Uma Plataforma para promover a Interoperabilidade entre Órgãos de Segurança Pública

Diogo Cirne Nunes[1], **Frederico Araújo da Silva Lopes**[2]

[1]Instituto Técnico-Científico de Perícia (ITEP)
Governo do Estado do Rio Grande do Norte – RN – Brasil

[2]Instituto Metrópole Digital (IMD)
Universidade Federal do Rio Grande do Norte (UFRN) – Natal – RN – Brasil

cirnediogo@gmail.com, fred@imd.com.br

Resumo. *De forma a acompanhar o avanço tecnológico, é comum buscar o desenvolvimento de técnicas que auxiliam na automatização de procedimentos anteriormente feitos inteiramente de forma manual. Assim, é comum que alguns serviços já estejam habituados a serem realizados de forma analógica, dificultando uma possível mudança nas práticas já enraizadas. Em especial, isso ocorre quando os procedimentos envolvem a ação de órgãos distintos, cada um com suas próprias práticas já estabilizadas há anos e distintas dos demais. Por outro lado, a interoperabilidade entre sistemas é utilizada de forma a permitir que as entidades envolvidas possam operar em conjunto de forma transparente para o usuário. Nesse contexto, este trabalho propõe uma plataforma de middleware que provê a interoperabilidade entre os órgãos policiais e de perícia criminal, visando a melhoria no serviço prestado por estes e a resposta cada vez mais rápida para a sociedade nos serviços de investigação de crimes contra a vida.*

Abstract. *In order to keep up with technological advances, it is usual to seek the development of techniques to help the automation of procedures previously performed entirely manually. However, many services are already used to being done in an analogical way, making it difficult for a change in the already ingrained practices, especially when the procedures involve the action of different organizations, each with their own practices that have been performed for years and years, each of them distinct from the others. On the other hand, interoperability between systems is used in order to allow the involved entities to operate together in a transparent way for the user. Considering this context, this work proposes a middleware platform to provide interoperability between police and forensic agencies, aiming at improving the service provided by them and a faster response for society in the investigations of life crimes.*

1. Introdução

O setor de Tecnologia da Informação e Comunicação (TIC) se depara com uma quantidade cada vez maior de troca de informações entre parceiros [Zacharewicz et al. 2020]. Com o crescimento dos sistemas de informação, o volume e a complexidade dos dados tornam-se cada vez mais difíceis de gerenciar, os dados são armazenados em várias estruturas independentes. Surge assim a necessidade de criar um sistema global que reúna

todas as ilhas de informação partilhadas entre os serviços. A homogeneidade dos sistemas não é possível devido a restrições financeiras e técnicas, bem como necessidades funcionais. É necessário desenvolver um processo de integração e interoperação sólido e eficiente de forma a partilhar este conhecimento com todos os sistemas de informação que dele necessitem [Cardoso et al. 2018]. A pesquisa sobre interoperabilidade está ganhando muita atenção em conferências, fóruns e exposições, além disso, cada vez mais a literatura da Indústria 4.0 menciona interoperabilidade, o que evidentemente enfatiza sua importância na quarta revolução industrial [Liao et al. 2017].

Tal cooperação entre instituições distintas é comum no setor de segurança pública. Para enfrentar com sucesso um desastre, é necessária a participação coordenada e colaborativa de múltiplos órgãos relacionados à segurança pública, que forneçam uma resposta condizente com as exigências do ambiente de emergência e de todos os afetados. Para isso, é necessária a troca permanente de informações entre os órgãos envolvidos que permita unir seus esforços e enfrentar a emergência da melhor maneira possível [Zambrano-Vizuete et al. 2018]. Ainda, certas ocorrências de competência da segurança pública são tratadas por uma variedade de atores e organizações. Independentemente do tamanho e se as ocorrências acontecem sem aviso ou são previsíveis e esperadas, elas só podem ser gerenciadas se todos os atores envolvidos na resposta cooperarem e reagirem de maneira eficiente e coordenada. Portanto, o fornecimento preciso e ideal de informações é um pré-requisito indispensável, porque as decisões dos atores individuais podem ter efeitos de longo alcance [Siemon et al. 2020].

Esse tipo de operação entre sistemas distribuídos de agências distintas gera novos problemas que não existem em sistemas centralizados, o que leva ao conceito de *middleware*, que oferece serviços de forma a suportar execução de aplicações distribuídas [Puder et al. 2011]. O próprio termo "*middleware*" sugere que ele se posiciona entre duas (ou mais) aplicações. Dessa forma, pode-se estabelecer que a solução proposta no presente trabalho atuará como um *middleware*, interagindo diretamente com os sistemas distribuídos sem que estes comuniquem-se diretamente entre si.

