Request for Proposal

Fornecedor para o Plano Integrado de Segurança da Informação e Prevenção a Fraudes em favor do processo de implementação do Open Insurance Brasil

São Paulo, junho de 2023

Conteúdo

1. Introdução

O Conselho Nacional de Seguros Privados (“CNSP”), no uso de suas atribuições, publicou a Resolução CNSP nº 415, de 20.07.2021 que dispõe sobre a implementação do Sistema de Seguros Aberto (“Open Insurance”). Por sua vez, a Superintendência de Seguros Privados (“SUSEP”) expediu a Circular SUSEP nº 635, de 20.07.2021, que dispõe sobre a regulamentação das diretrizes estabelecidas pelo CNSP para implementação do Open Insurance.

A referida Circular SUSEP nº 635/21 estabelece um cronograma de implementação, que teve início em 15 de dezembro de 2021, com o compartilhamento dos dados sobre canais de atendimento e produtos de seguros, previdência complementar aberta e capitalização disponíveis para comercialização, e contempla a implantação de serviços até junho de 2023.

A Estrutura Inicial responsável pela governança do processo de implementação do Open Insurance foi devidamente formalizada em agosto de 2021, contemplando três níveis: (i) estratégico, (ii) administrativo, e (iii) técnico.

O nível estratégico é integrado por um Conselho Deliberativo composto por até 06 (seis) conselheiros, indicados por 06 (seis) grupos, sendo 05 (cinco) de sociedades participantes e 01 (um) por um conselheiro independente. O Conselho Deliberativo é responsável por definir as diretrizes estratégicas para implementação do Open Insurance no Brasil.

O nível administrativo é composto pelo Secretariado integrado por um Secretário-Geral, responsável por executar as atividades operacionais e administrativas necessárias para o bom funcionamento da Estrutura Inicial responsável pela governança do projeto do Open Insurance, e suas respectivas equipes de apoio.

O nível técnico, por sua vez, é composto por Grupos Técnicos, formados por um Coordenador, um coordenador substituto e um número máximo de membros, indicados conforme Regimento Interno. Estes Grupos são responsáveis por apresentar as propostas técnicas para implementação do Open Insurance.

A Estrutura Inicial vigorará até 31 de outubro de 2022, podendo, no entanto, ser substituída a qualquer momento por uma estrutura definitiva responsável pela governança.

2. Objetivo

O objetivo desta RFP é receber propostas de fornecedores interessados em prestar os serviços de Avaliação, Implantação e Operação de Gestão de Segurança da Informação, de forma que se possa selecionar o fornecedor que melhor atenda às condições exigidas neste edital.

Por meio da análise das propostas recebidas, pretende-se identificar (i) sua capacidade para prestar os serviços aqui pretendidos; (ii) experiência prévia no âmbito do Open Insurance e Open Finance; e (iii) experiência prévia no mercado segurador.

3. Escopo

O escopo desta RFP é um *assessment* dos processos e tecnologias da Estrutura do Open Insurance relacionados à Segurança da Informação, e a construção e operação de um Plano Integrado de Segurança da Informação e Prevenção a Fraudes no Open Insurance Brasil. Os requerimentos mínimos e escopo dos serviços, bem como certas informações a serem fornecidas pela Estrutura Inicial, como parte de sua proposta, estão definidas nas seções abaixo.

Está fora do escopo desta RFP a realização de atividades nos ambientes tecnológicos das sociedades participantes do Open Insurance Brasil, limitando-se ao ambiente tecnológico centralizado da Estrutura.

3.1. Requerimentos gerais da RFP

O Fornecedor deve prover toda a gestão, profissionais, equipamentos, bens e suprimentos necessários para prestar serviços profissionais necessários e todas as condições desta RFP, incluindo, mas não se limitando, às especificações descritas na seção 3.2.

Para a estrutura do ambiente deverá ser utilizada uma das três (3) provedoras de solução em cloud do mercado, abaixo listadas, em ambientes hospedados no Brasil.

- AWS;

- Azure;
- GCP.

Os custos operacionais da estrutura serão de responsabilidade do Fornecedor da solução durante a vigência do contrato de prestação de serviços.

Qualquer plataforma utilizada deve preferencialmente ser integrada ao Diretório de Participantes do Open Insurance Brasil para fins de autenticação.

3.2. Requerimentos específicos de trabalho

A Estrutura Inicial busca apoio do Fornecedor para a elaboração e operação de um Plano Integrado de Segurança da Informação e Prevenção a Fraudes no Open Insurance Brasil.

