MANUAL DE SEGURANÇA

DO **OPEN INSURANCE**

Versão 1.3

Maio/2023

DETIC - DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO

Histórico de revisão

Data	Versão	Descrição das alterações
02/08/2021	1.0	Versão inicial.
02/06/2022	1.1	Inclusão de referências para as APIs da Fase 2 do Open Insurance e ajustes pontuais.
12/09/2022	1.2	Inclusão de referências para os serviços de iniciação de movimentação.
19/04/2023	1.3	Inclusão de requisitos de recertificação de certificados emitidos pela OpenID Foundation (conforme previamente comunicado através do OFÍCIO ELETRÔNICO Nº 1/2023/CGITI/DEATI/ SUPERINTENDENTE/SUSEP) e ajuste sobre o plano de resposta a incidentes de segurança.

Sumário

Apresentação

Este manual define as especificações de segurança no escopo do Open Insurance. A observância do disposto neste manual é obrigatória por parte das sociedades participantes, conforme definição prevista na regulamentação vigente.

Considerando o objetivo de compatibilidade entre o **Open Banking** e o **Open Insurance**, conforme previsto no inciso VII do art. 3º da Resolução CNSP nº 415, de 2021, este manual possui estrutura semelhante ao apresentado na Instrução Normativa BCB n° 99, de 2021, com adaptações necessárias para a realidade de produtos e serviços deste setor.

Termos de Uso

Este manual detalha os requisitos técnicos para a implementação dos elementos necessários à operacionalização do **Open Insurance**, complementando a regulamentação vigente sobre o tema.

O manual será revisto e atualizado periodicamente a fim de preservar a compatibilidade com a regulamentação, bem como para incorporar os aprimoramentos decorrentes da evolução do **Open Insurance** e da tecnologia.

Informações mais detalhadas e exemplos da aplicação deste manual poderão ser encontrados nos guias e tutorias disponíveis no Portal do **Open Insurance** no Brasil, na Área do Desenvolvedor (https://br-openinsurance.github.io/areadesenvolvedor/).

Sugestões, críticas ou pedidos de esclarecimento de dúvidas relativas ao conteúdo deste documento podem ser enviados à Susep por meio dos canais institucionais dessa autarquia ou diretamente através do e-mail openinsurance@susep.gov.br.

Referências

Estas especificações baseiam-se, referenciam, e complementam, quando aplicável, os seguintes documentos:

Referência	**Origem**
Resolução CNSP nº 415, de 2021	Normativo CNSP
Circular Susep nº 635, de 2021	Normativo Susep
Circular Susep nº 638, de 2021	Normativo Susep
Lei Geral de Proteção deDados (LGPD – Lei nº 13.709, de 2018)	http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm
BCP 195/RFC 7525	https://tools.ietf.org/html/rfc7525
Owasp API Top 10	https://owasp.org/www-project-api-security/
Sans Top 25 Software Erros	https://www.sans.org/top25-software-errors
CWE Top 25 SoftwareWeaknesses	https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html
NIST 800-88	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
DOD 5220.22-M	https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodm/522022m.pdf
ICP Brasil - Manual de Condutas Técnicas 7 –Volume I	https://www.gov.br/iti/pt-br/centrais-de-conteudo/mct-7-vol-1-v-2-2-pdf
Medida Provisória nº 2.200-2, de 24 de agosto de 2001	http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm

1. Introdução

Para garantir a segurança do **Open Insurance** no País, a regulamentação vigente estabelece a obrigatoriedade de se cumprir uma série de medidas, entre as quais as descritas neste manual.

Este manual detalha em termos operacionais as diretrizes de segurança estabelecidas pela Resolução CNSP nº 415 e pela Circular Susep nº 635, ambas de 2021. Ele contém tanto os requisitos mínimos de segurança obrigatórios para as sociedades participantes como para os demais elementos que compõem a Estrutura Responsável pela Governança do **Open Insurance**. Adicionalmente, devem ser observadas todas as exigências regulamentares sobre segurança cibernética, conforme Circular Susep nº 638, de 20221

No tocante aos requisitos obrigatórios para as sociedades participantes, este manual apresenta as seguintes seções: 2. governança, 3. dados públicos, 4. proteção, 5. detecção e 6. reação. Os requisitos obrigatórios para a Estrutura Responsável pela Governança constam da Seção 7.

Este manual prescreve os requisitos mínimos de segurança necessários para:

I - o compartilhamento de dados sobre canais de atendimento e produtos de que trata os arts. 1º e 2º do Anexo III da Circular Susep nº 635 de 2021;

II - o compartilhamento de dados de cadastro e de transações de que trata os arts. 3º até 6º do Anexo III da Circular Susep nº 635 de 2021.