Portanto este artigo apresenta uma plataforma em estágio de desenvolvimento que tem como objetivo geral a promoção de interoperabilidade entre sistemas de forças de segurança, sendo tal plataforma aplicada na prática no contexto do estado do Rio Grande do Norte (RN) no atendimento a ocorrências resultantes de crimes contra a vida. Assim, a plataforma buscará facilitar o compartilhamento de informações com interesses em comum entre os sistemas de informação dos órgãos parceiros e buscando fornecer um serviço de melhor qualidade para as investigações criminais e a elucidação de crimes, trazendo para a sociedade um ganho na área de segurança pública. Embora a plataforma esteja sendo primeiro aplicada ao RN, ela está sendo desenvolvida de modo a ser também usufruída em outros estados e contextos.

Os objetivos específicos deste trabalho são: (i) permitir que os órgãos da segurança pública tenham acesso fácil a dados referentes a ocorrências resultantes de crimes contra a vida de posse de outros sistemas; (ii) permitir que os sistemas de informação que compõem a plataforma possam receber alertas enviados pelos demais; (iii) armazenar histórico de mensagens entre os órgãos da segurança pública; (iv) validar informações em comum compartilhadas pelos órgãos parceiros; e (v) facilitar a inclusão futura de novos órgãos na plataforma desenvolvida.

O restante desse documento está organizado do seguinte modo: Na Seção 2 são apresentados alguns conceitos que devem ser conhecidos para o total entendimento do trabalho. Na Seção 3 é apresentado um resumo de alguns trabalhos que abordaram o mesmo tema. Em seguida, na Seção 4 é mostrado o projeto da arquitetura proposta. Na Seção 5 são apresentados os cenários de aplicação da solução proposta, assim como algumas das rotinas implementadas até o atual estágio de desenvolvimento. Por fim, na Seção 6 são mostradas as considerações finais do presente trabalho.

2. Fundamentação Teórica

Nessa Seção é apresentado o conceito de interoperabilidade (Subseção 2.1) e Informações sobre os órgãos de segurança do estado do Rio Grande do Norte, de modo a facilitar o entendimento do contexto em que esse trabalho está inserido.

2.1. Interoperabilidade

O conceito de interoperabilidade tem estado cada vez mais em evidência nos últimos anos, especialmente no que envolve a área de TIC. Nela, vemos a interoperabilidade como a habilidade que as aplicações detêm de colaborar, por meio de diferentes plataformas, de modo a disponibilizar suas funcionalidades ou criar outras [Di Martino et al. 2015].

No contexto da administração pública, [ENAP 2015] ressalta que a interoperabilidade trás como benefícios melhor prestação de serviço ao cidadão, melhor tomada de decisão pelos gestores, maior confiabilidade nas informações, melhor coordenação dos programas e serviços de governo, maior transparência nas ações de governo e racionalização dos investimentos em TIC, por meio do compartilhamento, reúso e intercâmbio de recursos tecnológicos.

O Glossário de Terminologias em Engenharia de Software do *Institute of Electrical and Electronics Engineers* (IEEE) define interoperabilidade como a habilidade de dois ou mais sistemas ou componentes de compartilhar informações e de usar as informações compartilhadas [IEEE 1990]. Neste conceito, temos o foco na compartilhamento dos dados, mas o conceito de interoperabilidade pode, ainda, ser mais abrangente. Para [Ragazzo et al. 2021], a interoperabilidade envolve o desenvolvimento de ferramentas de natureza técnica e regulatória para facilitar a interligação ou conexão entre sistemas (de forma mais ampla, entre instituições).

2.2. Órgãos da Segurança Pública

A segurança pública é administrada no Rio Grande do Norte pela Secretaria da Segurança Pública e da Defesa Social (SESED) que possui a ela diretamente vinculados a Polícia Militar, a Polícia Civil, o Corpo de Bombeiros Militar e o Instituto Técnico-Científico de Perícia do Rio Grande do Norte (ITEP), cada um com suas diferentes atribuições. No atendimento a ocorrências resultante de crimes contra a vida participam também as figuras do Centro Integrado de Operações de Segurança Pública (CIOSP) e da Divisão de Homicídios e Proteção à Pessoa (DHPP).

O CIOSP une as atuações dos órgãos da segurança pública e de outras áreas como a saúde, por meio dele os operadores policiais militares recebem a maior parte das denúncias sobre os crimes, realizam o registro das ocorrências por meio do sistema Central de Atendimento e Despacho do Rio Grande do Norte (CAD-RN) com todas as

informações pertinentes como relatos, localização, histórico, equipes que as atenderam, entre outras. A DHPP é a divisão da Polícia Civil especializada nas investigações de crimes de homicídio na região metropolitana de Natal. No local, a DHPP terá a sua disposição o Assistente de Cena de Crime (ACC), aplicativo móvel que visa auxiliar os policiais civis nas etapas iniciais da investigação, registrando o observado na cena do crime e gerando os documentos oficiais necessários aos procedimentos do órgão. Pelo ITEP, que no Rio Grande do Norte é órgão responsável por exercer as exames periciais de natureza criminal, é utilizado o Sistema Integrado de Gestão de Perícias (SIGEP) para o gerenciamento e controle de todos os exames periciais realizados pelo instituto, ao passo que está atualmente em fase de desenvolvimento um módulo adicional voltado especificamente para os exames em locais de crime contra a vida.

