros	Falla de proveedor cloud o de core financiero subcontratado.	Debida diligencia y control de terceros.
Reputacional / liquidez	Corridas de depósitos ante pérdida de confianza.	Prosofipo (cobertura limitada), supervisión CNBV.

El rasgo común de estos riesgos es su interdependencia: un incidente de ciberseguridad en un proveedor puede desencadenar una interrupción de continuidad, un incumplimiento de protección de datos y, en el peor caso, un problema de liquidez y reputación. Solo un enfoque integrado —no un conjunto de controles aislados— permite anticipar y contener ese efecto dominó.

8. Caso de estudio: la intervención de una SOFIPO en 2025

El episodio más ilustrativo del riesgo estructural del sector ocurrió en 2025. El 13 de junio de 2025, la Junta de Gobierno de la CNBV acordó la intervención con carácter de gerencia de una de las SOFIPOs más grandes del país —la octava por tamaño, con activos cercanos a 3,160 millones de pesos a diciembre de 2024—, lo que implicó la suspensión total de operaciones, la toma del control administrativo y la congelación del acceso al ahorro para más de 1.3 millones de usuarios. El 21 de agosto de 2025, la CNBV revocó su autorización para operar.

El caso expuso la brecha entre el crecimiento captador y la capacidad de respaldo: la cobertura de Prosofipo (25,000 UDIS por ahorrador) dejaba desprotegido el excedente de quienes tenían montos mayores, y los activos líquidos del fondo eran limitados frente al universo de afectados. Agencias calificadoras advirtieron que el episodio, más que un caso aislado, era una prueba para la confianza en todo el sector de ahorro y crédito popular.

Lecciones para la gestión GRC

- El gobierno corporativo y la administración de riesgos no son formalismos: su debilidad se traduce en pérdida patrimonial real para los usuarios.
- La trazabilidad de controles, límites de concentración y evidencia de cumplimiento es lo que permite a una entidad demostrar solidez —y al supervisor detectar deterioro a tiempo.
- El monitoreo continuo mediante indicadores de riesgo con umbrales habría anticipado señales de alerta que, en un esquema manual, pasan inadvertidas.

Fuentes: CNBV; El Financiero (19 jun. 2025); Proceso (19 jun. 2025); Moody's Local (jun. 2025). Caso descrito con información pública para fines ilustrativos.

9. Cómo NovaSec GRC habilita la gestión integral

NovaSec GRC es una plataforma SaaS en la nube, parametrizable, que integra gobierno, riesgo, cumplimiento, auditoría y continuidad en un solo ecosistema. Organiza su funcionalidad en trece módulos agrupados en los tres pilares del GRC, y está diseñada para operar en el contexto regulatorio de países de habla hispana, con presencia y partners en México. A continuación se describen los módulos y su aporte concreto a una SOFIPO o SOFOME.

9.1 Pilar Gobierno

- **Cuadro de Mando Integral (BSC):** visualiza indicadores de gestión y de riesgo operativo en dashboards ejecutivos, conectando los indicadores de riesgo con los resultados del negocio para el consejo y la dirección.
- **Gestión de proyectos:** planifica y ejecuta iniciativas de riesgo y cumplimiento con cronogramas, responsables y seguimiento de planes de acción; optimiza los tiempos de auditoría.
- **Gestión de políticas:** centraliza y distribuye políticas y procedimientos con control de lectura y aprobaciones, construyendo una base de cumplimiento para toda la organización.

9.2 Pilar Riesgo

- **Gestión de riesgos (ISO 31000):** identifica, evalúa y mitiga riesgos con matrices configurables, mapas de calor y valoración por impacto y probabilidad, con planes de tratamiento.
- **Activos de información (ISO 27001/SGSI):** cataloga y clasifica activos críticos, evalúa vulnerabilidades y prioriza controles de seguridad de la información.
- **Gestión de incidentes:** registra eventos, escala y resuelve con flujos automatizados, análisis de causa raíz y lecciones aprendidas.
- **Análisis de Impacto al Negocio (BIA):** cuantifica el impacto financiero y operativo de las interrupciones, identifica procesos críticos y sustenta la continuidad operacional.
- **Gestión de eventos:** captura y analiza eventos de riesgo operativo y pérdidas, alimentando el catálogo de riesgos e identificando patrones recurrentes.
- **Pruebas:** ejecuta y documenta el testing de controles internos y de planes de continuidad, con evidencias centralizadas y auditables.