III – o compartilhamento de serviço de iniciação de movimentação conforme definido no art. 2º, inciso VIII, da Resolução CNSP nº 415, de 2021

À medida que o **Open Insurance** abranger o compartilhamento de outros dados e serviços, novos requisitos de segurança poderão ser acrescentados a este manual, em complemento à regulamentação aplicável.

Ao longo deste documento será constante o uso de siglas para designar algumas expressões cotidianas dos profissionais da área de segurança da informação. Alguns exemplos das mais frequentemente utilizadas, com as correspondentes definições, são as seguintes:

I- ACL: Access Control List;

II- API: *Application Programming Interface*;

III- ETIR: Equipe de Tratamento de Incidentes;

IV- HTTP: *HyperText Transfer Protocol*;

V- ICP-Brasil: Infraestrutura de Chaves Públicas Brasileira;

VI- IP: *Internet Protocol*;

VII- NTP: *Network Time Protocol*;

VIII- PFS: *Perfect Forward Secrecy;*

IX- PGP: *Pretty Good Privacy;*

X- TCP: *Transmission Control Protocol;*

XI- TLS: *Transport Layer Security;*

XII- URI: *Uniform Resource Identifier;* e

XIII- UTC: *Universal Time Coordinated.*

2. Governança

2.1 As sociedades participantes do **Open Insurance** devem atender aos dispositivos aplicáveis da legislação e regulamentação vigente no país. Além disso, possuem a obrigação de acompanhar a edição e a revogação de eventuais normas com impacto no tema de forma a estar permanentemente em dia com as determinações legais.

2.2 Compõem, de forma não exaustiva, o rol de atos normativos cuja observância é essencial pelas sociedades participantes do **Open Insurance**:

I- Resolução CNSP nº 415, de 2021;

II- Circulares editadas pela Susep aplicáveis às sociedades participantes que dispõem sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e computação em nuvem; e

III- a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709, de 2018).

2.3 O plano de ação e resposta a incidentes das sociedades participantes deve abranger os procedimentos e os controles a serem utilizados na prevenção e resposta a incidentes que afetem sistemas, APIs e outros recursos relacionados à implementação e à operação do **Open Insurance**, de forma compatível com a política de segurança cibernética da sociedade e com a regulamentação vigente.

2.4 As sociedades participantes devem definir procedimentos e controles voltados à prevenção e ao tratamento de incidentes a serem adotados pelas empresas prestadoras de serviços a terceiros que manuseiem dados ou informações requeridas para a condução das atividades relativas ao **Open Insurance**, em compatibilidade com a política de que trata o item 2.3 e com a regulamentação vigente.

2.5 Os procedimentos e controles de que trata o item 2.4 devem ser divulgados às empresas prestadoras de serviços mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e sensibilidade das informações.

2.6 As sociedades participantes, previamente à contratação de serviços requeridos para a condução das atividades relativas ao **Open Insurance**, devem adotar procedimentos que contemplem a verificação da capacidade do potencial prestador de serviço de assegurar o cumprimento da legislação e da regulamentação vigente.

2.7 As instituições devem armazenar e processar os dados discriminados na etapa de consentimento segundo a finalidade para a qual foram compartilhados e de maneira segura, observadas a legislação e a regulamentação vigentes.

2.8 As sociedades participantes devem manter suas informações cadastrais permanentemente atualizadas no Diretório de Participantes do **Open Insurance**, observada a regulamentação vigente.

2.9 As sociedades participantes devem manter as suas certificações de segurança emitidas pela OpenID Foundation (OIDF) ativas e realizar a recertificação de acordo com as diretrizes a seguir. Estas diretrizes são válidas para todas as certificações de segurança emitidas pela OpenID Foundation (OIDF) no contexto do Open Insurance (FAPI, DCR, RP e CIBA).

Validade

Serão necessárias recertificações quando:

I. Houver exigência da Estrutura Responsável pela Governança do **Open Insurance,** motivada por mudança de versão de documentações OIDF ou no FAPI-BR, independente do tempo desde a última certificação.

- As mudanças na documentação serão analisadas pela Estrutura de Governança do **Open Insurance** e a necessidade de recertificação será comunicada às sociedades participantes.

II. Houver alteração de tecnologia e/ou infraestrutura de produção utilizada pela sociedade participante, independente do tempo desde a última certificação:

- Plataforma de hospedagem, tais como: AWS, Azure, Google Cloud, etc.;

- Tecnologias de plataforma OPIN. Exemplo: mudança de solução de mercado para desenvolvimento interno.