3. Trabalhos Relacionados

Foi realizada a busca na plataforma *Google Scholar* por alguns trabalhos que abordam a mesma temática e que foram desenvolvidos nos últimos anos. Dentre eles, o trabalho proposto por [Cinque et al. 2016] cita que *middlewares* são comumente utilizados para integração entre agências de segurança com informações heterogêneas, mas traz outras perspectivas a respeito da confiabilidade e da integralidade do sistema, com necessidade de requisitos como redundância e tolerância a falhas. Em [Elmhadhbi et al. 2020] é proposta uma solução para possibilitar o compartilhamento de informações de forma confiável e em tempo real entre os agentes de segurança e saúde pública, buscando a tradução dos símbolos e vocabulário que cada sistema está familiarizado. A solução proposta em [Cinque et al. 2017] tem o mesmo objetivo de compartilhar as informações entre agências de combate a desastres, sem a necessidade de um módulo central mas de nós distribuídos. Em [Rinjani et al. 2017], utiliza-se de um mediador que auxilia no compartilhamento de informações e disponibiliza telas para acompanhamento dos casos de modo que cada entidade recebe apenas as informações que lhe são úteis. [Pérez et al. 2017] propõem uma plataforma de interoperabilidade de dados entre agências que atuam no gerenciamento de incidentes e faz uso de uma infraestrutura central que armazena e gerencia todas as informações que é transmitida utilizando um mecanismo de *publish/subscribe*.

Outros trabalhos propõem sistemas com objetivos parecidos, mas com significativas diferenças em sua aplicação. Em [Xu et al. 2019] e [Xu et al. 2020], é utilizado *blockchain* para o compartilhamento de dados e segurança das informações enviadas; [Du et al. 2016] buscam o controle dos ativos relacionados ao atendimento de ocorrências em situações críticas; [Bojadjievski et al. 2018] focam nos aspectos da camada de transporte da solução e questões relacionadas à infraestrutura da rede; [Kapucu et al. 2018] utilizam dados estatísticos de diferentes agências de segurança pública para tomada de decisão, planejamento e governança; [Ivanc and Blažič 2016] focam na parte da segurança da informação e requisitos de segurança; [Mayer-Schönberger 2005] trata dos aspectos da troca de informações via canais de rádio; [Engelenburg et al. 2017] baseiam-se em serviços comerciais de fornecimento de mercadorias e como alguns aspectos podem ser utilizados para o sistema de segurança pública; [Alshawish et al. 2016] falam do potencial do uso de *BigData* para cidades inteligentes; [Kapucu and Haupt 2016] listam tecnologias usadas em segurança pública especificamente na comunicação via rádio; [Fraga-Lamas et al. 2016] apontam as dificuldades enfrentadas pelo setor de segurança pública para a utilização de tecnologias IoT (*Internet of Things*, ou Internet das Coisas);

[Kożuch and Sienkiewicz-Małyjurek 2016] trazem uma pesquisa sobre fatores decorrentes e causadores da coordenação entre unidades independentes da segurança pública; [Casey et al. 2019] propõem quais informações podem e devem ser compartilhadas entre os diferentes órgãos; [Kebande and Ray 2016] propõem um modelo de procedimento genérico para investigações por meios digitais utilizando IoT; por fim, [Casey et al. 2017] apresentam uma linguagem de dados específica baseada em JSON (*JavaScript Object Notation*) para a troca de informações de investigações criminais.

Dentre os trabalhos apresentados, pode-se identificar alguns pontos que distanciam do objetivo do presente trabalho, como o uso de tecnologias como *blockchain* ou *BigData* e de soluções descentralizadas, o foco em aspectos distintos como estatística e governança, a aplicação em realidades diferentes da segurança pública no Brasil ou escopos mais específicos como a definição das informações a serem compartilhadas. Com essas diferenças faz-se necessária a criação de uma nova solução, adequada à realidade dos órgãos que atuam no sistema de segurança pública local.

4. Arquitetura Proposta

Nesta Seção são apresentados detalhes sobre o desenvolvimento da plataforma de *middleware* proposta nesse trabalho, de modo a promover a interoperabilidade entre os diferentes sistemas de informação dos órgãos da segurança pública.

