Relatorio Descritivo Ciclo+

A presente invenção refere-se a um **sistema computacional multi-organizacional** baseado em uma **base lógica compartilhada**, na qual todas as entidades de dados possuem, como atributo técnico obrigatório, um identificador organizacional (orgId/tenantId). Tal identificador atua como elemento técnico de **filtragem automática e nativa** de todas as operações de leitura, escrita e processamento, impedindo tecnicamente qualquer forma de acesso cruzado ou vazamento de dados entre organizações distintas.

Cada operação no sistema é tratada como um **evento operacional estruturado**, submetido a uma **cadeia obrigatória e inseparável de validações técnicas**, compreendendo, em sequência:
(i) autenticação digital do usuário;
(ii) autorização hierárquica baseada em papéis e permissões (RBAC – Role-Based Access Control);
(iii) filtragem automática por identificador organizacional;
(iv) validação pré-execução por um motor de regras configurável;
(v) validação por uma máquina de estados formal que define transições permitidas;
(vi) exigência de captura obrigatória de evidência digital proporcional ao nível de risco da operação;
(vii) registro em auditoria imutável; e, quando aplicável,
(viii) liquidação financeira condicionada ao cumprimento de marcos verificáveis.

A **evidência digital válida** constitui requisito técnico indispensável para a progressão automática da máquina de estados e para a liberação financeira pelo módulo de liquidação condicionada, de modo que nenhuma operação crítica possa avançar ou liberar recursos sem a validação técnica dessa evidência.

O **módulo de liquidação condicionada** mantém valores em custódia lógica (escrow), liberando-os por tranches e/ou realizando split automático somente após o atendimento e registro, em auditoria, de marcos operacionais verificáveis. Caso determinado marco não seja validado, os valores permanecem retidos, sendo o motivo tecnicamente registrado no histórico do sistema.

A auditoria do sistema é implementada como um **registro imutável append-only**, compreendendo:

- hash criptográfico de cada evento e de suas respectivas evidências;
- encadeamento de hashes entre eventos consecutivos;
- carimbo temporal confiável; e, quando aplicável,
- geolocalização e assinatura/atestado do dispositivo responsável pelo registro, formando um lastro probatório tecnicamente resistente a adulterações.

O sistema compreende ainda uma **interface dedicada de auditoria e fiscalização**, acessível exclusivamente a técnicos e auditores autorizados, com permissões restritas à visualização e validação de dados (read-only), sendo tecnicamente vedada qualquer modificação de registros críticos.

A arquitetura do sistema permite a habilitação modular de funcionalidades operacionais por perfil de aplicação setorial, incluindo, sem limitação: estoque, projetos, custódia/consignação, intermediação digital, ordens de serviço, compliance e analytics. Tais módulos operam sobre um **núcleo patenteável inalterado**, que compreende: autenticação, autorização, filtragem organizacional, motor de regras, máquina de estados, exigência de evidência obrigatória, auditoria imutável e liquidação condicionada.

O sistema diferencia eventos por níveis de criticidade:

- Eventos rotineiros admitem **Evidência Tipo A**, composta por identificador/código e marca temporal;
- Eventos críticos exigem **Evidência Tipo B**, incluindo mídia, geolocalização e marca temporal, podendo incluir laudo técnico quando aplicável.

O sistema é projetado para operação eficiente em campo, contemplando:

- pré-validação local de dados;
- cache e sincronização assíncrona;
- idempotência de operações;
- confirmação imediata de status; e
- modo offline com fila de envio e verificação posterior.