

GESTÃO ESTRUTURADA DE COMUNICAÇÕES DE INTERDIÇÕES EM CONCESSIONÁRIAS FISCALIZADAS: PROPOSTA DE BANCO DE DADOS PARA REGISTRO, RASTREABILIDADE E ANÁLISE DE INCIDENTES REPORTADOS VIA WHATSAPP.

TRABALHO DE CONCLUSÃO APRESENTADO AO PROGRAMA DE PÓS-GRADUAÇÃO EM SEGURANÇA DA INFORMAÇÃO DA UNIVERSIDADE DE BRASÍLIA - UnB

Orientador: Prof. Dr. Daniel Chaves Café – FT/UnB
Discente: Gedielson Arnaldo Schmitt

RESUMO

Esta pesquisa aborda a gestão estruturada das comunicações de interdição em rodovias federais concedidas, com foco no tratamento de informações inicialmente reportadas por meio do WhatsApp e sua conversão em registros institucionais rastreáveis. O problema investigado decorre da necessidade de conciliar a celeridade operacional da comunicação por mensagens com os requisitos de integridade, padronização, segurança da informação, memória institucional e conformidade aplicáveis à Administração Pública. O objetivo geral consiste em avaliar possibilidades de arquiteturas e softwares para o registro estruturado de incidentes de interdição das concessionárias fiscalizadas no ambiente do Centro Nacional de Supervisão Operacional - CNSO/ANTT. A pesquisa é aplicada, exploratória e descritiva, com abordagem qualitativa e componente quantitativo para avaliação de desempenho. Propõe-se um fluxo de transição composto por captura controlada da mensagem, extração e normalização dos dados, uso assistido de modelos de linguagem, validação humana, armazenamento em banco de dados relacional e manutenção de trilhas de auditoria. A avaliação será realizada por meio de dados anonimizados e simulações, considerando completude dos campos, tempo de resposta, precisão, taxa de alucinação, conformidade dos prazos de comunicação, atualização dos eventos e rastreabilidade. Como resultado, apresenta-se um modelo de dados capaz de representar ocorrência, concessionária, rodovia, localização, anexos, tratativas, status e auditoria, sem substituir a validação humana nem presumir a existência de integração automática com o sistema oficial. Conclui-se que a automação assistida pode reduzir retrabalho e ampliar a padronização, desde que subordinada a controles de segurança, governança, proteção de dados e autorização institucional.

Palavras-chave: Interdições rodoviárias; WhatsApp; rastreabilidade; banco de dados; inteligência artificial; segurança da informação; LGPD.

ABSTRACT

This research addresses the structured management of road-closure communications on federal concession roads, focusing on the processing of information initially reported through WhatsApp and its conversion into traceable institutional records. The investigated problem arises from the need to reconcile the operational speed of messaging-based communication with the requirements of integrity, standardization, information security, institutional memory, and compliance applicable to Public Administration. The main objective is to assess architectures and software alternatives for the structured registration of road-closure incidents reported by supervised concessionaires within the National Operational Supervision Center environment. The research is applied, exploratory, and descriptive, combining a qualitative approach with a quantitative performance assessment component. The proposed transition workflow includes controlled message capture, data extraction and normalization, assisted use of language models, human validation, relational database storage, and audit trails. The evaluation will use anonymized data and simulations, considering field completeness, response time, precision, hallucination rate, compliance with communication deadlines, event updates, and traceability. As a result, a data model is presented to represent incidents, concessionaires, roads, locations, attachments, actions, status, and auditing, without replacing human validation or assuming the existence of automatic integration with the official system. The study concludes that assisted automation can reduce rework and improve standardization, provided that it remains subject to security controls, governance, data protection, and institutional authorization.

Keywords: road closures; WhatsApp; traceability; database; artificial intelligence; information security; LGPD.

1 INTRODUÇÃO

A fiscalização de rodovias federais concedidas depende da circulação tempestiva de informações sobre interdições, sinistros, falhas operacionais, alterações de tráfego e demais ocorrências capazes de afetar a segurança viária e a continuidade do serviço. Nesse ambiente, a comunicação inicial precisa ser rápida e suficiente para apoiar a tomada de decisão, mas também deve produzir registros íntegros, padronizados e recuperáveis para fins de acompanhamento operacional, auditoria, prestação de contas e memória institucional.

Na prática, parte dessas comunicações é realizada por aplicativos de mensagem, especialmente o WhatsApp. O canal oferece simplicidade e velocidade, características relevantes em situações distribuídas territorialmente e com necessidade de resposta imediata. Entretanto, a mensagem de origem não constitui, por si só, um registro estruturado de ocorrência: pode apresentar abreviações, campos ausentes, informações duplicadas, imagens sem descrição, horários ambíguos e diferentes formas de indicar rodovia, município, quilômetro, sentido ou causa do evento.

A utilização de canais não estruturados também cria desafios de governança. Informações relevantes podem permanecer dispersas em conversas, dificultando a identificação da versão mais atual, dos responsáveis por cada providência e do momento exato em que a Agência ou a concessionária tomou conhecimento do fato. Consequentemente, aumenta-se o risco de retrabalho, perda de histórico, inconsistência entre registros e dificuldade de reconstrução da linha do tempo do evento.

Esse problema é particularmente relevante no contexto do Centro Nacional de Supervisão Operacional, no qual as informações sobre ocorrências devem subsidiar supervisão, monitoramento e articulação institucional. A comunicação operacional precisa ser convertida em dado administrativo com campos definidos, regras de validação, controle de acesso e trilha de auditoria. Essa conversão deve preservar a agilidade do primeiro informe sem transformar o aplicativo de mensageria em repositório oficial ou substituir os sistemas institucionais da Agência.

A pesquisa parte, portanto, da seguinte questão: como estruturar um fluxo de captura, validação e armazenamento capaz de transformar comunicações de interdição originadas no WhatsApp em registros institucionais íntegros, rastreáveis e aderentes aos requisitos de segurança da informação e proteção de dados? A questão envolve dimensões técnicas e organizacionais, pois não se limita à escolha de uma ferramenta:

exige definir campos, responsabilidades, critérios de qualidade, mecanismos de atualização e limites para o uso de inteligência artificial.

A hipótese do estudo é que a combinação de formulário orientado, modelo de linguagem e validação humana pode reduzir o tempo de transcrição e ampliar a completude e a padronização dos registros, sem comprometer a rastreabilidade e a segurança. A hipótese não pressupõe lançamento automático em produção: a inteligência artificial será tratada como mecanismo de apoio e pré-preenchimento, enquanto a validação humana permanecerá necessária para campos críticos, especialmente classificação de criticidade, impacto, faixas, congestionamento, vítimas e previsão de liberação.

A relevância do trabalho é acadêmica e institucional. No plano acadêmico, a pesquisa articula gestão de incidentes, segurança da informação, governança de dados, modelagem relacional, inteligência artificial e proteção de dados. No plano institucional, a proposta pode contribuir para reduzir a dependência de soluções paralelas, melhorar a qualidade da informação recebida e fortalecer a capacidade de demonstrar quando uma ocorrência foi comunicada, quais providências foram adotadas e como o evento evoluiu.

PROBLEMA DE PESQUISA

Existe uma necessidade de comunicação célere de interdições totais ou parciais em rodovias concedidas. Essa comunicação é feita atualmente através de canais populares como o WhatsApp. Dentro de uma estrutura institucional, é necessário, estruturar um banco de dados e um fluxo de transição de dados que permitam registrar de forma íntegra, auditável e aderente à LGPD, as informações sobre interdições. O aplicativo WhatsApp utiliza um modelo de dados temporários, sendo impossível guardar comunicações por longos prazos. Para resolver esse problema, este projeto estuda possibilidades de adaptadores para o WhatsApp que registrem informações de forma definitiva em bancos de dados institucionais. O objetivo é registrar informações para estudo posterior assegurando rastreabilidade, memória institucional e suporte à tomada de decisão no contexto do CNSO e da fiscalização regulatória.

OBJETIVO GERAL

Propor um modelo de arquitetura de transição, registro e rastreabilidade para comunicações de interdições em rodovias federais concedidas, originalmente recebidas por mensagens de whatsapp, aplicável ao contexto do CNSO/ANTT. De forma específica, há a necessidade de um banco de dados e de um fluxo de captura, validação e armazenamento.

OBJETIVOS ESPECÍFICOS:

- 1. Identificar** os requisitos informacionais, operacionais, de segurança e de proteção de dados necessários ao tratamento institucional de comunicações de interdição;
- 2. Definir** um fluxo de captura controlada, extração, normalização, validação humana e registro das informações recebidas por canais autorizados de mensageria;
- 3. Modelar** uma estrutura relacional de dados para representar ocorrências, rodovias, concessionárias, localizações, responsáveis, tratativas, anexos e trilhas de auditoria;
- 4. Especificar** o uso de inteligência artificial como mecanismo assistido de extração e pré-preenchimento, subordinado à validação humana para classificação, correção e registro de campos críticos;
- 5. Estabelecer** critérios e métricas de referência para futura validação da proposta, incluindo completude, precisão de preenchimento, rastreabilidade, conformidade temporal, segurança e taxa de correção humana;
- 6. Demonstrar** conceitualmente a aplicação do modelo por meio de cenário simulado e dados anonimizados ou sintéticos, sem integração automática com sistemas institucionais em produção.

JUSTIFICATIVA:

A fiscalização de concessionárias de infraestrutura rodoviária demanda comunicações rápidas, confiáveis e rastreáveis sobre eventos críticos, sobretudo quando envolvem interdições, acidentes graves, impactos operacionais relevantes e possível repercussão institucional. O material-base da proposta destaca que, no cenário atual, parte significativa dessas comunicações ocorre por meio de aplicativo de mensagens, o que favorece agilidade operacional, mas fragiliza a gerenciabilidade, a auditoria, a preservação da evidência digital e a memória organizacional.

No contexto do CNSO, as informações operacionais são tratadas em ambiente tecnológico voltado ao processamento, armazenamento, análise e transformação de grande volume de dados em informação estratégica para a ANTT, com atuação ininterrupta de operadores e supervisores e uso de ferramentas como Sirad, Zabbix e Grafana. Esse contexto reforça a pertinência de uma solução estruturada que permita integrar o tratamento das comunicações de interdição à lógica de monitoramento, supervisão e apoio à decisão institucional.

A relevância acadêmica do tema decorre da convergência entre privacidade, segurança da informação, governança de dados e gestão de incidentes em infraestrutura crítica. A relevância prática, por sua vez, reside na possibilidade de propor um modelo aplicável à realidade administrativa do órgão, reduzindo dependência de Shadow IT (adoção de soluções de TI não homologadas formalmente), ampliando a rastreabilidade dos registros, fortalecendo a conformidade com a LGPD e viabilizando análises históricas e gerenciais mais consistentes.

METODOLOGIA

A pesquisa tem natureza aplicada, com abordagem qualitativa e exploratória, estruturada como estudo de caso voltado ao fluxo atual de comunicação de interdições em concessionárias fiscalizadas. O trabalho compreende levantamento do processo vigente, identificação de vulnerabilidades informacionais e proposição de arquitetura de transição entre o ambiente não estruturado de mensageria e um repositório estruturado com trilhas de auditoria.

A modelagem contempla definição de requisitos funcionais e de segurança da informação, elaboração de diagrama entidade e relacionamento, dicionário de dados e regras mínimas de integridade, disponibilidade, confidencialidade e não repúdio. Um exemplo é fornecido com dados de demonstração anonimizados, capaz de representar consultas gerenciais e cenários de acompanhamento de incidentes reportados no contexto operacional do CNSO e das rotinas de fiscalização descritas no material de visita.

ESTRUTURA PRELIMINAR DO TRABALHO

- **Capítulo 1 – Introdução:** Contexto, problema, objetivos e justificativa.
- **Capítulo 2 – Referencial teórico:** Gestão de incidentes em infraestrutura crítica, Shadow IT, riscos do uso de aplicativos de mensageria no setor público, princípios de segurança da informação, LGPD, modelagem de dados e trilhas de auditoria.
- **Capítulo 3 – Metodologia:** Análise do fluxo atual, estudo de caso, arquitetura de transição, modelagem de dados e especificação de requisitos de segurança.
- **Capítulo 4 – Resultados e discussão:** Descrição do banco proposto, dicionário de dados, simulação com dados anonimizados e avaliação de rastreabilidade e conformidade.
- **Capítulo 5 – Considerações finais:** Limitações, recomendações institucionais e trabalhos futuros.

DELIMITAÇÃO DE ESCOPO E ADERÊNCIA AO PPSI/UNB

A proposta está diretamente alinhada ao campo de Privacidade e Segurança da Informação ao tratar do registro estruturado de comunicações operacionais potencialmente sensíveis, com foco em integridade, rastreabilidade, auditoria, governança e conformidade regulatória. O trabalho também dialoga com o ambiente institucional descrito para o CNSO, no qual monitoramento tecnológico, supervisão operacional. A proposta contribui, assim, para a redução dos riscos associados ao shadow IT e para fortalecimento da cadeia de custódia digital no âmbito da regulação de Transportes Terrestres.

O trabalho consiste no desenho da solução, na modelagem do banco de dados, na definição do fluxo de informação e na validação por protótipo funcional, sem depender de integração direta com APIs externas ou implantação institucional completa.

CAPÍTULO 2 – REFERENCIAL TEÓRICO

2.1 Shadow IT e o uso não estruturado de aplicativos de mensageria no setor público

A adoção de soluções de Tecnologia da Informação (TI) não homologadas formalmente pelos setores competentes, fenômeno conhecido como Shadow IT, tornou-se uma realidade relevante na administração pública contemporânea.

Em termos práticos, trata-se do uso de aplicativos, sistemas ou recursos tecnológicos por servidores e colaboradores sem a devida validação institucional, muitas vezes motivado pela necessidade de dar resposta mais rápida às demandas operacionais, sobretudo quando os sistemas oficiais são percebidos como lentos, burocráticos ou insuficientemente aderentes à dinâmica do trabalho. Esse comportamento, embora impulse inovação, introduz vulnerabilidades de segurança, conformidade e governança de dados (Souza et al., 2021).

No âmbito do CNSO/ANTT, esse fenômeno pode ser observado, por exemplo, quando agentes e equipes operacionais recorrem ao WhatsApp para comunicar interdições, ocorrências em campo, alterações de fluxo, solicitações urgentes de apoio ou confirmação de providências relacionadas à fiscalização. Embora essa prática seja compreensível diante da exigência de agilidade e da amplitude territorial da atuação da ANTT, especialmente em um cenário de fiscalização distribuído por 32 concessionárias federais operadas por empresas privadas sob contrato com a Administração Pública, ela também revela uma lacuna entre a necessidade operacional e a governança tecnológica formal.

Sob essa perspectiva, o WhatsApp pode funcionar como um canal de resposta rápida, mas não substitui, com segurança jurídica e administrativa, os sistemas institucionais destinados ao registro, tramitação e preservação das informações. Em situações em que o sistema oficial não oferece retorno célere, não gera “sensação de segurança” suficiente para o usuário interno ou não permite rastreabilidade adequada, o agente tende a migrar para soluções paralelas, criando um ambiente de comunicação fragmentado. Isso afeta diretamente a fiscalização, pois compromete a uniformidade do fluxo informacional, dificulta a auditabilidade das decisões e pode enfraquecer a cadeia de custódia digital das evidências produzidas em campo.

