1. Visão Geral e Escopo da Solução

1.1 Introdução Executiva

Este documento detalha a arquitetura de referência para a **Plataforma SIGA (Sistema Integrado de Garantias e Análise)**, concebida como um ecossistema de originação digital proprietário (*Proprietary Digital Origination Platform*). A solução atua como o orquestrador central da esteira de crédito imobiliário e rural, eliminando dependências de interfaces legadas e centralizando a experiência do usuário.

A arquitetura adota uma estratégia **"Best-of-Breed"** para os motores de decisão, mas mantém a camada de experiência e gestão operacional 100% customizada (*Custom Frontend*). O SIGA orquestra microsserviços especializados para cobrir o ciclo de vida do cliente em quatro estágios críticos:

1. **Onboarding & Identity Trust:** Validação de identidade e prevenção à fraude (LexisNexis/Neurotech);
2. **Proprietary CRM & Operations:** Gestão customizada de leads, esteira e tarefas manuais (SIGA Ops);
3. **Credit Decisioning (Cérebro):** Motor de regras e pricing de crédito (XCurve);
4. **Collateral & Formalization (Músculos):** Gestão de garantias e esteira jurídica (Prognum).

A solução opera em modelo **Cloud-Native**, orientado a eventos (*Event-Driven*), garantindo que o Banco detenha o controle total sobre a jornada do cliente, desde a captura do lead até a emissão do contrato.

1.2 Objetivos Estratégicos da Arquitetura

A modernização da esteira visa atender aos seguintes pilares técnicos e de negócio:

- **Experiência Proprietária (Custom UX):** Substituição de telas genéricas de CRM (ex: Bitrix) por um Front-end customizado, permitindo fluxos de trabalho otimizados e aderentes à identidade visual e operacional do Banco.
- **Segurança "Gatekeeper" (Fail-Fast):** Implementação de barreiras de segurança nas etapas iniciais (Onboarding), bloqueando fraudes antes do consumo de recursos onerosos (Motores de Crédito).
- **Visão Unificada de Risco:** Consolidação dos vetores de risco de fraude (Neurotech), risco de crédito (XCurve) e risco de garantia (Prognum) em um dashboard de decisão único.
- **Sincronização Bidirecional (Core Bancário):** Garantir que a evolução do lead no Front-end customizado reflita em tempo real na visão "Cliente 360" do Core Bancário (Temenos).

1.3 Escopo Detalhado da Solução

A solução abrange a jornada completa do cliente, segmentada em **Domínios de Serviço** que interagem através de APIs RESTful. Abaixo detalha-se o fluxo funcional e técnico da arquitetura.

1.3.1 Camada de Canal e Entrada (Front SIGA & Orquestração)

O **Front SIGA** atua como a camada de experiência (*Experience Layer*). Diferente de soluções de mercado, esta interface é totalmente proprietária, desenhada para absorver tanto a entrada de dados do cliente quanto a operação dos analistas do banco.

- **Gestão de Sessão Omnichannel (siga.front.session):** Controle de tokens de acesso e persistência de estado da jornada (<200ms SLA).
- **Roteamento de Jornada (siga.journey.router):** Motor de navegação dinâmico que dita a próxima tela baseada no status do cliente, sem depender de fluxos estáticos de ferramentas de terceiros.
- **Formulários Dinâmicos (siga.ui.forms.dynamic):** Renderização de interfaces baseada em regras de produto, permitindo A/B testing e ajustes rápidos de *compliance*.

1.3.2 Domínio de Identidade e Prevenção à Fraude (Identity & Trust)

Alinhamento BIAN: Party Authentication & Fraud Detection

Antes de iniciar a esteira de crédito, o orquestrador submete o solicitante a um rigoroso processo de validação ("Know Your Customer" - KYC).

A. Validação de Identidade (Integração LexisNexis)

O fluxo de entrada exige a validação biométrica e documental síncrona:

- **Validação de Identidade (id.token.validate):** Validação de "Liveness" (prova de vida) e Face Match.
- **Verificação Documental (id.document.verify):** OCR e documentoscopia automatizada do RG/CNH.
- **Sanctions & Watchlist (id.watchlist.check):** Consulta bloqueante a listas restritivas (OFAC, PEP).

B. Motor Antifraude (Integração Neurotech)

Após a validação da identidade, o perfil é submetido ao score de fraude:

- **Device Fingerprinting (fraud.device.fingerprint):** Análise técnica do dispositivo (geolocalização, emuladores).
- **Score Antifraude PF (fraud.score.pf):** Geração de score (0-1000). Scores abaixo do *cutoff* encerram a esteira imediatamente (*Hard Reject*).

$$Diagrama: \ FluxodeSequênciadeOnboardingeValidação(Lexis/Nexis$$

1.3.3 Domínio de Gestão Operacional Proprietária (SIGA Ops)

Alinhamento BIAN: Customer Relationship Management & Case Management

Nesta arquitetura, a gestão do relacionamento não é terceirizada para um CRM externo (como Bitrix). O **SIGA Ops** é o módulo proprietário responsável por gerir o ciclo de vida da proposta.

- **Captura e Gestão de Lead (crm.lead.capture):** O microsserviço interno persiste o prospect e inicia o rastreamento da oportunidade na base de dados do SIGA.
- **Motor de Tarefas (crm.task.dispatch):** Ao invés de usar o kanban do Bitrix, o SIGA implementa seu próprio gerenciador de pendências. Caso uma regra de negócio falhe (ex: documento ilegível), o sistema gera um *ticket* interno para a fila de trabalho dos analistas na interface administrativa do SIGA.
- **Sincronização Cliente 360 (temenos.client.sync):** O módulo operacional garante que, embora o CRM seja proprietário, os dados sejam espelhados no **Temenos Transact**, mantendo a visão única do cliente atualizada no Core.

$$Diagrama: \ VisãoLógicadoMóduloOperacionalCusto$$

1.3.4 Domínio de Decisão de Crédito (Credit Decisioning)

Alinhamento BIAN: Credit Assessment & Underwriting

O núcleo da decisão financeira é processado pelo motor **XCurve**, acionado pelo orquestrador SIGA.

- **Execução de Políticas (credit.engine.core):** Processamento do motor de decisão parametrizado.
- **Consultas a Bureaus:** Orquestração de chamadas a bureaus externos e internos (Bureaus BASA).
- **Pricing (credit.pricing.calculate):** Definição da taxa de juros personalizada (RAROC).

1.3.5 Domínio de Garantias e Formalização (Collateral & Agreement)

Alinhamento BIAN: Collateral Asset Administration

A etapa final envolve a validação do ativo e a formalização jurídica via **Prognum**.

