**Apresentação dos detalhes técnicos do Funil de Consentimento da Plataforma de Coleta de Métricas**

**PORTA DE COLETA DE MÉTRICAS**

Sumário

[Introdução 3](#_heading=h.gjdgxs)

[Objetivo 4](#_heading=h.30j0zll)

[O que a plataforma não é 4](#_heading=h.1fob9te)

[Premissas Técnicas 4](#_heading=h.3znysh7)

[Terminologia 4](#_heading=h.2et92p0)

[Client e Server (Recepção e Transmissão) 5](#_heading=h.tyjcwt)

[PCM 5](#_heading=h.3dy6vkm)

[Reporte 5](#_heading=h.1t3h5sf)

[Software Statement 5](#_heading=h.4d34og8)

[Reporte, Validação e Processamento 5](#_heading=h.3rdcrjn)

[Reporte 5](#_heading=h.26in1rg)

[Validação e Processamento 6](#_heading=h.lnxbz9)

[Fluxo 6](#_heading=h.2s8eyo1)

[Modelo de reporte único 7](#_heading=h.35nkun2)

[Formas de Envio 9](#_heading=h.1ksv4uv)

[Recepção e retorno 9](#_heading=h.44sinio)

[Exemplos 10](#_heading=h.2jxsxqh)

[Payload Event Text 10](#_heading=h.z337ya)

[Payload Batch Text 11](#_heading=h.3j2qqm3)

**Introdução**

A plataforma de Coleta de Métricas foi idealizada com o objetivo de contabilizar as interações entre as sociedades participantes, de modo a promover um ambiente equitativo e não discriminatório. Trata-se de uma plataforma localizada no perímetro central, gerida pela Estrutura Inicial do Open Insurance. Entre as atribuições da Plataforma de Coleta de Métricas. O PCM monitora dois tipos de interações entre as Sociedades Seguradoras, os Reportes Transacionais e o Funil de Consentimento, assunto desse documento.

**Objetivo**

Para que o ecossistema do Open Insurance Brasil seja saudável para todas as Sociedades Participantes, Cidadãos e Reguladores, fez-se necessária a criação de uma plataforma que deverá concentrar dados sobre as etapas do Funil de Consentimento que vai do momento da criação de um consentimento (consent-created), até sua efetivação (consent-token-received), e a partir desses dados, gere indicadores relevantes à Implementação do Open Insurance e a disponibilização dos seus serviços à sociedade.

No intuito de manter a integridade e consistência dos dados enviados pelas Sociedades Participantes, estes, passarão por processo de validação antes de serão armazenados na base da Plataforma, para posteriormente serem utilizados na geração indicadores que serão utilizados tanto pelas Sociedades Participantes, quanto pela Estrutura Inicial Open Insurance Brasil (Secretariado), responsável por auditar e comunicar eventuais discrepâncias ou irregularidades no processo e disponibilidade dos serviços envolvidos durante o processo de Consentimento de Compartilhamento de Dados.

**Client e Server (Recepção e Transmissão)**

Em uma interação, a Seguradora que inicia o processo de consentimento é chamada de *client*, ao passo que a Seguradora detentora do Contrato e responsável por armazenar os dados do usuário, para que este possa compartilhá-los com outras Participantes é chamada de *server*.

Portanto, supondo a Seguradora A inicie um processo de Consentimento com a Seguradora B. A" é o *client* e "B" é o *server*. Obs.: Em contextos nos quais os termos "transmissor" e "receptor" são utilizados, eles passam a significar "server" e "client" respectivamente.

**Reporte do Funil de Consentimentos**

No contexto da API de Coleta de Métricas, um *reporte* do Funil de Consentimentos é o registro, passo a passo das etapas previstas até a conclusão de um Consentimento.