Nesse contexto, o uso informal de aplicativos de mensageria deve ser analisado não apenas como uma solução prática, mas como um risco de governança. Em um cenário de fiscalização rodoviária, uma interdição informada por WhatsApp pode até permitir resposta imediata, mas se essa comunicação não for formalmente registrada, ela pode perder valor probatório, gerar divergências de versão, dificultar a reconstrução cronológica dos fatos e comprometer a defesa institucional em eventual questionamento administrativo ou judicial.

Além disso, a circulação de informações em canais não estruturados dificulta o controle documental e a recuperação do histórico operacional. Mensagens podem reunir dados sobre concessionárias, rodovias, responsáveis, imagens e providências, sem vinculação uniforme a uma ocorrência. Quando essas informações permanecem dispersas em conversas, torna-se mais difícil identificar versões, reconstruir a sequência dos acontecimentos e acompanhar o tratamento institucional do evento. No âmbito desta pesquisa, essa limitação é examinada sob a perspectiva da organização e da rastreabilidade dos registros, sem avaliação de conformidade jurídica. (Freitas & Rodrigues, 2022).

Uma pesquisa da Zenvia com a Opinion Box (2024) evidenciou que 47% dos colaboradores brasileiros usam o WhatsApp pessoal para assuntos do trabalho, e 39% destacam que isso provoca erros operacionais, principalmente devido à mistura de conversas pessoais com as profissionais.

Exemplo prático no CNSO/ANTT

Imagine que um agente de fiscalização identifique, em rodovia concedida, um problema de sinalização, uma interdição parcial ou um evento que gere risco à segurança viária. Se ele comunica a situação apenas por WhatsApp ao gestor de plantão, sem posterior registro em sistema oficial, a informação pode se dispersar, ser apagada, ficar inacessível ou não integrar o histórico formal do caso. Mais tarde, se houver questionamento sobre atraso na resposta, falha de atuação ou responsabilidade por danos a usuários, a instituição pode ter dificuldade para demonstrar quando recebeu a informação, quem a recebeu, quais providências foram adotadas e em qual tempo.

Outro exemplo ocorre quando há reclamação de usuário por supostos perdas ou danos decorrentes de evento em rodovia concedida. Para uma defesa institucional eficiente, não basta confiar em mensagens informais. A apuração deve buscar suporte em fontes formais e verificáveis, como: registros do centro de controle operacional, relatórios de ocorrência, ordens de serviço, comunicados oficiais da concessionária, registros de atendimento ao usuário, autos de fiscalização, fotografias datadas, vídeos, boletins de ocorrência, relatórios técnicos, mapas de evento, comunicações internas

formalizadas e, se aplicável, registros do contrato de concessão e dos anexos operacionais. É esse conjunto documental que permite reconstruir a cronologia dos fatos e sustentar tecnicamente a resposta da ANTT em eventual procedimento administrativo ou ação judicial.

E onde se buscaria tais informações para embasar defesa?

Em caso de reclamação de usuário sobre perdas, danos ou falhas de serviço, a fundamentação defensiva deve-se buscar prioritariamente em fontes oficiais e rastreáveis, como:

- ✓ Sistema institucional de registros e ocorrências;
- ✓ Relatórios da fiscalização;
- ✓ Comunicações formais com a concessionária;
- ✓ Registros de atendimento ao usuário;
- ✓ Documentos contratuais da concessão;
- ✓ Evidências fotográficas e audiovisuais com data e contexto;
- ✓ Autos de infração, notificações e despachos;
- ✓ Relatórios técnicos de vistoria;
- ✓ Histórico de manutenção, sinalização e intervenção na rodovia.

Na prática, isso significa que o WhatsApp pode até servir como meio de pré-comunicação, mas jamais deve ser tratado como repositório principal de prova. A informação relevante precisa ser convertida em registro institucional, sob pena de fragilizar a memória administrativa e a capacidade de defesa da ANTT.

Dessa forma, o Shadow IT no CNSO/ANTT não deve ser compreendido apenas como desvio tecnológico, mas como sintoma de uma tensão estrutural entre agilidade operacional e governança formal. O uso não estruturado do WhatsApp emerge como resposta a limitações do sistema oficial, porém cria riscos concretos de segurança, rastreabilidade, padronização e responsabilização. Para que a fiscalização seja juridicamente segura e administrativamente consistente, é indispensável que toda comunicação operacional relevante seja absorvida por fluxos institucionais formais, garantindo preservação da prova, integridade documental e suporte adequado à atuação técnica da Agência.

A informalidade do canal leva à perda de histórico de interações, memória técnica e institucional bem como, gera aumento de retrabalho.

2.2 Pipeline de Extração Transformação e Carga (ETL, do inglês Extract, Transform and Load) para dados não estruturados em ambientes de emergência e monitoramento

Pereira & Silva (2023) propõem um pipeline ETL especificamente projetado para mensagens de emergência. O fluxo inclui coleta de mensagens, de áudio e texto, transcrição automática de áudio via ASR, e classificação do conteúdo por meio de Processamento de Linguagem Natural (PLN), além da carga em um banco de dados estruturado para alimentar dashboards de apoio à decisão. Embora o estudo de caso seja uma proposta de arquitetura de um banco de dados do WhatsApp, estruturá-los e disponibilizá-los para análise gerencial é um grande desafio.

A conversão dessas mensagens não estruturadas, tais como textos curtos, áudios, imagens e registros informais produzidos em aplicativos de mensageria, em dados analíticos organizados configura um desafio recorrente nos processos de Extração, Transformação e Carga (ETL). Mehmood & Anees (2020), em contextos de emergência e monitoramento, tal desafio torna-se ainda mais complexo em razão da heterogeneidade das fontes, da velocidade de circulação das informações e da necessidade de processamento em tempo reduzido.

Khattach et al. (2025) avançam ao propor uma arquitetura *end-to-end* para análise de dados de IoT em tempo real, utilizando Apache Kafka para ingestão, Apache Spark para processamento ETL e InfluxDB para armazenamento de séries temporais. Este modelo demonstra que é possível construir sistemas escaláveis e resilientes para monitoramento de eventos críticos, um requisito que está implícito na fiscalização de rodovias concedidas.

Essas literaturas especializadas indicam que os principais entraves associados a pipelines ETL concentram-se, sobretudo, na variedade dos dados e na exigência de tratamento em tempo real, especialmente quando se trata de conteúdos semiestruturados ou não estruturados.

No âmbito da Agência, essa problemática adquire relevância operacional e institucional significativa. Em cenários de fiscalização de rodovias concedidas, a comunicação entre agentes de campo, centrais operacionais e unidades de apoio demanda celeridade, confiabilidade e rastreabilidade. Entretanto, quando os sistemas institucionais apresentam baixa responsividade, limitações de usabilidade ou insuficiente sensação de segurança informacional para o usuário interno, observa-se a tendência de utilização de aplicativos de mensageria, como o WhatsApp, para encaminhamento de ocorrências, interdições, alterações de tráfego e solicitações de apoio emergencial. Embora tal prática possa atender à urgência da operação, ela produz um fluxo informacional disperso, não padronizado e de difícil consolidação posterior, comprometendo a governança dos dados e a formalização dos registros.

Essa questão torna-se ainda mais sensível diante da amplitude da atuação regulatória da ANTT, que abrange atualmente **32 concessionárias federais**, com projeção de expansão para mais **8 concessionárias** nos próximos meses, todas operadas por instituições privadas sob contrato com o órgão federal. Em um ambiente dessa magnitude, a perda de alguns minutos na transmissão de uma ocorrência pode comprometer a eficiência da resposta institucional, retardar o acionamento de equipes, ampliar o impacto de um incidente e intensificar riscos à integridade física dos usuários e à continuidade do serviço. Nessa perspectiva, a comunicação em tempo real deixa de ser mera conveniência operacional e passa a constituir elemento essencial da fiscalização e da gestão do risco.

Nesse contexto, o emprego de um pipeline ETL voltado para dados não estruturados apresenta-se como solução tecnicamente adequada para a organização e o aproveitamento dessas informações. O processo pode ser compreendido em três etapas: na extração, realizam-se a captação de mensagens, áudios, imagens e documentos encaminhados por canais operacionais; na transformação, procede-se à limpeza dos dados, à transcrição automática de áudios, à classificação semântica do conteúdo, à padronização de datas, locais e tipos de evento, bem como à identificação das unidades responsáveis; na carga, os dados tratados são inseridos em bases estruturadas aptas a subsidiar painéis gerenciais, relatórios de monitoramento e sistemas de apoio à decisão. Desse modo, informações originalmente dispersas podem ser convertidas em evidências organizadas e passíveis de análise institucional.

Além disso, a incorporação de técnicas de Processamento de Linguagem Natural e automação analítica contribui para reduzir as perdas de informação típicas das comunicações espontâneas. Mensagens redigidas de forma abreviada, áudios sem transcrição e imagens sem metadados dificultam a interpretação posterior dos fatos e comprometem a reconstituição da linha do tempo dos eventos. Um pipeline devidamente estruturado mitigaria tais limitações ao permitir a classificação dos registros por criticidade, localidade, horário e natureza da ocorrência, favorecendo a produção de inteligência operacional e o acompanhamento sistemático das demandas de fiscalização.

No caso de reclamações de usuários relativas a perdas, danos ou falhas de atendimento, a existência de dados organizados assume especial importância. A disponibilidade de registros cronologicamente consistentes e formalmente tratados permite identificar o momento exato da comunicação, a equipe responsável pelo recebimento da ocorrência, as providências adotadas e o tempo de resposta institucional. Tal estrutura fortalece a capacidade de defesa administrativa e judicial, ao mesmo tempo em que amplia a transparência e a confiabilidade dos processos internos. Assim, a consolidação de dados não estruturados em bases analíticas estruturadas contribui diretamente para a segurança jurídica, a eficiência operacional e a qualificação da fiscalização pública.

Dessa forma, conclui-se que a aplicação de pipelines ETL ao contexto do CNSO/ANTT ultrapassa a dimensão meramente tecnológica, assumindo papel estratégico na integração entre comunicação operacional, monitoramento em tempo real e tomada de decisão. Em um cenário regulatório complexo, no qual a tempestividade da informação pode influenciar a segurança dos usuários e a efetividade da prestação do serviço, a transformação de dados dispersos em informação estruturada revela-se condição indispensável para uma atuação fiscalizatória moderna, responsiva e tecnicamente consistente.

2.3 Modelagem de banco de dados relacional para rastreabilidade de incidentes e fundamentação da modelagem relacional

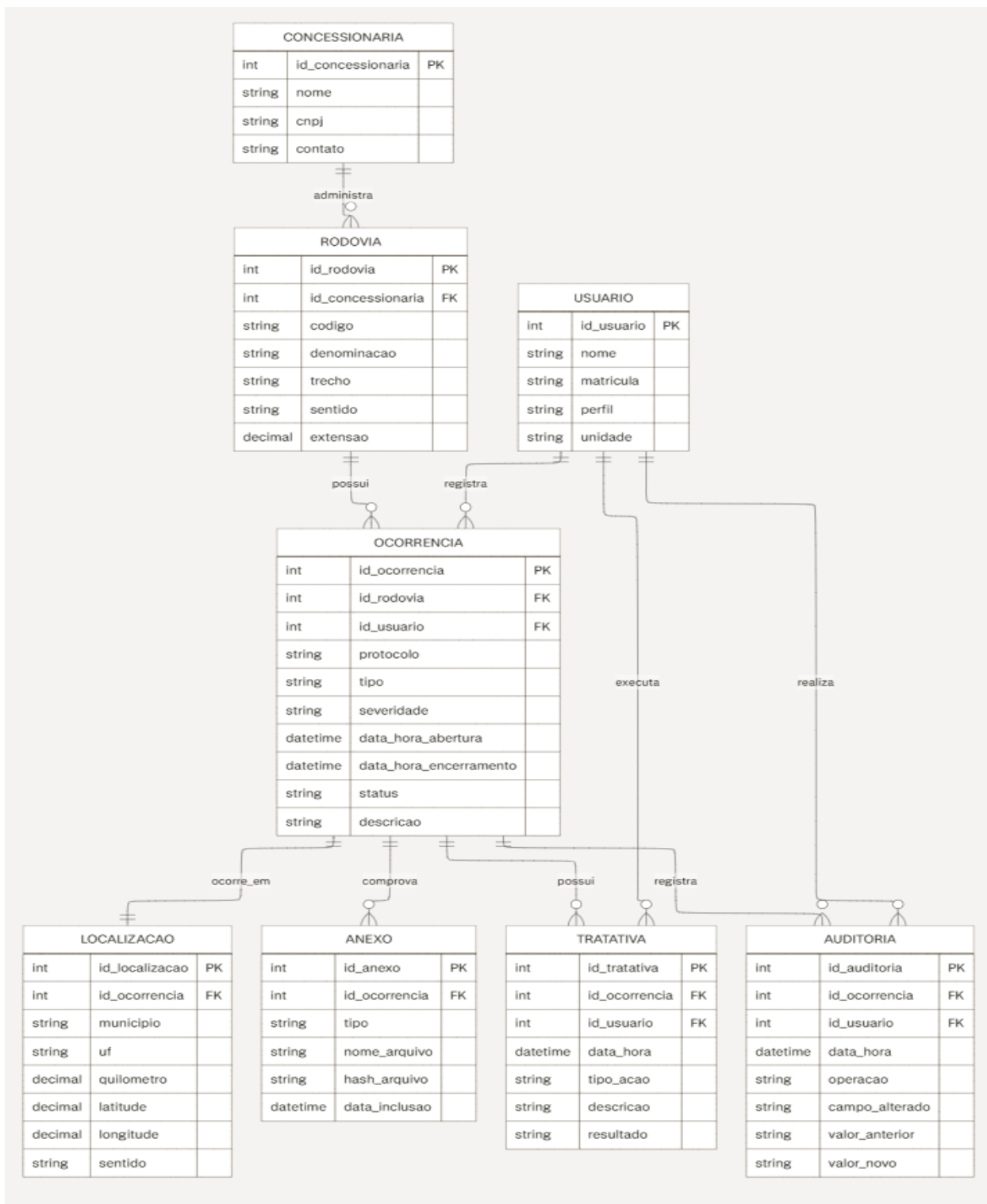
A construção de um banco de dados relacional destinado ao registro de incidentes de interdição em rodovias concedidas demanda uma estrutura lógica capaz de representar, de forma integrada, os diversos elementos que compõem a ocorrência e suas repercussões operacionais, administrativas e regulatórias. Nesse sentido, a modelagem deve contemplar entidades centrais e auxiliares, tais como rodovia, concessionária, ocorrência, localização, responsáveis pela inserção e tratamento das informações, documentos comprobatórios e trilhas de auditoria, de modo a assegurar consistência, integridade e rastreabilidade dos registros.

A literatura especializada evidencia que esquemas relacionais orientados ao vínculo entre ativos regulados, agentes responsáveis e eventos monitorados contribuem para a redução de redundâncias, a melhoria da qualidade da informação e o fortalecimento da transparência institucional (CORDEIRO; SANTOS, 2023). Em ambientes regulatórios, tal modelagem permite não apenas o armazenamento estruturado dos eventos, mas também a geração de estatísticas confiáveis, a consolidação de histórico operacional e o suporte à tomada de decisão baseada em evidências (CORDEIRO; SANTOS, 2023).

