CNSEG

Os reflexos do OPIN no Sistema de Controles Internos, Estruturas de Gestão de Riscos e Atividades de Auditoria Internas

EY
Building a better working world

Agenda

1. Contexto
2. Desafios para implementação dos requisitos
3. Abordagem recomendada
4. Por que EY?

O Open Insurance é uma nova estrutura de compartilhamento de dados que resultam do Open Finance

Definição do Open Insurance

O Open Insurance, ou Sistema de Seguros Aberto, é a possibilidade de consumidores de produtos e serviços de seguros, previdência complementar aberta e capitalização **permitirem o compartilhamento de suas informações entre** diferentes sociedades autorizadas/credenciadas pela Susep, **de forma segura, ágil, precisa e conveniente**.

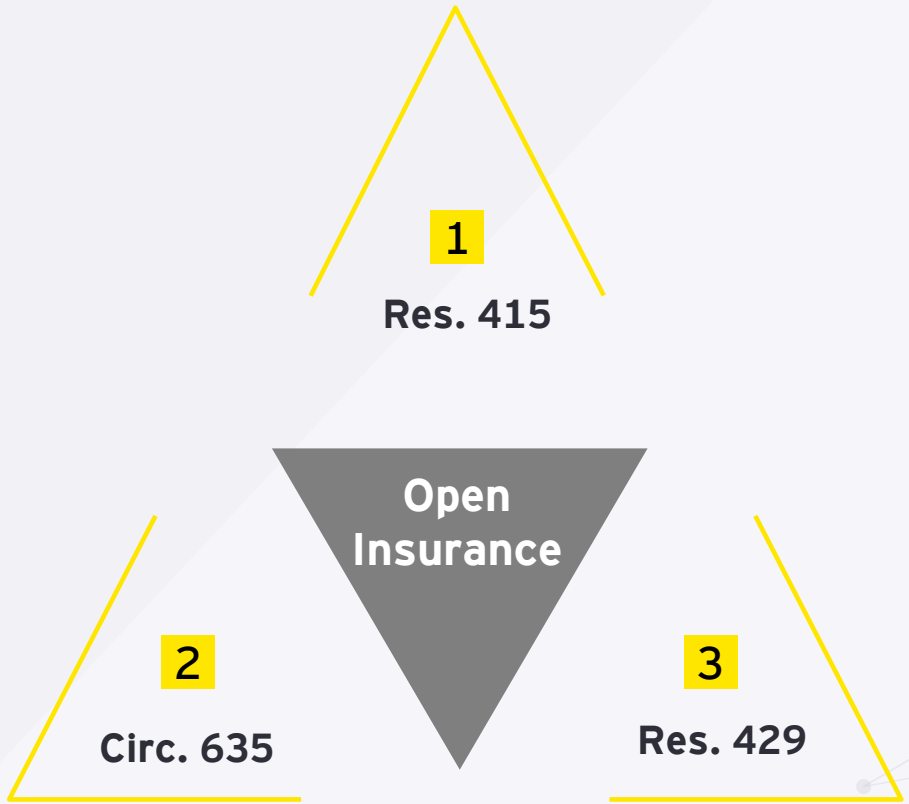
Para entregar esses benefícios ao consumidor, o Open Insurance **operacionaliza e padroniza o compartilhamento de dados e serviços** por meio de abertura e integração de sistemas, com privacidade e segurança.

[1] Resolução CNSP 415/2021

O Open insurance encontra-se regulamentado com base nas resoluções emitidas pelo Conselho Nacional de Seguros Privados (CNSP) e SUSEP

Regulamentação do Open Insurance

O Open Insurance[1] é a possibilidade de consumidores de produtos e serviços de seguros, previdência complementar aberta e capitalização **realizarem o compartilhamento de suas informações** entre diferentes sociedades autorizadas/credenciadas pela SUSEP. Este sistema encontra-se regulamentado resoluções da CNSP e circular SUSEP.



1 RESOLUÇÃO CNSP 415/2021 (revogada pela resolução CNSP 450/ 2022)

- Dispõe sobre a **implementação do *Open Insurance*** pelas sociedades seguradoras, entidades abertas de previdência complementar e sociedades de capitalização.