- **Avaliação de Garantia (documents.avm.request):** Disparo de avaliação automática (AVM) ou laudo de engenharia.
- **Esteira Jurídica:** Análise de matrícula e certidões (documents.certidao.issue).
- **Formalização Digital (documents.digital.sign):** Geração de CCB e orquestração de assinaturas (ICP-Brasil).

$$Diagrama: \ DiagramadeContextodeArquitetura(Macr$$

1.4 Premissas da Arquitetura

1. **Single Sign-On (SSO):** A autenticação do usuário deve ser federada, permitindo navegação fluida entre os canais do banco.
2. **Zero Trust Network:** Nenhuma comunicação entre microsserviços é confiável por padrão; todas exigem mTLS e tokens de serviço.
3. **Human-in-the-Loop:** O sistema deve prever pontos de parada (breakpoints) para análise manual no Backoffice proprietário caso as regras automáticas de fraude ou crédito retornem "Gray Zone" (Zona Cinzenta).

2. Princípios Arquiteturais e Padrões

Esta seção detalha os alicerces técnicos e conceituais que governam o design do SIGA. A arquitetura segue rigorosamente os padrões de **Composable Banking**, permitindo que módulos de negócio (identidade, crédito, garantias) sejam orquestrados como ativos independentes, porém integrados.

2.1 Fundamentos da Arquitetura (Cloud-Native & API-First)

A plataforma é construída sobre quatro pilares fundamentais, alinhados às melhores práticas de arquitetura distribuída e escalável:

1. **API-First Design:** Todas as funcionalidades do SIGA (sejam do front-end ou motores de backend) são expostas via APIs RESTful documentadas (OpenAPI 3.0), garantindo desacoplamento entre canais e regras de negócio.
2. **Microsserviços por Domínio:** A lógica é segregada em contextos delimitados (*Bounded Contexts*). Uma falha no módulo de "Garantias" não deve impactar o módulo de "Onboarding".
3. **Stateless Orchestration:** O orquestrador central do SIGA não retém regras de negócio

complexas ("Hard Coded"). Ele atua como uma máquina de estados finita, delegando a execução lógica para os motores especializados (XCurve, Prognum, Neurotech).

4. **Imutabilidade e Rastreabilidade:** Todas as transações críticas geram logs de auditoria imutáveis, garantindo conformidade total com regulamentações bancárias.

2.2 Alinhamento ao Padrão BIAN (Banking Industry Architecture Network)

Para garantir a interoperabilidade e a padronização semântica com o ecossistema do Banco (especialmente com o Core Temenos), o SIGA adota o *BIAN Service Landscape v13.0*.

Cada módulo da arquitetura do SIGA foi mapeado para um **Domínio de Serviço BIAN** correspondente. Isso facilita a governança de dados e a integração futura com outros sistemas legados.

Módulo SIGA	**Domínio de Negócio BIAN (Business Domain)**	**Domínio de Serviço BIAN (Service Domain)**	**Justificativa Arquitetural**
Identity Trust (LexisNexis)	*Risk & Compliance*	**Party Authentication**	Validação biométrica e documental do proponente como pré-requisito de acesso.
Antifraude (Neurotech)	*Risk & Compliance*	**Fraud Detection**	Análise comportamental e de dispositivo para mitigação de riscos operacionais.
SIGA Ops (CRM)	*Sales & Service*	**Customer Relationship Management**	Gestão centralizada do relacionamento, histórico de interações e pipeline de vendas.
Motor de Crédito (XCurve)	*Consumer Banking*	**Consumer Loan (Underwriting)**	Avaliação de capacidade de

			pagamento, cálculo de rating e precificação de risco.
Garantias (Prognum)	*Operations & Execution*	**Collateral Asset Administration**	Gestão do ciclo de vida da garantia, desde a avaliação (AVM) até o registro cartorário.

$$Diagrama: \ MapadeDomíniosBIANdoSIGAa$$

Descrição sugerida para o diagrama: Uma representação visual tipo "Landscape" onde cada caixa colorida representa um módulo do SIGA, rotulada com seu respectivo Domínio BIAN.

2.3 Padrão API Gateway ("The Front Door")

O SIGA utiliza o padrão de **API Gateway** como ponto único de entrada para todo o tráfego externo (Internet, Parceiros e Canais). Este componente é crítico para a segurança e governança da plataforma.

2.3.1 Funções do Gateway

O API Gateway atua na borda (*Edge*) da arquitetura, implementando políticas transversais antes que a requisição atinja os microsserviços do SIGA:

- **Autenticação Centralizada & SSO:** Interceptação de todas as requisições para validação de tokens JWT (OAuth2/OpenID Connect), garantindo que apenas usuários autenticados acessem a esteira.
- **Rate Limiting & Throttling:** Proteção dos motores de backend (especialmente XCurve e Neurotech, que possuem custo por transação) contra ataques de *DDoS* ou picos abusivos de uso.
- **Roteamento Inteligente:** Direcionamento de tráfego baseada em versão de API (*Canary Deployment*), permitindo testes A/B de novas políticas de crédito sem impacto total na base.
- **Transformação de Protocolo:** Conversão de chamadas REST modernas do front-end para eventuais protocolos legados (ex: SOAP) exigidos por sistemas satélites do Banco, quando necessário.

$$Diagrama: \ PadrãoAPIGatewayeCamadasde.$$

Descrição sugerida:
Um diagrama de arquitetura mostrando: Cliente (App/Web) ->

$$WAF$$

->

$$APIGateway$$

->

$$LoadBalancer$$

->

$$ClusterKubernetesSIGA$$

.

2.4 Arquitetura Orientada a Eventos (Event-Driven Architecture)

Dada a natureza de longa duração de certos processos de crédito imobiliário (ex: Análise Jurídica, Laudo de Engenharia), o SIGA não pode depender exclusivamente de chamadas síncronas (HTTP Request/Response), sob risco de *timeout* e bloqueio de recursos.

A arquitetura implementa um modelo híbrido:

1. **Fluxos Síncronos (Bloqueantes):** Utilizados para decisões em tempo real que afetam a UX imediata (ex: Login, Validação Biométrica, Score de Fraude Preliminar).
2. **Fluxos Assíncronos (Não-Bloqueantes):** Utilizados para processos pesados. O SIGA dispara o comando e libera a sessão do usuário. A resposta é recebida posteriormente via **Webhooks** ou consumo de filas (Kafka/RabbitMQ).
    - *Exemplo:* A solicitação de vistoria do imóvel é enviada à Prognum. Quando o laudo fica pronto (dias depois), a Prognum notifica o SIGA via Webhook, que então atualiza o status do processo e notifica o cliente via Push/Email.