Sob esse enfoque, a ocorrência deve ser tratada como entidade nuclear do modelo, em torno da qual gravitam os demais componentes do sistema. Essa concepção mostra-se adequada ao contexto da fiscalização rodoviária, no qual cada incidente precisa ser vinculado a atributos temporais, espaciais, operacionais e funcionais, viabilizando o acompanhamento do evento desde o seu registro inicial até o encerramento formal da tratativa (ATAMANENKO, 2019).

No modelo abaixo proposto, a Ocorrência funciona como núcleo integrador das informações operacionais, administrativas e regulatórias, enquanto a Auditoria assegura a rastreabilidade das operações realizadas sobre o registro.

Figura I: Modelo relacional proposto para rastreabilidade de incidentes no CNSO/ANTT.



Fonte: Elaboração do autor, com base em Cordeiro e Santos (2023) e nos requisitos do estudo.

Como referência para a estruturação do modelo supracitado, adotou-se, de forma adaptada, a lógica relacional apresentada por Cordeiro e Santos (2023), na qual o evento regulatório é associado aos ativos fiscalizados, aos agentes responsáveis e às informações necessárias à sua contextualização e rastreabilidade. Aplicada ao contexto das interdições rodoviárias, essa abordagem resulta em um modelo centrado na entidade **Ocorrência**, relacionada às entidades **Concessionária**, **Rodovia**, **Localização**, **Usuário**, **Tratativa**, **Anexo** e **Auditoria**. A concessionária administra uma ou mais rodovias; cada rodovia pode possuir diversas ocorrências; e cada ocorrência deve estar vinculada a uma localização específica, a um responsável pelo registro, às providências adotadas, aos documentos comprobatórios e ao histórico de alterações. Essa organização reduz a redundância, preserva a integridade referencial e permite reconstruir a trajetória do incidente desde sua comunicação inicial até o encerramento da tratativa. No modelo proposto, a entidade Ocorrência funciona como núcleo integrador das informações operacionais, administrativas e regulatórias, enquanto a entidade Auditoria assegura a rastreabilidade das operações realizadas sobre o registro.

Aplicação ao contexto do CNSO/ANTT

No contexto do CNSO/ANTT, a necessidade de uma modelagem relacional estruturada decorre da complexidade operacional envolvida na fiscalização de 32 concessionárias federais, com projeção de ampliação para mais 8 unidades concedidas nos próximos meses. Trata-se de um ambiente marcado por elevada dispersão geográfica, fluxo contínuo de ocorrências, multiplicidade de atores institucionais e necessidade de resposta tempestiva a incidentes que podem afetar diretamente a segurança viária e a continuidade do serviço concedido.

O uso recorrente de aplicativos de mensagens, especialmente o WhatsApp, evidencia a necessidade de mecanismos institucionais mais aderentes à dinâmica da fiscalização. Embora esses canais favoreçam a comunicação imediata, eles não asseguram, por si sós, a padronização, a indexação e a vinculação das mensagens, áudios, imagens e documentos a um registro único de ocorrência. A ausência dessa estrutura dificulta a reconstrução da linha do tempo do evento e a identificação dos responsáveis pelo recebimento, tratamento e encerramento da demanda. Assim, em atividades de auditoria, fiscalização, prestação de contas ou defesa institucional, a inexistência de registros estruturados pode limitar a demonstração objetiva da tempestividade das providências adotadas e da regularidade da resposta operacional.

Limitações do modelo informal baseado em mensageria

Embora os aplicativos de mensageria ofereçam velocidade de comunicação, sua utilização como mecanismo principal de registro de incidentes revela limitações incompatíveis com a governança informacional exigida no setor público regulador. A informalidade desses canais favorece a dispersão de dados, a duplicidade de registros, a ausência de padronização terminológica e a perda de informações relevantes ao longo do tempo.

No âmbito da fiscalização rodoviária, tais limitações tornam-se particularmente críticas. Uma interdição parcial, um sinistro, uma falha de sinalização ou um atendimento emergencial comunicado apenas por mensagens instantâneas pode até mobilizar providências imediatas, mas dificilmente produzirá, por si só, um histórico formal suficientemente robusto para subsidiar análises gerenciais, auditorias, respostas regulatórias ou defesa institucional. A inexistência de um identificador único da ocorrência, de vínculo automático com a rodovia e a concessionária, e de mecanismo formal de atualização do status do evento, reduz a confiabilidade do processo de monitoramento.

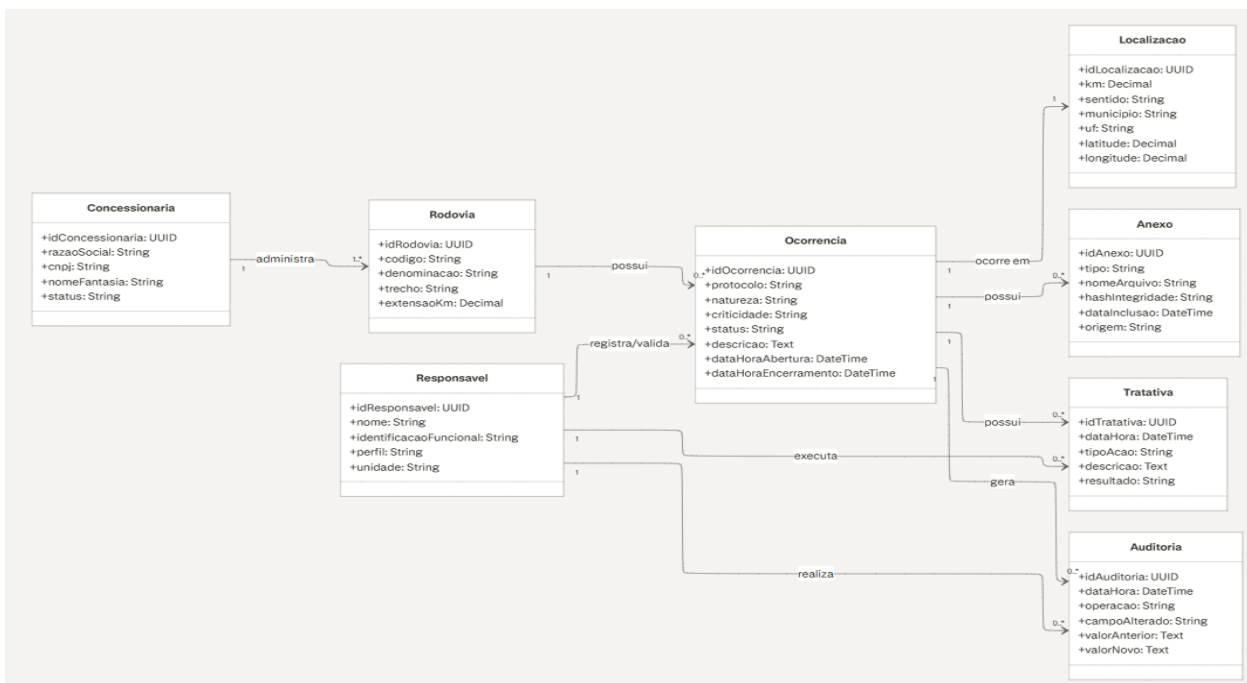
Além disso, em um cenário de resposta emergencial, a precariedade do fluxo informacional pode acarretar perdas de tempo relevantes para os usuários e para as equipes envolvidas. O atraso na consolidação de uma informação crítica pode representar a diferença entre um atendimento célere e um retardamento que potencialize o cenário do incidente, ampliando seus efeitos materiais, operacionais e reputacionais.

Proposta de estrutura relacional para o banco de dados de incidentes

Diante dessas limitações, propõe-se a adoção de um banco de dados relacional centrado na entidade Ocorrência, concebida como núcleo agregador das demais dimensões informacionais. A partir dessa estrutura, cada incidente passaria a ser registrado com identificação única, vinculando-se, de forma normalizada, às entidades complementares necessárias ao monitoramento integral do evento.

A Figura III apresenta o diagrama de classes conceitual proposto para o registro e a rastreabilidade de incidentes de interdição. O modelo posiciona a classe “**Ocorrência**” como núcleo da estrutura, relacionando-a às informações de contexto territorial e regulatório, aos registros de tratamento do evento, às evidências documentais e aos mecanismos de auditoria. Dessa forma, busca-se assegurar que cada alteração e providência permaneça associada ao respectivo incidente, preservando a consistência, a integridade e a possibilidade de reconstituição de sua trajetória operacional.

Figura II: Diagrama de classes conceitual para registro e rastreabilidade de incidentes de interdição rodoviária.



Fonte: Elaboração do autor (2026).

Diante dessas limitações, propõe-se a adoção de um banco de dados relacional centrado na “**Ocorrência**”, concebida como núcleo agregador das dimensões informacionais necessárias ao acompanhamento do incidente. Cada evento deve receber identificador único e ser relacionado, de forma normalizada, à concessionária, à rodovia, à localização, aos responsáveis pelo registro e tratamento, às providências adotadas, aos documentos comprobatórios e às trilhas de auditoria. A Figura III representa essas relações em um diagrama de classes conceitual, evidenciando a função integradora da Ocorrência e os vínculos necessários à preservação da rastreabilidade durante todo o ciclo de vida do evento. A tabela abaixo traduz melhor a figura II:

Tabela 1: Relações do modelo

Relação	Interpretação
Concessionária → Rodovia	Uma concessionária pode administrar uma ou mais rodovias ou segmentos concedidos
Rodovia → Ocorrência	Uma rodovia pode ter múltiplas ocorrências registradas
Ocorrência → Localização	Cada ocorrência possui uma localização operacional específica, com km, sentido, município e coordenadas
Ocorrência → Tratativa	Um incidente pode demandar várias providências durante seu ciclo de vida
Ocorrência → Anexo	Uma ocorrência pode reunir diversas evidências, como imagem, vídeo, áudio, ofício ou relatório
Ocorrência → Auditoria	O histórico de operações preserva criação, alteração, atualização e encerramento do evento
Responsável → Ocorrência/Tratativa/Auditoria	Permite identificar quem registrou, validou, tratou ou modificou a informação

Fonte: Elaboração do autor (2026).

A entidade Rodovia deve armazenar os dados estruturantes da via concedida, incluindo código, denominação, trecho, sentido e extensão. A entidade Concessionária deve reunir as informações da empresa responsável pela operação da rodovia ou segmento correspondente, permitindo a associação direta entre o evento e a parte regulada. A entidade Localização deve contemplar quilometragem, coordenadas geográficas, município, unidade federativa e demais elementos que permitam o posicionamento preciso da ocorrência.

A entidade Ocorrência, por sua vez, deve registrar os atributos essenciais do incidente, tais como natureza do evento, data e hora de abertura, severidade, descrição sintética, situação operacional, data e hora de encerramento e classificação quanto ao impacto. Já a entidade Responsável deve identificar o agente ou servidor que registrou, validou, tratou ou encerrou a ocorrência, permitindo atribuição funcional e controle de responsabilidades.

De igual modo, a entidade Anexo deve reunir os elementos probatórios associados ao evento, como fotografias, vídeos, áudios transcritos, relatórios técnicos, ofícios, comunicações formais e documentos encaminhados pela concessionária. A entidade Tratativa deve registrar as providências adotadas ao longo do ciclo de vida da ocorrência, incluindo acionamentos, encaminhamentos, atualizações de status e medidas corretivas. Por fim, a entidade Auditoria deve preservar o histórico de alterações, com marcação temporal, usuário responsável e natureza da modificação efetuada.

Essa lógica é compatível com modelos conceituais que tratam o incidente como entidade central vinculada a múltiplas dimensões de contexto, como tempo, local, participantes e agentes responsáveis (ATAMANENKO, 2019). Também se mostra aderente a abordagens que utilizam bancos de dados de incidentes para monitoramento de barreiras, análise de falhas e gestão de riscos em ambientes regulados (ALVES; LIMA, 2021).

Benefícios operacionais e institucionais da modelagem proposta

A adoção de uma modelagem relacional com essas características tende a produzir ganhos expressivos para o CNSO/ANTT. Em primeiro lugar, promove a centralização da informação em ambiente institucional único, reduzindo a dependência de canais paralelos e mitigando a dispersão documental. Em segundo lugar, amplia a confiabilidade dos registros, ao associar cada incidente a atributos padronizados e relações formalmente definidas entre rodovia, concessionária, local, agentes responsáveis e providências adotadas.

Em termos operacionais, o modelo favorece a obtenção de informações em tempo real, com potencial para alimentar painéis gerenciais, estatísticas de recorrência, mapas de criticidade e indicadores de desempenho regulatório. Isso permite identificar padrões

de incidência, avaliar tempos médios de resposta, monitorar o comportamento das concessionárias e orientar ações preventivas e corretivas com base em evidências consistentes (ALVES; LIMA, 2021).

Sob o ponto de vista jurídico-administrativo, o banco de dados também fortalece a capacidade de defesa institucional. Em reclamações de usuários relativas a perdas, danos, demora no atendimento ou suposta omissão regulatória, a existência de registros formalmente estruturados possibilita reconstituir a linha do tempo do evento, demonstrar providências adotadas e comprovar a atuação da ANTT e das concessionárias com maior precisão. A base relacional, portanto, não apenas organiza a operação, mas também qualifica a responsabilização, a prestação de contas e a segurança jurídica.

2.5 Governança da informação e rastreabilidade operacional

A proposta de um banco de dados para o registro de interdições exige a definição de regras de organização, atualização e recuperação das informações. No contexto deste trabalho, a governança da informação é abordada em sua dimensão operacional, considerando a identificação dos responsáveis pelo registro, a padronização dos campos e a manutenção do histórico das providências.

Cada ocorrência deve possuir um identificador próprio e estar relacionada à concessionária, à rodovia, à localização e às comunicações que lhe deram origem. Essa organização permite reunir mensagens sucessivas sobre um mesmo evento e distinguir o registro inicial de suas atualizações.

A rastreabilidade operacional corresponde à possibilidade de reconstruir o percurso da informação, qual comunicação originou a ocorrência, quando ela foi recebida, quem realizou a extração, quais campos foram sugeridos, quem validou o conteúdo e quais alterações foram registradas. Para representar esse percurso, o modelo prevê referências à origem, identificação dos responsáveis, registros temporais e controle de versões.

O histórico de alterações deve indicar a operação realizada, o campo modificado, os valores anterior e posterior, o responsável e o momento da alteração. Seu objetivo é permitir o acompanhamento das mudanças e a recuperação do contexto de cada decisão de registro ou atualização.

A associação de anexos à ocorrência complementa essa estrutura. Fotografias, documentos e outros arquivos devem ser identificados e vinculados ao evento correspondente, com registro da origem e do momento de inclusão. A existência desses vínculos contribui para a organização documental, mas não equivale à comprovação criptográfica de integridade ou autenticidade.

No CNSO/ANTT, esse modelo pode apoiar a consulta ao histórico dos eventos, o acompanhamento das tratativas e a identificação de pendências. A contribuição analisada é a estruturação das informações para uso operacional e gerencial. A avaliação de conformidade com a LGPD, a validação de cadeia de custódia forense e a comprovação de não repúdio não fazem parte do escopo desta pesquisa.