Para isso, foram inicialmente identificados os requisitos da solução. Conforme [Rodrigues 2008], os requisitos de um sistema são utilizados como base para o projeto, pois são eles que justificam o *software*, e que é na fase de análise de requisitos que as funcionalidades do sistema são definidas. De forma complementar, [Fernandes and Machado 2017] expõem que, no contexto de desenvolvimento de sistemas, os requisitos são as propriedades que os sistemas devem manifestar quando estiverem desenvolvidos e expressam as necessidades dos usuários e as restrições que são apresentadas a um sistema, devendo ser consideradas durante o projeto. Dessa forma, foi feito o levantamento dos seguintes requisitos da aplicação proposta: 1. Cada sistema distribuído deverá ter um componente dedicado (um *proxy*) responsável pelo encaminhamento das mensagens com o *middleware*, de forma a criar uma plataforma com diversos sistemas heterogêneos mas de baixo acoplamento; 2. Novos sistemas externos poderão ser adicionados à plataforma, por meio de um novo componente dedicado (*proxy*), sem prejudicar o funcionamento dos demais existentes e em execução; 3. O *middleware* deverá possuir módulos para comunicação síncrona e assíncrona para se adaptar à heterogeneidade dos sistemas que farão parte da plataforma; 4. O *middleware* deverá receber requisições e respostas de qualquer sistema externo e encaminhá-las ao sistema de destino; 5. O *middleware* deverá receber alertas de qualquer sistema externo e encaminhá-los aos sistemas interessados. 6. O *middleware* deverá possuir um módulo dedicado ao monitoramento dos sistemas a ele integrados, verificando se algum deles encontra-se indisponível; 7. O *middleware* deverá possuir um módulo de gerenciamento de *logs*; 8. A aplicação deverá ser capaz de analisar as informações que trafegam por ela e validar se os dados apresentam consistência a concordância.

Uma vez definidos os requisitos, é hora de definir como a aplicação estará estruturada de forma a atendê-los. Na Figura 1 é mostrada esta estrutura, nela, o painel na cor cinza engloba os componentes desenvolvidos no escopo do presente trabalho, como o

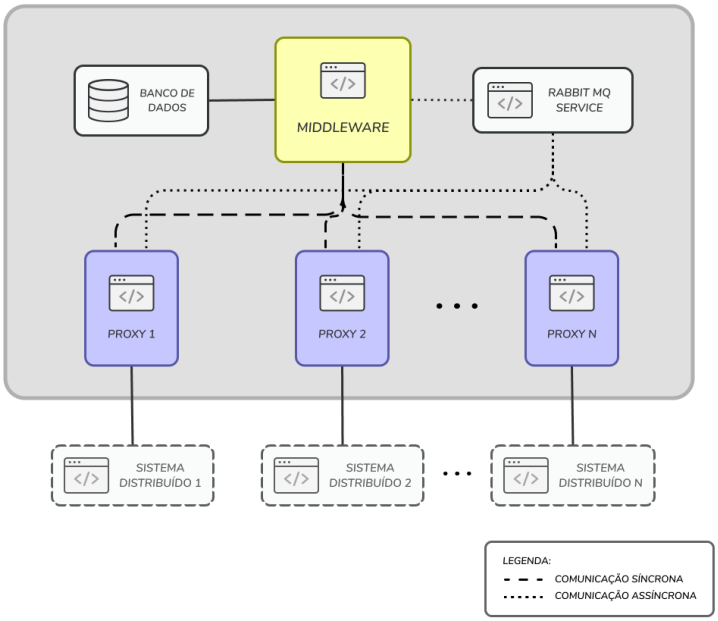

Figura 1. Visão geral da arquitetura proposta

middleware, que é o componente central de toda a aplicação, representado pelo bloco na cor amarela, os *proxies*, que são os componentes dedicados de comunicação com os sistemas externos, representados pelos blocos de cor azul, além do servidor de banco de dados e do serviço que funciona como uma central de mensageria, por meio do mecanismo *RabbitMQ*. As linhas tracejadas na Figura 1 representam a comunicação síncrona entre o *middleware* e os *proxies*, ao passo que as linhas pontilhadas representam a comunicação assíncrona, gerenciada pelo serviço *RabbitMQ*.

Na Figura 2 é exibida a arquitetura interna de um *proxy*, representado pela cor azul. Ele é composto pelos componentes *HTTP Server* e *HTTP Client*, para recebimento e envio de requisições via HTTP, *RabbitMQ Consumer* e *RabbitMQ Producer*, responsáveis por receber e enviar requisições via *RabbitMQ* (e que se conectam ao *middleware*por meio do serviço mensageria dedicado a comunicações via *RabbitMQ*) e um módulo *API Matcher* que atua como o padrão de projeto *Facade*, ou seja, uma interface disponibilizada ao sistema distribuído ao qual ele é dedicado e que não necessitará conhecer detalhes do funcionamento do *proxy* nem tampouco do *middleware*, ele apenas necessita reconhecer a fachada a ele disponibilizada.