9.3 Pilar Cumplimiento

- **Indicadores de gestión:** define KRIs y KPIs con umbrales que activan alertas tempranas antes de que el riesgo se materialice.
- **Auditoría basada en riesgos:** planifica auditorías priorizando las áreas de mayor exposición y documenta hallazgos con evidencia trazable.
- **Cumplimiento normativo:** mapea requisitos regulatorios, evalúa brechas y genera reportes listos para entes de control y reguladores.

- **Gestión de hallazgos:** administra planes de acción con responsables, fechas y seguimiento hasta el cierre efectivo, integrando auditoría interna y compliance.

Descripción de módulos con base en la información publicada en novasec.co/modulos-grc.

9.4 Mapeo: los cinco dominios de una SOFIPO/SOFOME sobre los módulos NovaSec

El siguiente cuadro traduce cada obligación de gestión de una entidad financiera popular a los módulos que la soportan, mostrando por qué un modelo unificado supera a un conjunto de herramientas aisladas:

Dominio de la entidad	Necesidad regulatoria/operativa	Módulos NovaSec que lo habilitan
Cumplimiento	PLD/FT, protección al usuario y de datos, reportes a CNBV/CONDUSEF/UIF.	Cumplimiento normativo · Gestión de políticas · Indicadores de gestión
Riesgos	Administración integral de riesgos, riesgo común, pérdidas operativas.	Gestión de riesgos · Gestión de eventos · Gestión de incidentes
Seguridad de la información	Clasificación de activos, gestión de incidentes de datos (ISO 27001).	Activos de información · Gestión de incidentes
Continuidad del negocio	BIA, planes de continuidad y pruebas periódicas (ISO 22301).	Análisis de Impacto al Negocio (BIA) · Pruebas
Auditoría	Auditoría interna basada en riesgos, hallazgos y cierre trazable.	Auditoría basada en riesgos · Gestión de hallazgos · Pruebas
Gobierno	Apetito de riesgo, reporte al consejo, roles y responsabilidades.	Cuadro de Mando Integral (BSC) · Gestión de proyectos

Elaboración propia. El mapeo es orientativo; la parametrización final depende del perfil de cada entidad.

10. Hoja de ruta de implementación y modelo de madurez

La transición hacia un GRC integrado no requiere una transformación de años. Una SOFIPO o SOFOME puede avanzar por fases, priorizando los dominios de mayor exposición regulatoria:

Fase 1 — Cimientos (semanas 1 a 4)

- Inventario de obligaciones regulatorias (CNBV/CONDUSEF/UIF) y de activos de información críticos.
- Definición del apetito de riesgo por el consejo y de la matriz de riesgos base.
- Carga de políticas vigentes y asignación de responsables.

Fase 2 — Operación (semanas 5 a 12)

- Activación del monitoreo con KRIs y umbrales de alerta.
- Registro estructurado de eventos e incidentes; primer BIA de procesos críticos.
- Mapa de cumplimiento normativo con evaluación de brechas.

Fase 3 — Aseguramiento (a partir del mes 4)

- Auditoría interna basada en riesgos con hallazgos y planes de acción trazables.
- Pruebas de controles y de continuidad documentadas.
- Reporte ejecutivo integrado al consejo y preparación de evidencia para el supervisor.

Modelo de madurez sugerido

Nivel	Característica
Nivel 0	Gestión reactiva en hojas de cálculo y correos; sin fuente única de verdad.
Nivel 1	Inventario de riesgos y políticas centralizadas; controles documentados.
Nivel 2	Evaluación periódica de riesgos y algunos KRIs con responsables definidos.
Nivel 3	Monitoreo continuo, dashboard ejecutivo y auditoría integrada al GRC.
Nivel 4	Gestión basada en datos, alertas tempranas y evidencia lista para el regulador.