2.5 Padrões de Resiliência e Tolerância a Falhas

Para garantir a alta disponibilidade exigida por uma plataforma crítica de originação, aplicamos os seguintes padrões de resiliência na comunicação entre o Orchestrator e os Parceiros (Lexis, Neurotech, XCurve, Prognum):

- **Circuit Breaker:** Se um parceiro externo (ex: XCurve) falhar consecutivamente, o "disjuntor" abre, impedindo novas requisições inúteis e permitindo que o sistema falhe graciosamente (ex: salvando a proposta para reprocessamento posterior) ao invés de travar a thread.
- **Retry Pattern com Backoff Exponencial:** Em caso de falhas transientes de rede, o sistema tenta reenviar a requisição com intervalos crescentes (1s, 2s, 4s...) antes de desistir.
- **Dead Letter Queues (DLQ):** Mensagens ou transações que falharam definitivamente após todas as tentativas são enviadas para uma fila morta (DLQ) para análise manual e reprocessamento pela equipe de sustentação, garantindo que *nenhum lead seja perdido*.

3. Domínios de Negócio e Serviços (Business & Service Domains)

A arquitetura do SIGA segue uma decomposição orientada a domínios de negócio (*Domain-Driven Design*), alinhada aos padrões de *Service Landscape* da BIAN. Esta estrutura organiza a aplicação em capacidades funcionais autônomas, garantindo que cada componente (LexisNexis, Neurotech, SIGA Ops, XCurve e Prognum) opere como um ativo de serviço reutilizável dentro do ecossistema do Banco.

3.1 Mapeamento de Capacidades (Capability Map)

A tabela abaixo estabelece o relacionamento formal entre os módulos tecnológicos do SIGA e as capacidades de negócio BIAN que eles implementam.

Domínio de Negócio (Business Area)	**Domínio de Serviço (Service Domain)**	**Componente Responsável**	**Principais Funções Técnicas (Microserviços)**	**Descrição da Capacidade**
Risk & Compliance	*Party Authentication*	**LexisNexis**	id.token.validate id.document.ve	Validação inequívoca da identidade do proponente

			rify	(KYC) e autenticidade documental.
Risk & Compliance	*Fraud Detection*	**Neurotech**	fraud.score.pf fraud.device.fingerprint	Detecção preditiva de fraude comportamental e análise de risco do dispositivo.
Sales & Service	*Customer Relationship Management*	**SIGA Ops**	crm.lead.capture crm.task.dispatch	Gestão do ciclo de vida do lead, orquestração de tarefas e visão 360º da oportunidade.
Consumer Banking	*Consumer Loan (Underwriting)*	**XCurve**	credit.engine.core credit.pricing.calculate	Execução de políticas de crédito, cálculo de capacidade de pagamento e definição de limites.
Banking Operations	*Collateral Asset Administration*	**Prognum**	documents.avm.request documents.digital.sign	Avaliação, gestão e formalização jurídica das garantias vinculadas ao contrato.

3.2 Detalhamento dos Domínios e Serviços

3.2.1 Domínio de Identidade e Segurança (Identity & Trust)

Este domínio atua como o "Gatekeeper" da arquitetura. Sua responsabilidade primária é

garantir que apenas identidades legítimas e livres de sanções acessem a esteira de crédito, mitigando riscos operacionais antes da análise financeira.

A. Serviço de Validação de Identidade (LexisNexis)

Implementa o padrão *Zero Trust* na entrada do usuário.

- **Funções Principais:**
  - **Biometria Facial (Liveness Detection):** Previne ataques de apresentação (*spoofing*) garantindo a presença física do usuário.
  - **Documentoscopia Automatizada:** Extração de dados via OCR e validação forense da autenticidade do documento (RG/CNH/DNI).
  - **Background Check (Sanctions):** Varredura automática em listas de restrição (OFAC, Interpol, PEP - Pessoas Expostas Politicamente).
- **Integração:** Comunicação síncrona via API REST segura (mTLS). O retorno positivo gera um "Token de Confiança" que autoriza o avanço para a etapa de fraude.

B. Serviço de Detecção de Fraude (Neurotech)

Atua como uma camada de inteligência comportamental.

- **Funções Principais:**
  - **Score Antifraude (0-1000):** Modelo preditivo que avalia a probabilidade de a transação ser fraudulenta baseada em histórico e comportamento.
  - **Device Fingerprinting:** Coleta e analisa metadados do dispositivo (IMEI, IP, Geolocalização, Proxy) para identificar padrões de ataque (ex: múltiplas propostas de um mesmo emulador).
  - **Behavioral Pattern:** Detecção de anomalias na navegação (ex: preenchimento de formulário rápido demais para um humano).
- **Política de Fail-Fast:** Se o fraud.score.pf estiver abaixo do *cutoff* definido pelo Banco, o sistema nega o crédito imediatamente, economizando custos de consulta aos bureaus de crédito na etapa seguinte.

$$Diagrama: \ FluxodeDecisãodeRiscoPreliminar(Gate$$

Legenda Sugerida: Diagrama de Sequência detalhando a interação: Front -> LexisNexis (Valida) -> Neurotech (Analisa) -> Decisão (Go/No-Go).

3.2.2 Domínio de Gestão de Clientes e Operações (SIGA Ops)

Este domínio substitui o uso de CRMs genéricos por uma solução proprietária focada na eficiência operacional da esteira de crédito.

A. Serviço de Gestão de Leads e Oportunidades

Centraliza a "Verdade Única" sobre o andamento da proposta.

- **Funções Principais:**
  - **Lead Capture & Enrichment:** Criação automática do dossiê do cliente após a validação de identidade.
  - **Pipeline Sync:** Sincronização de status com o **Temenos Transact** (Módulo Client 360), garantindo que a agência visualize o lead digital.
  - **Activity Logging:** Registro imutável de todas as interações (logs de chamadas, uploads, e-mails) para auditoria.

B. Serviço de Gestão de Tarefas (Workflow Engine)

Orquestra o trabalho humano quando a automação encontra exceções.

- **Funções Principais:**
  - **Task Dispatch:** Distribuição inteligente de pendências (ex: "Análise de Renda Manual") para a fila de analistas baseada em disponibilidade e skill.
  - **SLA Tracking:** Monitoramento em tempo real do tempo de atendimento de cada tarefa (ops.review.sla), disparando alertas de escalonamento para gerentes.

$$Diagrama: \ MáquinadeEstadosdoLead(WorkflowOperc$$

Legenda Sugerida: Diagrama de Estados mostrando as transições do Lead: Novo -> Em Análise de Fraude -> Em Análise de Crédito -> Pendência Manual -> Aprovado -> Contratado.