Os requerimentos mínimos e escopo dos serviços são definidos abaixo, assim como requerimentos adicionais a serem executados conforme avaliação da Estrutura Inicial, mediante Ordens de Serviço.

3.2.1. Requerimentos mínimos

Esta seção descreve os requerimentos da execução contínua do Plano Integrado de Segurança da Informação e Prevenção a Fraudes:

i. Identificação dos objetivos estratégicos para Segurança da Informação;

ii. Avaliação de *gaps* em requisitos de segurança com base nos manuais e normativos de segurança da SUSEP;

iii. Avaliações de *gaps* em requisitos de segurança com base nos controles descritos em *frameworks* ou padrões de Segurança da Informação, como por exemplo ISO 27001 ou NIST;

   a. Não é necessário que os frameworks propostos se limitem aos mencionados acima, ou que as propostas se limitem a um único framework;

   b. Não é considerada parte do escopo a realização do processo de obtenção de certificações de segurança em algum *framework* ou padrão pela Estrutura;

iv. Avaliação técnica do ambiente da Estrutura para identificação de *gaps* e vulnerabilidades;

v. Construção de visão dos principais riscos de fraudes inerentes as atividades da Estrutura e do ecossistema;

vi. Desenho de política, normas, procedimentos e demais documentos necessários para a implementação das especificações de segurança;

   a. Também deve contemplar o mapeamento de necessidades de ajustes contratuais com fornecedores da Estrutura para acomodar atividades não previstas.

vii. Criação e adequação dos processos e tecnologias;

viii. Estruturação dos processos e controles de prevenção a fraude;

ix. Estabelecimento de KRIs/ KPIs;

x. Estabelecimento de Programa de Conscientização interno e externo;

xi. Estruturação do Plano de Ação e Resposta a Incidentes;

xii. Estabelecimento de processos de classificação de informação;

xiii. Mapeamento dos principais ativos de SI da Estrutura;

xiv. Definição, implementação e operação do SOC;

xv. Gestão de Vulnerabilidades e Patches nas camadas de infraestrutura e códigos de propriedade do Open Insurance. A solução proposta deve suportar futura integração com *pipelines* de CI/CD;

xvi. Avaliação de comportamentos anômalos no ambiente;

xvii. Monitoramento dos ambientes do ecossistema e dos fornecedores;

   a. Tecnologias que possam monitorar o ambiente tecnológico de fornecedores envolvidos na entrega do Open Insurance são desejáveis, porém na inexistência de tais tecnologia um

modelo de gestão processual é aceitável;

xviii. Monitoramento de *deep web* / *dark web* (Threat Intel);

xix. Prevenção a fraudes através de análises em dados provenientes do ecossistema;

a. A principal fonte de dados a ser considerada é a Plataforma de Coleta de Métricas, que armazena métricas de compartilhamento de dados e serviços dos participantes do ecossistema.

b. Monitoramento de mercado sobre casos de fraudes nos sistemas Open e demais ambientes (órgãos de controle como CNSEG, FENASEG, FEBRABAN etc.)

3.2.2. Requerimentos adicionais executados mediante Ordens de Serviço

Os requerimentos desta seção representam requisitos adicionais a serem executados conforme demanda do contratante, portanto não devem constar no Cronograma referencial de implementação, porém devem estar presentes na Proposta técnica submetida e precificados individualmente na Proposta comercial, para que sejam executados pontualmente mediante Ordens de Serviço, conforme seção 3.2.3.

i. Avaliação técnica periódica do ambiente da Estrutura para identificação de *gaps* e vulnerabilidades;

ii. Aplicação periódica de *Assessments* de Segurança da Informação em fornecedores críticos;

iii. Execução de cenários de incidentes de testes de continuidade de negócios e planos de ação e resposta a incidentes;

iv. Realização de um fórum de disseminação da cultura de segurança cibernética;

a. Deve contemplar as opções de que o fórum seja realizado virtualmente, ou localmente.

v. Processo periódico/automatizado de busca de dados pessoais armazenados no ambiente (PII)

vi. Realização periódica de testes de penetração;

vii. Realização periódica de outros testes de segurança no ambiente;

a. Como por exemplo (mas não limitadas a) engenharia social, de testes de *red team* / *blue team;*

viii. Realização de auditorias em fornecedores;

Além de demais atividades identificadas caracterizadas por uma execução pontual.