11. Beneficios y valor de negocio

Adoptar un GRC unificado no es solo una respuesta al regulador; es una decisión de eficiencia y resiliencia. La propuesta de valor de NovaSec, según la información publicada por la compañía, se traduce en beneficios tangibles:

Hasta −60%	**Semanas**	**+95%**
Reducción de la carga operativa al integrar gobierno, riesgo, cumplimiento, auditoría y continuidad.	Tiempo de implementación de la plataforma SaaS parametrizable, no meses.	Tasa de renovación de clientes reportada por NovaSec.

A ello se suma la eliminación de reprocesos, la trazabilidad de extremo a extremo (riesgo → control → prueba → hallazgo → cierre), la visibilidad ejecutiva en tiempo real y una cultura de riesgo compartida entre áreas. Para una entidad supervisada, la capacidad de producir evidencia consistente y auditable ante la CNBV, la CONDUSEF o el auditor externo reduce de forma directa el riesgo de multas y observaciones. NovaSec reporta más de 45 organizaciones usuarias, más de 1,000 procesos en gestión activa y más de 50,000 usuarios en la región, con acompañamiento y partners en México.

Fuentes: novasec.co (cifras publicadas por la compañía). Los resultados pueden variar según la entidad y su nivel de madurez.

12. Tendencias y desafíos emergentes

Supervisión reforzada post-2025

Las reformas de julio de 2025 y los eventos del sector anticipan una supervisión más exigente sobre diversificación de riesgos, capacidad de pago, continuidad y solidez patrimonial. Las entidades que ya operen con evidencia estructurada tendrán ventaja.

Inteligencia artificial y analítica en el GRC

La IA comienza a aplicarse a la detección de anomalías, el análisis de riesgo en tiempo real y la priorización de controles. Integrada a los KRIs dentro del GRC, potencia la alerta temprana; adoptarla será un diferenciador competitivo.

Ciberresiliencia y protección de datos

Con la nueva LFPDPPP vigente y una superficie de ataque creciente por la operación digital, la seguridad de la información y la continuidad dejan de ser proyectos de TI para convertirse en obligaciones de gobierno. El inventario de activos, la gestión de incidentes y las pruebas de continuidad son la base de la ciberresiliencia.

Gestión de terceros (riesgo de n-ésima parte)

El modelo fintech-SOFIPO depende de proveedores tecnológicos críticos y de sus subcontratistas. Ampliar la visibilidad más allá del primer nivel y formalizar la debida diligencia y el derecho de auditoría sobre terceros será cada vez más relevante.

13. Conclusiones

El sector de SOFIPOs y SOFOMEs vive una tensión entre un crecimiento acelerado —impulsado por los neobancos y el crédito no bancario— y una capacidad de gestión de riesgos que, en muchas entidades, sigue anclada en hojas de cálculo y procesos manuales. Los hechos de 2025, incluidas las reformas regulatorias de julio y la intervención de una SOFIPO relevante, demuestran que la gestión del cumplimiento, el riesgo, la seguridad de la información, la continuidad y la auditoría ya no puede tratarse como un conjunto de tareas aisladas.

El GRC integrado es la respuesta: eleva los riesgos al nivel del consejo, conecta las decisiones con el apetito de riesgo, asegura el cumplimiento ante la CNBV, la CONDUSEF, la UIF y la autoridad de protección de datos, y protege la operación frente a incidentes e interrupciones. Un TPRM y un cumplimiento desconectados del GRC carecen de trazabilidad y capacidad de respuesta.

Para SOFIPOs y SOFOMEs, migrar de la gestión reactiva a un modelo GRC unificado, auditable y basado en datos —como el que habilita NovaSec GRC— es hoy una condición de resiliencia, competitividad y confianza.

