ANEXO IV.1

CONECTIVIDADE, SEGURANÇA E NÍVEIS DE SERVIÇO

Data	Versão	Estado Atual	Autor
31/01/2025	1.0	Criação do documento	Signatárias
06/03/2025	2.0	Ajuste após OE Nº 6, Parecer Eletrônico Nº 4/2025	Signatárias
14/05/2025	3.0	Ajuste após OE Nº 15, Parecer Eletrônico Nº 12/2025	Signatárias

Sumário

1. APRESENTAÇÃO

Este Anexo IV.1 – CONECTIVIDADE, SEGURANÇA E NÍVEIS DE SERVIÇO detalha os requisitos técnicos e de segurança para o acesso ao Ambiente de Interoperabilidade.

2. COMPONENTES DO AMBIENTE DE INTEROPERABILIDADE

O Ambiente de Interoperabilidade possui quatro componentes principais, são eles:

a) **PLATAFORMA INTEGRADA** – Atua como o núcleo central, facilitando a comunicação e o fluxo de dados entre diferentes sistemas e serviços. É composta por diversas ferramentas e tecnologias que permitam a integração de dados, aplicações e processos de negócio.

Características Principais:

- **Interoperabilidade**: Suporta múltiplos protocolos e formatos de dados, permitindo a comunicação entre sistemas heterogêneos.
- **Orquestração**: Coordena e gerencia fluxos de trabalho complexos, garantindo que os dados sejam processados e transmitidos de forma eficiente.
- **Segurança**: Implementa mecanismos de autenticação, autorização e criptografia para proteger os dados em trânsito e em repouso.
- **Escalabilidade**: Capaz de crescer conforme a demanda, suportando um grande volume de transações e usuários.

b) **REDSHIFT -** Repositório de dados principal do SRO (Sistema de Registro de Operações), utilizado para processamento, validação e consultas na base.

c) **BUCKET S3 -** Utilizado como armazenamento temporário para arquivos durante om processo de ingestão de dados na Plataforma.

d) **PARQUETS -** Apache Parquet é um formato de armazenamento de coluna de dados otimizado para a análise de grandes volumes de dados. É um formato aberto, disponível para qualquer projeto no ecossistema Hadoop.

3. PREMISSAS TÉCNICAS E SEGURANÇA

Toda a comunicação entre as Signatárias e a Plataforma Integrada será realizada através de acesso via conta AWS, por meio dos serviços disponíveis para acessar e armazenar os dados e os perfis de cada Signatária.

Os serviços de Redshift e SecretManager garantem que cada Signatária tenha permissão para acessar apenas os seus dados integrados na Plataforma.

É de responsabilidade das Signatárias, inclusive as que estejam em processo de homologação junto ao Regulador, realizar e manter Conexão Operacional Ativa na AWS para que seja possível acesso aos Ambientes de Interoperabilidade.

Os métodos de autenticação nas contas AWS do ambiente da Plataforma Integrada se dão por relações de confiança com as contas repassadas pelas Signatárias, de forma que a visualização e acesso de cada uma é limitada aos seus respectivos recursos, respeitando os princípios de privilégio mínimo. Também existe a conectividade estabelecida entre a rede local e a Virtual Private Cloud da Plataforma, essa conexão é estabelecida por meio se uma conexão VPN que utiliza o protocolo IPSEC, autenticando a partir de uma PRE-SHARED KEY. Os acessos aos serviços são controlados a partir de regras em grupos de segurança que liberam regras de entrada para os CIDR das rotas das VPN´s nos protocolos e portas necessárias ao acesso.

4. AMBIENTES

A Plataforma Integrada possui quatro instâncias de ambiente, disponível exclusivamente para Signatárias, SUSEP e Fornecedor de Tecnologia, com

infraestruturas segregadas em Desenvolvimento (DEV), Homologação do Fornecedor de Tecnologia, Homologação SUSEP e Registradoras e Produção.

Os ambientes possuem tecnologia RLS (Row-Level Secutirty) que restringe a cada Signatária, acessar apenas os seus dados. Exclusivamente a SUSEP terá permissão irrestrita de acesso aos dados integrados no Redshift para consultas, análises e extração de relatórios.