3.2.3 Domínio de Decisão de Crédito (Credit Decisioning)

O "Cérebro Financeiro" da plataforma, isolado no motor **XCurve** para garantir flexibilidade nas políticas de risco sem necessidade de *deploy* de código.

A. Serviço de Motor de Crédito

- **Funções Principais:**
  - **Bureau Orchestration:** Consulta e consolidação de dados de múltiplos bureaus (Serasa, SCR, Bureaus Internos BASA).
  - **Policy Rules Execution:** Aplicação de árvores de decisão complexas (ex: "Se Renda > X e Score > Y e Garantia = Rural, então Limite = Z").
  - **Pricing & Limit:** Cálculo dinâmico da taxa de juros e limite aprovado baseado no risco calculado (RAROC).

3.2.4 Domínio de Garantias e Formalização (Collateral & Agreement)

Os "Músculos" da operação, responsáveis pela materialização do ativo e do contrato jurídico

via **Prognum**.

A. Serviço de Administração de Garantias

- **Funções Principais:**
  - **AVM Trigger (Automated Valuation Model):** Disparo automático para avaliação do valor do imóvel baseado em dados de mercado.
  - **Legal Validation:** Análise da situação jurídica da matrícula do imóvel (ônus, gravames).

B. Serviço de Formalização Contratual

- **Funções Principais:**
  - **Contract Generation:** Geração dinâmica da Cédula de Crédito Bancário (CCB) em PDF com os dados aprovados.
  - **Digital Signature Orchestration:** Coleta de assinaturas digitais com validade jurídica (ICP-Brasil) e envio para registro eletrônico.

$$Diagrama: \ MapadeIntegra\c{c}\~{a}odeServi\c{c}os(ServiceIntegrati$$

Legenda Sugerida: Visão de alto nível mostrando como os serviços de Identidade, Operações, Crédito e Garantias se conectam através do Barramento de Eventos do SIGA.

4. Arquitetura de Aplicação e Componentização de Serviços

A arquitetura de aplicação do SIGA evolui do modelo de microsserviços tradicional para uma topologia de **Microsserviços Especializados e Workers Assíncronos**. Esta estrutura é mandatória para suportar a carga cognitiva dos motores de decisão externos (Neurotech) e os requisitos de processamento intensivo de conformidade (FNO/Audit Packs), sem degradar a experiência do usuário (UX) no *Frontend*.

A solução é orquestrada em um cluster Kubernetes (OKE), segregando cargas de trabalho em três camadas funcionais: **Core Banking Services**, **Decision Wrappers** e **Compliance Workers**.

4.1. Camada de Orquestração de Decisão (Decision Wrappers)

Diferente de simples *proxies* de API, os *Wrappers* são componentes inteligentes responsáveis

por isolar a complexidade dos parceiros externos, gerenciar estados de autenticação e implementar resiliência (Circuit Breakers).

4.1.1. Serviço de Gestão de Antifraude (ms-decision-integrator)

Este componente é o único ponto de contato com o motor *Decision Runner* (Neurotech), abstraindo a lógica de *Workflow* do restante do banco.

5. **Responsabilidade Primária:** Orquestrar o fluxo híbrido de submissão de propostas.
6. **Funções Críticas (Baseado na Spec Neurotech):**
    - **Gestão de Sessão OAuth:** Gerencia o ciclo de vida do *Bearer Token* do Portal Riskpack, realizando renovação automática antes da expiração (evitando latência de login na chamada crítica).
    - **Adaptive Routing (Síncrono/Assíncrono):** Decide dinamicamente entre chamar o método Submit (Síncrono) ou SubmitAsync baseado na latência média das últimas 50 requisições (telemetria em tempo real).
    - **Polling Manager:** Se a submissão for assíncrona, este serviço agenda e executa as chamadas de GetSubmission até obter o StatusCode: 0100 (Concluído) ou 0200 (Stop), persistindo o resultado na TB_NEUROTECH_TRANSACTION.
7. **Stack Tecnológica:** Java/Quarkus (Baixo footprint de memória) + Redis (Cache de Token).

4.1.2. Serviço de Identidade e KYC (ms-identity-trust)

Responsável pela integração com a *LexisNexis* para validação cadastral e PLD (Prevenção à Lavagem de Dinheiro).

- **Responsabilidade Primária:** Sanitização de dados cadastrais e execução de *background checks*.
- **Funções Críticas:**
    - **Orquestração de PLD:** Submete o CPF/CNPJ para validação de PEP (Pessoas Expostas Politicamente) e Sanções.
    - **Normalização de Evidência:** Recebe o *raw payload* da LexisNexis e extrai apenas os dados necessários para o enquadramento FNO, descartando ruído.

4.2. Camada de Conformidade e Auditoria (Compliance Layer)

Esta camada introduz componentes focados exclusivamente em atender os requisitos não-funcionais de auditoria do TCU e retenção de dados, desacoplando essas operações pesadas da esteira de venda.

4.2.1. Ingestor de Auditoria (ms-audit-logger)

Sidecar ou serviço dedicado que atua como *Firehose* de logs normativos.

- **Responsabilidade:** Garantir que nenhum evento de negócio seja perdido, mesmo sob alta carga.
- **Mecanismo de Ação:**
  - Recebe eventos via gRPC (baixa latência) dos demais microsserviços.
  - Calcula o SHA-256 do payload imediatamente (garantia de integridade na origem).
  - Persiste o log na TB_AUDIT_TRAIL e despacha o payload bruto para o *Object Storage* (Bucket Bronze/WORM) de forma assíncrona via fila (Kafka/OCI Streaming).
- **Justificativa:** Retira a responsabilidade de "gravar no disco/storage" dos serviços de negócio, reduzindo a latência da transação principal.

4.2.2. Worker de Empacotamento de Evidências (worker-evidence-assembler)

Processo *batch* ou *event-triggered* responsável por gerar os artefatos de prestação de contas exigidos pela Portaria do FNO.

- **Responsabilidade:** Construção dos "Evidence Packs" (TB_EVIDENCE_PACK).
- **Workflow de Execução:**
  - **Trigger:** Acionado na finalização de uma proposta (Status: CONTRACT_SIGNED) ou sob demanda (auditoria).
  - **Coleta:** Varre a TB_AUDIT_TRAIL usando o ID_CORRELATION para buscar todos os logs e documentos daquela jornada.
  - **Enriquecimento Neurotech:** Consulta o endpoint /gerarPDF do Painel de Regras da Neurotech (via ms-decision-integrator) para baixar o dossiê visual da decisão.
  - **Selagem:** Compacta todos os arquivos, gera o manifesto (manifest.json), calcula o hash final do pacote e o move para o *Archive Tier* (WORM).