2 CIRCULAR SUSEP 635/2021

- Dispõe sobre a **regulamentação das diretrizes estabelecidas** pelo Conselho Nacional de Seguros Privados – CNSP para a implementação do *Open Insurance*.

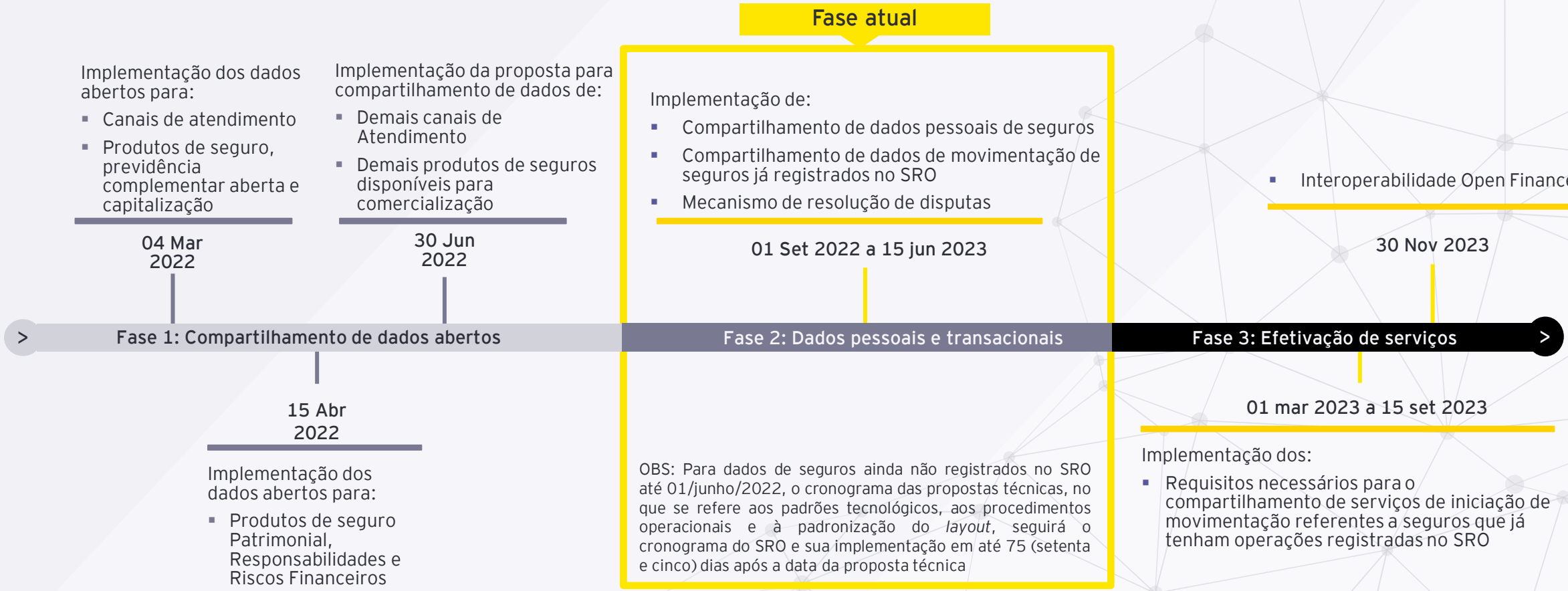
3 RESOLUÇÃO CNSP 429/2021 (revogada pela resolução CNSP 450/ 2022)

- Dispõe os **requisitos para credenciamento e funcionamento das SISS** (sociedades iniciadoras de serviço de Seguro) no âmbito do *Open Insurance* **e dispõe sobre as SPOCs**

[1] Resolução CNSP 415/2021

Para sua implementação, a SUSEP definiu um cronograma com prazos dispostos em fases, observando data máxima para implementação de requisitos

Cronograma de implementação



A data final para implementação do compartilhamento de dados pessoais e de serviços não poderá ultrapassar **15 de setembro de 2023**

A fase 2 atual trata do início do compartilhamento de dados pessoais de seguros conforme exigência SUSEP...