III. A certificação anterior completar 12 meses desde a data de submissão.

Submissão

O pedido de certificação deve ser submetido até a data de expiração e todo o processo deve ser concluído em até 60 dias após a data de expiração.

3. Proteção

3.1 O acesso aos dados e ao serviço de iniciação de movimentação relacionados a seguros no âmbito do **Open Insurance** deve ser realizado exclusivamente por meio de APIs.

3.2 Os sistemas e APIs relacionados ao **Open Insurance** devem ser mantidos em rede interna segregada logicamente de redes ordinariamente utilizadas por estações de trabalho ou redes sem fio.

3.3 As sociedades transmissoras de dados devem implementar controles de tráfego de entrada e saída, de forma a permitir apenas o necessário para comunicação com as APIs de **Open Insurance**.

3.4 As sociedades devem implementar criptografia na comunicação com as APIs de **Open Insurance** expostas publicamente, por meio doprotocolo TLS na versão 1.2 ou superior, utilizando cifras (*cipher suites*) que atendam ao requisito de *perfect forward secrecy* (PFS).

3.5 As funcionalidades "TLS *Session Resumption*" e "TLS *Renegotiation*" devem ser desabilitadas.

3.6 As sociedades devem aplicar controles de segurança na camada de aplicação que permitam a inspeção de ameaças e o bloqueio de ataques de injeção de código, entre outros, adequados às tecnologias utilizadas nas APIs.

3.7 As sociedades não devem expor os repositórios de dados utilizados no **Open Insurance** diretamente à internet.

3.8 As sociedades participantes devem verificar e garantir que a quantidade, a ordem, o formato, o tamanho e o conteúdo dos campos das requisições de acesso às APIs, bem como suas respostas, estejam de acordo com os estabelecidos pelas definições de **Open Insurance**.

3.9 Para a comunicação segura com APIs e assinatura de mensagens no âmbito do **Open Insurance**, devem ser utilizados certificados digitais válidos, emitidos por autoridade certificadora participante da ICP-Brasil, de acordo com os padrões para certificação digital estabelecidos pela Estrutura Responsável pela Governança do **Open Insurance**.

3.10 Os certificados digitais de que trata o item 3.9 devem contemplar mecanismos para a proteção dos canais de comunicação e para a assinatura ou criptografia de mensagens trocadas com APIs.

3.11 Admite-se, enquanto os certificados digitais de que trata o item 3.9 não estiverem disponíveis, o uso de certificados digitais emitidos pelo serviço de Diretório da Estrutura Responsável pela Governança do Open Insurance.

3.12 O disposto nos itens 3.9 e 3.10 aplica-se, no que couber, aos certificados requeridos para as contratações de parceria para fins de compartilhamento de dados previstas na regulamentação vigente.

3.13 Para o estabelecimento de conexões TLS das chamadas de *endpoints* confidenciais devem ser utilizados os seguintes algoritmos:

I- 'TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256'; e

II- 'TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384'.

3.14 Os certificados utilizados para comunicação de sistemas *Front-End*, acessados diretamente por clientes das sociedades participantes, em especial para realizar autenticação, devem ser do tipo *Extended Validation* (EV) e podem ser emitidos por autoridade certificadora em funcionamento.

3.15 Os procedimentos e controles relativos à criptografia devem contemplar meios seguros de armazenamento, transferência, utilização e destruição de segredos ou chaves empregados no âmbito do **Open Insurance**, observada a regulamentação vigente.

3.16 Recomenda-se utilizar os seguintes algoritmos criptográficos para proteção e armazenamento de segredos no âmbito do **Open Insurance**:

I- 'AES-256bits' ou superior;

II- 'SHA-256bits' ou superior; e

III- 'RSA-2048bits' ou superior.

3.17 É recomendável que os segredos e as chaves utilizados para autenticar, proteger e garantir a integridade de dados sejam gerados de maneira a respeitar processos de duplo controle e tratamento de segredo (*split-knowledge*), armazenando registros de log que incluam data de geração, participantes e responsáveis pela custódia, quando aplicável e de forma compatível com a regulamentação vigente.

3.18 As sociedades participantes devem implementar procedimentos e controles de segurança para análise de vulnerabilidades nas etapas de desenvolvimento e de utilização em produção das versões das APIs utilizadas no **Open Insurance**, observada a regulamentação vigente.

3.19 As vulnerabilidades de que trata o item 3.18 devem ser categorizadas e priorizadas de acordo com classificação de risco.