La madurez futura dependerá de la integración tecnológica. Las entidades que sigan gestionando riesgos con hojas de cálculo enfrentarán brechas no detectadas, falta de evidencia ante auditorías y criterios inconsistentes. Las que adopten una plataforma GRC estarán mejor preparadas para crecer con solidez y para responder ante el regulador y sus usuarios.

14. Glosario

- **SOFIPO:** Sociedad Financiera Popular. Entidad autorizada y supervisada por la CNBV bajo la LACP para captar ahorro del público y otorgar crédito.
- **SOFOME:** Sociedad Financiera de Objeto Múltiple (E.R. o E.N.R.). Realiza crédito, arrendamiento y factoraje conforme al art. 87-B de la LGOAAC.
- **GRC:** Gobierno, Riesgo y Cumplimiento. Marco que unifica la dirección, la gestión de riesgos y el cumplimiento en un solo sistema.
- **CNBV:** Comisión Nacional Bancaria y de Valores. Supervisor prudencial de SOFIPOs y de SOFOMEs E.R.
- **CONDUSEF:** Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. Registra y protege a los usuarios.
- **Prosofipo:** Fondo de Protección de Sociedades Financieras Populares y de sus Ahorradores. Cubre depósitos hasta 25,000 UDIS.
- **LACP:** Ley de Ahorro y Crédito Popular (2001). Marco de las SOFIPOs.
- **LGOAAC:** Ley General de Organizaciones y Actividades Auxiliares del Crédito. Marco de las SOFOMEs.
- **LFPIORPI:** Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita (ley antilavado).
- **UIF:** Unidad de Inteligencia Financiera de la SHCP. Recibe reportes de operaciones.
- **LFPDPPP:** Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Nueva ley vigente desde el 21 de marzo de 2025.
- **BIA:** Business Impact Analysis. Análisis del impacto de interrupciones sobre procesos críticos (base de la continuidad, ISO 22301).
- **KRI / KPI:** Indicadores clave de riesgo y de desempeño con umbrales que activan alertas.
- **Riesgo común:** Exposición agrupada de personas vinculadas por lazos familiares o patrimoniales, relevante para límites de financiamiento.
- **Apetito de riesgo:** Nivel de riesgo que el consejo define como aceptable; base estratégica del GRC.

15. Referencias y normativa clave

Normativa mexicana

- Ley de Ahorro y Crédito Popular (LACP). Cámara de Diputados.
- Ley General de Organizaciones y Actividades Auxiliares del Crédito (LGOAAC), arts. 87-B y 95 Bis.
- Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita (LFPIORPI).
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares (DOF, 20 de marzo de 2025).
- Disposiciones de carácter general aplicables a las entidades de ahorro y crédito popular; reformas publicadas en el DOF el 23 y 25 de julio de 2025.

Fuentes institucionales y de mercado

- CNBV — Sector de Ahorro y Crédito Popular; SOFOMES; Entidades Autorizadas (Sofipos).
- CONDUSEF — Sociedades Financieras Populares y SOFOM.
- Moody's Local México — Análisis del sector Sofipos, junio de 2025.
- El Financiero, Proceso, El CEO, ecollect — cobertura del sector (2025).
- INEGI — Valor de la UMA 2025 ($113.14 diario) y 2026 ($117.31 diario).

Estándares internacionales

- ISO 31000 (gestión de riesgos), ISO/IEC 27001 (seguridad de la información), ISO 22301 (continuidad del negocio), NIST Cybersecurity Framework, COSO ERM.

NovaSec GRC

- Sitio oficial y descripción de módulos: novasec.co · novasec.co/modulos-grc · Software GRC para México

Aviso: Este documento tiene fines informativos y de divulgación. No constituye asesoría legal, regulatoria ni financiera. Las cifras y disposiciones citadas provienen de fuentes públicas verificadas a la fecha de elaboración (julio de 2026) y pueden cambiar; se recomienda validar la normativa vigente con las fuentes oficiales (CNBV, CONDUSEF, DOF) antes de tomar decisiones.