MERC GROUP

THINK GROWTH. THINK MERC.

Radar regulatório

# Open Insurance e o Registro de *Operações* o que muda nos controles do setor de seguros

Open Insurance e o SRO entram na prioridade máxima da SUSEP em 2026 e deslocam o risco para os controles de TI, o consentimento e o registro.

| NORMA BASE | PÚBLICO | EDIÇÃO | DATA |
| --- | --- | --- | --- |
| LC 213/2025 · Plano de Regulação SUSEP 2026 | Seguradoras, EAPC e sociedades de capitalização | Edição 2026 | Agosto de 2026 |

O compartilhamento de dados no setor de seguros deixou de ser projeto e virou obrigação operacional. A SUSEP colocou a revisão do Open Insurance no grupo de prioridade máxima do seu Plano de Regulação para 2026 e avançou com as normas que disciplinam tanto o ecossistema de compartilhamento quanto o Registro de Operações (SRO). Para seguradoras, entidades de previdência complementar aberta e sociedades de capitalização, a consequência não é apenas de conformidade: é uma transferência de risco para dentro dos controles de tecnologia, da jornada de consentimento e da integridade do registro das operações. E tudo isso passa a ser objeto de evidência auditável.

Este radar trata do tema técnico, não de nenhuma companhia em particular. O ponto de partida regulatório é a nova Lei de Seguros (Lei Complementar nº 213, de 2025), que redesenhou o arcabouço do setor, somada ao Plano de Regulação da SUSEP para 2026, que formaliza a prioridade do Open Insurance e da agenda de dados. O que era um diferencial de inovação passou a ser um requisito com trilha de auditoria.

Radar regulatório

# Resumo

01 **A SUSEP classificou a revisão do Open Insurance**

A SUSEP classificou a revisão do Open Insurance como prioridade máxima em 2026 e avançou com as normas de implementação do compartilhamento de dados e do Registro de Operações (SRO), o que muda a natureza do risco: de estratégico para operacional e controlável.

02 **O risco se desloca para três frentes testáveis:**

O risco se desloca para três frentes testáveis: controles gerais de tecnologia e segurança das APIs, a jornada de consentimento e revogação sob a LGPD, e a integridade, a existência e a completude do registro das operações no SRO.

03 **O tratamento contábil não muda por si, mas a qua**

O tratamento contábil não muda por si, mas a qualidade da informação que alimenta reservas técnicas, prêmios e sinistros passa a depender de dados que trafegam entre instituições, o que eleva a exigência sobre conciliação e sobre a asseguração de prestadores de serviço.

04 **Para a auditoria e a asseguração independentes,**

Para a auditoria e a asseguração independentes, o eixo é a efetividade dos controles: relatório de asseguração sobre controles de prestadores (NBC TO 3402 / ISAE 3402), testes de controles gerais de TI e evidência sobre a conciliação entre o registrado, o compartilhado e o contabilizado.

| P | A |
|---|---|
| **Compartilhamento (Open Insurance)** | APIs padronizadas, consentimento explícito, escopo de dados e serviços versionado |
| **Registro de Operações (SRO)** | Registro das operações em entidade registradora autorizada |

| P | A |
| --- | --- |
| **Proteção de dados** | Base legal, minimização e finalidade do tratamento sob a LGPD |
| **Governança e terceiros** | Responsabilidade da instituição sobre serviços terceirizados e provedores |

Agenda SUSEP

## O que a agenda regulatória colocou em movimento

A leitura correta do Open Insurance é a de um sistema de compartilhamento de dados e serviços de seguros, previdência e capitalização, operado por interfaces padronizadas e acionado pelo consentimento do titular. O paralelo com o compartilhamento no sistema bancário é útil, mas não é perfeito: os dados de seguros carregam informação sensível sobre saúde, patrimônio e sinistralidade, o que aumenta a exigência sobre finalidade, minimização e segurança. O Plano de Regulação da SUSEP para 2026 classifica a revisão do Open Insurance no grupo de prioridade máxima, sinal de que a implementação sai da fase de desenho e entra na fase de operação supervisionada.

O Registro de Operações completa o quadro. A lógica do SRO é a mesma que o mercado financeiro já conhece em outros registros: operações passam a ser registradas em entidades registradoras autorizadas, criando uma fonte independente sobre o que foi contratado, quando e em que condições. Para o setor de seguros, isso significa que a operação deixa de existir apenas nos sistemas internos da instituição e passa a ter um espelho externo. Esse espelho é, ao mesmo tempo, um ganho de transparência para a supervisão e uma nova superfície de conciliação que precisa fechar com a contabilidade e com os sistemas de apólice e sinistro.

A nova Lei de Seguros deu a moldura. Ao reorganizar o contrato de seguro e o arcabouço do setor, a Lei Complementar nº 213, de 2025, sustentou uma agenda regulatória em que dados, registro e supervisão prudencial andam juntos. A consequência prática é que a instituição que trata o Open Insurance e o SRO como projetos de tecnologia isolados, sem governança de controle e sem trilha de evidência, corre o risco de descobrir a lacuna no pior momento: durante uma fiscalização ou durante a auditoria das demonstrações.