3.2.3. Ordens de Serviço

Além das atividades contidas na presente RFP, as Partes (Cliente e Fornecedor) poderão celebrar Ordens de Serviço adicionais para a efetiva implementação da estrutura do Open Insurance Brasil. As ordens de serviços significam uma solicitação de Serviço submetida pelo Cliente, que atua em nome e por conta e ordem das Participantes, ao Fornecedor, devidamente assinada por ambas as Partes, e que será regida pelas disposições e termos do contrato posteriormente firmado.

O prazo da Ordem de Serviço começa na Data de Entrada em Vigor do contrato e continuará por 12 (doze) meses (Prazo Inicial da Ordem), a menos que seja extinta (total ou parcialmente). O Prazo Inicial ou qualquer prazo de renovação em andamento será renovado automaticamente, por períodos iguais e sucessivos de 12 (doze) meses (“Prazo de Renovação da Ordem”), a menos que uma das Partes manifeste intenção expressa de não renová-lo (total ou parcialmente), mediante notificação por escrito à Parte contrária com antecedência mínima de 6 (seis) meses em relação ao término do Prazo Inicial ou do Prazo de Renovação da Ordem de Serviços em andamento, e observado, em caso de não renovação, o Período de Transição estabelecido no Contrato.

Em qualquer das hipóteses de Extinção de uma Ordem de Serviço, o Fornecedor deverá, a critério e sob requerimento do Cliente, continuar prestando os Serviços referentes à Ordem de Serviço em questão e cumprindo suas obrigações contratuais por um período de transição de 6 (seis) meses, para permitir que o Cliente negocie, celebre e implemente contrato análogo com outro fornecedor (“Período de Transição”).

É facultado ao Cliente dispensar o Período de Transição, no todo ou em parte dentro de 90 (noventa) dias do início do Período de Transição, as Partes vão acordar mutuamente em relação a um plano de migração para o Cliente ou para um terceiro indicado pelo Cliente dos dados contidos nos sistemas do Fornecedor ou armazenados pelo Fornecedor (ou por terceiros contratados pelo Fornecedor); e dos contratos com terceiros que devam ser mantidos válidos para a continuidade da utilização das Entregas e demais frutos da Ordem de Serviço em questão (“Plano de Migração”). O Plano de Migração deverá conter o prazo que a migração deverá ser concluída.

O Fornecedor deverá entregar ao Cliente toda a documentação técnica e outros documentos e materiais necessários para a continuidade dos Serviços englobados pela Ordem de Serviço em questão; e o Cliente e as Participantes continuarão a ter acesso aos sistemas como costumavam ter durante o prazo regular do Contrato inicial.

4. Conteúdo mínimo da proposta comercial

Para ser elegível para avaliação, uma proposta deve cumprir pelo menos as seções definidas abaixo; o não cumprimento pode resultar em desqualificação. Os respondentes devem preencher, rotular e separar cada seção e numerar todas as páginas. O conteúdo e a sequência da proposta devem ser como demonstrados abaixo:

- Capa;
- Sumário;
- Lista de anexos;
- Apresentação da empresa;
- Proposta técnica que atenda a todo o escopo desta RFP;
- Proposta técnica adicional ao escopo;
- Cronograma referencial de implementação;
- Proposta comercial;
- Estimativas e premissas para definição do modelo de negócios, se necessário.

As seções estabelecidas devem conter, no mínimo, as informações detalhadas abaixo:

4.1. Capa

a. Nome e endereço da empresa participante;
b. Nome, cargo, telefone e e-mail do responsável pela proposta, caracterizado como contato principal;
c. Data;
d. Versão do documento;

4.2. Apresentação da empresa:

a. Descrição da capacidade técnica e operacional para realizar/executar as atividades descritas no escopo desta RFP. Sugere-se destacar os seguintes tópicos:
   i. Experiência prévia em Gestão de Segurança da Informação e Prevenção a Fraudes;
   ii. Desejável: conhecimento prévio das operações do Open Insurance ou Open Finance em outros países;
b. Descrição das qualificações da empresa e da equipe responsável por realizar/executar as atividades descritas no escopo de trabalho desta RFP;
c. Apresentação da experiência da empresa para a realização/execução das atividades descritas no escopo desta RFP.
   i. Descrever a experiência da empresa com Gestão de Segurança da Informação e Prevenção a Fraudes;
   ii. Apresentar pelo menos dois casos de implementação bem-sucedida de Gestão de Segurança da Informação e Prevenção a Fraudes.

4.3. Proposta técnica que atenda a todo o escopo desta RFP:

a. Detalhamento da solução proposta, fornecendo uma descrição das características e requisitos,

incluindo:

i. Descrição das atividades, governança, papéis e responsabilidades da solução proposta;

ii. Descrição da arquitetura técnica da solução e suas características em termos de escalabilidade, disponibilidade e segurança;

iii. Descrição das funcionalidades a serem desenvolvidas para a solução, se houver.