No contexto da fiscalização rodoviária, a governança de dados assume relevância prática imediata. Ocorrências de interdição, sinistros, falhas de sinalização, reclamações de usuários e registros operacionais podem envolver dados pessoais de operadores, testemunhas, prepostos de concessionárias, usuários identificados, agentes públicos e demais envolvidos na ocorrência. Em razão disso, a estrutura informacional deve ser concebida segundo os princípios da necessidade, da adequação e da minimização, evitando a coleta excessiva de informações e restringindo o tratamento ao estritamente necessário para a finalidade fiscalizatória (BAGATINI; GUIMARÃES; SANTANA, 2021).

Aplicação da LGPD ao CNSO/ANTT

Sob a ótica da LGPD, o sistema do CNSO/ANTT deve prever regras claras sobre quem pode inserir, consultar, alterar e excluir informações. Em um cenário prático, o agente que registra uma interdição em tempo real deve ter acesso apenas aos campos necessários à sua atuação, enquanto gestores, auditores e áreas jurídicas devem dispor de perfis diferenciados de visualização e tratamento. Essa segmentação funcional é fundamental para reduzir riscos de uso indevido, proteger a privacidade dos envolvidos e fortalecer a confiabilidade institucional. Do mesmo modo, deve haver política definida para retenção e descarte dos dados, considerando a finalidade administrativa, os prazos legais e os critérios de preservação documental (COELHO; CARVALHO, 2025; BAGATINI; GUIMARÃES; SANTANA, 2021).

Na prática, isso significa que o registro de um incidente não deve expor dados pessoais em excesso, tampouco manter informações além do tempo necessário à sua finalidade. Se uma ocorrência puder ser formalizada com identificação funcional do agente e descrição objetiva do fato, não há justificativa para a retenção indiscriminada de dados irrelevantes à apuração. Em termos de governança, a aplicação da LGPD no CNSO/ANTT exige, portanto, a adoção de fluxos institucionais que combinem utilidade operacional e proteção dos titulares, sem comprometer a atividade fiscalizatória.

Cadeia de custódia digital e não repúdio

Outro aspecto central é a cadeia de custódia digital, especialmente quando os registros de interdição podem futuramente servir como prova em processos administrativos, auditorias ou ações judiciais. A cadeia de custódia não se limita à preservação física de documentos, mas envolve, no ambiente digital, a garantia de que os registros permaneçam íntegros, autênticos e auditáveis ao longo do tempo. Em termos

práticos, isso implica registrar quem criou o evento, em que data e hora, quais alterações foram realizadas, quem consultou o conteúdo, quais anexos foram inseridos e quando a ocorrência foi encerrada.

Dentro dessa cadeia, ao se atender ao requisito de não-repúdio e auditabilidade, esse processo é analisado por Sebastian (2026) no contexto de *Shadow AI*. O autor propõe o framework DART, que inclui a realimentação organizacional. Este conceito é adaptável à essa proposta pois cada registro de interdição mantém um registro de auditoria completo, como, quem reportou, quando, qual foi a ação tomada, quando foi resolvido, permitindo que a organização aprenda com os incidentes passados e melhore seus processos de fiscalização.

A literatura recente sobre ambientes digitais automatizados destaca que a rastreabilidade e os ciclos de retroalimentação organizacional são indispensáveis para a confiabilidade dos processos informacionais, especialmente em contextos marcados por alto volume de dados e necessidade de resposta rápida (SEBASTIAN, 2026). Tal compreensão é plenamente adaptável ao cenário do CNSO/ANTT, uma vez que cada registro de interdição deve manter um log de auditoria completo, permitindo identificar quem reportou, quando houve o registro, qual providência foi adotada e em que momento a ocorrência foi resolvida.

Aplicação prática no CNSO/ANTT

No CNSO/ANTT, a importância dessa cadeia é evidente. Imagine-se uma ocorrência de interdição em trecho de rodovia concedida, com impacto sobre a fluidez do tráfego e potencial repercussão para usuários. Caso a informação tenha sido inicialmente transmitida por aplicativo de mensageria, mas posteriormente formalizada em sistema institucional, é indispensável que o sistema preserve o vínculo entre a comunicação original e o registro oficial. Dessa forma, torna-se possível demonstrar não apenas o conteúdo da informação, mas também a sequência de providências adotadas, o tempo de resposta e os responsáveis por cada etapa do tratamento.

Em eventual questionamento sobre demora, omissão ou falha de atuação, a existência dessa trilha constitui elemento decisivo para a defesa institucional e para a verificação da regularidade do procedimento. Sob essa perspectiva, a cadeia de custódia digital não se limita a um requisito probatório, mas se converte em instrumento de gestão e aprendizado organizacional. Quando cada ocorrência é devidamente registrada, auditada e resolvida com rastreabilidade, a instituição passa a dispor de um acervo técnico capaz de subsidiar análises históricas, identificar gargalos e aprimorar os protocolos de fiscalização.

Síntese analítica

A implementação de um banco de dados de interdições deve, portanto, ser acompanhada de políticas robustas de privacidade, controles de acesso, trilhas de auditoria e mecanismos de retenção e descarte alinhados à LGPD. Mais do que atender a exigências normativas, essa estrutura fortalece a legitimidade da atuação fiscalizatória, aumenta a segurança institucional e melhora a qualidade das decisões administrativas. Ao transformar registros operacionais em dados governados, auditáveis e juridicamente sustentáveis, o CNSO/ANTT amplia sua capacidade de resposta, reduz riscos de exposição indevida e consolida uma cultura organizacional orientada pela integridade da informação.

2.6 Sistemas de monitoramento em tempo real e apoio à decisão no contexto do CNSO, monitoramento em tempo real como requisito operacional

Esta proposta menciona explicitamente as ferramentas Sirad, Zabbix e Grafana utilizadas no ambiente do Centro de Segurança Operacional (CNSO) da ANTT. Ferreira et al. (2025) apresentam uma implementação integrada de Zabbix, Grafana e ZeroTier para monitoramento de rede em tempo real. Os autores validam o uso de *dashboards* interativos para visualizar tráfego, temperatura, processamento e uso de memória, garantindo maior segurança cibernética e capacidade de resposta a falhas.

Souza e Oliveira (2024) estendem essa discussão ao propor a integração entre Grafana e Zabbix para a supervisão de infraestrutura em tempo real, consolidando dados dispersos em um *single pane of glass*. Embora voltado à infraestrutura de TI, o conceito de “painel único” é aplicável à supervisão de interdições rodoviárias. No contexto do CNSO/ANTT, o *dashboard* deve priorizar, em tempo real, as interdições ativas, com identificação da concessionária, rodovia, quilômetro, sentido, município, tipo e criticidade da ocorrência, extensão ou impacto estimado no tráfego, faixas afetadas, horário de início, tempo transcorrido, previsão de liberação, status da tratativa, responsáveis e recursos acionados. O painel também pode apresentar indicadores consolidados, como quantidade de ocorrências por concessionária e trecho, tempo médio de resposta, recorrência de eventos e histórico de interdições, apoiando a priorização operacional, o acompanhamento da atuação das concessionárias e a tomada de decisão baseada em evidências.

As informações prioritárias para o painel são:

- Ocorrências e interdições ativas.
- Criticidade, tipo de evento e impacto estimado.
- Concessionária, rodovia, trecho, quilômetro, sentido, município e faixas afetadas.
- Horário de início, tempo transcorrido e previsão de liberação.
- Situação da ocorrência e últimas atualizações.

- Responsáveis, providências adotadas e recursos acionados.
- Indicadores históricos: recorrência, quantidade de eventos e tempo médio de resposta por trecho e concessionária.

Kontogiannis & Asiminidis (2021) propõem um sistema de gestão de incidentes em autoestradas (*Resources Management System – RMS*) que integra sensoriamento (túneis), rastreamento de recursos humanos e algoritmos de aprendizado de máquina para estimar tempos de resposta. Os autores utilizam agentes inteligentes (*bots*) para recomendar qual equipe deve ser alocada a cada incidente. Este RMS – que, assim como sua proposta, utiliza WhatsApp como um dos canais de comunicação – demonstra que é viável construir sistemas de apoio à decisão para rodovias a partir de dados não estruturados.

A implantação de sistemas de monitoramento em tempo real e de apoio à decisão é estratégica para a supervisão de interdições rodoviárias no CNSO/ANTT, especialmente diante da dispersão geográfica das concessões, do volume de eventos e da necessidade de resposta tempestiva. Por meio de painéis integrados, o centro de controle pode consolidar informações sobre interdições ativas, localização e criticidade dos eventos, impactos no tráfego, recursos mobilizados, status das tratativas e histórico de ocorrências. Essa visualização unificada reduz a dependência de comunicações fragmentadas, amplia a consciência situacional e subsidia decisões operacionais mais rápidas e fundamentadas (FERREIRA et al., 2025; SOUZA; OLIVEIRA, 2024).

Apoio à decisão e alocação de recursos

Outro aspecto relevante é a incorporação de mecanismos automatizados de apoio à decisão. Em ambientes complexos, sistemas dessa natureza podem sugerir a equipe mais adequada para cada incidente com base em critérios como localização, especialidade, disponibilidade, carga de trabalho e criticidade do evento (KONTOGIANNIS; ASIMINIDIS, 2021). No CNSO/ANTT, essa funcionalidade teria utilidade direta na gestão de interdições e na resposta a incidentes em rodovias concedidas, sobretudo quando a malha sob fiscalização é extensa e a distribuição territorial impõe restrições de tempo e logística.

Imagine, por exemplo, um acidente em rodovia concedida que exija a mobilização simultânea de concessionária, equipe de fiscalização e eventuais órgãos de resposta. Um sistema integrado pode indicar quais recursos estão disponíveis, qual equipe se encontra mais próxima, qual trecho apresenta menor tempo estimado de deslocamento e quais incidentes anteriores naquela localidade demandaram providências semelhantes. Desse modo, a decisão deixa de se apoiar exclusivamente na experiência individual do operador e

passa a ser orientada por dados operacionais acumulados, histórico de ocorrências e critérios comparáveis de priorização (KONTOGIANNIS; ASIMINIDIS, 2021).

Relação com rastreabilidade e análise forense

Sob a perspectiva da análise forense e da governança da informação, esses sistemas também oferecem vantagens importantes. Ao registrar eventos e ações em tempo real, com trilhas de auditoria e histórico de alterações, a plataforma favorece a reconstrução posterior do curso dos fatos e fortalece a capacidade de prestação de contas. Isso é especialmente relevante quando se busca demonstrar que a resposta institucional foi tempestiva e compatível com a gravidade do incidente.

No caso do CNSO/ANTT, a existência de um ambiente integrado de monitoramento permite que a informação operacional deixe de circular apenas em fluxos informais e passe a integrar um ecossistema institucional rastreável. Dessa forma, cada registro de interdição, cada atualização de status e cada encaminhamento ficam preservados em base única, o que amplia a confiabilidade dos dados e facilita sua utilização em auditorias, sindicâncias e análises posteriores.

Síntese analítica

Dessa forma, no contexto do CNSO/ANTT, os sistemas de monitoramento em tempo real e apoio à decisão representam uma evolução necessária para a fiscalização moderna. Ao substituir a fragmentação informacional por visualização integrada, ao reduzir a dependência de canais informais e ao apoiar a escolha das melhores ações em tempo oportuno, tais sistemas contribuem para elevar a eficiência operacional, a segurança dos usuários e a qualidade da governança institucional. Trata-se, portanto, de uma solução que articula tecnologia, inteligência analítica e responsabilidade regulatória em benefício da atuação fiscalizatória (FERREIRA et al., 2025; SOUZA; OLIVEIRA, 2024; KONTOGIANNIS; ASIMINIDIS, 2021).

CAPÍTULO 3 – METODOLOGIA

3.1 Natureza e abordagem da pesquisa

A pesquisa é aplicada, exploratória e descritiva, com abordagem predominantemente qualitativa e componente quantitativo de avaliação de desempenho. O objeto é o fluxo de comunicação de interdições recebido por WhatsApp e sua conversão em registro estruturado no Sistema de Registro de Interdições da ANTT, cuja tela de cadastro apresenta campos padronizados para situação, datas, horários, concessionária, estado, rodovia, sentido, quilômetro, área afetada, direção, faixas, causa e detalhamento.

3.2 Hipótese

H0 — Hipótese nula: a combinação de formulário orientado, modelo de linguagem e validação humana não produz melhoria relevante, em comparação ao preenchimento manual, no tempo de transcrição, na completude ou na padronização dos registros; ou produz erros que inviabilizam seu uso assistido.

H1 — Hipótese alternativa: a combinação de formulário orientado, modelo de linguagem e validação humana apresenta potencial para reduzir o tempo de transcrição das comunicações de interdição e aumenta a completude e a padronização dos registros, sem comprometer a rastreabilidade e os requisitos de segurança.

A inteligência artificial será empregada exclusivamente como mecanismo de apoio à decisão e de pré-preenchimento. A validação humana permanecerá obrigatória para a classificação da ocorrência, a correção de informações, o tratamento de campos críticos e qualquer lançamento no sistema institucional.

3.3 Unidade de análise e amostra

O estudo de caso será conduzido com dados de teste anonimizados, sem inserção de informações reais no ambiente produtivo. A comunicação utilizada como caso-base informa: concessionária ECO101; cidade de Linhares/ES; sentido norte; BR-101-ES, km 137+800; data e hora da evidência de 16/08/2026 às 19h58; ocorrência de atendimento mecânico não decorrente de sinistro de trânsito; interdição parcial; registro INT0005160; ausência de protocolo; equipe de apoio da concessionária deixando o local; fonte CFTV.

A unidade de análise desta pesquisa corresponde a cada ocorrência de interdição ou evento operacional comunicado à ANTT, podendo ser constituída por uma mensagem isolada ou por um conjunto de mensagens relacionadas ao mesmo fato. Para fins de classificação e seleção da amostra, serão adotados os três níveis de criticidade estabelecidos no Ofício Circular SEI nº 3064/2026/CESTI/GCNSO/SUTEC/DIR-ANTT, referente ao Processo nº 50500.071770/2025-31.

O **Nível 1: Crítico** corresponde a ocorrências de elevada gravidade, com impacto significativo na segurança viária ou na continuidade operacional da rodovia, ou com potencial de repercussão institucional ou midiática. Entre os critérios previstos estão múltiplos feridos graves ou óbitos, envolvimento de transporte coletivo ou cargas perigosas, interdição total ou parcial superior a três horas com congestionamento relevante, colapsos estruturais e deslizamentos de grande porte com bloqueio total da rodovia. Essas ocorrências devem ser comunicadas ao CNSO em até 60 minutos após sua verificação.

O **Nível 2: Significativo** abrange ocorrências com impacto relevante à operação ou à segurança viária, que exigem monitoramento e acompanhamento, embora não configurem, inicialmente, situação crítica. Enquadram-se nessa categoria, entre outras hipóteses, óbito isolado, feridos leves ou moderados em número reduzido, interdição parcial com lentidão significativa superior a 5 km, deslizamentos de pequeno ou médio porte sem bloqueio total e situações que demandem operação assistida. O prazo de comunicação também é de até 60 minutos.