4.1. Ambiente de Desenvolvimento

O ambiente de desenvolvimento é utilizado pelos desenvolvedores do Fornecedor de Tecnologia para criar, testar e ajustar novas funcionalidades e correções antes que elas sejam movidas para estágios mais avançados de teste e produção.

Geralmente restrito aos desenvolvedores e alguns membros da equipe de QA (Quality Assurance). Pode ser configurado para ser menos estável e mais flexível, permitindo ajustes rápidos e testes frequentes, recursos computacionais limitados, já que o foco é a funcionalidade e não a performance.

A segurança deste ambiente é menos rigorosa em comparação aos outros ambientes, mas ainda assim precisa de medidas básicas de segurança para proteger dados sensíveis.

4.2. Ambiente de Homologação do Fornecedor de Tecnologia

O ambiente de homologação do Fornecedor de Tecnologia é utilizado para validar as funcionalidades desenvolvidas em um contexto que replica o ambiente de produção o mais próximo possível em termos de configuração e recursos computacionais suficientes para permitir testes de performance e carga. Este ambiente poderá estar em versão posterior à promovida ao ambiente Homologação SUSEP e Registradoras. Além do Fornecedor, Signatárias e SUSEP poderão acessar este ambiente.

O nível de segurança deve ser similar ao de produção para garantir que os testes reflitam condições reais.

4.3. Ambiente de Homologação SUSEP e Registradoras

O ambiente de homologação SUSEP e Registradoras é utilizado para validar as funcionalidades desenvolvidas em um contexto que replica o ambiente de produção o mais próximo possível em termos de configuração e recursos computacionais suficientes para permitir testes de performance e carga. Este ambiente deverá estar na versão a ser promovida ao ambiente de Produção. Além do Fornecedor, Signatárias e SUSEP poderão acessar este ambiente.

O nível de segurança deve ser similar ao de produção para garantir que os testes reflitam condições reais.

4.4. Ambiente de Produção

O Ambiente de Interoperabilidade, estará disponível somente para Signatárias autorizadas e que estejam com a conta AWS devidamente ativa, em infraestrutura exclusiva e segregada dos demais ambientes não-produtivos.

Signatárias terão acesso apenas aos seus próprios registros e a SUSEP à totalidade dos dados finais integrados por todas as Signatárias habilitadas.

Este ambiente tem configurações otimizadas para desempenho, estabilidade e segurança máxima. Recursos computacionais dimensionados para suportar a carga de trabalho real, com mecanismos de escalabilidade para atender a picos de demanda.

Contém dados reais e atualizados, com políticas rigorosas de segurança e privacidade.

5. NÍVEIS DE SERVIÇO

Define os requisitos de capacidade técnica para atender aos níveis de serviços estabelecidos para as operações do Ambiente de Interoperabilidade:

5.1 Tempo de Resposta da Recepção do Comando

O tempo de resposta depende do serviço AWS utilizado, das configurações do ambiente e da latência da rede. Abaixo, alguns exemplos típicos de tempo de resposta:

- **AWS API Gateway:** Latência média de **10ms a 100ms** para requisições processadas dentro da mesma região.
- **AWS Lambda:** Respostas típicas variando de **1ms a 300ms**, dependendo de fatores como o cold start e a configuração de memória.
- **AWS S3 e DynamoDB:** Operações simples geralmente têm tempos de resposta de **10ms a 50ms**.

Os resultados de sucesso ou falha, juntamente com um identificador único da transação, são gerados automaticamente pelos serviços AWS e podem ser monitorados com ferramentas como o **Amazon CloudWatch** ou **AWS X-Ray** para rastrear requisições e identificar gargalos.

Caso necessário, você pode configurar métricas adicionais para monitorar os tempos de resposta em tempo real e otimizar os componentes da aplicação.

Para a versão 2 o tempo médio de processamento de ingestão de 15(quinze) minutos e o tempo de processamento do Data Quality varia entre 1 hora para os leiautes de Documento e Endosso e 1,5 minutos para os demais leiautes.