4.3. Camada Core de Negócio (Operational Services)

Serviços que implementam as regras de negócio bancárias e do FNO.

4.3.1. Motor de Elegibilidade FNO (ms-fno-eligibility)

4. **Função:** Aplica as regras da Matriz de Elegibilidade (Tamanho do produtor x Localização x Finalidade).
5. **Interação com Dados:** Utiliza as tabelas dimensionais (dim_localizacao, dim_cnae) carregadas no *Autonomous Database* para validar se o proponente se enquadra nas regras do fundo constitucional.

4.3.2. Gestor de Propostas (ms-proposal-core)

5. **Função:** Máquina de estados central da proposta (Saga Orchestrator).
6. **Responsabilidade:** Mantém o estado da TB_PROPOSTA e coordena as chamadas para os *Wrappers* de decisão. Ele não executa regras complexas, apenas orquestra o fluxo (ex: "Se aprovado no ms-decision-integrator, chame ms-credit-pricing").

4.4. Diagrama de Responsabilidade por Componente (Resumo Físico)

Componente (ID)	Tipo	Scaling Strategy	Dependência Externa	Artefato de Dados Principal
ms-decision-integrator	API (Stateless)	CPU-Bound (Crypto/Parsing)	Neurotech Decision Runner	TB_NEUROTECH_TRANSACTION
ms-identity-trust	API (Stateless)	I/O-Bound (HTTP Requests)	LexisNexis API	TB_KYC_RESULT
ms-audit-logger	Stream Processor	High Throughput	OCI Object Storage	TB_AUDIT_TRAIL
worker-evidence-assembler	Background Job	Memory-Bound (Zip/PDF)	Neurotech Painel (PDF)	TB_EVIDENCE_PACK
ms-proposal-core	API (Stateful Logic)	Transaction-Bound	Autonomous DB (ATP)	TB_PROPOSTA

5. Integrações Sistêmicas e Contratos de Interface

A arquitetura de integração da Plataforma SIGA é estruturada sobre uma camada de **Interoperabilidade Gerenciada**, onde todas as trocas de dados com parceiros externos (Neurotech, LexisNexis) e barramentos governamentais são estritamente mediadas pelos componentes *Decision Wrappers*.

Este modelo arquitetural estabelece o isolamento mandatório entre o *Core Bancário* e os fornecedores externos, garantindo a governança centralizada de credenciais, a aplicação uniforme de políticas de resiliência (Circuit Breakers) e a auditoria de fronteira exigida pelos órgãos de controle.

Os contratos de interface detalhados a seguir constituem a norma técnica para o desenvolvimento dos microsserviços.

5.1. Protocolos de Interoperabilidade e Segurança

Todas as interfaces de integração devem implementar, obrigatoriamente, os seguintes controles não-funcionais:

8. **Protocolo de Transporte:** Utilização exclusiva de HTTPS com TLS 1.3 para garantia de confidencialidade em trânsito.
9. **Rastreabilidade de Jornada:** Injeção mandatória do *header* HTTP X-Correlation-ID em todos os *Requests* externos, propagando o UUID único da jornada de crédito.
10. **Gestão de Credenciais:** Segredos (client_id, client_secret, certificados) devem ser injetados em tempo de execução via *OCI Vault*. É vedada a presença de credenciais em código-fonte ou variáveis de ambiente não criptografadas.
11. **Auditoria de Fronteira (Raw Log):** O *payload* integral (Request e Response brutos) de cada interação externa deve ser processado para cálculo de hash (SHA-256) e persistido assincronamente na entidade TB_AUDIT_TRAIL antes da execução da regra de negócio, garantindo não-repúdio.

5.2. Integração de Identidade e PLD (LexisNexis)

Esta integração operacionaliza os processos de *Know Your Customer* (KYC) e Prevenção à Lavagem de Dinheiro (PLD/FT), utilizando as suítes InstantID e Bridger Insight da LexisNexis.

5.2.1. Especificação do Fluxo

- **Componente Executor:** ms-identity-trust
- **Gatilho de Execução:** Evento de negócio onboarding.docs.uploaded
- **Padrão de Comunicação:** Síncrono (REST POST)

5.2.2. Contrato de Dados (Interface Specification)

O payload deve aderir estritamente ao schema definido para maximizar a assertividade dos motores de antifraude e sanções.

Objeto	Atributo Crítico	Definição Técnica e Regra de Preenchimento
Request	cpf_cnpj	Identificador fiscal sanitizado (apenas dígitos numéricos).
	biometria_hash	Hash criptográfico ou vetor de características da face capturada (evitar tráfego de imagem bruta na API de

		dados).
	consentimentos_lgpd	Objeto contendo o *timestamp* e o IP de origem do aceite dos termos de uso e privacidade.
Response	provider_case_id	**Chave de Rastreio:** Identificador único da transação gerado pela LexisNexis. Deve ser persistido na coluna provider_ref da tabela TB_KYC_RESULT.
	score_identity	Inteiro (0-1000) indicando a probabilidade de fraude sintética ou documental.
	pld_screening_result	Lista estruturada de *matches* positivos em listas restritivas (OFAC, ONU, PEP, Mídia Adversa).
	doc_validation_status	Enumeração do status de validação documental (ex: VERIFIED, ALTERED, INCONCLUSIVE).

5.2.3. Requisito de Evidência

O provider_case_id retornado deve ser vinculado inequivocamente ao ID_CORRELATION na trilha de auditoria. O relatório detalhado de PLD (Dossiê PDF/JSON) deve ser baixado e armazenado no *Bucket Bronze* (WORM) para fins de comprovação regulatória junto ao COAF e Banco Central (Circular 3.978).

5.3. Integração de Risco e Fraude (Neurotech - Decision Runner)

A integração com o motor *Decision Runner* (DR) implementa o padrão de **Fluxo Híbrido Adaptativo**, capaz de alternar dinamicamente entre execução síncrona e assíncrona

conforme a complexidade da política de crédito e a latência da rede.

5.3.1. Gestão de Autenticação (OAuth 2.0)

O microsserviço ms-decision-integrator deve implementar uma máquina de estados para gestão do token de acesso ao Portal Riskpack (RA):

- **Autenticação:** Execução de POST /oauth/login enviando as credenciais de serviço (client_id, secret_id).
- **Cacheamento Seguro:** O access_token deve ser armazenado em cache distribuído (Redis) com TTL configurado para expires_in - 60s.
- **Renovação Proativa:** O sistema deve renovar o token antes de sua expiração total para evitar latência adicional durante a transação de crédito.