A arquitetura proposta para o *middleware* está representada conforme exposto na Figura 3, com seus componentes internos dentro do painel representado na cor amarela. Ele possui os componentes *HTTP Server*, *HTTP Client*, *RabbitMQ Consumer* e *RabbitMQ Producer*, que atuarão, a exemplo dos *proxies*, de forma a receber e enviar mensagens via HTTP ou *RabbitMQ*. O *Message Processor* é o componente do *middleware* responsável por receber as mensagens enviadas pelos *proxies*, encaminhando-as aos módulos adequados para tratá-las, e vice-versa.

Os módulos integrantes do *middleware* possuem funções específicas: o *Manager* tem a função de processá-las as mensagens recebidas, entender de que se trata a informação dada por cada uma delas e tomar a decisão a seu respeito; o *Monitor* deverá

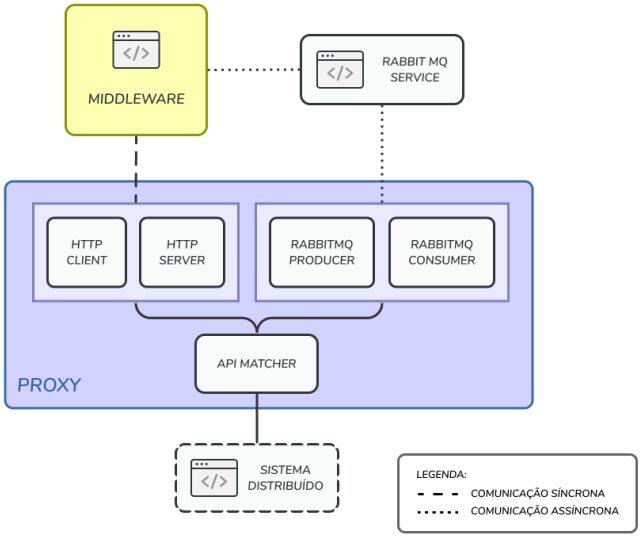

Figura 2. Visão interna dos *proxies*

atuar de forma a monitorar se cada *proxy* e sistema externo continuam ativos, detectando se algum deles ficar indisponível e tomar as medidas adequadas a cada caso; o *Logger* é o módulo utilizado para registro do histórico de requisições, respostas e tramitação de mensagens em geral; já o módulo *Validator* é aquele responsável por analisar os dados trafegados pelo *middleware*, verificando a confiabilidade e coerência das informações enviadas pelos diversos sistemas a ele conectados. Por fim, o *DAO* é um componente, definido como um padrão de projeto, que tratará das operações de escrita e leitura no banco de dados, podendo se acionado por qualquer um dos módulos.

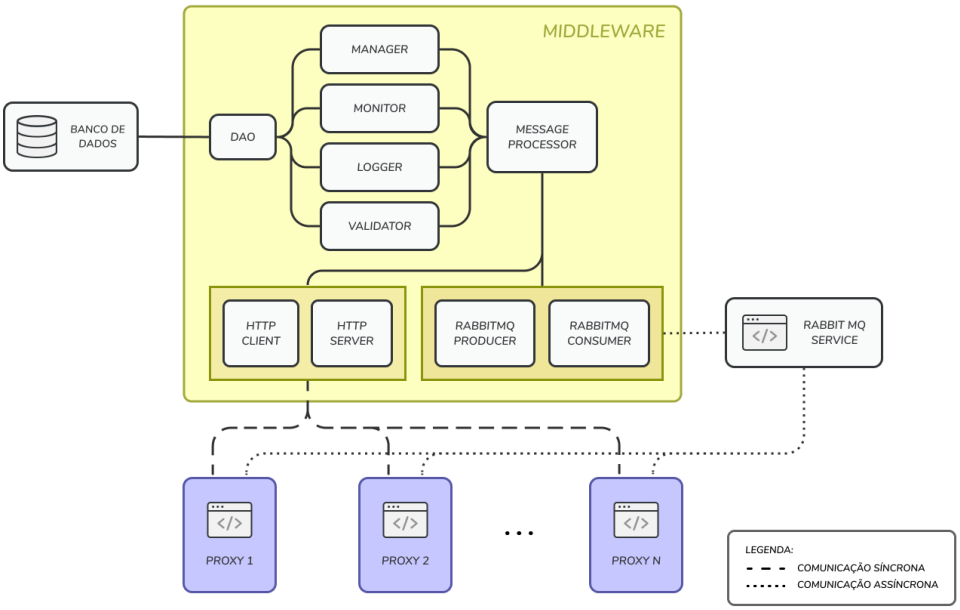

Figura 3. Visão interna do *middleware*

5. Estudo de Caso

A aplicação proposta neste trabalho deverá atuar de forma conjunta com os sistemas de informação dos órgãos atuantes nos atendimentos a ocorrências resultantes de crimes contra a vida, com o foco, em primeiro momento, na interoperabilidade de três sistemas distintos, o SIGEP (do ITEP), o CAD-RN (usado no CIOSP) e o ACC (da DHPP).