4.4. Proposta técnica adicional ao escopo (se houver):

a. Detalhes da solução técnica adicional proposta, fornecendo uma visão macro dos entregáveis e requisitos;

b. Descrição da arquitetura técnica da solução, se houver;

c. Descrição da interlocução do escopo adicional proposto com o escopo definido nesta RFP.

4.5. Cronograma referencial de implementação

a. Detalhes do cronograma estimado para implantação da solução, contendo prazos para entregas e validações;

b. Levantamento das principais entradas e dados necessários que devem ser enviados pela Estrutura Inicial.

4.6. Proposta comercial

a. Equipe envolvida na solução e se em tempo integral ou parcial;

b. Premissas de preços, se aplicáveis (por exemplo, número de horas de manutenção);

c. Valor mensal, com detalhamento dos valores das variáveis, se for o caso.

4.7. Estimativas e premissas para definição do modelo de negócios (se necessário)

a. Estimativas e premissas para definir o modelo comercial (por exemplo, número dos usuários);

b. Especificação dos números/suposições utilizadas.

É fundamental que a empresa possa atender a todo o escopo contido nesta RFP.

Em caso de diferenças significativas entre as respostas fornecidas pelas empresas participantes, espera-se que a Estrutura Inicial entre em contato para obter informações adicionais e/ou estimativas.

5. Cronograma

As propostas devem ser submetidas pelas empresas participantes no prazo estabelecidos conforme o cronograma abaixo:

Atividade	Responsável	Data limite
Envio do RFP aos potenciais participantes	Secretariado	12/06
Confirmação da Participação por e-mail e envio de perguntas sobre a RFP	Participante	19/06
Envio de Respostas às Perguntas sobre RFP	Secretariado	26/06
Entrega da Proposta Técnica e Comercial	Participante	03/07
Comunicação dos resultados do RFP	Secretariado	24/07

6. Diretrizes de aplicação

As propostas devem ser submetidas pelas empresas participantes no prazo estabelecidos conforme o cronograma da seção 5.

As propostas devem ser enviadas para o e-mail secretariado@opinbrasil.com.br, com assunto [RFP Segurança da Informação][Proposta técnico-comercial] Nome da empresa.

Os arquivos das propostas devem ser enviados como anexo, em formato PDF.

A empresa participante reconhece que:

a. Entre a Estrutura Inicial e a empresa participante, não há vínculo ou compromisso, expresso ou implícito, de exclusividade ou contratação de serviços, e nenhuma outra relação está sendo estabelecida como resultado de receber qualquer informação, bem como, caso seja de interesse contratar os serviços, não determina nenhum dos seus termos, condições ou modelo contratual;

b. Este documento de RFP não constitui qualquer oferta, proposta ou pré-contrato.

A Estrutura Inicial reserva-se ao direito de alterar o escopo do trabalho apresentado, para desistir ou alterar qualquer um dos requisitos contidos neste documento de RFP, a qualquer momento, sem incorrer em qualquer ônus ou ressarcimento às empresas que apresentarem suas propostas.

Quaisquer dúvidas ou esclarecimentos sobre este processo de RFP devem ser enviadas para os e-mails descritos acima.

7. Alterações e Cancelamento desta RFP

A Estrutura Inicial reserva-se ao direito de emitir alterações a este documento de RFP e revisar, alterar, modificar ou corrigir qualquer uma de suas partes.

A Estrutura Inicial também se reserva ao direito de cancelar está RFP, a qualquer momento e, nesse caso, a empresa não tem direito a qualquer tipo de indenização.

Este documento e quaisquer propostas apresentadas não representam qualquer obrigação ou promessa da Estrutura Inicial de adquirir qualquer produto ou serviço oferecido ou apresentado por uma empresa.

8. Proposta Comercial

Ao responder à RFP, a empresa deve estar ciente de que a proposta é uma oferta formal de prestação de serviços à Estrutura Inicial e permanecerá válida por pelo menos 120 (cento e vinte) dias a partir do envio da RFP.

O preço dos serviços na proposta comercial deve ser definitivo, incluindo todos os impostos aplicáveis, e ser apresentado em reais (BRL).

Os pagamentos serão realizados e o contrato firmado com uma empresa brasileira ou uma entidade representativa do Fornecedor localizada no Brasil.

As condições de pagamento comercial propostas devem seguir as diretrizes da Open Insurance Brasil.