5.3.2. Estratégia de Submissão Híbrida

O *Decision Wrapper* deve selecionar o endpoint de submissão adequado baseando-se na tipologia da proposta e na saúde do serviço externo.

Cenário A: Fast Track (Síncrono)

- **Método:** POST /api/v1/workflow/submit
- **Aplicabilidade:** Políticas de fraude preliminar (*Fail-Fast*), validação de regras de negócio simples e consultas de *Bureau*.
- **Comportamento:** O sistema aguarda a resposta HTTP com o objeto RuleResult e Outputs já calculados.

Cenário B: Deep Analysis (Assíncrono)

- **Método:** POST /api/v1/workflow/submitAsync
- **Aplicabilidade:** Políticas de Crédito FNO (alta complexidade), Análise de Renda detalhada ou acionamento automático por *Circuit Breaker* (latência > 3.000ms).
- **Workflow de Processamento:**
  - Recebimento imediato do OperationCode (Protocolo).
  - Inicialização de rotina de *Polling* no endpoint GET /submission/{OperationCode} com *backoff* exponencial.
  - Monitoramento até a obtenção dos status finais: Concluído (0100) ou Stop (0200).

5.3.3. Contrato de Payload (Decision Runner Standard)

A estrutura de dados deve respeitar a taxonomia de Inputs (Variáveis de Decisão) e Properties (Metadados de Contexto) exigida pelo motor.

```
{
  "Policy": "POLITICA_CREDITO_FNO_V2",
  "Inputs": [
    { "Name": "vl_renda_declarada", "Value": 5000.00 },
    { "Name": "cd_cnae_principal", "Value": "0111301" },
```

```
   { "Name": "fl_zona_prioritaria", "Value": true }
  ],
  "Properties": [
   { "Name": "USUARIO", "Value": "system_siga_prod" },
   { "Name": "RETORNO_FILTRO_MODO", "Value": "exclusao" },
   { "Name": "RETORNO_FILTRO_VARIAVEIS", "Value": "debug_trace;raw_db_dump" }
  ]
}
```


5.3.4. Artefatos de Auditoria (Painel de Regras)

Para cada decisão de crédito (Aprovada ou Reprovada), o sistema deve executar mandatoriamente:

- Persistência do OperationCode na tabela TB_NEUROTECH_TRANSACTION.
- Acionamento do *Worker de Evidência* para consumir o serviço de **Geração de PDF do Painel**, obtendo a representação visual da árvore de decisão.
- Armazenamento deste artefato no *Archive Tier* (WORM) como prova material da motivação técnica do deferimento ou indeferimento.

5.4. Ingestão de Dados Públicos e Abertos

Para o enriquecimento de dados e validação de enquadramento no FNO (CNAE e Localização), a arquitetura utiliza estratégias de ingestão otimizadas para reduzir a dependência de disponibilidade externa em tempo real.

- **Fontes Oficiais:** API de Dados Abertos do Banco Central (BCB), IBGE (Localidades) e PNDR (Integração Regional).
- **Componentes:** OCI Functions para orquestração e API Gateway para exposição interna.
- **Estratégia de Atualização:**
  - **Dados Voláteis** (Taxas, Índices, Selic): Consulta *on-demand* com cache de curta duração (TTL 1h).
  - **Dados Estáticos** (Municípios, Lista de CNAEs): Processo de *ETL Batch* diário para atualização das tabelas dimensionais (dim_localizacao) no *Autonomous Database*. As regras de crédito devem consumir estas tabelas locais para garantir performance e alta disponibilidade.

6. Arquitetura de Dados, Persistência e Governança

A arquitetura de dados do SIGA foi desenhada para atender aos requisitos de alta disponibilidade transacional e rigorosa conformidade normativa exigida pela Portaria MIDR nº 1.627/2023. O modelo de persistência adota uma abordagem híbrida, combinando bancos de

dados relacionais para controle operacional e *Object Storage* imutável (WORM) para evidências auditoráveis.

6.1. Modelo de Dados Físico e Entidades de Compliance

O modelo de dados físico expande as camadas lógicas para incluir estruturas dedicadas à rastreabilidade fim-a-fim, integridade de transações externas e empacotamento de evidências regulatórias. A persistência é segregada em três domínios principais: Operacional, Auditoria/Compliance e Integração de Risco.

6.1.1. Camada de Auditoria e Rastreabilidade (Audit Trail)

A entidade `TB_AUDIT_TRAIL` atua como o indexador mestre para todos os eventos do sistema, garantindo a correlação entre ações de negócio e os artefatos armazenados em mídia imutável. Esta estrutura suporta a reconstrução linear de qualquer jornada de crédito para fins de auditoria do TCU e CGU.

Atributo (Coluna)	Tipo de Dado	Restrição	Descrição Técnica e Finalidade Normativa
ID_EVENTO	UUID	PK	Identificador único e universal do evento de auditoria.
DT_EVENTO	TIMESTAMP	NOT NULL	Data e hora exata da ocorrência (UTC), sincronizada via NTP para garantia de *timestamping*.
ID_CORRELATION	UUID	INDEX	**Chave de Jornada:** Identificador único da sessão/proposta que agrupa todos os eventos, desde o *onboarding* até a cessão. Essencial para visão

			End-to-End.
NM_EVENTO	VARCHAR(100)	NOT NULL	Taxonomia padronizada do evento (ex: credit.policy.scored, fno.eligibility.checked, contract.signed).
ID_ACTOR	VARCHAR(50)	NOT NULL	Identificação do executor (CPF do operador, CNPJ do sistema parceiro ou Service Account ID).
VL_PAYLOAD_HASH	CHAR(64)	NOT NULL	Hash SHA-256 do *payload* trafegado. Assegura a integridade e o não-repúdio do conteúdo processado.
URI_IMMUTABLE_POINTER	VARCHAR(512)	NOT NULL	Endereço lógico do objeto bruto (JSON/PDF) no *OCI Object Storage* (Bucket com retenção WORM ativa).
NR_RULE_VERSION	VARCHAR(20)	NULL	Versão da política de negócio ou regra de crédito vigente na execução (ex: v2.1-2026).

6.1.2. Camada de Integração Antifraude (Neurotech Integration)

Para suportar a integração com o motor *Decision Runner* (Neurotech) e seus fluxos híbridos (síncrono e assíncrono), o modelo de dados prevê a persistência detalhada do ciclo de vida da análise de risco, indo além do *score* numérico para armazenar o dossiê completo de decisão.