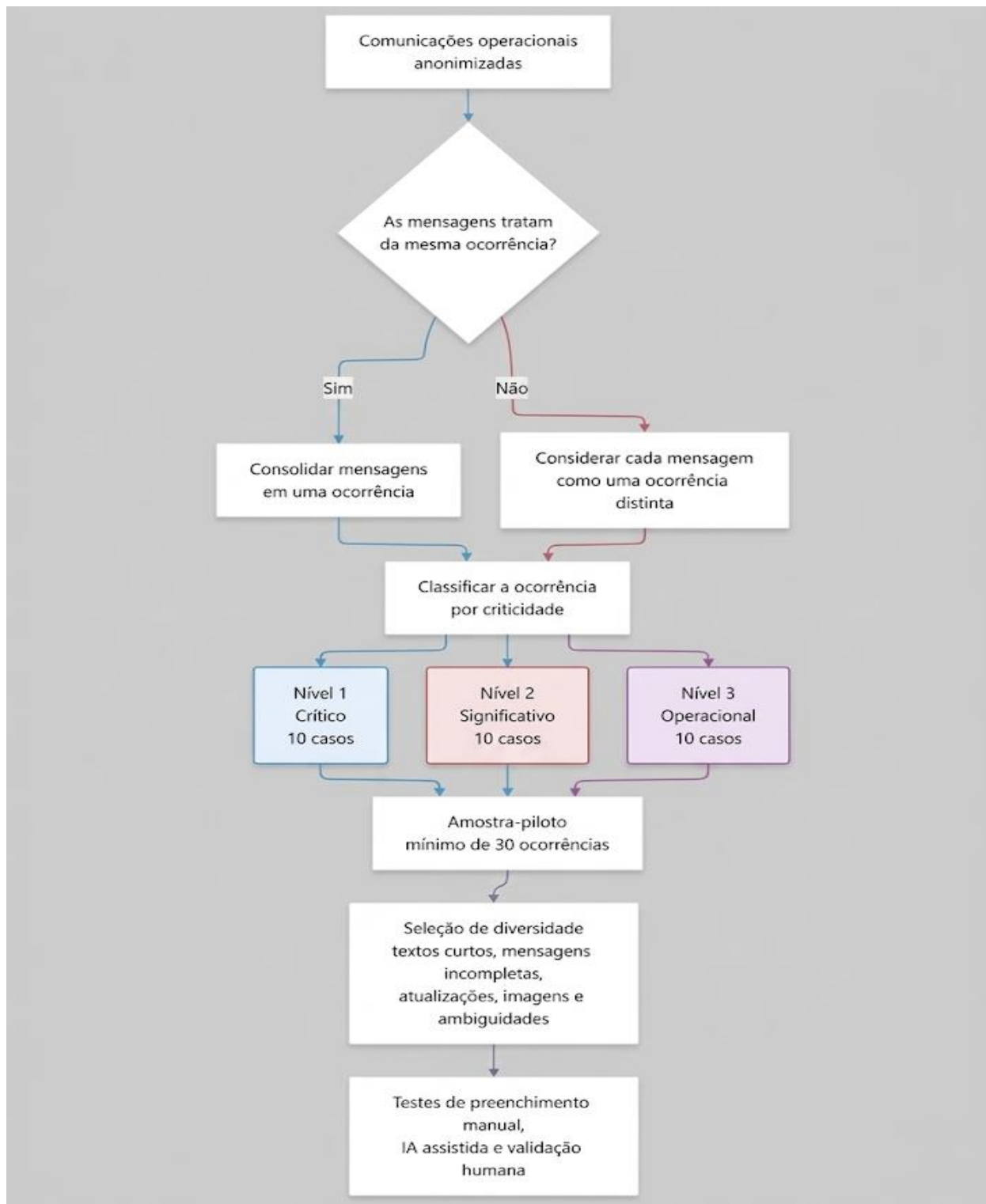
O **Nível 3: Operacional** compreende ocorrências rotineiras, sem impacto relevante à segurança viária ou à continuidade operacional da rodovia, como pane mecânica ou pane seca em local seguro, acidentes sem vítimas e sem obstrução de faixas, remoção de objetos sem interrupção do fluxo e atendimentos rapidamente normalizados. Para esses casos, o prazo de comunicação é de até 180 minutos. Os critérios de classificação são não cumulativos, e a ocorrência pode ser reclassificada caso surjam informações que alterem sua gravidade ou seu impacto operacional.

Com base nessa classificação, a amostra-piloto será composta por, no mínimo, 30 ocorrências anonimizadas, distribuídas equilibradamente entre os três níveis, com dez casos de cada categoria. A seleção buscará contemplar diferentes formatos e condições de comunicação, incluindo mensagens textuais curtas, registros incompletos, atualizações sucessivas, imagens anexadas e situações com ambiguidade de preenchimento. As ocorrências serão utilizadas para demonstrar a aplicação do fluxo de extração, normalização, classificação preliminar e validação humana, sem inserção de dados reais no ambiente produtivo.

Como caso-base da demonstração, será utilizada a comunicação anonimizada contendo os elementos já supracitados. Considerando exclusivamente as informações disponíveis, o caso será tratado como **classificação preliminar de Nível 3: Operacional**, pois não há indicação de vítimas, congestionamento superior a 5 km, interdição prolongada ou outro critério de maior gravidade. Essa classificação deverá ser revista caso informações posteriores demonstrem impacto operacional relevante, hipótese em que o evento poderá ser reclassificado para o Nível 2 ou Nível 1.

A unidade de análise corresponde a cada ocorrência de interdição, formada por uma mensagem isolada ou por um conjunto de mensagens relacionadas ao mesmo evento. A amostra-piloto será composta por, no mínimo, 30 ocorrências anonimizadas, distribuídas entre três níveis de criticidade: crítico, significativo e operacional. Para cada nível, serão selecionados preferencialmente dez casos que representem diferentes situações de comunicação, tais como mensagens textuais curtas, registros incompletos, atualizações sucessivas, imagens anexadas e informações com ambiguidade de preenchimento. A Figura III apresenta a organização da amostra e o percurso analítico previsto.

Figura III: Classificação das ocorrências e composição da amostra-piloto segundo a Matriz de Criticidade do CNSO.



Fonte: Elaboração do autor, com base no Ofício Circular SEI nº 3064/2026/CESTI/GCNSO/SUTEC/DIR-ANTT.

Como interpretar a figura

- **Unidade de análise:** Uma ocorrência, não necessariamente uma única mensagem. Se várias mensagens tratam do mesmo incidente, elas são agrupadas;
- **Classificação:** Cada ocorrência é enquadrada em nível 1, 2 ou 3, conforme os critérios de criticidade adotados na pesquisa;
- **Amostra mínima:** 30 Ocorrências, com dez casos por nível, para garantir equilíbrio inicial entre as classes;
- **Diversidade da amostra:** Dentro de cada nível devem existir exemplos completos e incompletos, textos, imagens, atualizações e casos ambíguos;
- **Etapa seguinte:** Os mesmos casos serão empregados para comparar o preenchimento manual, a extração por IA e a validação humana.

A comunicação do caso-base não deve ser classificada automaticamente apenas por conter uma interdição parcial. Pela matriz fornecida, a classificação depende do impacto e dos critérios objetivos: o nível 2 contempla, entre outros casos, interdição parcial com lentidão significativa, enquanto o nível 3 contempla ocorrências rotineiras sem impacto relevante à segurança viária ou à continuidade operacional. Como o print não informa duração, extensão do congestionamento, vítimas, bloqueio de faixa ou lentidão significativa, a classificação provisória mais defensável é nível 3 – operacional, sujeita à revisão. Caso a interdição parcial tenha causado lentidão significativa ou impacto superior a 5 km, deve ser reclassificada para nível 2. A classificação é dinâmica.

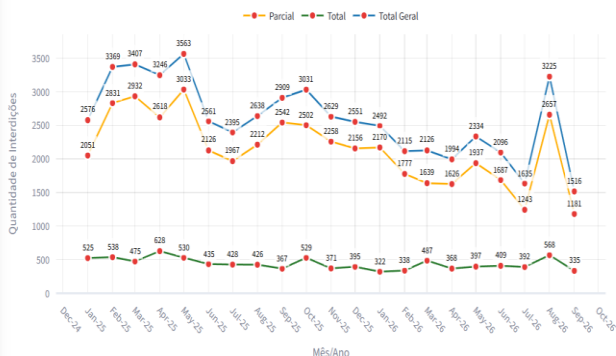
Figura IV: Interdição 08/09/2026 - CONCEBRA - BR-060

	ID: 8074 Data e Hora: 08/09/2026 - 10:09:00 Concessionária: CONCEBRA Rodovia: BR-060 Situação: Finalizada Término: 08/09/2026 - 17:34:00 Operador: Kamila Da Silva Vasconcelos Tipo: Parcial Cadastrado por: Kamila Da Silva Vasconcelos Feriado: Não
Descrição Às 10h36 USA02.2 informa vítima (condutor) do sexo masculino, preso às ferragens já em óbito dentro do veículo. Passageiro do sexo masculino em estado moderado, já foi atendido pelas equipes do SAMU, viaturas USB e EUA de Alexânia/GO no local, onde o mesmo foi removido pela EUA do SAMU para o HEANA. Às 10:54h PRF conduziu o câmbio para o local. OBS: Veículo se encontra com o teto ao solo, baú danificado com carga de café (Pacotes em fardos), espalhado em canteiro, sem interferências de faixas. Às 12h25 Fechamento da primeira faixa em sentido sul para realização da perícia. Trânsito pela segunda faixa e acostamento fluindo normalmente até a chegada do IML. Às 13:35h chegada do IML no local às 13:39h chegada da polícia científica no local. Obs.: Primeira faixa sentido sul permanece fechada para realização da perícia, Trânsito pela segunda faixa e acostamento fluindo normalmente às 15:01h foi feito a retirada do corpo do veículo às 15:16h fechamento total sentido sul, aproximadamente 40 minutos para remoção do veículo, PRF juntamente com nossa equipe prestando apoio no local. Às 16h02 Veículo retirado do local, sendo removido em contrafluxo pelo acostamento, no sentido sul, por aproximadamente 200 metros, até uma entrada de propriedade, em área de fuga, onde será removido por guincho particular, devido às condições em que se encontra. Às 16h08 Liberado a segunda faixa para os veículos, a primeira faixa ainda permanece fechada devido ao processo de retirada de resíduos do local. OBS: Trânsito fluindo lentamente pelo local, cerca de 4km de retenção. Antes: Às 10:36h USA02.2 informa vítima (condutor) do sexo masculino, preso às ferragens já em óbito dentro do veículo. Passageiro do sexo masculino em estado moderado, já foi atendido pelas equipes do SAMU, viaturas USB e EUA de Alexânia/GO no local, onde ele foi removido pela EUA do SAMU para o HEANA. Às 10:54h PRF informou a posição para o local. OBS: Veículo se encontra com o teto ao solo, baú danificado com carga de café (Pacotes em fardos), espalhado em canteiro, sem interferências de faixas. Às 12h25 Fechamento da primeira faixa em sentido sul para realização da perícia. Trânsito pela segunda faixa e acostamento fluindo normalmente até a chegada do IML.	

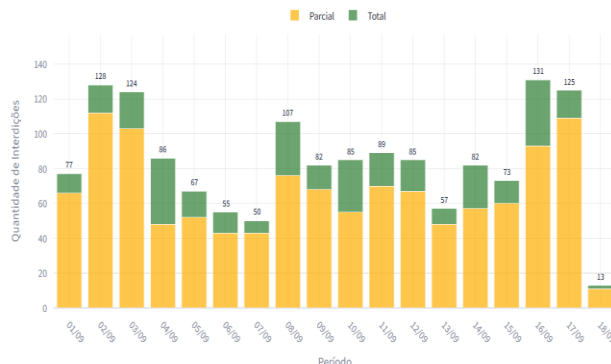
Fonte: Painel Gerencial CNSO/ANTT.

Figura V: Trajetórias da quantidade de interdições de toda base do CNSO à esquerda e do período selecionado à direita.

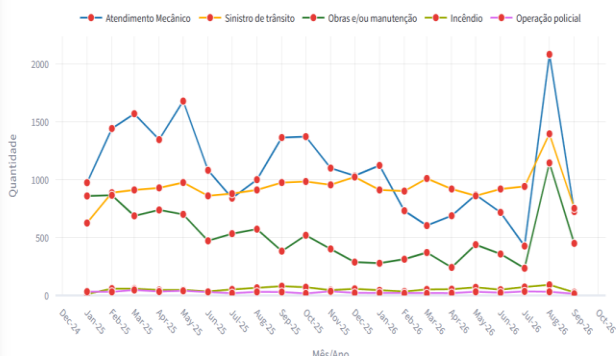
Quantidade de Interdições - Histórico(Fixo)



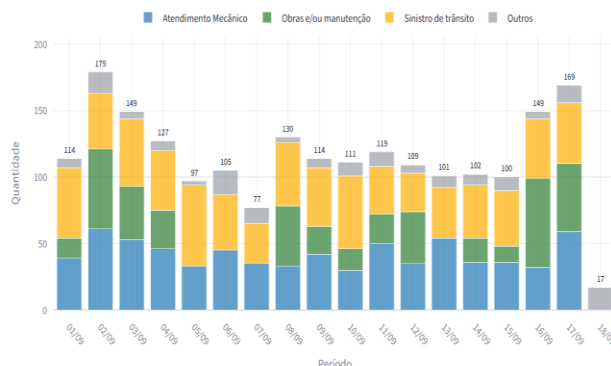
Quantidade de Interdições - Período Selecionado



Quantidade por Causa - Histórico(Fixo)



Quantidade por Causa - Período Selecionado



Fonte: Painel Gerencial CNSO/ANTT.

3.4 Fluxo experimental

O fluxo proposto será composto pelas etapas seguintes:

1. Recepção da mensagem no canal operacional autorizado;
2. Resposta padronizada, automática ou semiautomática, com link para o formulário institucional e orientação de preenchimento;
3. Captura controlada da mensagem, dos anexos e dos metadados necessários, evitando coleta excessiva de dados pessoais;
4. Extração e transformação do conteúdo por regras determinísticas e, quando aplicável, por LLM;
5. Geração de JSON conforme o esquema definido neste trabalho;
6. Validação humana dos campos obrigatórios, dos valores normalizados e da criticidade;
7. Registro no sistema oficial, manualmente ou por integração autorizada;
8. Atualização do evento a cada 120 minutos ou sempre que houver informação relevante, conforme as diretrizes apresentadas pelo pesquisador;
9. Encerramento, preservação dos registros e geração do log de auditoria.