9. Contrato de Serviço

O contrato de prestação de serviços será assinado entre o Secretariado, por meio da Peers Consulting, em nome, por conta e ordem das participantes do Open Insurance Brasil, e o fornecedor por um período de 12 (doze) meses, e pode no futuro ser atribuído, em parte ou no todo, a critério da Estrutura Inicial, para a Estrutura Definitiva, que será a contratante final.

10. Resumo dos critérios de avaliação e próximos passos

As propostas técnicas e comerciais serão avaliadas pelo Conselho Deliberativo e pelos Grupos Técnicos envolvidos. A avaliação das propostas e a seleção pela vencedora será baseada em informações fornecidas pelas empresas participantes da concorrência.

A Estrutura Inicial selecionará, a seu exclusivo critério, as empresas, podendo rejeitar informações enviadas incompletamente ou aquelas recebidas após a data apresentada no cronograma de atividades.

As empresas participantes serão avaliadas com base em sua experiência e capacidade de fornecer suporte para a Estrutura Inicial, de acordo com o escopo definido na seção 3, incluindo, mas não se limitando a:

- Atendimento do prazo de implementação;
- Adesão ao escopo do trabalho proposto neste documento;
- Preço;
- Recursos técnicos e solução.

Durante o processo de avaliação, a Estrutura Inicial pode pedir às empresas que esclareçam informações sobre suas propostas. As empresas não serão autorizadas a fazer mudanças em suas propostas, a menos que explicitamente solicitadas pela Estrutura Inicial.

Um erro na proposta pode fazer com que a Estrutura Inicial a rejeite; no entanto ela pode, a seu exclusivo critério, mantê-la e fazer certas correções.

11. Confidencialidade

O conteúdo deste documento é de propriedade das empresas que compõem a Estrutura Inicial. Os fornecedores participantes somente poderão utilizá-lo para preparar suas propostas, que deverão ser apresentadas de acordo com o aqui estabelecido.

Desde já, o fornecedor participante deste processo obriga-se a manter em absoluta confidencialidade todas as informações, dados e documentos aos quais poderá ter acesso durante o processo.

Não poderá, portanto, divulgá-los, cedê-los, doá-los, repassá-los, vendê-los, reproduzi-los por quaisquer meios, ou transferi-los, a qualquer título, em qualquer tempo e circunstância, ainda que após o término desse processo, mesmo não sendo vencedor, tampouco usá-los em benefício próprio ou de terceiros ou para finalidade diversa da especificada neste edital, salvo mediante autorização expressa das empresas que compõem a Estrutura Inicial.

Desta forma, o fornecedor participante irá adotar todas as providências necessárias para que seus funcionários, técnicos, sócios e prestadores de serviços tomem ciência da natureza sigilosa do conteúdo deste documento e toda informação veiculada ao longo deste processo de concorrência, garantindo que respeitarão a integridade de sua guarda.

Todos os requisitos legais a que o fornecedor participante esteja submetido, especialmente no que se refere à coleta, processamento, manutenção, divulgação, descarte, segurança e proteção de dados pessoais deverão ser observadas.

O fornecedor participante, no caso de NÃO ser considerado vencedor ou um dos vencedores deste processo, obriga-se a destruir, imediatamente à data da divulgação do vencedor, todas as informações, dados e documentos aos quais terá acesso durante o processo.

12. Links úteis

Portal do Cidadão:

https://opinbrasil.com.br/

Portal do Participante:

https://opinbrasil.com.br/participante/como-participar/modelo-de-participacao/

Portal do Desenvolvedor:

https://br openinsurance.github.io/areadesenvolvedor/#introducao

Documentos de Referência – SUSEP:

https://www.gov.br/susep/pt-br/assuntos/open-insurance/documentos_de_referencia

Circular SUSEP nº 638 / 2021:

https://www.in.gov.br/en/web/dou/-/circular-susep-n-638-de-27-de-julho-de-2021-335760591

Manual de Segurança do Open Insurance

https://www.gov.br/susep/pt-br/assuntos/open-insurance/arquivos/manual-de-seguranca-do-open-insurance-v1-2.pdf

Especificação técnica da Plataforma de coleta de métricas

https://br-openinsurance.github.io/areadesenvolvedor/#plataforma-de-coleta-de-metricas

Workshops realizados – Destaque ao workshop de Apresentação da Plataforma de Coleta de Métricas

https://br-openinsurance.github.io/areadesenvolvedor/#workshops

Ferramenta de Implementação Open ID:

https://www.certification.openid.net/login.html