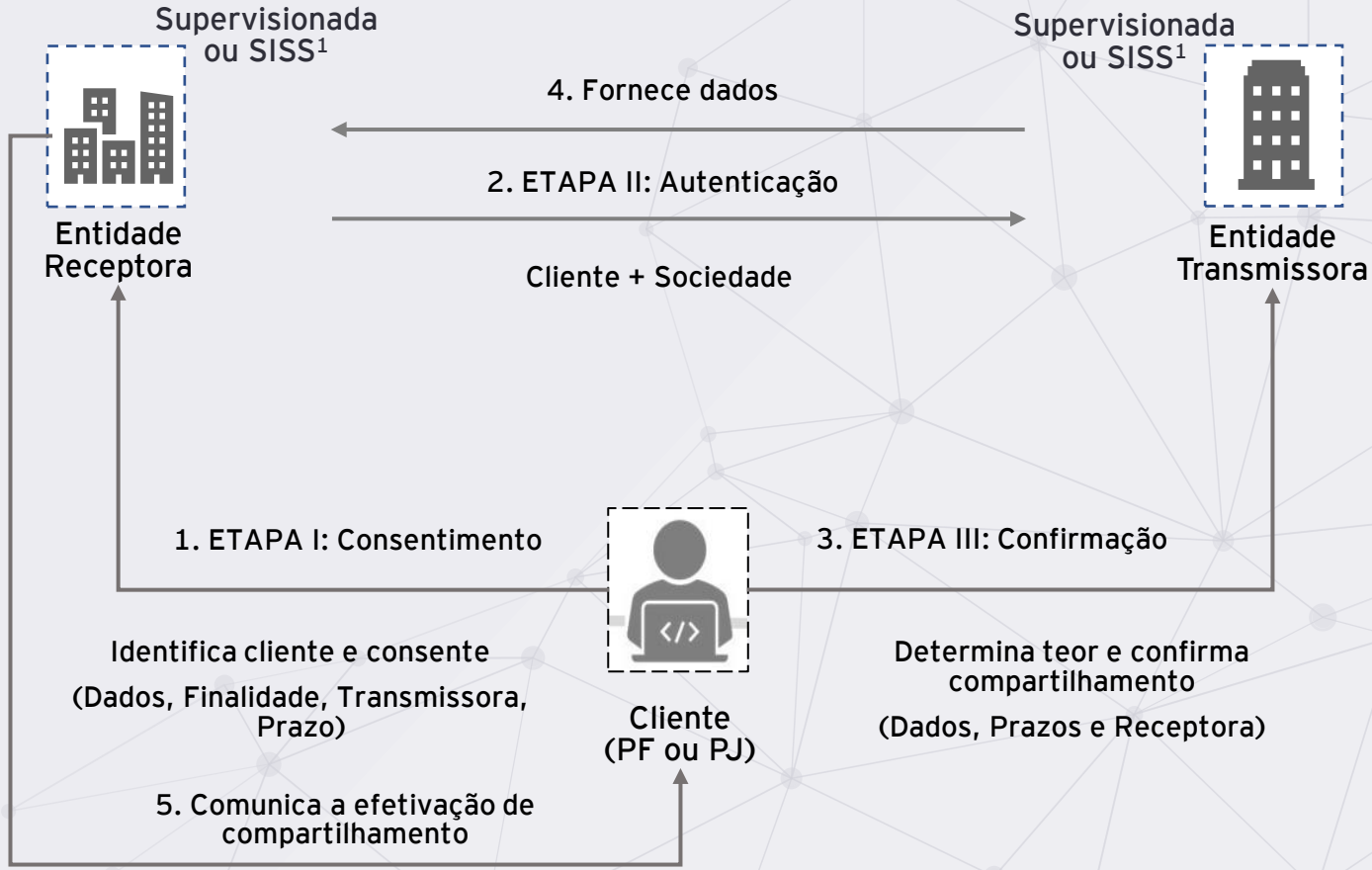
Visão da Jornada do Cliente

Fase 1: Compartilhamento de dados abertos

Fase 2: Dados pessoais e transacionais

Fase 3: Efetivação de serviços

Para que haja o compartilhamento de dados pessoais, é necessário que os clientes deem o consentimento antes de iniciar a movimentação.