3.20 Os participantes devem implementar processos de revisão periódica das configurações dos sistemas e das APIs utilizados no **Open Insurance**, para garantir que somente portas e serviços autorizados estejam habilitados, observada a regulamentação vigente.

3.21 As sociedades participantes devem garantir que portais e aplicações relacionados à implementação e à operação do **Open Insurance** possuam meios de autenticação adequados e controle de autorização em observância à regulamentação vigente.

3.22 O processo de autenticação deve ser sempre realizado por meio de canal de comunicação seguro, utilizando criptografia TLS 1.2 ou superior, em compatibilidade com a regulamentação vigente.

3.23 Os acessos remotos para administração de sistemas ou da infraestrutura relacionados ao **Open Insurance** devem ser realizados mediante uso de múltiplos fatores de autenticação, observada, no que couber, a compatibilidade com a regulamentação vigente.

3.24 As sociedades devem implementar processo formal de aplicação de *patch* que contemple os sistemas relacionados à implementação do **Open Insurance**, de forma compatível com a política de segurança cibernética da sociedade, observada regulamentação vigente.

3.25 Os sistemas e APIs relacionados ao **Open Insurance** devem possuir relógio sincronizado com fonte confiável de tempo, por exemplo, por meio do uso do protocolo NTP.

3.26 As APIs e os sistemas relacionados ao **Open Insurance** devem ser implementados usando padrões de configuração segura (*hardening*), observada a regulamentação vigente.

4. Detecção

4.1 As sociedades devem manter trilhas de auditoria contendo, no mínimo, endereço IP de origem da chamada, porta de comunicação origem da chamada, data, hora, sistema, usuário (quando aplicável, inclusive os administradores), objeto, falha ou sucesso da ação das configurações realizadas nos sistemas e APIs relacionados ao **Open Insurance**, observadas a legislação e regulamentação vigentes.

4.2 As sociedades participantes devem monitorar os registros relativos aos acessos das APIs relacionadas ao **Open Insurance**, em especial os registros que indicarem erros internos (ex.: status HTTP 500) ou requisições inválidas (ex.: status HTTP 400), observada a regulamentação vigente.

4.3 As sociedades participantes devem monitorar a volumetria e o padrão das requisições às APIs relacionadas ao **Open Insurance**, para detecção de incidentes relacionados aos incisos I a IV do item 5.5.

5. Reação

5.1 É facultado às sociedades participantes transmissoras de dados implementar bloqueio de acessos às suas APIs, com vistas a tratar riscos cibernéticos ou para tratar incidentes cibernéticos em andamento. A implementação desses bloqueios deve ser compatível com a política de segurança cibernética da sociedade. Os bloqueios devem ser notificados para a estrutura de governança do Diretório de Participantes.

5.2 Em caso de comprometimento de qualquer credencial relacionada ao **Open Insurance**, a sociedade participante deve revogá-la tempestivamente perante o Diretório de Participantes e compartilhar essa informação com as demais sociedades participantes, observada a regulamentação vigente.

5.3 No caso de comprometimento de certificados de segurança, a sociedade participante do **Open Insurance** deve solicitar tempestivamente a revogação do certificado comprometido à autoridade certificadora e compartilhar essa informação com a Estrutura Responsável pela Governança do **Open Insurance** e com as demais

sociedades participantes, observada a regulamentação vigente.

5.4 Sem prejuízo do dever de sigilo e da livre concorrência, as sociedades participantes devem compartilhar com as demais sociedades participantes e com a Estrutura Responsável pela Governança do **Open Insurance** informações sobre incidentes cibernéticos que afetem os serviços do **Open Insurance**, observando a regulamentação vigente.

5.5 No âmbito do **Open Insurance**, observada a regulamentação vigente, o plano de ação e resposta a incidentes deve contemplar, no mínimo, procedimentos para prevenir e responder a incidentes que possam implicar:

I- acesso não autorizado;

II- vazamento de dados;

III- negação de serviço; e

IV- falha na integridade de dados.

6. Estrutura Responsável pela Governança do Open Insurance

6.1 Cada sociedade deve cadastrar no Diretório de Participantes os dados de contato de seus representantes para tratamento de incidentes com, no mínimo, e-mail, chaves criptográficas PGP (se houver) e campo para dados adicionais. Tais dados devem ser disponibilizados pelo Diretório para acesso aos demais participantes.

6.2 Cada sociedade deve disponibilizar os contatos de e-mail das equipes de segurança conforme a RFC 2142 (*abuse* e *security*).