A arquitetura da versão 3 contempla o processamento otimizado dos leiautes, levando em média 1h30 na execução completa de todos os leiautes juntos, o tempo de processamento para cada leiaute separadamente está levando cerca de 10 a 15 minutos para leiautes maiores (exemplo: documento e sinistro) e 5 a 10 minutos para leiautes menores (exemplo: Cosseguro, CTT etc.) em ambiente de homologação.

Levando em consideração o tempo médio de 1h30 a Plataforma tem capacidade de processar aproximadamente 223 arquivos dentro de 1 dia.

Tempo médio por arquivo = 6,43 minutos ou 386 segundos (90 minutos / 14 arquivos = 6,43 minutos).

1 dia = 24h x 60min x 60s = 86400 total de segundos de um dia.

Capacidade = 86.400s / 386s = 223 arquivos por dia (aproximadamente).

Para a versão 3, a Plataforma deverá suportar 10 mil transações por segundo (TPS), tendo sido verificado uma carga de 10 mil eventos por segundo, onde cada evento representa um registro processado com sucesso (por exemplo: 10 mil arquivos enviados ou 10 mil registros lidos de um arquivo e processados). Devendo a Plataforma estar apta a suportar um processamento médio de 50 milhões de registros em um dia com média de 3 horas de processamento para este volume e picos de 100 milhões de registros em um dia. A Capacidade de armazenamento deve suportar 1 Bilhão de registros mensalmente.

5.2. Tempo estimado para consultas à base

Nas consultas a bases de dados na AWS, especialmente usando Amazon Athena ou Amazon Redshift, é fundamental entender que o tempo estimado para o retorno das consultas depende diretamente dos dados e complexidade da consulta.

Seguem abaixo algumas métricas contabilizando com a média de registros da V2 e estimando o mesmo tempo para a V3:

- Leiaute Documento com 70700 registros demora em média 23 minutos;
- Leiaute Endosso com 40900 registros demora em média 45 minutos;
- Leiaute Complementar Auto com 19000 registros demora em média 35 segundos;
- Leiaute CCG com 566 registros demora em média 31 segundos;
- Leiaute Movimentação de Prêmio com 382100 registros demora em média 11 minutos;
- Leiaute Movimentação de Sinistro com 492500 registros demora em média 2 minutos;

5.3. Timeout de Recepção

O tempo limite para quebra de conexão depende do serviço AWS e pode ser configurado conforme as necessidades do cliente. O timeout para validação de estrutura do arquivo na Plataforma Integrada é de 5 minutos.

Alguns limites padrão incluem:

- **Amazon API Gateway**: O tempo limite padrão para recepção de respostas é de 29 segundos.
- **Elastic Load Balancer (ELB/ALB):** O timeout padrão pode ser configurado pelo cliente, com valor máximo de 4.000 segundos.
- **AWS Lambda:** O timeout de execução pode ser configurado, com limite máximo de 15 minutos.

5.4. Limite Tamanho Requisição

O limite próprio do Bucket S3 é de 5gb por arquivo. A partir desse tamanho, é necessário utilizar o upload multipart, que divide automaticamente o arquivo em partes menores.

5.5. Disponibilidade

A AWS garante alta disponibilidade para seus serviços com SLAs (Acordos de Nível de Serviço) específicos para cada serviço.

- **Amazon S3:** 99,99% de disponibilidade para acesso aos dados.
- **Amazon DynamoDB:** 99,99% de disponibilidade para operações de leitura e gravação.
- **Amazon EC2 e RDS:** 99,95% de disponibilidade por região (quando configurados em múltiplas zonas de disponibilidade).

A AWS recomenda práticas de arquitetura resiliente, como o uso de múltiplas zonas de disponibilidade para minimizar o impacto de falhas.

5.6. Taxa de Erros por Dia

A AWS mantém taxas de erro extremamente baixas, geralmente abaixo de 0,01%. Esses erros podem ser monitorados em tempo real com ferramentas como Amazon CloudWatch e AWS X-Ray, que ajudam a diagnosticar falhas e melhorar o desempenho do sistema.

5.7. Requisições por Segundo por ER Origem

O limite de requisições por segundo depende do serviço utilizado, e a AWS oferece escalabilidade dinâmica para ajustar a capacidade conforme necessário. A responsabilidade pela monitoração e respeito aos limites é do cliente.