Fonte: CNSeg; EY

[1] A atuação das Sociedades Iniciadoras de Serviços de Seguros (SISS) ocorre apenas na Fase 3

... E requer que os participantes prestem ao cliente informações sobre os consentimentos às partes envolvidas

Obrigações dos Participantes

Fase 1: Compartilhamento de dados abertos

Fase 2: Dados pessoais e transacionais

Fase 3: Efetivação de serviços

A Jornada de Compartilhamento, após o consentimento dado pelo cliente, terá início na sociedade receptora (receptora dos dados do cliente da sociedade transmissora). O compartilhamento será realizado através de canais digitais.

- Participantes devem assegurar a possibilidade da **revogação do consentimento a qualquer tempo**
- Participantes são responsáveis pela **confiabilidade, pela integridade, pela disponibilidade, pela segurança e pelo sigilo** em relação ao compartilhamento de dados e serviços em que esteja envolvida
- Participantes devem **disponibilizar interfaces dedicadas ao compartilhamento** de dados e serviços
- **Participantes devem informar aos seus clientes que as demandas a respeito do compartilhamento de dados e serviços** podem ser apresentadas por meio dos canais de atendimento das participantes
- No caso das interfaces para o **compartilhamento dos dados abertos** de seguros (Fase 1), as sociedades participantes **devem assegurar o seu acesso gratuito ao público**

[1] Fonte: CNSeg; EY

Para garantir essas obrigações e efetivo desenvolvimento da operação, a Resolução 415/2021 (*) estabelece uma série de requisitos que precisam ser observados pela 2ª e 3ª linha

Requisitos regulatórios

1 Registros

Registros das demandas dos clientes e dos canais de atendimento para compartilhamento de dados e serviços

Registros do consentimento, da autenticação, da confirmação e da revogação do consentimento dos clientes

2 Dados

Governança de dados estruturados, segregados por clientes, tipos de dados e serviços compartilhados

Disponibilizar de dados confiáveis, íntegros e padronizados sobre as informações consentidas

3 Operabilidade

Garantir a disponibilidade das interfaces, os testes de continuidade do negócio (cenários de indisponibilidade das interfaces) e monitoramento da quantidade de chamadas e dos indicadores de desempenho das interfaces usadas no compartilhamento de dados e serviços

Garantir a interoperabilidade entre o *Open Insurance* e o *Open Banking*

4 Segurança

Infraestrutura segura, realizar a gestão de Incidentes de violação da segurança dos dados, categorizados e priorizados de acordo com os planos de resposta e criticidade dos sistemas

Garantir a confidencialidade / sigilo das credenciais de identificação e autenticação do cliente

5 Fraudes

Identificar fraudes associadas a demandas dos clientes para compartilhamento de dados e serviços e das providências adotadas para o seu tratamento

6 Políticas e Normativos

Revisar de políticas e normativos internos como, por exemplo, de Gestão de Riscos, Controles Internos, Plano de Continuidade de Negócio e de Segurança Cibernética, a fim de incluir os papeis, responsabilidades, diretrizes e impactos trazidos com o *Open Insurance*

(*) Revogada pela Resolução 450/2022

Neste sentido, as áreas de 2ª e 3ª linha terão um papel chave para garantir o atendimento aos requisitos regulatórios e assegurar um ambiente seguro, íntegro e operativo do OPIN

Modelo de 3 Linhas na perspectiva do *Open Insurance*

Conselho / Gestão Executiva

Supervisão de performance

- Estabelece a estratégia de implementação do *Open Insurance* e recursos (pessoas, tecnologia, investimentos)
- Propõe diretrizes e aprova as políticas revisadas necessárias
- Avalia as atividades de implementação sob a ótica de riscos e também de oportunidades
- Aprova o Relatório Anual referente ao compartilhamento

Três linhas

Auditoria interna 3ª linha

Testar e Verificar

- Realiza testes independentes e periódicos com vistas a assegurar a confiabilidade, a disponibilidade, a integridade, a segurança e o sigilo do compartilhamento de dados e serviços, bem como a implementação e a efetividade dos requisitos

Funções de Controle 2ª linha

Desenhar e facilitar

- Avalia os riscos e controles dos novos processos ou processos alterados de forma conjunta com os *Risk-Owners*
- Recomenda e orienta a 1ª linha para melhorias
- Verifica o impacto sobre o perfil de riscos na companhia, mensura os respectivos níveis de riscos e compatibilidade ao apetite
- Realiza o monitoramento dos indicadores de riscos (Exemplos: Incidentes, Indisponibilidade, Fraudes)
- Compila e direciona questões de risco/controles a gestão executiva/conselho
- Estabelece procedimentos em caso de indisponibilidade, prazo de reinício ou normalização, tratamento de incidentes e execução dos testes