Este processe inicia-se em uma Seguradora Client, quando o usuário, previamente autenticado, concorda em compartilhar seus dados, armazenados em uma Seguradora Server, da qual já é cliente. Ao selecionar a Seguradora Detentora dos Dados (Server) e concordar em ser direcionado para ela, em background, entre Client e Server, cria se um consent-created (Id de Consentimento), que será utilizado durante as etapas do processo de consentimento, até seu desfecho final, com sua conclusão, ou não.

O reporte das etapas do funil de consentimento deve ser compartilhado com a Plataforma de Coleta de Métricas seguindo o mesmo modelo de comunicação existente para os Reportes Transacionais, onde também será validado, processado e armazenado com a finalidade de gerar indicadores relevantes para a implementação do Open Insurance Brasil entre as Sociedades Participantes.

**Software Statement**

Um participante do Open Insurance é sempre identificado pelo seu organisationId (com "s"). O organisationId possui um ou mais software statements, que identifica uma instância de software autorizada a consumir os serviços do ecossistema.

**Reporte, Validação e Processamento**

**Reporte**

O dado que é enviado pelas sociedades participantes é chamado de reporte, nesse caso: Reporte do Funil de Consentimento. A Plataforma de Coleta de Métricas tem por objetivo receber, processar e armazenar informações relacionadas as etapas do funil de consentimento e entre solicitações de dados que ocorrem após sua conclusão.

**Validação e Processamento**

Quando um Reporte é recebido pelas APIs da plataforma, esta, por sua vez inicia o processo de validação e posterior enriquecimento com as informações cadastradas no Diretório. Após esse processo, uma resposta é enviada para o solicitante com o status code da requisição, e um log é armazenado pela plataforma para conferências e auditorias posteriores.

**Fluxo**

De forma simples, em acordo com a Guia de Experiência do Usuário e as etapas que ocorrem em background, um usuário (cidadão), concorda em compartilhar seus dados armazenados em outra seguradora, da qual já é cliente. Para isso, é preciso que na Seguradora Cliente ele selecione a Seguradora Server e seja redirecionado para ela.

Chegando a Seguradora Server, detentora dos contratos com o usuário, este precisa se autenticar, definir o que permite compartilhar e autorizar o consentimento de compartilhamento de dados. Após isso, ele é redirecionado para a Seguradora Client, que iniciou o processo e esta agora, em posse do access token gerado, pode passar a realizar consultas, de acordo com o que foi permitido no consentimento gerado.

O desenho a seguir não visa demonstrar tudo o que ocorre durante o Funil de Consentimentos, mas exemplificar que este processo depende do usuário e de duas seguradoras, Client e Server.

 *(Esboço – Fluxo do Funil de Consentimento simplificado)*


*(Etapas do Funil de Consentimento – Server e Client)*

**Modelo de reporte do Funil de Consentimento**

O reporte contém dados que se referem às etapas que ocorrem durante o processo de Consentimento de Compartilhamento de Dados que envolve as ações o usuário e das Seguradoras Client e Server. Cada Reporte representa o avanço entre as etapas do funil de Consentimento.

**Server**

/event-api/v1/server-event (para envio unitário de dados)

/event-api/v1/server-batch (para envio de dados em massa)

**Client**

/event-api/v1/client-event/(para envio unitário de dados)

/event-api/v1/client-batch/ (para envio de dados em massa)

**Campos obrigatórios**

**consentId**

O consentId é o identificador único do consentimento e deverá ser um URN - Uniform Resource Name. Um URN, conforme definido na [RFC8141](https://tools.ietf.org/html/rfc8141) é um Uniform Resource Identifier - URI - que é atribuído sob o URI scheme "urn" e um namespace URN específico, com a intenção de que o URN seja um identificador de recurso persistente e independente da localização. Considerando a string urn:bancoex:C1DD33123 como exemplo para consentId temos:

Etapa do funil de consentimento.