Um dia simples da rotina dos órgãos citados começa no início do plantão dos servidores. Os servidores do ITEP se registrarão por meio do SIGEP, em seguida os operadores do CIOSP buscarão, via CAD-RN, as informações das equipes de plantão. A requisição transitará por meio da plataforma em desenvolvimento, na qual o *middleware* receberá a requisição do CAD-RN, a enviará ao SIGEP, aguardará a resposta, a enviará de volta ao CAD-RN. O cadastramento das equipes da DHPP poderá seguir o mesmo fluxo, a depender dos procedimentos adotados. Após o cadastramento das equipes, estas ficam de prontidão aguardando um novo chamado.

Quando surgir uma nova ocorrência resultante de crime contra a vida, ela será cadastrada no CAD-RN pelos operadores do CIOSP, que também abrirão um chamado a ser comunicado às equipes do ITEP e da DHPP. O chamado será enviado pelo CAD-RN para o *middleware* que transmitirá o alerta para o SIGEP e o ACC, previamente cadastrados como interessados. Os usuários destes dois sistemas poderão solicitar mais informações sobre a ocorrência, enviando uma requisição para a plataforma que a encaminhará ao CAD-RN e devolverá a resposta recebida. Quando as equipes iniciarem o deslocamento ao local da ocorrência, o CIOSP tabém deve ser comunicado.

Após a chegada das equipes do ITEP e da DHPP ao local, estas poderão trocar informações sobre a cena de crime, fazendo a requisição por meio dos seus sistemas próprios, que transitará pela plataforma, até chegar ao sistema de destino e devolver a resposta. O *middleware* também fará a verificação dos dados que trafegam pela plataforma de forma que, caso seja detectado um conflito entre as informações analisadas com outras já obtidas anteriormente, o *middleware* enviará alerta para os sistemas envolvidos.

Durante todo o tempo de operação da plataforma é feito o monitoramento dos sistemas a ela conectados. A cada período de tempo a ser determinado o *middleware* enviará aos sistemas CAD-RN, SIGEP e ACC uma requisição de monitoramento. Ao receber a requisição, cada sistema responderá mostrando que encontra-se disponível. Caso alguma das requisições resultem em *timeout*, o *middleware* considerará que o sistema encontra-se indisponível. Durante a execução dos cenários descritos, também será registrado em *log* e na base de dados as informações que forem consideradas importantes. Por fim, ao concluir o plantão e uma nova equipe chegar para o plantão seguinte, todo o procedimento é reiniciado.

Todos os cenários descritos encontram-se em fase de desenvolvimento. Dentre eles, será mostrada com mais detalhes a implementação dos procedimentos seguidos quando é registrada uma nova ocorrência resultante de um crime contra a vida pelo CIOSP, conforme diagrama da Figura 4.

O primeiro passo a ser tomado é o envio de alertas do CAD-RN para todos os interessados na informação comunicando o surgimento de uma nova ocorrência a ser atendida. Na Figura 5 é mostrado, por meio do diagrama de sequência, o fluxo de tramitação da informação de nova ocorrência.