Risco de controles

## Por que isso é assunto de auditoria, e não só de TI

O reconhecimento e a mensuração das operações de seguro seguem as normas contábeis já vigentes, inclusive o padrão de contratos de seguro. O que muda com o Open Insurance e o SRO não é a regra de contabilização em si, e sim a origem e o trânsito da informação que alimenta essa contabilização. Prêmios, sinistros, provisões e reservas técnicas dependem de dados que, cada vez mais, trafegam entre instituições e são espelhados em um registro externo. Quando o dado se move, o controle sobre a sua integridade se torna o centro da evidência.

A partir daí, o trabalho de auditoria e de asseguração se organiza em torno de controles testáveis. Os controles gerais de tecnologia — acesso, mudança, operação e segurança das APIs — passam a ser relevantes para a confiabilidade dos números. A jornada de consentimento vira um controle com efeito jurídico e reputacional: um compartilhamento sem base válida é um passivo potencial, não um recurso. E a integridade do registro no SRO precisa ser testada nos três atributos clássicos de qualquer registro: existência do que está lá, completude do que deveria estar e tempestividade do que foi registrado.

| P | A |
|---|---|
| **Controles gerais de TI e APIs** | O acesso, a mudança e a segurança das interfaces são controlados e monitorados? |
| **Controles de prestadores** | O provedor que opera a infraestrutura tem controles com asseguração independente? |
| **Consentimento e dados** | Cada compartilhamento tem base legal, finalidade e trilha de revogação? |
| **Registro no SRO** | O registrado concilia com a apólice, o sinistro e a contabilidade? |

Asseguração

## Implicações práticas para quem opera no setor

A primeira implicação é de governança. O Open Insurance e o SRO precisam de um dono, de um comitê que responda por eles e de uma política de gestão de mudança que trate cada nova versão de manual ou de escopo como um evento controlado, não como uma atualização silenciosa de sistema. A ausência de versionamento formal é uma das lacunas mais comuns, e é justamente a que gera achado em fiscalização.

A segunda implicação é de dados. A instituição precisa saber, com precisão, quais dados compartilha, com quem, com que base legal e por quanto tempo. O mapeamento de dados deixou de ser exigência abstrata da LGPD e passou a ser insumo direto do controle: sem ele, não há como demonstrar finalidade nem responder a uma revogação de consentimento com trilha de auditoria. A terceira implicação é de conciliação. O SRO cria uma fonte externa que precisa fechar com o interno; qualquer diferença entre o registrado, o compartilhado e o contabilizado é um sinal de controle que merece explicação documentada.

A quarta implicação é de terceiros. Boa parte da operação de compartilhamento e de registro apoia-se em provedores. A responsabilidade, porém, permanece com a instituição regulada. Isso torna o relatório de asseguração sobre os controles do prestador — no padrão NBC TO 3402, equivalente ao ISAE 3402 — um instrumento central, e não um luxo: é a forma organizada de a instituição obter conforto sobre controles que ela não opera diretamente, mas pelos quais responde.

Prática

## Caso anonimizado

Uma seguradora de médio porte estruturou o compartilhamento de dados como um projeto de tecnologia conduzido por um fornecedor, com foco em cumprir o cronograma de conexão. As interfaces funcionavam, mas a jornada de consentimento não guardava trilha completa da revogação, e o registro das operações não era conciliado com a contabilidade em base regular. Nenhum número estava errado no fechamento; o problema era a ausência de evidência de que os controles operavam. Quando a asseguração independente entrou, a lacuna apareceu não como erro contábil, mas como limitação de controle: não havia como demonstrar, de forma tempestiva, que cada compartilhamento tinha base válida e que o registrado espelhava o contratado. A correção foi de governança e de trilha, não de contabilidade, e teria custado uma fração do esforço se tivesse sido desenhada como controle desde o início.

FAQ

## Como a MERC pode ajudar

A MERC é uma auditoria especializada no mercado financeiro e trata Open Insurance e SRO como o que eles são: um problema de controle e de evidência, antes de ser um problema de tecnologia. O trabalho combina a auditoria independente das demonstrações com a avaliação dos controles gerais de tecnologia, da jornada de consentimento e da integridade do registro. Quando o conforto necessário é sobre a efetividade de controles de um prestador de serviço, o instrumento adequado é um trabalho de asseguração razoável e limitada no padrão NBC TO 3402, que dá à instituição — e aos seus supervisores — uma base independente sobre controles que ela não opera diretamente. O objetivo é simples: transformar a conformidade de dados em trilha auditável, antes que a fiscalização peça a evidência que ainda não existe.

Radar regulatório

# Perguntas frequentes

MERC GROUP

PRÓXIMO PASSO

# Do requisito ao *teste* que o sustenta.

A MERC e firma de auditoria independente registrada na CVM, especializada em mercado financeiro. Estruturamos o trabalho do diagnostico a evidencia: leitura do requisito, desenho dos testes, trilha de auditoria e o relatorio que sustenta a conclusao. Fale com a equipe pelo canal de contato.


| | |
|---|---|
| SITE | www.mercgroup.com.br |
| CONTEÚDO | www.mercgroup.com.br/insights |
| E-MAIL | contato@mercgroup.com.br |
| TELEFONE | +55 11 98196 1447 |