Exemplos comuns incluem:

- **API Gateway**: Limite padrão de 10.000 requisições por segundo, com possibilidade de aumento mediante solicitação.
- **DynamoDB**: Capacidade configurável, permitindo milhões de requisições por segundo.
- **S3**: Não há limites rígidos, mas recomenda-se distribuir requisições por múltiplos prefixos.

Na AWS, as quotas (ou limites) para VPNs variam conforme o tipo de VPN utilizado. Aqui estão os principais detalhes sobre as quotas da VPN para a Plataforma Integrada:

- Largura de banda máxima por túnel de VPN - Até 1,25 Gbps
- Máximo de pacotes por segundo (PPS) por túnel da VPN - Até 140.000
- Número máximo de conexões para nós RA3(nosso tipo) - 2.000

5.8. Retentativas por Indisponibilidade

A AWS recomenda usar estratégias de retentativa com backoff exponencial para falhas temporárias, garantindo uma abordagem eficiente para lidar com falhas transitórias. O

Amazon SQS e o Amazon SNS oferecem retentativas automáticas para operações falhas.

5.9. Tempo até Acionamento por Indisponibilidade

O sistema utiliza o DataDog para monitorar os processos na Plataforma Integrada e em caso de falhas, o Fornecedor de Tecnologia em atividade, atuará para correção. As Signatárias e SUSEP poderão acionar a o Fornecedor de Tecnologia em atividade solicitando a investigação da eventual indisponibilidade.

5.10. Níveis de serviço associados à API do Seguro Garantia

5.10.1. Requisitos não-funcionais

a) Princípios, Definições e Recomendações:

A implementação da API do Seguro Garantia deverá obedecer aos princípios definidos na Seção 3 do Manual de APIs do Open Insurance, bem como deverá seguir as definições e recomendações das Seções 4.1, 4.2 e 4.5 do mesmo documento. Quanto à recomendação 4.5 do referido Manual, as versões devem ser publicadas em um Portal do Desenvolvedor para o SRO.

5.10.2. Requisitos de Performance

a) Deve suportar 50 requisições por minuto, com até 5 chaves de acesso simultâneas;
b) As requisições que excederem os limites poderão ser enfileiradas ou recusadas, caso em que deverão ser respondidas com o código de status HTTP 429 (Too Many Requests).
c) Tempo de resposta de até 0.5s para consultas unitárias de apólice;
d) Tempo de resposta de até 2.0s para consultas de apólices em lote e consultas por seguradora, tomador e beneficiário;
e) As requisições que excederem os limites de requisições deverão ser desprezadas no cálculo do tempo de resposta.

5.10.3. Requisitos de Suporte

a) Esta API deverá contemplar um projeto Swagger que contenha modelagem, documentação legível por humano e ferramenta de geração de código;
b) Os recursos e documentação desta API deverão ser publicados em ambiente web que contemple área de uso restrito da SUSEP e outros usuários determinados por esta;
c) O ambiente web citado deverá permitir o reaproveitamento para futuras APIs, compondo um Portal do Desenvolvedor para o SRO, nos moldes do Portal existente para o Open Insurance;
d) O Portal deverá listar esta e outras APIs em produção, suas versões atuais, datas em que entraram em produção, link para suas especificações e lista de mudanças desde a última publicação;
e) O Portal deverá apresentar o cronograma de homologação das APIs, indicando versão, data de divulgação, data prevista de entrada em produção e outras informações relevantes;
f) O Portal deverá incluir cronograma de paradas desta e outras APIs;
g) O Portal deverá incluir tutoriais com todas as informações necessárias para o desenvolvimento, testes e entrada em produção de aplicações consumidoras desta e outras APIs no âmbito da INTEROP. Cada tutorial deve conter todos os passos necessários para o completo desenvolvimento das aplicações clientes, instruções para obtenção de credenciais, processo de autenticação e autorização nas APIs, instruções para realização de testes, e contatos de suporte;
h) Devem ser fornecidos exemplos de código fonte e de telas no mínimo para as linguagens .NET, Python e JavaScript.