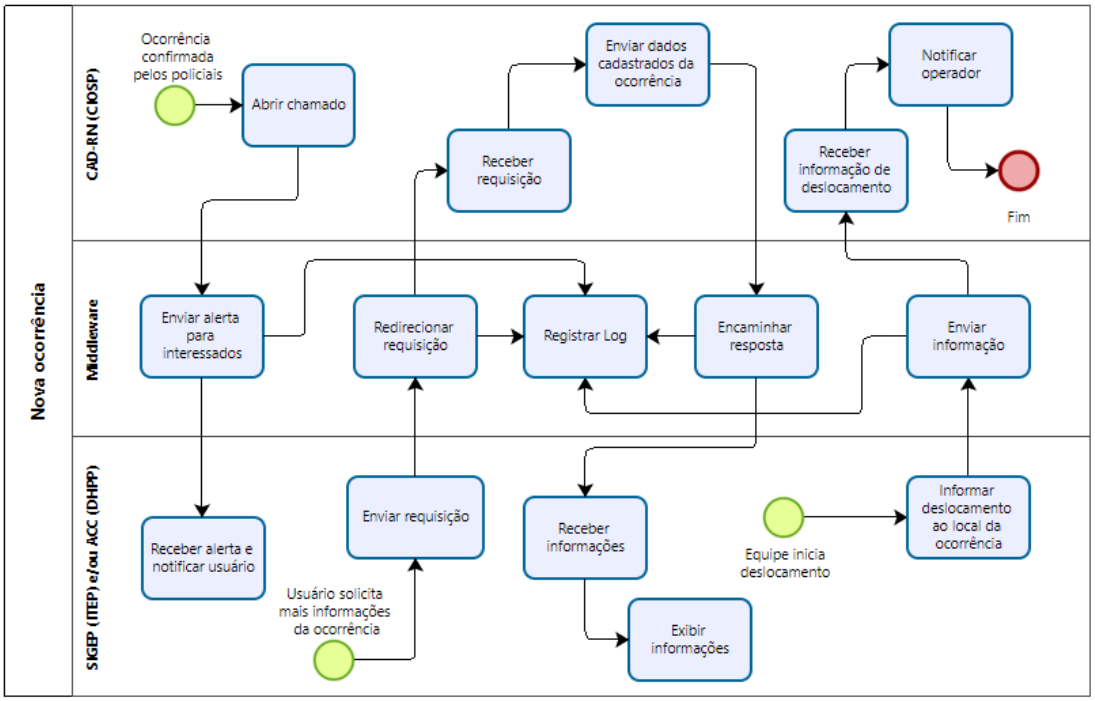

Figura 4. Cenário para atendimento a uma ocorrência

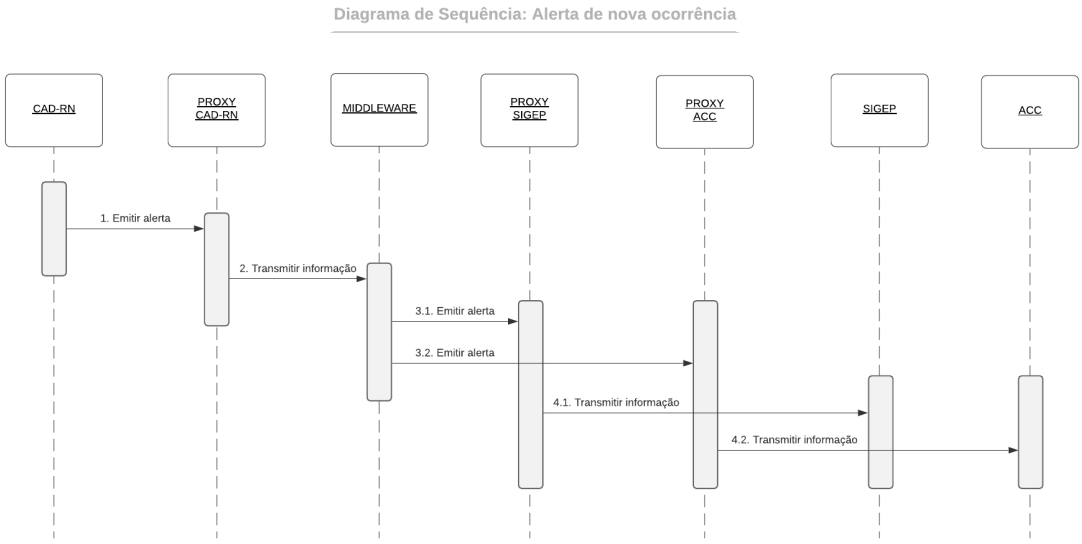

Figura 5. Diagrama de sequência para a emissão de alerta de nova ocorrência registrada

O fluxo se inicia no sistema CAD-RN, que emite o alerta via *RabbitMQ*, enviando como parâmetro o identificador da ocorrência para que ela possa ser referenciada futuramente. O alerta é recebido pelo *proxy* do CAD-RN, que o transmite novamente por um canal de comunicação diferente. O *middleware*, previamente inscrito para receber essa

informação proveniente do CAD-RN, o reconhece e emite um novo alerta repassando o identificador informado (Figura 6). Neste momento, receberão o alerta todos que tiverem previamente demonstrado interesse, que é o caso na aplicação atual, do SIGEP e do ACC. Como SIGEP é um dos interessados em ser informado quando houver uma nova ocorrência, ele receberá o alerta proveniente do *middleware*, por meio do seu *proxy* correspondente, isto é, o *proxy* do receberá o alerta e o transmitirá para o SIGEP (Figura 7) pelo canal de comunicação estabelecido entre eles, o SIGEP então receberá a informação com o identificador da ocorrência dado pelo CAD-RN no início do fluxo de tramitação da mensagem. O mesmo ocorre com o ACC, sendo ele um dos interessados no alerta de novas ocorrências. Não há necessidade de resposta à mensagem recebida, visto não se tratar de uma requisição, e sim de uma notificação.

```
node index.js
[MIDDLEWARE] Iniciando Middleware ...
[MIDDLEWARE] HTTP Server escutando na porta 3000.
[MIDDLEWARE] Conectado ao serviço RabbitMQ.
[MIDDLEWARE] Recebido alerta do CAD-RN que informa sobre nova ocorrência.
[MIDDLEWARE] Emitindo alerta aos interessados.
```