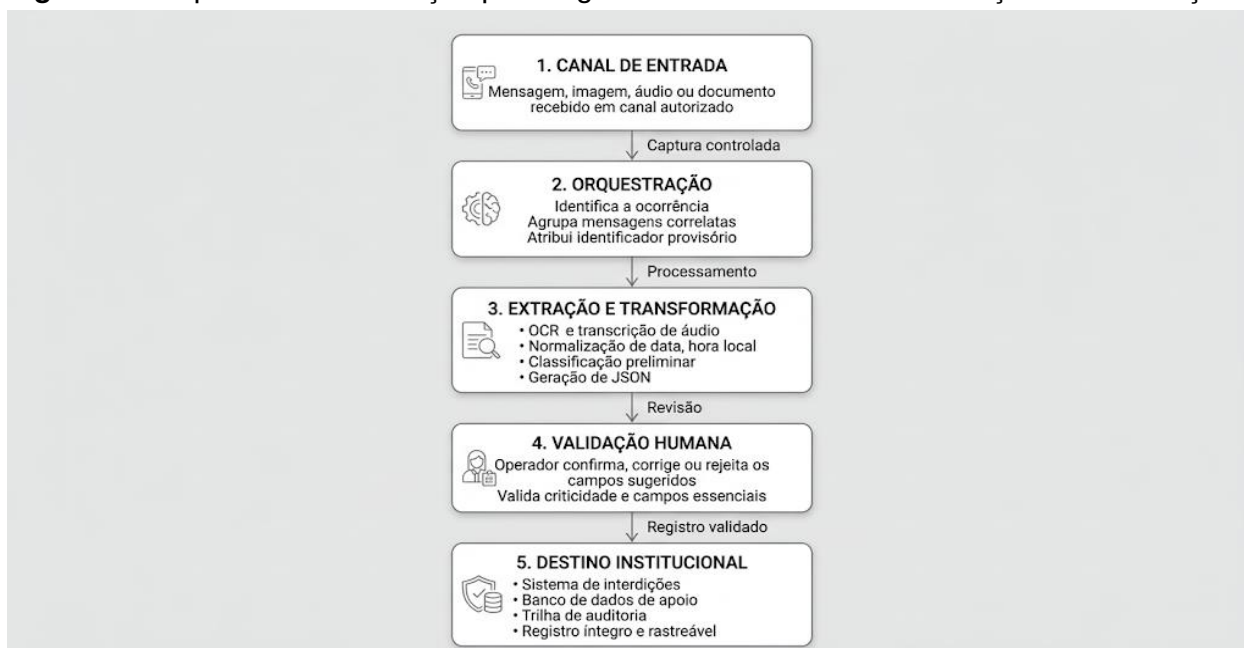
O envio inicial deve observar os prazos indicados no material institucional analisado: níveis 1 e 2, em até 60 minutos; nível 3, em até 180 minutos. A matriz anexada também apresenta esses prazos e indica, no nível 1, impacto elevado, e nos níveis 2 e 3, critérios progressivamente menores. A atualização da criticidade deve ocorrer quando surgirem novas vítimas, aumento do congestionamento, ampliação da duração ou repercussão institucional.

3.5 Arquitetura de transição

A arquitetura experimental proposta está organizada em cinco camadas sequenciais, conforme apresentado na Figura V. A primeira camada corresponde ao **Canal de Entrada**, responsável pelo recebimento de mensagens, imagens, áudios ou documentos em canal autorizado. Em seguida, a camada de **Orquestração** identifica a ocorrência, agrupa comunicações relacionadas, atribui identificador provisório e encaminha o conteúdo para tratamento. A terceira camada, de **Extração e Transformação**, realiza procedimentos como OCR, transcrição de áudio, normalização temporal e geográfica, classificação preliminar e geração de estrutura JSON.

Na quarta camada, de **Validação**, o operador confirma, corrige ou rejeita os campos sugeridos, especialmente aqueles relacionados à criticidade e às informações essenciais da ocorrência. Por fim, a camada de **Destino Institucional** realiza o registro validado no sistema de interdições e no banco de dados de apoio, preservando a trilha de auditoria. Dessa forma, a automação é empregada como mecanismo de pré-processamento e apoio ao preenchimento, sem substituir a decisão humana ou autorizar o lançamento automático de informações críticas.

Figura VI: Arquitetura de transição para registro estruturado de comunicações de interdições.



Fonte: Elaboração do autor (2026).

A integração automatizada entre a arquitetura proposta e os sistemas institucionais da ANTT constitui etapa posterior e condicionada à avaliação técnica e à autorização formal das áreas competentes. Antes de qualquer integração, devem ser verificados a disponibilidade de interface de programação documentada, a existência de ambiente de homologação, os mecanismos de autenticação e autorização, os perfis de acesso, os limites de consumo do serviço, os requisitos de registro de logs e os procedimentos de reversão em caso de falha. Dessa forma, os testes devem ocorrer exclusivamente em ambiente controlado, com credenciais institucionais e dados anonimizados ou sintéticos, de modo a preservar a segurança, a integridade e a rastreabilidade das informações.

3.6 Estratégias de preenchimento

Serão comparadas três condições:

- Manual, operador lê a mensagem e preenche o formulário;
- IA assistida, LLM gera o JSON; operador revisa e envia;
- Automação autorizada, serviço gera JSON, valida regras e envia à API homologada, com aprovação humana para campos críticos.

A demonstração será realizada com dados sintéticos ou anonimizados. O uso de modelos de linguagem ficará restrito à extração e ao pré-preenchimento de campos, sem envio automático ao ambiente produtivo. A escolha de ferramentas e eventual integração institucional constituem etapas posteriores, dependentes da disponibilidade de ambiente de testes e de autorização das áreas responsáveis.

3.7 Prompt experimental

Prompt-base: *"Você é um assistente de estruturação de ocorrências rodoviárias. Extraia somente informações presentes na mensagem. Não invente valores. Quando um campo não estiver informado, use null e inclua-o em **campos_pendentes**. Normalize datas para ISO 8601 e quilometragem para o formato **km 000+000**. Classifique provisoriamente a criticidade usando os critérios fornecidos, mas marque **revisao_humana: true** quando faltarem dados de impacto, duração, congestionamento, vítimas ou bloqueio. Retorne exclusivamente JSON válido conforme o esquema. Preserve a mensagem original em campo separado e não exponha dados pessoais desnecessários."*

O prompt será ajustado por ciclos. Cada alteração deverá ser documentada em etapas, justificada e vinculada aos resultados dos testes, evitando ajustes direcionados a um único caso.

Tabela 2: Testes

Código	Teste	Procedimento	Métricas principais
T1	Completeness manual	Operador preenche o formulário a partir da mensagem	PF, tempo, erros
T2	Extração por LLM	Modelo gera JSON sem inserção no sistema	PF, precisão, campos inventados
T3	IA com validação humana	Operador revisa a saída da LLM	tempo total, correções, aceitação
T4	Comparação de modelos	Mesma mensagem e prompt em modelos distintos	completeness, precisão, consistência
T5	Mensagem incompleta	Omissão deliberada de campos obrigatórios	taxa de alucinação, pendências corretas
T6	Atualização do evento	Segunda mensagem altera status, horário ou impacto	rastreabilidade, atualização correta
T7	Criticidade dinâmica	Caso começa no nível 3 e recebe informação de impacto	reclassificação e prazo
T8	API homologada	Requisição controlada, se autorizada	sucesso, latência, integridade, logs
T9	Segurança	Teste de acesso por perfis e rejeição de payload inválido	autorização, validação e auditoria

Nota: PF corresponde à precisão de preenchimento, calculada pela razão entre o número de campos corretamente preenchidos e o número total de campos aplicáveis à ocorrência. Campos não informados na mensagem original não são considerados erros, desde que sejam registrados como ausentes ou pendentes para validação posterior.

Fonte: Elaboração do autor com base nos documentos da pesquisa.

3.8 Métricas

A completeness de preenchimento será calculada por:

$$PF = \frac{N_{\text{itens corretamente preenchidos}}}{N_{\text{itens totais aplicáveis}}}$$

Itens não informados na mensagem não devem ser penalizados como erro de extração, desde que o sistema retorne **null** e os inclua em **campos_pendentes**. Será calculada também a completeness dos campos obrigatórios e a completeness ponderada, atribuindo maior peso a data/hora, local, rodovia, km, sentido, tipo de ocorrência, interdição e criticidade.

O TTR (*time to respond*) será medido como o tempo entre a disponibilidade da mensagem e o primeiro registro utilizável no sistema. Serão registrados separadamente: tempo de leitura, tempo de extração, tempo de revisão e tempo de envio. Para evitar

comparação inadequada, a pesquisa distinguirá TTR operacional e tempo total de processamento.

Outras métricas:

- Precisão de campo, campos corretos divididos pelos campos preenchidos;
- Revocação de campo, campos corretos identificados divididos pelos campos informados na mensagem;
- Taxa de alucinação: valores preenchidos sem evidência na mensagem.
- Taxa de rejeição, casos em que o operador rejeitou a saída da IA;
- Taxa de correção humana, campos alterados pelo operador dividido pelos campos sugeridos;
- Acurácia da criticidade, classificação compatível com a matriz e com a avaliação de referência;
- Conformidade temporal, proporção de registros dentro de 60 ou 180 minutos, conforme o nível;
- Atualização tempestiva, proporção de atualizações feitas em até 120 minutos ou após informação relevante;
- Rastreabilidade, presença de identificador da ocorrência, referência à mensagem de origem, identificação do responsável pelo tratamento, data/hora das operações, versão do registro e histórico de alterações;
- Disponibilidade e erro de integração, requisições aceitas, rejeitadas e indisponíveis na API homologada.

3.9 Validação e análise

Dois avaliadores independentes revisarão os casos e formarão um gabarito de referência. Divergências serão resolvidas por consenso ou por terceiro avaliador. Resultados quantitativos serão apresentados por média, mediana, amplitude e intervalo interquartil. Para amostras maiores, poderão ser aplicados teste de Wilcoxon para tempos pareados e análise de concordância entre avaliadores. A análise qualitativa examinará a coerência do fluxo proposto, as ambiguidades de interpretação, a ausência de campos, a classificação preliminar das ocorrências e a capacidade do modelo de representar a origem, as atualizações e as providências adotadas.

3.10 Cuidados metodológicos e delimitação da demonstração

A demonstração utilizará dados sintéticos ou anonimizados, evitando a exposição de informações que permitam identificar pessoas. As mensagens e os anexos empregados terão finalidade ilustrativa e serão utilizados para demonstrar a organização dos campos e o funcionamento conceitual do fluxo.

O tratamento proposto manterá a distinção entre informação expressamente presente na fonte, valor normalizado e campo ausente ou pendente. A inteligência artificial não deverá completar informações sem evidência, e os campos críticos permanecerão sujeitos à revisão humana.

Não serão realizados testes em ambiente produtivo ou alterações em registros institucionais reais. O estudo não contempla avaliação de conformidade com a LGPD, elaboração de relatório de impacto à proteção de dados ou validação de mecanismos criptográficos de integridade. Essas exclusões delimitam a análise acadêmica e não representam autorização para uso operacional da solução.

CAPÍTULO 4 – RESULTADOS E DISCUSSÃO

4.1 Resultados da Proposta e Delimitação do Escopo

Este capítulo apresenta os resultados decorrentes da proposição de um modelo para transformar comunicações informais de interdição em registros institucionais estruturados, rastreáveis e passíveis de acompanhamento pelo CNSO/ANTT. O resultado central do trabalho consiste na definição de uma arquitetura de transição composta por canal de entrada autorizado, organização das comunicações, extração e normalização assistidas por inteligência artificial, validação humana obrigatória e registro em ambiente institucional com trilha de auditoria.

A proposta também compreende um modelo relacional de dados, um fluxo de tratamento das informações, um esquema de estruturação em JSON, regras de validação para campos críticos e critérios de qualidade relacionados à completude, precisão, rastreabilidade, conformidade e segurança da informação. O escopo da pesquisa concentra-se na especificação e na demonstração conceitual dessa arquitetura, sem contemplar sua implantação em ambiente produtivo, integração efetiva com sistemas institucionais ou aferição empírica de desempenho operacional. Tais atividades constituem etapas posteriores de validação técnica e institucional, condicionadas à autorização, à disponibilidade de ambiente de homologação e às regras de segurança e governança de dados aplicáveis.

O planejamento institucional da ANTT já registrou o desenvolvimento do sistema de interdições como iniciativa estruturante, incluindo a entrega do sistema, treinamento de usuários dos CCOs e definição de padrões mínimos de qualidade e frequência dos dados. O relatório também registra a conclusão do desenvolvimento em 99% e pendências relativas a treinamento e padrões de dados, o que reforça a pertinência de estudar a qualidade da entrada e o fluxo de adoção.

Tabela 3: Simulação do caso-base - A mensagem analisada permite preencher os seguintes campos com evidência direta:

Campo	Valor simulado	Evidência
Natureza	Interdição	Título e texto do comunicado
Situação	Ativo no momento da comunicação	Comunicado de atualização de interdição
Data real	16/08/2026	Mensagem
Hora real	19:58	Evidência CFTV e mensagem
Concessionária	ECO101 / Eco101	Identificação do comunicado
Estado	ES	Linhares/ES e BR-101-ES
Rodovia	BR-101	BR101-ES-KM137+800
Tipo de rodovia	Rodovia federal concedida	Contexto do comunicado
Sentido	Norte	Mensagem
KM	137+800	Mensagem
Área afetada	Parcial	“Interdição Parcial”
Direção	Norte	Derivada do sentido; confirmar no sistema
Total de faixas	Não informado	Deve permanecer pendente
Faixas interditadas	Não informado	Deve permanecer pendente
Causa	Atendimento mecânico não decorrente de sinistro de trânsito	Mensagem
Observações	Equipe de apoio da concessionária atuava no local e deixava o local na evidência de 19h58; fonte CFTV	Mensagem
Protocolo	Não há	Mensagem
Registro	INT0005160	Mensagem
Criticidade	Provisoriamente nível 3; revisão necessária	Ausência de dados de impacto
Previsão de liberação	Não informada	Deve permanecer pendente

Fonte: Elaboração do autor com base nos documentos da pesquisa.

A simulação demonstra que a IA pode reduzir a transcrição, mas não deve completar campos ausentes por inferência. Por exemplo, não é admissível deduzir o número de faixas, a faixa efetivamente bloqueada, o tamanho do congestionamento ou o horário previsto de liberação.

Tabela 4: Dicionário de dados proposto

Entidade/campo	Tipo	Obrigatório	Regra
id_ocorrencia	UUID	Sim	Identificador único e imutável
registro_antt	Texto	Não	Número INT, quando existente
origem_mensagem_id	Texto	Sim	Referência à mensagem ou comunicação que originou o registro
concessionaria_id	Inteiro	Sim	Chave estrangeira
data_inicio_real	Data	Sim	ISO 8601
hora_inicio_real	Hora	Sim	Fuso America/Sao_Paulo
data_previsao_liberacao	Data	Não	Não preencher por estimativa
hora_previsao_liberacao	Hora	Não	Não preencher por estimativa
estado	Código UF	Sim	Domínio oficial
rodovia	Texto/código	Sim	Normalizar BR-101
tipo_rodovia	Domínio	Sim	Federal concedida, conforme cadastro
sentido	Domínio	Sim	Norte, Sul, Leste, Oeste ou ambos
km	Decimal/texto normalizado	Sim	Ex.: 137+800
municipio	Texto	Não	Linhares
area_afetada	Domínio	Sim	Total, parcial ou acostamento
direcao	Domínio	Sim	Conforme circulação afetada
total_faixas	Inteiro	Não	Valor confirmado pela fonte
faixas_interditadas	Texto	Não	Faixas ou quantidade confirmada
causa	Domínio/texto	Sim	Atendimento mecânico sem sinistro
nivel_criticidade	Inteiro	Sim	1, 2 ou 3, com justificativa
justificativa_criticidade	Texto	Sim	Critérios e evidências
observacoes	Texto	Não	Síntese objetiva
plano_acao	Texto	Não	Providências adotadas
providencias	Texto	Não	Ações e próximos passos
fonte	Domínio	Sim	CFTV, concessionária, equipe etc.
campos_pendentes	JSON	Sim	Campos ausentes ou ambíguos
criado_por	Identificador	Sim	Usuário ou serviço
criado_em	Timestamp	Sim	Registro de criação
atualizado_em	Timestamp	Sim	Última atualização
versao	Inteiro	Sim	Incremental
status	Domínio	Sim	Aberta, em atendimento, liberada, encerrada

Fonte: Elaboração do autor com base nos documentos da pesquisa.