Interpretar e desenvolver

- Monitora a aderência dos *Risk-Owners* as políticas, procedimentos, framework e estratégia
- Acompanha os planos de ação face a deficiências

***Risk-Owners* 1ª linha**

Monitorar e reportar

- Implementação dos requisitos definidos pela regulação (Resoluções, Manuais Técnicos e correlatos)
- "Proprietário" do processo de implementação e sustentação: identifica, gerencia, mitiga e reporta o risco
- Realiza o rastreamento de dados de incidentes ou de perdas e implementa os planos de ação
- Elabora o Relatório Anual referente ao compartilhamento de dados e serviços em que a sociedade esteve envolvida

Requisitos

- Políticas e Normativos
- Registros
- Dados
- Operabilidade
- Segurança
- Fraudes

Relatório Anual

O Open Insurance é uma disrupção no mercado trazendo consigo impacto no modelo operacional e, consequentemente, um conjunto de desafios para as áreas de 2ª e 3ª linha

Desafios para as áreas de 2ª e 3ª linha

Planejamento e Complexidade de Implementação

- Prazos e requisitos são complexos e concorrem com projetos internos das companhias
- Frentes de implementação e processos são multidisciplinares trazendo maior complexidade para as funções de controle e auditoria interna

Novos riscos

- Riscos oriundos da confiabilidade, integridade, disponibilidade, segurança, sigilo e gestão do consentimento
- Outros riscos de negócio também devem ser incorporados no escopo das funções de controle e da auditoria interna
- Avaliação e atualização no perfil de risco atual, incluindo ações de mitigação de forma a cobrir todo o universo de risco

Processos e Controles

- Implementação de processos e controles a fim de garantir a confiabilidade, a disponibilidade, a integridade, a segurança e o sigilo do compartilhamento de dados e serviços, incluindo a convergência com os dados do SRO

Compliance dos Requisitos Regulatórios

- Além dos prazos, os requisitos regulatórios estão sendo construídos e detalhados em tempo de implementação pelo mercado, agravando o risco de Compliance e abrindo fontes de novos riscos com a implementação
- Requisitos são complexos em temos operacionais e abrangem áreas que tipicamente são fontes significativas de riscos

Governança e Políticas

- Por se tratar de um projeto "cross", as companhias por vezes não possuem uma governança definida para o projeto, com papeis e responsabilidades bem definidos, atuando por meio de silos
- Atuação limitada das funções de controle e auditoria interna nos programas de implementação

Dados e Sistemas

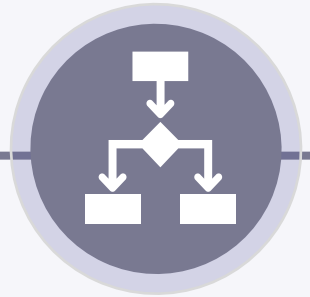
- Investimento massivo em dados e sistemas a fim de viabilizar as exigências do Open Insurance
- Requer, todavia, sistematização do monitoramento contínuo dos riscos pelas áreas de controle e supervisão, reportando resultados e atuando em ações de resposta tempestivas

Consideramos que este papel será chave em 3 pilares principais: Governança e Política, Processos e Controles, além de Dados e Reporte

Pilares de Atuação

Governança e Política

- Impulsiona a transparência no tratamento de riscos do programa, incluindo identificação, registro e gerenciamento;
- Garante que haja estrutura e processos com papeis e responsabilidades definidos, além de políticas que aculturem e normatizem as diretrizes corporativas.



Processos e Controles

- Determina a avaliação dos processos para identificar riscos, controles e lacunas de controles no inventário, além de auxiliar no mapeamento da infraestrutura de tecnologia da companhia a fim de encontrar ou determinar gaps face aos requisitos regulatórios ou das diretrizes corporativas.