5.10.4. Requisitos de Segurança

a) Deverá contemplar o tráfego de dados criptografado;
b) O acesso será realizado por máquina, por meio de chave, senha de acesso, e VPN;

c) Deverá contemplar trilhas de auditoria que permitam identificar as consultas associadas a cada chave e senha de acesso.

5.10.5. Requisitos de Disponibilidade

a) A API do Seguro Garantia deverá ter disponibilidade mínima de 99% medida a cada 24 horas (indisponibilidade de até 14,4 minutos por dia);
b) Disponibilidade mínima de 99,5% do tempo a cada 1 mês (indisponibilidade de até 216 minutos por mês);

5.11. Níveis de serviço associados à API do Consumidor

A API de consulta do Consumidor, disponibilizada por cada registradora homologada no SRO, é consumida e consolidada pela SUSEP para prover serviços de consulta a cidadãos e empresas, por meio da plataforma do governo (gov.br), e a analistas da própria autarquia.

5.11.1. Requisitos de Performance

a) Deve suportar 1500 requisições por minuto, com até 120 acessos simultâneos;
b) As requisições que excederem os limites poderão ser enfileiradas ou recusadas, caso em que deverão ser respondidas com o código de status HTTP 429 (Too Many Requests);
c) Tempo de resposta de até 2s;
d) Limite de 200 apólices em uma mesma chamada;
e) Atraso de até 2 dias úteis entre o registro na registradora e a disponibilização via API. Atraso total de até 4 dias úteis entre a emissão da apólice e a disponibilização via API;
f) SUSEP incluirá mecanismo de autenticação por desafio/resposta para evitar consultas automatizadas.

5.11.2. Requisitos de Suporte

a) Esta API deverá contemplar um projeto Swagger que contenha modelagem, documentação legível por humano e ferramenta de geração de código;
b) Os recursos e documentação desta API deverão ser publicados em ambiente web que contemple área de uso restrito da SUSEP e outros usuários determinados por esta. A documentação deverá conter, além dos casos de uso da API, suas versões atuais, datas em que entraram em produção, link para suas especificações e lista de mudanças desde a última publicação;
c) Deverão ser criados tutoriais com todas as informações necessárias para o desenvolvimento, testes e entrada em produção de aplicações consumidoras desta e outras APIs. Cada tutorial deve conter todos os passos necessários para o completo desenvolvimento das aplicações clientes, instruções para obtenção de credenciais, processo de autenticação e autorização nas APIs, instruções para realização de testes, e contatos de suporte.

5.11.3. Requisitos de Disponibilidade

a) A API deverá ter disponibilidade de 99% medida a cada 24 horas (indisponibilidade de até 14,4 minutos por dia);
b) Disponibilidade mínima de 99,5% do tempo a cada 1 mês (indisponibilidade de até 216 minutos por mês);
c) Necessidades de paradas para manutenção deverão ser previamente informadas à SUSEP, preferencialmente com um cronograma pré-definido.

5.11.4. Requisitos de Segurança

a) Deverá contemplar o tráfego de dados criptografado;
b) O acesso será realizado por máquina, por meio de credenciais de acesso e VPN;
c) A API poderá ser utilizada apenas a partir dos endereços IP fornecidos pela SUSEP;

d) Deverá contemplar trilhas de auditoria que permitam identificar as consultas associadas a cada chave e senha de acesso. Para isso, deverão ser armazenados os seguintes dados: Token utilizado na consulta, data e hora da consulta, parâmetros de entrada enviados na consulta, resultado da consulta (sucesso ou erro);

5.11.5. Autenticação

O processo de autenticação utilizará o protocolo OAuth 2.0 através do uso de Client Id e Client Secret fornecido à SUSEP pelas registradoras. De posse do Client Id e do Client Secret deverá ser consumida uma api para geração de um Token. O Token retornado por esta api deverá ser utilizado na chamada das próximas apis. O Token gerado terá tempo de expiração de 15 minutos e o mesmo deverá ser controlado por quem estiver consumindo as apis. Quando o Token expirar, é necessário consumir novamente a api para obtenção de um novo Token.