6.3 O acesso às áreas restritas do Diretório de Participantes deve ser:

I - permitido apenas a usuários autorizados pelas instituições participantes ou pela Estrutura Responsável pela Governança do **Open Insurance**; e

II - condicionado à autenticação por múltiplos fatores.

6.4 Os acessos ao Diretório devem ser registrados em trilhas de auditoria, que devem conter, no mínimo, data e hora do acesso na *timezone* UTC, endereço IP de origem da chamada, porta de comunicação origem da chamada, URI acessada, método HTTP utilizado e status de retorno, observada a legislação e a regulamentação vigentes.

6.5 A Estrutura Responsável pela Governança do **Open Insurance** deve implementar e manter política de segurança cibernética formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados, com vistas a contemplar as atividades de que trata o art. 9 do Anexo II da Circular Susep nº 635, de 2021.

6.6 A política de que trata o item 6.5 deve contemplar:

I- os procedimentos e controles para reduzir a vulnerabilidade a incidentes;

II- a execução, no mínimo anual, de testes de intrusão;

III- os mecanismos para disseminação da cultura de segurança cibernética; e

IV- a difusão de boas práticas de segurança cibernética aos participantes e a outras partes interessadas na implementação e na operaçãodo **Open Insurance** no Brasil.

6.7 A Estrutura Responsável pela Governança do **Open Insurance** deve implementar e manter plano de ação e resposta a incidentes visando à implementação da política de segurança cibernética de que trata o item 6.5.

6.8 O plano de ação e resposta mencionado no item 6.7 deve contemplar as rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção, no monitoramento e na resposta a incidentes que afetem os serviços definidos no art. 9 do Anexo II da Circular Susep nº 635, de 2021.

6.9 O monitoramento dos serviços de que trata o item 6.8 deve ser realizado de forma permanente e estar disponível 24 horas por dia, 7 dias por semana.

6.10 A política referida no item 6.5 deve ser aprovada pelo Conselho Deliberativo da Estrutura Responsável pela Governança do **Open Insurance**, após prévia avaliação técnica. O plano de ação e resposta a incidentes mencionado no item 6.7 deve ser comunicado para ciência do Conselho Deliberativo da Estrutura Responsável pela Governança do Open Insurance, após prévia avaliação técnica.

6.11 Os testes de intrusão mencionados no inciso II do item 6.6 devem ser realizados com independência e imparcialidade por pessoa natural ou empresa especializada contratada para essa finalidade.

6.12 As vulnerabilidades identificadas nos testes de intrusão devem ser documentadas e tempestivamente tratadas pela Estrutura Responsável pela Governança do **Open Insurance**.

6.13 A Estrutura Responsável pela Governança do **Open Insurance** deverá instituir Equipe de Tratamento de Incidentes responsável por:

I- prevenir e tratar incidentes cibernéticos que afetem as atividades de que trata o art. 9 do Anexo II da Circular Susep nº 635, de 2021;

II- monitorar a utilização de credenciais de acesso dos participantes as atividades referenciadas no Inciso I; e

III- responder por eventuais violações de acesso caso utilizadas as credenciais de que trata o Inciso II.

6.14 É responsabilidade da Equipe de Tratamento de Incidentes que trata o item 6.13 no âmbito de suas atribuições, apoiar o tratamento de incidentes que possam implicar risco ao funcionamento de sistemas relacionados à implementação do **Open Insurance**, especialmente para promover:

I- a difusão e o compartilhamento de indicadores de comprometimento e de informações de inteligência cibernética; e

II- o monitoramento e o tratamento de incidentes envolvendo as atividades de que trata o art. 9 do Anexo II da Circular Susep nº 635, de 2021.

6.15 As informações sobre incidentes cibernéticos citados no Inciso I do item 6.13 devem ser:

I- compartilhadas com os representantes para tratamento de incidentes das sociedades participantes; e

II- disponibilizadas à Susep, observada a regulamentação em vigor.

6.16 A Estrutura Responsável pela Governança do **Open Insurance** deve disponibilizar no Portal do **Open Insurance** no Brasil:

I- os padrões de segurança e dos certificados digitais para fins de compartilhamento de dados e de serviços no escopo **Open Insurance**, observada a regulamentação em vigor; e

II- as instruções para subsidiar a emissão de certificados digitais requeridos para as contratações de parceria para fins de compartilhamento previstas na regulamentação em vigor.

6.17 O Diretório de Participantes do **Open Insurance** deve disponibilizar mecanismos que permitam às autoridades registradoras a validação de atributos dos certificados digitais de que trata o item 3.9.