Atributo (Coluna)	Tipo de Dado	Restrição	Descrição Técnica e Finalidade Normativa
ID_TRANSACTION	BIGINT	PK	Identificador sequencial interno do SIGA para a transação de risco.
ID_PROPOSTA	BIGINT	FK	Referência à proposta de crédito na camada operacional (TB_PROPOSTA).
CD_OPERATION_CODE	VARCHAR(50)	INDEX	**Chave Externa:** Código retornado pelos métodos Submit ou SubmitAsync. Obrigatório para recuperação futura do PDF via GetSubmission.
ST_WORKFLOW	VARCHAR(20)	NOT NULL	Estado do fluxo: SUBMITTED, PENDING, COMPLETED, STOP_FAIL ou APPROVED.
JSON_INPUTS	CLOB/JSON	NOT NULL	Snapshot dos dados enviados (Inputs) ao motor, garantindo auditoria do que foi

			submetido à análise.
JSON_OUTPUT_FULL	CLOB/JSON	NOT NULL	Dossiê completo retornado pela política (Properties, RuleResults, Outputs), constituindo a defesa técnica da decisão.
DT_LAST_UPDATE	TIMESTAMP	NOT NULL	Data da última atualização de status (via *polling* ou *callback*).

6.1.3. Camada de Gestão de Evidências (Evidence Packaging)

A entidade `TB_EVIDENCE_PACK` gerencia o ciclo de vida dos pacotes de prestação de contas. Esta estrutura lógica agrupa documentos, logs e relatórios em um único artefato auditável, conforme exigido para inspeções do FNO.

Atributo (Coluna)	**Tipo de Dado**	**Restrição**	**Descrição Técnica e Finalidade Normativa**
ID_PACK	UUID	PK	Identificador único do pacote de evidência.
TP_PACK	VARCHAR(30)	NOT NULL	Tipologia: FNO_MONTHLY_REPORT, TCU_AUDIT_REQUEST, SCR_3040_CESSAO.
DT_GENERATION	DATE	NOT NULL	Data de fechamento e selagem do pacote.

ST_PACK	VARCHAR(15)	NOT NULL	Status: OPEN (coleta), SEALED (fechado/imutável), SENT (transmitido).
HASH_MANIFEST	CHAR(64)	NOT NULL	**Assinatura Digital:** Hash SHA-256 do arquivo manifest.json. Garante que nenhum documento foi alterado após o fechamento.
URI_STORAGE_LINK	VARCHAR(512)	NOT NULL	Link para o arquivo consolidado (.zip) no armazenamento de longa duração.

6.2. Estratégia de Armazenamento e Retenção (Tiering)

A arquitetura utiliza o OCI Object Storage com políticas de ciclo de vida (*Lifecycle Policies*) para gerenciar a retenção de dados conforme sua classificação:

6.2.1. Classificação de Tiers

12. **Hot Tier (Operacional):**
    - **Uso:** Transações correntes, uploads de documentos recentes e logs de *troubleshooting* imediato.
    - **Performance:** Baixa latência (< 10ms).
    - **Retenção:** Ativo enquanto a proposta estiver em curso ou até 90 dias após liquidação.
13. **Infrequent Access (Histórico Recente):**
    - **Uso:** Consultas de propostas liquidadas ou recusadas (D+90 até D+365).
    - **Acesso:** Disponível para *Business Intelligence* e reanálises.
14. **Archive/WORM (Audit Vault):**
    - **Uso:** Logs normativos (TB_AUDIT_TRAIL), pacotes de evidência (TB_EVIDENCE_PACK) e contratos assinados.
    - **Política WORM (Write Once, Read Many):** Configuração de *Retention Rules* bloqueando exclusão e modificação.

    - **Prazo de Retenção:** Mínimo de **10 anos** para dados FNO e PLD/FT, conforme Lei nº 9.613/1998 e Portaria MIDR.

6.3. Arquitetura em Camadas (Medallion Architecture)

O fluxo de dados segue o padrão *Medallion* para garantir qualidade e governança desde a ingestão até o reporte regulatório.

- **Camada Bronze (Raw Ingestion):**
    - Dados brutos ingeridos via CDC (*GoldenGate*) ou eventos (*Kafka*).
    - Armazenamento em formato nativo (JSON/Avro) sem transformações.
    - **Imutabilidade:** Esta camada é a fonte da verdade para auditoria técnica.
- **Camada Silver (Conformed & Cleansed):**
    - Dados padronizados, tipados e deduplicados.
    - Aplicação de regras de *Data Quality* (Tabela fact_dq_kpi).
    - Enriquecimento com dados mestres (Tabelas dim_beneficiario, dim_localizacao).
- **Camada Gold (Curated & Regulatory):**
    - Dados modelados para consumo de negócio e regulatório (*Star Schema*).
    - Geração automática dos extratores SCR 3040 e Relatórios Mensais FNO.
    - Agregações pré-calculadas para performance de dashboards.

6.4. Segurança e Privacidade de Dados

6. **Criptografia:** Todos os dados em repouso são criptografados (TDE/AES-256) com chaves gerenciadas pelo OCI Vault (FIPS 140-2 Nível 3).
7. **Mascaramento (Data Masking):** Ambientes não-produtivos utilizam o *Oracle Data Safe* para anonimizar PII (Dados Pessoais Identificáveis) nas tabelas TB_CLIENTE e TB_PROPOSTA, garantindo conformidade com a LGPD.

7. Infraestrutura Cloud, SRE e Volumetria

A infraestrutura da Plataforma SIGA é provisionada sobre a Oracle Cloud Infrastructure (OCI), adotando uma topologia **Cloud-Native Elástica** projetada para suportar a forte sazonalidade do crédito rural (Picos de Safra) com eficiência de custos, garantindo a perenidade dos dados de auditoria sem desperdício de recursos na entre-safra.

Esta especificação define os parâmetros físicos de *Compute*, *Storage* e *Networking* necessários para atingir os SLAs de negócio (Latência < 200ms) e os requisitos regulatórios, ajustados para uma volumetria anual de **10 milhões de requisições**.

7.1. Topologia Física e Zonas de Disponibilidade

A arquitetura utiliza uma estratégia **Multi-Region Active-Passive** para garantir resiliência

catastrófica, com segregação lógica de ambientes para compliance.