5.11.6. Regras de negócio mapeadas

a) Deverão ser retornados todos os documentos - apólices, bilhetes e certificados - que possuam o segurado identificado pelo número do documento (CPF ou CNPJ);
b) Quando a data de referência não for informada deverão ser considerados os documentos que se encontram vigentes no dia da consulta;
c) Quando a data de referência for informada deverão ser considerados os documentos que se encontravam vigentes na data informada. Nesta situação, o documento a ser retornado deverá contemplar todos os endossos emitidos e vigentes até a data de referência da consulta;
d) Na primeira versão da API, o valor do prêmio a ser retornado poderá ser o valor do prêmio informado na emissão da apólice (sem considerar os endossos emitidos e vigentes até a data de referência da consulta). Em uma segunda versão da API, o valor do prêmio deverá ser retornado

considerando-se também os endossos emitidos e vigentes até a data de referência da consulta;

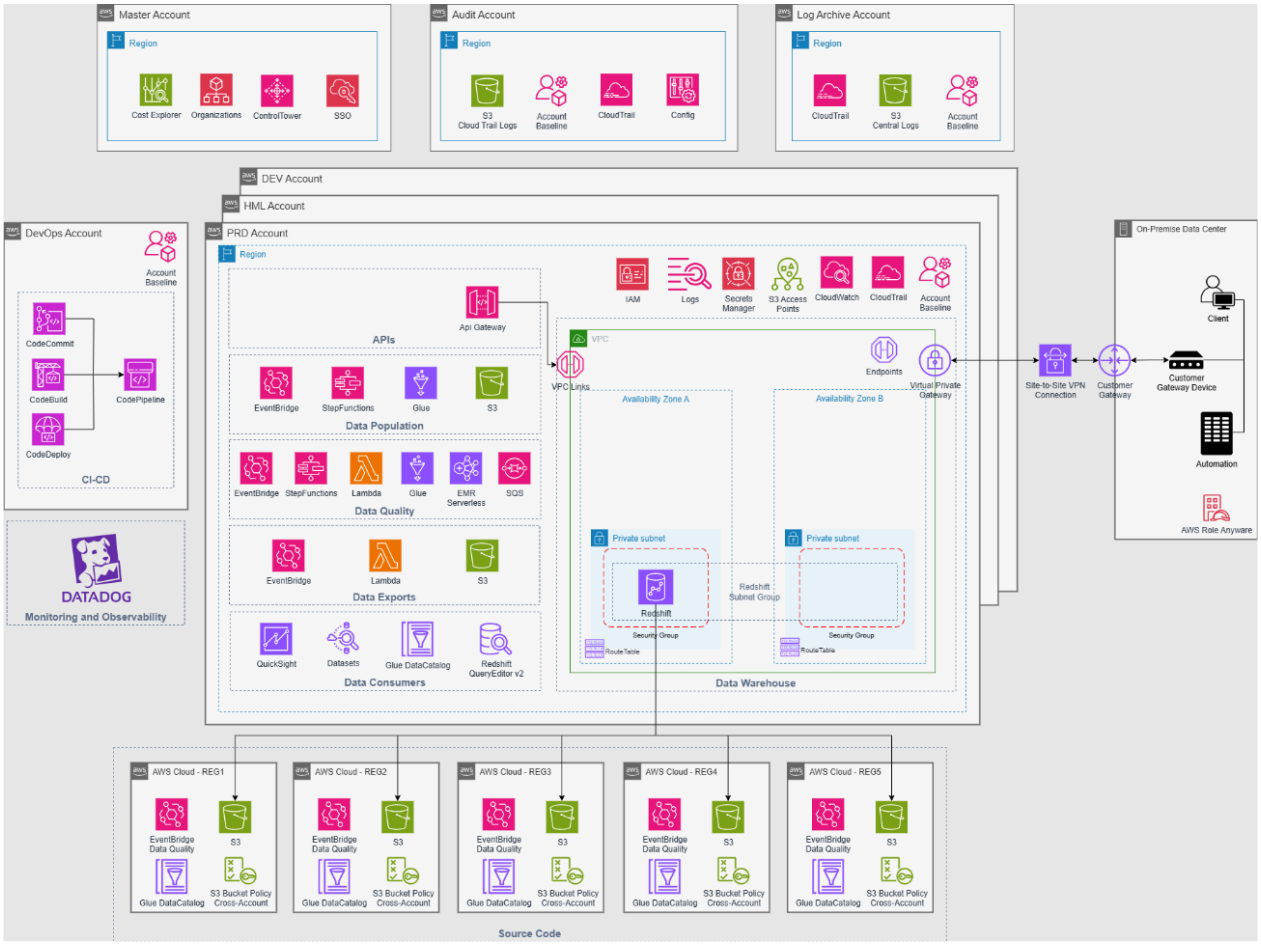
e) O valor do prêmio a ser retornado será o valor em reais, com 2 casas decimais;
f) As coberturas dos documentos deverão ser listadas sem duplicidade. Ou seja, se um documento tiver mais de um objeto segurado e cada um dos objetos segurados tiverem uma mesma cobertura, no retorno da API deverá ser exibida a cobertura apenas uma vez;
g) A descrição da cobertura deve seguir a descrição existente na tabela de coberturas vigente. Para cobertura de código 99, a descrição a ser informada será o nome atribuído pela seguradora internamente. Nesta situação, a descrição da cobertura deverá ser informada no campo código descrição;
h) Previsão de uma infraestrutura escalável, comportando futuro aumento no volume de chamados.