A entidade de anexos deverá registrar o identificador do arquivo, seu tipo, nome, tamanho, origem, data de recebimento e relação com a ocorrência. A finalidade dessa entidade é organizar os documentos associados ao evento e permitir sua recuperação. O modelo não contempla verificação criptográfica dos arquivos..

Figura VII: JSON da ocorrência simulada

JSON

```
{
  "schema_version": "1.0",
  "source": {
    "channel": "whatsapp",
    "message_id": null,
    "received_at": null,
    "original_text": "Atualização de Interdição: ECOVIAS CAPIXABA - 16/08/2026 - 19:58min - ATENDIMENTO MECÂNICO NÃO DECORRENTES DE SINISTRO DE TRÂNSITO. Cidade: Linhares/ES. Sentido: Norte. BR101-ES-KM137+800. Na evidência colhida às 19h58min, foi observada a atuação da equipe de apoio da concessionária, que, no momento, deixava o local. Protocolo nº: Não há. Registro de Interdição: INT0005160. Interdição Parcial. Fonte de informação: CFTV.",
    "attachments": [
      {
        "type": "image",
        "sha256": null,
        "description": "Imagem de CFTV anexada à comunicação"
      }
    ]
  },
  "event": {
    "nature": "interdicao",
    "status": "ativo_no_momento_da_verificacao",
    "record_id": "INT0005160",
    "protocol": null,
    "concessionaire": "ECO101",
    "state": "ES",
    "municipality": "Linhares",
    "highway": "BR-101",
    "highway_type": "federal_concedida",
    "direction": "Norte",
    "km": "137+800",
    "affected_area": "parcial",
    "total_lanes": null,
    "closed_lanes": null,
    "cause": "atendimento mecânico não decorrente de sinistro de trânsito",
    "real_start_date": "2026-08-16",
    "real_start_time": "19:58:00-03:00",
    "release_forecast_date": null,
    "release_forecast_time": null,
    "source_type": "CFTV",
    "criticality": {
      "level": 3,
      "status": "provisoria",
      "justification": "Ocorrência aparentemente rotineira, sem evidência de vítimas, congestionamento significativo ou bloqueio total. Confirmar impacto operacional.",
      "human_review_required": true
    },
    "observations": "Na evidência de 19h58, a equipe de apoio da concessionária foi observada deixando o local."
  }
}
```

```
"action_plan": null,
"measures_taken": "Atendimento mecânico pela equipe de apoio da concessionária; situação deve
ser atualizada no sistema.",
"pending_fields": [
  "message_id",
  "received_at",
  "total_lanes",
  "closed_lanes",
  "congestion_length_km",
  "release_forecast",
  "confirmation_of_clearance",
  "criticality_impact_evidence"
],
},
"governance": {
  "extraction_method": "Ilm_assisted",
  "prompt_version": "prompt-1.0",
  "human_validation": {
    "required": true,
    "validated": false,
    "validated_by": null,
    "validated_at": null
  },
},
"audit": {
  "created_by": null,
  "created_at": null,
  "updated_at": null,
  "version": 1
}
}
```

Fonte: Elaboração do autor com base nos documentos da pesquisa.

4.2 Discussão sobre criticidade e prazo

A mensagem permite afirmar que houve interdição parcial, mas não permite concluir, sem informação adicional, se ocorreu impacto relevante. O preenchimento deve, portanto, distinguir o fato observado da classificação normativa. A classificação provisória em nível 3 é uma hipótese de trabalho baseada na ausência de evidência de impacto relevante; não substitui a validação do operador.

Se a concessionária informar que houve lentidão significativa, bloqueio de faixa com repercussão ou extensão superior ao limite indicado na matriz, o evento deve ser elevado para nível 2, com observância do prazo de comunicação de até 60 minutos. Se surgirem múltiplas vítimas, óbito, bloqueio total, envolvimento de carga perigosa, grande congestionamento ou repercussão institucional, o evento pode alcançar nível 1. O nível 1 também possui prazo de até 60 minutos. O nível 3 admite até 180 minutos, mas o envio deve ocorrer assim que a ocorrência for verificada, sem utilizar o prazo como justificativa para atraso evitável.

4.3 Análise conceitual de rastreabilidade e consistência dos registros

A rastreabilidade da proposta é analisada a partir da capacidade do modelo de representar a origem e o histórico de cada ocorrência. Para isso, a estrutura deve permitir identificar a comunicação inicial, o responsável pela extração, a versão do prompt quando aplicável, os valores sugeridos, a revisão humana, as alterações realizadas e as providências associadas ao evento.

A análise considera também a distinção entre informação disponível, informação normalizada e informação pendente. Campos ausentes na mensagem não devem ser preenchidos como fatos confirmados. A classificação de criticidade deve permanecer vinculada às evidências disponíveis e às revisões registradas.

Tabela 5: Critérios de análise conceitual da proposta:

Dimensão	Elementos previstos no modelo	Critério de análise
Identificação	Identificador único da ocorrência	Possibilidade de distinguir e relacionar os registros de cada evento
Vinculação à origem	Referência à mensagem ou comunicação inicial	Possibilidade de identificar a fonte do registro
Responsabilidade	Identificação de quem extraiu, revisou e atualizou	Associação das operações aos respectivos responsáveis
Compleitude	Campos obrigatórios e indicação de pendências	Distinção entre informações disponíveis e ausentes
Consistência	Domínios, formatos e relações entre entidades	Representação coerente dos dados e de seus vínculos
Temporalidade	Datas e horários de recebimento, registro e atualização	Possibilidade de reconstruir a sequência das operações
Atualização	Versões, status e providências	Representação da evolução do evento
Histórico	Operação, valores anterior e posterior, responsável e data/hora	Recuperação das alterações realizadas
Estruturação	Campos normalizados e representação em JSON	Organização dos dados para consulta e intercâmbio futuro

Fonte: Elaboração do autor com base nos documentos da pesquisa.

4.4 Riscos e controles

Os principais riscos considerados na proposta são o preenchimento de valores sem evidência, a interpretação incorreta de localização e horários, a classificação inadequada da criticidade, a duplicação de ocorrências, a ausência de vínculo entre mensagens e anexos, a perda do histórico de atualizações e o registro automático de informações não revisadas.

As medidas propostas incluem indicação de campos ausentes ou pendentes, referência à fonte de cada informação, revisão humana dos campos críticos, associação de mensagens ao identificador da ocorrência, identificação dos anexos e manutenção do histórico de alterações. O fluxo também prevê a distinção entre comunicação inicial, atualização e encerramento.

Essas medidas são apresentadas como componentes do desenho conceitual. Sua implementação, eficácia e desempenho deverão ser verificados em etapa posterior, mediante testes em ambiente controlado. Não são avaliados mecanismos de hash, garantias de imutabilidade dos registros ou requisitos de conformidade com a LGPD.

CAPÍTULO 5 – CONSIDERAÇÕES FINAIS

5.1 Conclusões

O trabalho apresenta uma arquitetura conceitual para transformar comunicações de interdição recebidas pelo WhatsApp em registros estruturados, relacionados às respectivas ocorrências e acompanhados de histórico de tratamento. A contribuição está na definição do fluxo e do modelo relacional, com destaque para a organização dos campos, a identificação da origem, o registro de atualizações e a validação humana.

A demonstração ilustra a aplicação do modelo, mas não comprova ganhos de tempo, precisão ou desempenho em operação real. Esses efeitos permanecem como hipóteses a serem examinadas em validação futura. Da mesma forma, o estudo não demonstra integridade criptográfica, conformidade com a LGPD ou admissibilidade probatória dos registros.

5.2 Limitações

- O estudo parte de uma comunicação ilustrativa e de uma matriz fornecida pelo pesquisador, não de uma base estatística consolidada;
- A existência, o formato e as permissões de uma API do sistema de interdições não foram confirmados publicamente; a página do sistema não retornou conteúdo acessível na consulta realizada;
- O formulário exibido não permite inferir todos os domínios internos, códigos e regras de validação do sistema;
- Os resultados de tempo, precisão e completude dependem da execução dos testes com operadores e mensagens reais anonimizadas;

- Modelos de linguagem podem variar em desempenho, custo, latência e política de retenção;
- O WhatsApp não deve ser tratado como repositório oficial nem como prova isolada; a solução deve priorizar a formalização no sistema institucional.
- Não foram implementados ou avaliados mecanismos criptográficos de integridade de mensagens e anexos;
- A pesquisa não compreende avaliação de conformidade com a LGPD;
- A rastreabilidade é examinada como capacidade de representar origem, responsáveis, versões e histórico, sem equivaler à validação de cadeia de custódia forense ou à garantia de autenticidade dos registros;

5.3 Recomendações institucionais

1. Publicar um catálogo oficial de campos, domínios, códigos, criticidade, prazos e regras de atualização;
2. Disponibilizar ambiente de homologação e documentação de API, caso a integração seja autorizada;
3. Implantar resposta padronizada no canal operacional, sempre direcionando para o sistema institucional;
4. Adotar validação humana obrigatória para criticidade, localização, faixas, vítimas, congestionamento e previsão de liberação;
5. Criar painel de qualidade com PF, TTR, completude dos campos críticos, reclassificações e atrasos;
6. Manter trilha de auditoria com versão do prompt, modelo, operador e alterações;
7. Definir procedimentos operacionais de organização, consulta, atualização e arquivamento dos registros, com atribuição de responsabilidades e preservação do histórico das ocorrências;
8. Capacitar usuários dos CCOs e equipes do CNSO, especialmente quanto à distinção entre comunicação inicial e atualização;
9. Definir procedimento de contingência para indisponibilidade do sistema, com posterior reconciliação e registro do motivo;
10. Proibir o envio automático para produção sem autorização formal, testes de segurança e aprovação do gestor do sistema.

5.4 Trabalhos futuros

- Ampliar a amostra e executar experimento controlado com operadores;
- Comparar modelos de linguagem locais e serviços corporativos autorizados;
- Avaliar OCR, transcrição de áudio e leitura de imagens de CFTV;

- Construir um protótipo de banco relacional e painel gerencial;
- Testar integração REST em homologação, incluindo autenticação, autorização, idempotência e tratamento de erros;
- Avaliar explicabilidade da classificação de criticidade;
- Medir impacto da capacitação dos parceiros na qualidade das mensagens;
- Avaliar, em ambiente de homologação, a recuperação do histórico das ocorrências, o tratamento de atualizações sucessivas e a associação entre mensagens, registros e anexos;
- Investigar interoperabilidade com SIR e demais sistemas institucionais, evitando duplicidade de lançamento.

5.5 Síntese final

A proposta é tecnicamente viável como arquitetura assistida e academicamente adequada como estudo de caso. A automação deve reduzir retrabalho, não reduzir responsabilidade. O ganho institucional esperado não está apenas em preencher mais campos, mas em produzir registros tempestivos, explicáveis, íntegros e auditáveis, capazes de apoiar a supervisão operacional e a prestação de contas.

Esses resultados serão buscados por meio de um fluxo controlado de tratamento das comunicações: captura em canal autorizado, identificação e agrupamento de mensagens relacionadas a uma mesma ocorrência, extração e normalização dos dados, geração de estrutura padronizada para pré-preenchimento e validação humana obrigatória antes do registro institucional. A proposta também prevê a associação de cada ocorrência à concessionária, rodovia, localização, criticidade, responsáveis, tratativas, anexos e histórico de alterações, preservando a trilha de auditoria ao longo de todo o ciclo de vida do evento.

Dessa forma, a informação recebida em formato não estruturado deixa de permanecer isolada em mensagens e passa a compor um registro institucional único, consultável e passível de análise. A classificação conforme os níveis crítico, significativo e operacional, somada aos prazos de comunicação e à atualização periódica dos eventos, permite que o modelo apoie o acompanhamento tempestivo das ocorrências e a produção de evidências para fins operacionais, gerenciais e de prestação de contas.

REFERÊNCIAS NORMATIVAS CONSULTADAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR 10520:2023: informação e documentação - citações em documentos - apresentação. Rio de Janeiro: ABNT, 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 17 ago. 2026.

AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES. Relatório de Resultados do Plano de Gestão Anual 2025. Brasília, DF, 2026. Documento consultado para contextualização do desenvolvimento do sistema de interdições. Disponível no portal institucional da ANTT. Acesso em: 17 ago. 2026.

AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES. Ofício Circular SEI nº 2963/2026/DG-ANTT. Diretrizes para padronização, prazos e atualização da comunicação de ocorrências e sinistros de trânsito em rodovias federais concedidas. Documento fornecido pelo pesquisador, a ser conferido no SEI e citado conforme a versão oficial.

REFERÊNCIAS

ALVES, D. T. S.; LIMA, G. B. A. Estabelecimento de um banco de dados de incidentes em dutos terrestres para apoiar a gestão de riscos operacionais no Brasil – Parte 2: Proposta do diagrama de gravata borboleta e estatísticas de falhas. *Segurança de Processos e Proteção Ambiental*, v. 155, 2021.

ATAMANENKO, Y. Conceptual model bases of geoprostatic data for registration and cartographing of accident. *Engineering Geodesy*, v. 66, p. 104-115, 2019.

BAGATINI, J. A.; GUIMARÃES, J. A. C.; SANTANA, R. C. G. Gerenciamento dos dados pessoais em arquivos: uma perspectiva centrada no indivíduo com base na LGPD. *Acervo*, v. 34, n. 3, 2021.

COELHO, F. C.; CARVALHO, A. M. A. A Ciência da Informação e a Lei Geral de Proteção de Dados Pessoais (LGPD): Uma Revisão Sistemática de Literatura. *Inf. Inf.*, v. 30, n. 01, p. 24-54, 2025.

CORDEIRO, G.; SANTOS, R. Relational database design for incident tracking in regulatory agencies. *Data & Knowledge Engineering*, v. 148, 2023.

FERREIRA, L. G. T. et al. Network monitoring using Zabbix, Grafana, and ZeroTier. *Revista Caderno Pedagógico*, v. 22, n. 14, 2025.

FREITAS, A. C.; RODRIGUES, R. C. Governança de dados em agências reguladoras: desafios da Lei de Acesso à Informação e LGPD. *Revista de Administração Pública*, v. 56, n. 6, 2022.

GOMES, H. P.; LIMA, S. M. WhatsApp as an official communication channel: risks and opportunities in public safety. *Government Information Quarterly*, v. 39, n. 3, 2022.