Dados e Reporte

- A partir de reportes contínuos, é possível entender o progresso da implementação das exigências, avaliar/desenhar os mecanismos de acompanhamento e controle e garantir um plano de ação tempestivo

A atuação das Funções de Controle tem um papel primordial na implementação do *Open Insurance* a fim de apoiar o desenho do processo futuro em Compliance com as exigências regulatórias e atuar na identificação de riscos tempestivamente

A Governança e Política devem ser claras e constantemente avaliadas para garantir o tratamento adequado aos riscos

Pilares de Atuação

Governança integrada

Um dos principais fatores que limitam qualquer programa de transformação é a disponibilidade das equipes em apoiar e se envolver com a implementação. Criar um ambiente favorável é vital para o sucesso do programa.

- **A estratégia precisa estar definida com todos os stakeholders internos** de forma a garantir os investimentos que se façam necessários para a implementação dos requisitos.
- **As funções de controle devem participar e integrar o programa de implementação**, avaliando os riscos e controles do projeto, a fim de evitar retrabalho no futuro ou mitigar riscos decorrentes da implementação
- A Auditoria Interna deve se manter independente, mas alavancar o espectro dos riscos geridos pelas demais linhas de defesa e se **concentrar naqueles riscos relevantes e/ou não observados para cobertura total do risco**

Revise as Políticas imediatamente

- As funções de controle devem apoiar a administração na revisão das Políticas de Gestão de Riscos, Controles Internos, Plano de Continuidade de Negócio, Governança de Dados e Segurança de Informação
- As políticas devem **prever os requisitos regulatórios** e, não obstante, **a estratégia da companhia em lidar com as especificidades do seu negócio e dos riscos assumidos**

Se prepare para o Relatório Anual

- O Relatório Anual referente ao compartilhamento de dados e serviços deverá ser aprovado em Conselho, sendo objeto de auditoria, tanto interno quanto de fiscalização do regulador, e de reponsabilidade do Diretor nomeado
- Deverá ser apresentado em até 90 dias da data base de dezembro

A Governança e Política

Governança integrada entre as linhas para entregar, inovar e garantir o Compliance alinhado com a estratégia da Seguradora **Nomeação de um Diretor responsável** pelo compartilhamento

Rever as políticas de riscos que são impactadas pelo Open Insurance (Gestão de Riscos, PCN, Segurança etc.) garantindo tratamento adequado aos requisitos mínimos

Comunicar constantemente e reforçar a estratégia de implementação para articulação interna e externa entre as diversas frentes em um cenário dinâmico de revisões técnicas

Incluir os processos (novos ou alterados) **no escopo de atuação** das funções de controle e no **plano de auditoria**, avaliando gaps e oportunidades do programa para a administração

Apoiar a definição de estratégias de mitigação de riscos ainda na fase de desenho da solução

Estabelecer pessoas dedicadas para acompanhar as discussões internas e externas antecipando desafios e impactos na implementação e operação

Os Processos e Controles implementados precisam ser construídos de forma atender ao requisito definido pelo regulador e a estratégia da companhia

Pilares de Atuação

Reavalie seu modelo

Pense em quais serviços você deve fornecer e o que deve parar, o que poderia ser feito por um terceiro e **o que você precisa melhorar, investir para garantir o atendimento aos requisitos do Open Insurance**

Identifique o impacto no perfil de risco da Seguradora

- Avalie quais mudanças necessárias para atender o Open Insurance em termos de processos e desenvolvimentos em sistemas e dados e **identifique os riscos no perfil de risco da Seguradora**
- Como parte da função de controle, **compile e direcione as questões de risco/controles a gestão executiva/conselho**
- **Estabeleça procedimentos em caso de indisponibilidade, prazo de reinício ou normalização, tratamento de incidentes e execução dos testes**
- Como **auditoria interna, avalie quais testes devam ser percorridos** com vistas a assegurar a confiabilidade, a disponibilidade, a integridade, a segurança e o sigilo do compartilhamento de dados e serviços, bem como a implementação e a efetividade dos requisitos

Faça parte da mudança "gradual" dos processos e dos testes no plano

- **Cubra todo o universo de risco para organização** considerando os impactos trazidos com o Open Insurance no modelo operacional com o atendimento aos requisitos regulatórios
- Realize uma **análise completa da causa raiz/origem e um monitoramento contínuo dos riscos** identificando problemas em tempo real
- Forneça **reportes tempestivos a alta liderança dos resultados do monitoramento**