15. **Região Primária (Active):** OCI GRU (São Paulo). Hospeda 100% da carga transacional em operação normal.
16. **Região de Disaster Recovery (Passive):** OCI VCP (Vinhedo). Mantém réplicas síncronas dos dados críticos e infraestrutura mínima (*Pilot Light*) desligada ou hibernada, pronta para *Hydration* (subida automática) em caso de desastre.
17. **Conectividade Híbrida:** Link dedicado *OCI FastConnect* dimensionado para a carga transacional ajustada (ex: 1 Gbps redundante), interligando o Data Center On-Premise do BASA à VCN do SIGA com latência < 2ms.

7.2. Dimensionamento Computacional e Volumetria (Capacity Planning)

O dimensionamento dos recursos foi recalibrado para a volumetria projetada de **10 milhões de requisições/ano**. Dado o perfil de tráfego, a prioridade é a **elasticidade horizontal**: o ambiente opera com footprint mínimo na maior parte do ano e escala agressivamente durante as janelas de safra.

7.2.1. Camada de Microsserviços (OKE)

O cluster Kubernetes (Oracle Container Engine for Kubernetes) utiliza *Cluster Autoscaler* para reduzir custos de computação durante períodos de baixa demanda.

- **Node Pools:** Segregação de *workloads* para otimização de recursos.
  - **API Pool (Critical):** Shapes E4.Flex (AMD EPYC) com configuração mínima de Alta Disponibilidade (3 nós distribuídos em 3 Fault Domains). O *Horizontal Pod Autoscaler (HPA)* gerencia a densidade de pods baseando-se na métrica http_request_rate.
  - **Worker Pool (Batch):** Shapes otimizados para memória para o worker-evidence-assembler. Configurado para escalar a zero (0 nós) quando não houver fila de processamento de PDFs, maximizando a economia.
- **Ingress Controller:** OCI Load Balancer flexível (Shape 10Mbps-400Mbps) que ajusta a banda automaticamente conforme o tráfego de entrada.

7.2.2. Camada de Banco de Dados (Autonomous Database)

A persistência utiliza o Oracle Autonomous Database com **Auto-Scaling de OCPU** para pagar apenas pelo processamento utilizado no momento exato.

- **Core Transacional (ATP):**
  - **Configuração:** OCPU Auto-Scaling ativado.
  - **Sizing:** Baseline inicial de **2 OCPUs** (mínimo para HA) podendo escalar automaticamente até **Max OCPUs** durante os picos de safra, sem *downtime*.
  - **Storage:** Exadata Infrastructure gerenciada.
- **Data Warehouse (ADW/Lakehouse):**
  - **Estratégia:** Otimizado para processamento *Batch* noturno ou mensal (relatórios

FNO/SCR). O banco pode ser desligado ou reduzido drasticamente fora das janelas de fechamento contábil.

7.2.3. Camada de Ingestão de Dados (GoldenGate Hub)

Componente dimensionado para garantir a consistência dos dados sem superprovisionamento.

- **Serviço:** OCI GoldenGate for Big Data (Managed).
- **Parâmetros de Performance:**
  - **Throughput Alvo:** Capacidade de absorver "rajadas" (*bursts*) de ingestão durante processamentos em lote e picos de safra sem gerar *Lag* superior a 15 segundos.
  - **Otimização:** Uso de *Batch SQL* para agrupar transações menores, garantindo eficiência mesmo com volume moderado.

7.3. Estratégia de Armazenamento Imutável e Backup

A estratégia de armazenamento foca na segurança jurídica e conformidade (Portaria MIDR), mantendo custos baixos através de *Tiering* automático.

7.3.1. Configuração WORM (Write Once, Read Many)

Todos os *Buckets* designados como repositórios de evidência (audit-trail, evidence-packs) possuem **Retention Rules** bloqueadas.

8. **Política:** Time-Bound Retention.
9. **Duração:** 10 Anos.
10. **Custo-Eficiência:** Objetos com mais de 90 dias são movidos automaticamente para a classe **Archive Storage** (custo ~10x menor que o Standard), visto que o acesso a logs antigos é raro (apenas em auditorias).

7.3.2. Replicação Cross-Region (DR de Evidências)

7. **Mecanismo:** Replicação assíncrona automática para a região VCP.
8. **Consistência:** O bucket de destino herda as regras WORM, garantindo que a evidência replicada também seja imutável e à prova de adulteração.

7.4. Observabilidade e Engenharia de Confiabilidade (SRE)

O monitoramento prioriza a **Saúde do Negócio** e a detecção de anomalias, visto que o volume absoluto é baixo.

7.4.1. The Golden Signals (Adaptados para Baixo Volume/Alta Criticidade)

- **Disponibilidade Sintética (Availability):**

    - Como o tráfego pode ser intermitente, utiliza-se *Synthetic Canaries* (robôs que simulam propostas a cada 5 min) para garantir que o sistema está "vivo" mesmo sem usuários reais logados.
- **Latência de Integração (Latency):**
    - Métrica: neurotech_response_time.
    - Alerta: Disparar se Latência Síncrona > 3s (independente do volume, a experiência do usuário deve ser rápida).
- **Erros de Conformidade (Errors):**
    - Métrica Crítica: Falha na geração do Evidence Pack. Qualquer erro aqui deve gerar um ticket P1 (Prioridade 1), pois compromete a prestação de contas do FNO.
- **Saturação de Recursos (Saturation):**
    - Monitoramento do uso de OCPUs do Banco de Dados para validar se o *Auto-Scaling* está respondendo adequadamente aos picos de safra.

7.4.2. Rastreamento Distribuído

Implementação de *OpenTelemetry* para rastreio total da jornada, essencial para *troubleshooting* rápido em um ambiente onde cada transação tem alto valor financeiro.

7.5. Plano de Continuidade de Negócios (DR/BCP)

O plano de recuperação garante a continuidade das operações com RTO/RPO agressivos, justificados pela criticidade do FNO, não pelo volume.

7.5.1. Métricas de Recuperação (SLA)

- **RTO (Recovery Time Objective):** < 30 minutos. Tempo para "hidratar" (ligar) o ambiente em VCP e virar o DNS. Aumentamos ligeiramente o RTO em relação ao modelo anterior para permitir um DR mais econômico (*Pilot Light*).
- **RPO (Recovery Point Objective):** < 5 minutos. Garantido pelo Data Guard.

7.5.2. Procedimento de Failover Econômico

- **Detecção:** Falha confirmada na região GRU.
- **Hidratação (Scale-Up):** Scripts Terraform/Ansible aumentam a contagem de nós do OKE em VCP (que estava em 0 ou 1) para a capacidade operacional.
- **Switchover:** O Autonomous Database Standby em VCP assume como Primary.
- **Redirecionamento:** DNS Global aponta para VCP.