KHATTACH, O.; MOUSSAOUI, O.; HASSINE, M. End-to-End Architecture for Real-Time IoT Analytics and Predictive Maintenance Using Stream Processing and ML Pipelines. *Sensors*, v. 25, n. 9, 2945, 2025.

KONTOGIANNIS, S.; ASIMINIDIS, C. Proposed Management System and Response Estimation Algorithm for Motorway Incidents. *Energies*, v. 14, 2736, 2021.

MAGNET FORENSICS. Digital Forensics: Artifact Profile - WhatsApp Messenger. 2016. Disponível em: <https://www.magnetforensics.com/blog/artifact-profile-whatsapp-messenger/>. Acesso em: 15 maio 2026.

MEHMOOD, E.; ANEES, T. Challenges and Solutions for Processing Real-Time Big Data Stream: A Systematic Literature Review. *IEEE Access*, v. 8, p. 119123-119143, 2020.

NISCHCHAL, S. Forensic Analysis of WhatsApp: A Review of Techniques, Challenges, and Future Directions. *Journal of Forensic Science and Research*, v. 8, p. 019-024, 2024.

PEREIRA, J. C.; SILVA, M. M. From unstructured messages to structured dashboards: ETL pipeline for emergency calls. *Information Systems*, v. 115, 2023.

PRABOWO, W. A.; MOHSEN, F.; SELAMAT, S. R. Forensic Analysis of WhatsApp: A Review of Techniques, Challenges, and Future Directions (Msgstore.db.crypt14 analysis). *Journal of Big Data*, 2024. (Título adaptado a partir do conteúdo do PDF)

PRABOWO, et al. Deciphering the Msgstore.db.crypt14 File. 2024. Disponível em: <https://www.semanticscholar.org/paper/WhatsApp-Mobile-Applications-in-the-Lens-of-Digital-Prabowo-Mohsen/8ecf2591c171f522e963eca>. Acesso em: 15 maio 2026.

SEBASTIAN, G. Digital shadow AI risk theory (DART): A framework for managing data disclosure and privacy risks of AI tools at work. *Technological Forecasting & Social Change*, v. 229, 124697, 2026.

ŠEDIVCOVÁ, L.; POTANČOK, M. Shadow IT Management Concept for Public Sector. In: *CONFENIS*, 2019, p. 65-73.

SOUZA, F. J.; OLIVEIRA, L. C. Grafana and Zabbix integration for real-time infrastructure supervision. *International Journal of Network Management*, v. 34, 2024.

SOUZA, J. P. et al. Shadow IT and the digital transformation: a systematic literature review. *Gestão & Produção*, v. 28, 2021.

ZENVIA / OPINION BOX. *Uso de WhatsApp pessoal no trabalho aumenta erros e expõe empresas a risco de dados*. Tecflow, 2024. (Estudo de mercado citado na proposta)

APENDICE A

Análise forense e extração de dados do WhatsApp, possibilidades técnicas e fundamentos técnicos da extração de dados do WhatsApp

A análise forense de dados oriundos do WhatsApp ocupa posição relevante no campo da investigação digital contemporânea, especialmente em contextos nos quais a aplicação é utilizada como canal recorrente de comunicação operacional. Sob o ponto de vista técnico, a literatura indica que o aplicativo armazena parte substancial de suas informações em bancos de dados locais, com destaque para estruturas em SQLite e arquivos criptografados associados ao histórico de mensagens e metadados, como o backup criptografado do histórico de conversas do WhatsApp em dispositivos Android (Prabowo et al., 2024).

Em complemento, a documentação técnica de ferramentas forenses especializadas aponta que, em dispositivos Android, artefatos relevantes incluem bases como msgstore.db e wa.db, as quais podem conter conteúdos de mensagens, identificadores de contatos, status de envio, registros temporais e dados de anexos, além de, em certos casos, informações geográficas vinculadas às interações (Magnet Forensics, 2016).

A extração desses dados requer o acesso à chave de criptografia, que fica armazenada no dispositivo do usuário. Estes autores demonstram que, mesmo em dispositivos não enraizados, é possível extrair a chave e decifrar o banco de dados utilizando ferramentas como WhatsApp-Chave, Extrator de Banco de Dados, permitindo a recuperação de mensagens, contatos, timestamps e metadados de mídia.

Essas características demonstram que o WhatsApp não constitui apenas um meio efêmero de comunicação interpessoal, mas também uma fonte potencialmente rica de evidências digitais. A possibilidade de recuperar mensagens, contatos, anexos, carimbos temporais e informações de contexto técnico torna viável a reconstrução de eventos comunicacionais com razoável nível de detalhamento, desde que sejam observados métodos adequados de preservação, extração e análise (Nishchal, 2024). Assim, a análise forense do aplicativo apresenta utilidade não apenas em investigações criminais, mas também em auditorias, apurações administrativas e reconstrução de fluxos operacionais em ambientes institucionais.

Relevância da análise forense no contexto do CNSO/ANTT

No âmbito do CNSO/ANTT, a análise forense do WhatsApp passa a ter relevância prática para a compreensão de como as comunicações de fato ocorrem na rotina da fiscalização. Quando um agente utiliza o aplicativo para comunicar uma interdição, um sinistro, um bloqueio de faixa, uma falha de sinalização ou o acionamento emergencial de uma concessionária, os dados gerados por essa interação podem constituir importante fonte de reconstrução do evento. A recuperação dos registros permite identificar quando a mensagem foi enviada, quem a recebeu, se houve leitura, quais arquivos foram compartilhados e em que sequência se deram os encaminhamentos subsequentes, fornecendo elementos úteis à compreensão da dinâmica decisória em situações críticas (Nishchal, 2024).

Possibilidades probatórias e reconstrução de linha do tempo

A literatura forense destaca que a análise do WhatsApp possibilita a extração de elementos capazes de subsidiar a reconstituição cronológica de eventos, o que inclui mensagens textuais, dados de envio e recebimento, confirmações de leitura, informações sobre mídias e, em determinados casos, artefatos que revelam relações entre participantes e dispositivos (Nishchal, 2024). Tais elementos são particularmente relevantes em ambientes regulatórios, nos quais a rastreabilidade das decisões e a demonstração da tempestividade das providências adotadas assumem papel central.

Ainda no contexto do CNSO/ANTT, caso um usuário alegue prejuízo decorrente de atraso no atendimento, a análise forense dos registros de mensageria pode auxiliar na verificação de quando o fato foi comunicado internamente, qual setor tomou ciência da ocorrência, quando houve acionamento da concessionária e se a comunicação entre as equipes ocorreu de forma tempestiva. Embora tais dados não substituam o registro oficial em sistema institucional, eles podem funcionar como fonte complementar de evidência, especialmente quando a formalização da informação não ocorreu de maneira simultânea.

De igual modo, em ocorrências envolvendo controvérsias sobre perdas, danos ou falhas de atendimento, a recuperação de mensagens e metadados pode contribuir para a formação de acervo probatório mais robusto. A partir desses elementos, torna-se possível reforçar a coerência entre narrativas institucionais e registros técnicos, reduzindo incertezas e fortalecendo a capacidade de defesa administrativa e judicial da Agência e dos demais atores regulados.

Limitações, cautelas metodológicas e governança da evidência digital

Apesar das possibilidades técnicas identificadas, a análise forense do WhatsApp impõe cautelas relevantes. A extração de dados depende de condições técnicas específicas, do acesso ao dispositivo ou a seus vestígios digitais, da preservação adequada dos artefatos e da utilização de ferramentas validadas para leitura e interpretação das bases recuperadas (Prabowo et al., 2024; Nishchal, 2024). Além disso, a volatilidade dos dados, as atualizações frequentes do aplicativo, os mecanismos de criptografia e as diferenças entre sistemas operacionais impõem desafios adicionais à consistência dos resultados obtidos.

No plano institucional, essas limitações reforçam a necessidade de não se tratar o WhatsApp como repositório principal de informação administrativa sensível. Em vez disso, a análise forense deve ser compreendida como recurso subsidiário, útil para reconstrução de fluxos informacionais, validação de comunicações e recuperação excepcional de evidências em casos específicos. A dependência exclusiva de canais informais tende a fragilizar a governança da informação, dificultando auditorias, comprometendo a cadeia de custódia e ampliando riscos relacionados à proteção de dados, à conformidade regulatória e à segurança jurídica.

Para o CNSO/ANTT, essa constatação é especialmente sensível, pois o ambiente de fiscalização exige equilíbrio entre celeridade operacional e formalidade documental. A eventual extração forense de comunicações em mensageria instantânea pode ser tecnicamente possível, mas não elimina a necessidade de que informações críticas sejam incorporadas tempestivamente a sistemas institucionais estruturados, aptos a garantir integridade, indexação, auditabilidade e preservação do histórico administrativo.

Implicações para o aprimoramento institucional da fiscalização

A análise forense do WhatsApp, quando observada no contexto do CNSO/ANTT, revela um duplo aspecto. De um lado, demonstra que o aplicativo pode servir como fonte relevante de evidência digital, apta a recuperar mensagens, registros temporais, contatos e anexos que ajudem a reconstruir incidentes operacionais e a identificar o fluxo efetivo das comunicações (Prabowo et al., 2024; Magnet Forensics, 2016; Nishchal, 2024). De outro, evidencia que a recorrência do uso dessa ferramenta em processos sensíveis da fiscalização decorre, em grande medida, de lacunas percebidas nos sistemas oficiais.

Dessa forma, a utilidade forense do WhatsApp não deve ser interpretada como justificativa para sua adoção informal como solução institucional permanente. Ao contrário, sua análise técnica evidencia a urgência de desenvolver sistemas próprios, mais responsivos e aderentes ao cotidiano operacional, capazes de absorver com segurança e rastreabilidade as informações que hoje circulam em canais paralelos. Nesse sentido, a forense digital contribui não apenas para recuperar dados pretéritos, mas também para demonstrar, de forma concreta, quais requisitos funcionais um sistema institucional precisa atender para reduzir a dependência da mensageria informal.

Síntese analítica

Conclui-se, portanto, que a análise forense e a extração de dados do WhatsApp constituem possibilidades técnicas relevantes para a reconstrução de eventos, identificação de participantes, recuperação de metadados e estabelecimento de linhas do tempo comunicacionais em ambientes regulatórios. No contexto do CNSO/ANTT, tais possibilidades assumem valor prático na apuração de incidentes, na verificação da tempestividade das respostas e no apoio à defesa institucional em situações de controvérsia.

Entretanto, a principal contribuição dessa perspectiva não reside apenas na recuperação de evidências, mas na demonstração das fragilidades de modelos de comunicação excessivamente dependentes de ferramentas informais. Em um ambiente de fiscalização rodoviária com elevada complexidade operacional, a consolidação de sistemas institucionais estruturados permanece condição indispensável para assegurar governança da informação, segurança documental e rastreabilidade compatível com as exigências da Administração Pública e da regulação federal (Nishchal, 2024; ABNT, 2023).

APENDICE B

Figura I: Código da estrutura apresentada acima, com a relação dos elementos mencionados.

CÓDIGO

```
erDiagram
    CONCESSIONARIA ||--o{ RODOVIA : administra
    RODOVIA ||--o{ OCORRENCIA : possui
    OCORRENCIA ||--|| LOCALIZACAO : ocorre_em
    OCORRENCIA ||--o{ TRATATIVA : possui
    OCORRENCIA ||--o{ ANEXO : comprova
    OCORRENCIA ||--o{ AUDITORIA : registra
    USUARIO ||--o{ OCORRENCIA : registra
    USUARIO ||--o{ TRATATIVA : executa
    USUARIO ||--o{ AUDITORIA : realiza
```

```
CONCESSIONARIA {
    int id_concessionaria PK
    string nome
    string cnpj
    string contato
}
RODOVIA {
    int id_rodovia PK
    int id_concessionaria FK
    string codigo
    string denominacao
    string trecho
    string sentido
    decimal extensao
}
OCORRENCIA {
    int id_ocorrencia PK
    int id_rodovia FK
    int id_usuario FK
    string protocolo
    string tipo
    string severidade
    datetime data_hora_abertura
    datetime data_hora_encerramento
    string status
    string descricao
}
LOCALIZACAO {
    int id_localizacao PK
    int id_ocorrencia FK
    string municipio
    string uf
    decimal quilometro
    decimal latitude
    decimal longitude
    string sentido
}
```



```
USUARIO {  
    int id_usuario PK  
    string nome  
    string matricula  
    string perfil  
    string unidade  
}  
TRATATIVA {  
    int id_tratativa PK  
    int id_ocorrencia FK  
    int id_usuario FK  
    datetime data_hora  
    string tipo_acao  
    string descricao  
    string resultado  
}  
ANEXO {  
    int id_anexo PK  
    int id_ocorrencia FK  
    string tipo  
    string nome_arquivo  
    datetime data_inclusao  
}  
AUDITORIA {  
    int id_auditoria PK  
    int id_ocorrencia FK  
    int id_usuario FK  
    datetime data_hora  
    string operacao  
    string campo_alterado  
    string valor_anterior  
    string valor_novo  
}
```

Fonte: Elaboração do autor, com base em Cordeiro e Santos (2023) e nos requisitos do estudo.

APENDICE C

Figura II: Código da figura III “classes conceitual para registro e rastreabilidade de incidentes de interdição rodoviária”.

CÓDIGO

```
classDiagram
    direction LR

    class Concessionaria {
        +idConcessionaria: UUID
        +razaoSocial: String
        +cnpj: String
        +nomeFantasia: String
        +status: String
    }

    class Rodovia {
        +idRodovia: UUID
        +codigo: String
        +denominacao: String
        +trecho: String
        +extensaoKm: Decimal
    }

    class Localizacao {
        +idLocalizacao: UUID
        +km: Decimal
        +sentido: String
        +municipio: String
        +uf: String
        +latitude: Decimal
        +longitude: Decimal
    }

    class Ocorrencia {
        +idOcorrencia: UUID
        +protocolo: String
        +natureza: String
        +criticidade: String
        +status: String
        +descricao: Text
        +dataHoraAbertura: DateTime
        +dataHoraEncerramento: DateTime
    }

    class Responsavel {
        +idResponsavel: UUID
        +nome: String
        +identificacaoFuncional: String
        +perfil: String
        +unidade: String
    }

    class Tratativa {
```



```
+idTratativa: UUID
+dataHora: DateTime
+tipoAcao: String
+descricao: Text
+resultado: String
}

class Anexo {
+idAnexo: UUID
+tipo: String
+nomeArquivo: String
+dataInclusao: DateTime
+origem: String
}

class Auditoria {
+idAuditoria: UUID
+dataHora: DateTime
+operacao: String
+campoAlterado: String
+valorAnterior: Text
+valorNovo: Text
}

Concessionaria "1" --> "1..*" Rodovia : administra
Rodovia "1" --> "0..*" Ocorrencia : possui
Ocorrencia "1" --> "1" Localizacao : ocorre em
Responsavel "1" --> "0..*" Ocorrencia : registra/valida
Ocorrencia "1" --> "0..*" Tratativa : possui
Responsavel "1" --> "0..*" Tratativa : executa
Ocorrencia "1" --> "0..*" Anexo : possui
Ocorrencia "1" --> "0..*" Auditoria : gera
Responsavel "1" --> "0..*" Auditoria : realiza
```

Fonte: Elaboração do autor (2026).