B Processos e Controles

Cobrir todo o universo de risco para a organização, considerando os requisitos regulatórios e a estratégia da companhia

Planejar o monitoramento contínuo de risco usando painéis de controle e definir as ações corretivas como, por exemplo, para incidentes, fraudes ou desempenho das interfaces

Apoiar no desenho dos controles e realizar testes de auditoria ainda na fase de desenho do programa, quando possível

Reportar resultados seguindo a governança estabelecida na Seguradora com vistas aos mecanismos de controle e ao plano de auditoria

Manter disponível e assegurar as informações necessárias para atender ao regulador como, por exemplo, os testes de controles, resultados e ações de correção

Incluir no programa de testes a observância do consentimento, os dados e registros, a estratégia e resultados da continuidade do negócio, e a segurança das informações

Os Dados e Reporte trazem consigo um desafio a parte: não são cobertos hoje pelas companhias e precisam atender o relatório anual da companhia

Pilares de Atuação

Novos dados disponíveis

No novo ambiente de dados abertos, haverá **um conjunto de dados atualmente não disponíveis pelas Seguradoras que requerem atenção** sobre o seu uso e tratamento a fim de manter sigilo e seguro as informações do cliente

- De um lado, **as transmissoras de dados e serviços** deverão garantir a confiabilidade, integridade, disponibilidade, segurança e sigilo realizando a gestão do consentimento do segurado
- Do outro, **as receptoras de dados e serviços** deverão manter os dados e trata-los observando o consentimento do segurado, em relação aos tipos de dados, a finalidade do uso e respectivo prazo

Neste sentido, deve-se **observar a governança de dados e registrar as demandas** dos clientes e dos canais de atendimento para compartilhamento de dados e serviços, além da **autenticação, da confirmação e da revogação do consentimento dos clientes**

Resolva alguns desafios imediatos

- Disponibilidade tempestiva de dados, sua confiabilidade e integridade são fatores críticos que as Seguradoras por vezes possuem
- É imprescindível que haja um acompanhamento e um programa robusto sobre os controles dos processos geradores destas informações

Reporte anual

- Adicionalmente, as Seguradoras deverão reportar ao regulador um Relatório Anual, a ser aprovado pela administração, com uma série de informações sobre registros de demandas (clientes, canal), incidentes, testes, monitoramento etc.
- É crucial o planejamento antecipado dos riscos envolvidos nessa elaboração, garantindo a sua integridade e disponibilidade dos dados a serem reportados.

C Dados e Reporte

Confiabilidade dos dados transmitidos requer atenção e devem refletir corretamente os tipos de dados consentidos pelo segurado e sua experiência com a Seguradora

Integridade dos dados transmitidos nos padrões estabelecidos no sistema aberto

Disponibilidade dos dados no ato de consentimento do segurado, viabilizando a transmissão da informação, observando as regras estabelecidas no sistema aberto

Segurança dos dados transmitidos e recepcionados com controles para garantir corretamente o teor do consentimento do segurado, e monitoramento e ações corretivas em casos de violação

Gestão do consentimento com controles sobre a autenticação, confirmação e revogação, incluindo as credenciais de identificação dos clientes

Reporte anual ao regulador de demandas do cliente e canais de atendimento, dos incidentes e resultados dos testes, das chamadas e desempenho das interfaces com **integridade, disponibilidade e confiabilidade**

Neste sentido, recomendamos que as áreas se prepararem e antecipem as necessidades para garantir o Compliance regulatório e mitigar riscos decorrentes do novo ambiente aberto

Pilares de Atuação

01 Definir Estratégia e Estrutura de entrega

- Defina a estratégia para apoiar na implementação
- Destine recursos internos para acompanhar as discussões acerca da implementação e avaliar antecipadamente impactos no perfil de risco da seguradora
- Aborde gaps de processos, pessoas dados, segurança, tecnologia
- Identifique os principais riscos para acompanhamento da implementação.