Etapas do Cliente:

* consent-created
* user-redirected
* user-redirected-back
* consent-token-received
* refresh-token-used
* resource-accessed
* consent-revoked

Etapas do Servidor:

* consent-created
* user-redirected
* user-authentication-failed
* user-authenticated
* consent-authorized
* consent-rejected
* authorization-code-created
* user-redirected-back
* consent-token-generated
* refresh-token-used
* resource-accessed
* consent-revoked
* consent-expired

**correlationId**

O correlationId é utilizado para identificar um evento/reporte enviado à Plataforma de Coleta de Métricas, a informação é obrigatória, e única para cada etapa reportada.

**Timestamp**
Data/Hora UTC no formato ISO8601 com milissegundos (YYYY-MM-DDTHH:mm:ss.sssZ) do momento em que a chamada foi disparada, imediatamente antes do primeiro byte enviado na requisição.

**clientOrgId**

Identificação da organização do cliente

**clientSSId**

Identificador do Software Statement do cliente, sendo opcional para endpoints de fase1.

**serverOrgId**

Identificador da organização para onde a chamada foi feita

**serverASId**

Identificador do Authorization Server do servidor

**Formas de Envio**

Os eventos deverão ser enviados através de seus respectivos endpoints seguindo seu escopo, client ou server. Os eventos podem ser enviados em lote ou individualmente. O limite operacional estabelecido para o envio em lote (batch) é de no máximo 5.000 reportes por requisição. Em todos os casos, o dado é previamente validado de forma síncrona e processado de forma assíncrona.

**Recepção e retorno**

Quando um reporte chega nos endpoints da API, ele passa pelo processo de validação, após essa etapa cria-se o atributo eventId, que o identifica unicamente na plataforma. Caso o formato do reporte não passe pela validação, será enviada a resposta informando o status DISCARDED com o correlationID e message, contendo informações sobre o erro. Se o reporte passar pela validação, será enviada a resposta com o status ACCEPTED com o eventId e correlationID

**Exemplos**

**eventBody**

{

 "consentId": "urn:bancoex:C1DD33123",

 "step": "consent-created",

 "correlationId": "577869e5-4c63-4b19-9235-a18d22c80986",

 "additionalInfo": {

 "consent-user": "invalid-credentials",

 "authentication-failure-reason": "invalid-credentials",

 "user-redirected-back-status": "success",

 "token-kind": "consent-token",

 "rejected-by": "user",

 "revoked-by": "user",

 "expired-by": "authorization-timeout"

 },

 "timestamp": "2022-11-07T17:26:32Z",

 "clientOrgId": "1fb79963-4bff-4204-9370-93aceb8a2f0d",

 "clientSSId": "2a59c2a3-529f-41c6-97e3-77395e9951ca",

 "serverOrgId": "ff66b95a-d817-4fbe-949a-c5912e240189",

 "serverASId": "f8cd7b48-197d-419b-8680-f42226111b6f"

}

**batchBody**

## {

##  "organisationId": "c1ddd896-1145-4177-9b58-8a6e310557e2",

##  "events": [

##  {

##  "consentId": "urn:bancoex:C1DD33123",

##  "step": "consent-created",

##  "correlationId": "577869e5-4c63-4b19-9235-a18d22c80986",

##  "additionalInfo": {

##  "consent-user": "invalid-credentials",

##  "authentication-failure-reason": "invalid-credentials",

##  "user-redirected-back-status": "success",

##  "token-kind": "consent-token",

##  "rejected-by": "user",

##  "revoked-by": "user",

##  "expired-by": "authorization-timeout"

##  },

##  "timestamp": "2022-11-07T17:26:32Z",

##  "clientOrgId": "1fb79963-4bff-4204-9370-93aceb8a2f0d",

##  "clientSSId": "2a59c2a3-529f-41c6-97e3-77395e9951ca",

##  "serverOrgId": "ff66b95a-d817-4fbe-949a-c5912e240189",

##  "serverASId": "f8cd7b48-197d-419b-8680-f42226111b6f"

##  }

##  ]

## }