5.11.7. Descrição dos erros de validação mapeados

As descrições abaixo deverão ser retornadas nas mensagens de erro.

a) O CPF informado é inválido;
b) O CNPJ informado é inválido;
c) A data de referência é inválida (deve conter uma data no formato AAAA-MM-DD);
d) Token não enviado;
e) Token inválido;
f) Token expirado;
g) Limite de requisições simultâneas atingido.

5.12. Aspectos operacionais da Plataforma Integrada V2 e V3



6. GRADE DE HORÁRIOS

A Plataforma Integrada desempenha um papel essencial na centralização e gestão dos dados relativos a seguros, previdência complementar aberta, capitalização e resseguros. Para garantir a eficiência e a continuidade das operações, é fundamental que a grade de horários seja clara e rigorosamente seguida.

A Plataforma Integrada no ambiente produtivo permanece ativa todos os dias, durante 24 horas.

Os envios de arquivos e consultas poderão ser realizados a qualquer momento.

O processamento dos dados e as validações ocorrem, para V2 e V3, da seguinte maneira:

I - Em V2, o processo de ingestão dos dados no Redshift se inicia às 00h30, com duração prevista de aproximadamente 15 minutos;

II - Em V2, o processamento do Data Quality ocorre quando os arquivos são enviados para a Plataforma;

III - Em V3, o processamento e as validações iniciam às 00h00. Ainda não há estimativa de duração dessa atividade qual será avaliada num prazo máximo de 90 dias a contar da data de início da obrigatoriedade da implantação em produção da V3.

A grade de horário de disponibilidade está disposta da seguinte forma:

- Plataforma Integrada – 24 (vinte e quatro) horas por dia, 7(sete) dias por semana
- Consulta Consumidor – 24 (vinte e quatro) horas por dia, 7(sete) dias por semana
- Consulta Seguro Garantia - 24 (vinte e quatro) horas por dia, 7(sete) dias por semana

I - Processamento e Integração de Registros: Na V3, o processamento dos registros enviados tem início às 00:00, incluindo no fluxo a verificação da qualidade dos dados e a carga no Data Lake;

II - Na V2, o processamento dos registros enviados começa às 00:30, também incorporando a verificação da qualidade dos dados e a carga no Data Lake.

Assinado por:
Eduardo Juliano
1055D70EFBBA4BB...

CIP S.A.

Assinado por:
Celso Lanzelotti
454081741CC4434...

MAPS Services S.A.

Assinado por:
Marcelo Rodrigues Costa
2140CFCE74DC479...

B3 Brasil, Bolsa, Balcão

DocuSigned by:
Gabriel Lorandos Germani
434CC0DA090746E...

Central de Serviços de Registro e Depósito aos Mercados Financeiro e de Capitais S.A