02 Definir e Revisar a Governança e Políticas

- Reveja as políticas de riscos que são impactadas pelo Open Insurance (ERM, PCN, Cyber etc.) garantindo tratamento adequado aos requisitos mínimos
- Defina o Diretor responsável de compartilhamento
- Estabeleça a governança do programa incluindo a 2ª e 3ª linha, antecipando riscos na implementação e operação

03 Identificar o Gap de Cobertura dos Riscos

- Identifique o impacto no perfil de risco com as alterações nos processos, dados e sistemas, incluindo o atendimento aos requisitos e prazos regulatórios
- Avaliar as ações de mitigação dos riscos de forma a cobrir todo o universo de risco

04 Certificar os Controles e Criar ações Mitigatórias

- Apoiar e testar a implementação de processos e controles a fim de garantir a confiabilidade, a disponibilidade, a integridade, a segurança e o sigilo do compartilhamento de dados e serviços
- Atualizar, implementar e executar o plano de continuidade de negócio considerando, no mínimo, procedimentos, prazo, tratamento e resultados

Plano de implementação

Crie um plano claro e tático para garantir a cobertura de todos os riscos envolvidos, o atendimento aos requisitos regulatórios e participe do programa de implementação antecipando riscos e garantindo os princípios do OPIN

A EY se posiciona como a parceira para essas iniciativa dada sua experiência no tema e trânsito fluído entre os agentes de mercado

Why EY?

Conhecimento em Open Insurance

Estamos apoiando a governança da implementação do OPIN para determinação dos requisitos técnicos, procedimentos operacionais e escopo de dados e serviços

- Atuamos na definição das características técnicas do sistema conforme demandas regulatórias
- Mediamos a deliberação de padrões tecnológicos e procedimentos operacionais para compartilhamento de dados
- Auxiliamos na convergência de interesses na definição de direitos e obrigações dos diversos players

Profundo conhecimento no mercado Segurador

Somos especializados no mercado Segurador...

... possuímos uma forte experiência e credenciais únicas no mercado brasileiro

... temos experiência relevante em projetos de Seguros relacionados a pesquisas, estratégia, regulação, dados, tecnologia e transformação

... apresentamos atuação relevante junto aos principais Stakeholders, que nos permite conhecer de forma atempada as principais discussões

... participamos de discussões regulatórias e de requerimentos atuais

Por que EY?

Condução de projetos regulatórios

Temos vastar experiência com projetos regulatórios

- Apoio perante o regulador nas discussões relacionadas a diversos temas do mercado segurador (contábil, investimentos, proteção do mercado, regulação etc.)
- Debates junto a diversos stakeholders internos e externos, incluindo órgãos públicos como SPE, IMK e outras entidades de regulação suportando tecnicamente o posicionamento do mercado segurador
- Elaboração de diversos estudos técnicos junto a CNSEG e suas federações

Especialista em Open Finance

Somos especialistas em Open Finance

- Parceiro selecionado para condução do projeto de Open Investment - Fase 4 do *Open Banking*
- Monitoramento Independente do andamento da Implementação do OB Fase 2 e 3 em 11 Conglomerados S1 e S2 com reporte semanal ao BACEN
- Suporte a Banco S1 na frente de Dados para Open Banking
- Suporte a 2 bancos S1 na operacionalização do Open Banking
- Suporte a Fintech no desenho das jornadas de onboarding e autenticação para PISP

Os profissionais da EY apresentam experiência relevante em Seguros e está preparado para atender de maneira efetiva

Nossos Contatos

Nuno Vieira
Sócio líder do Setor de Seguros para Latam South
E-mail: nuno.vieira@br.ey.com

Marcelo Lustosa
Sócio de Riscos e Regulação no Mercado de Seguros
E-mail: marcelo.lustosa@br.ey.com

Demétrio Carrion
Sócio de Cybersecurity
E-mail: demetrio.carrion@br.ey.com

João Herculano
Sócio de Technology Risk
E-mail: joao.herculano@br.ey.com

Chen Wei Chi
Sócio de Serviços Financeiros – Líder Transformação de Negócios
E-mail: chen.weichi@br.ey.com

Natália Grigolin
Gerente Sênior de Prevenção a Lavagem de Dinheiro
E-mail: natalia.grigolin@br.ey.com

Yolanda Gonçalves
Gerente de Cybersecurity
E-mail: Yolanda.Goncalves@br.ey.com

Telma Luchetta
Sócia de Data & Analytics
E-mail: telma.pexe@br.ey.com

The better the question. The better the answer.
The better the world works.