Figura 6. Execução do Middleware durante rotina de emissão de alerta sobre nova ocorrência

```
node index.js
[SIGEP PROXY] Iniciando proxy ...
[SIGEP PROXY] HTTP Server escutando na porta 3002.
[SIGEP PROXY] Conectado ao serviço RabbitMQ.
[SIGEP PROXY] Middleware enviou alerta de nova ocorrência.
[SIGEP PROXY] Transmitindo informação para o SIGEP.
```

Figura 7. Execução do Proxy SIGEP durante rotina de emissão de alerta sobre nova ocorrência

SIGEP e ACC são avisados sempre que é registrada uma nova ocorrência de crime contra a vida, no entanto o único dado obtido é o identificador da ocorrência. Para poder proceder ao seu atendimento, é preciso obter mais informações, como de que se trata a ocorrência, a localização para deslocamento e possíveis relatos que estimularam a criação do chamado. Portanto eles podem enviar requisições ao CAD-RN e obter mais dados sobre a ocorrência da qual foram notificados. O fluxo de mensagens par essa funcionalidade está representado na Figura 8.

O procedimento é feito por meio de requisições via HTTP, de forma que o SIGEP (ou ACC) envia a requisição com o identificador da ocorrência obtido previamente (na Figura 9 é mostrada a simulação do SIGEP no procedimento descrito), o *proxy* recebe a requisição e a encaminha para o o *middleware*, este redireciona a requisição para o CAD-RN por meio do *proxy* a ele dedicado. O CAD-RN enviará a resposta (na Figura 10 é vista a simulação e execução do sistema CAD-RN) que fará todo o caminho inverso até ser recebido pelo requisitante, neste exemplo o SIGEP (Figura 9).

A comunicação de deslocamento das equipes funciona de forma semelhante ao envio de alertas de novas ocorrências.

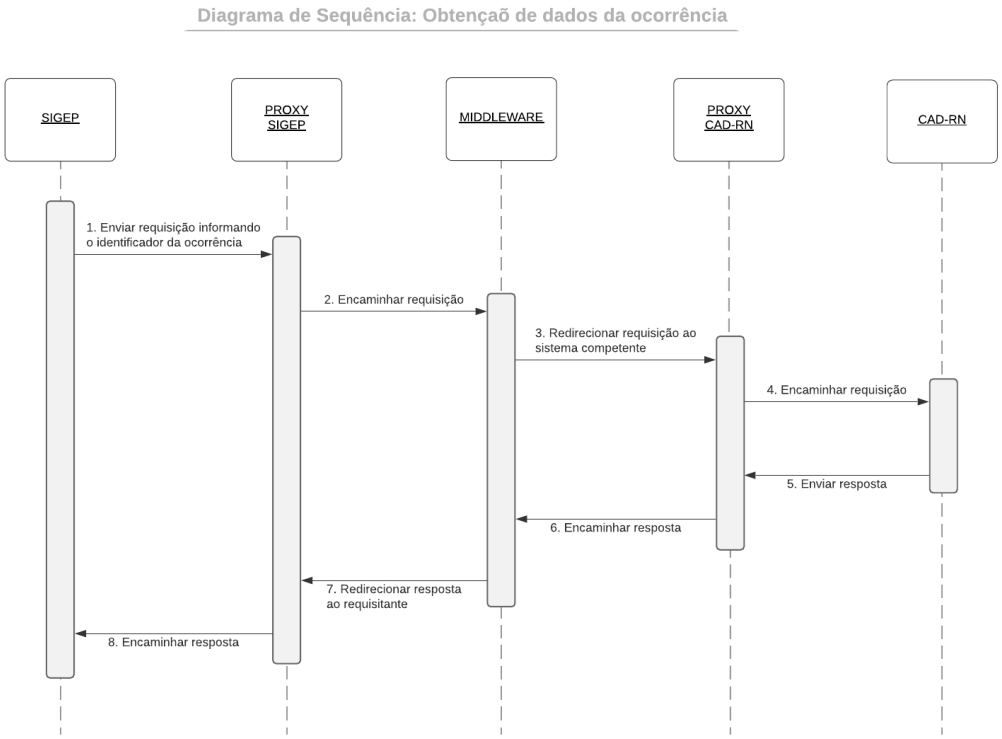

Figura 8. Diagrama de sequência para obtenção de dados cadastrados da ocorrência

```
node index.js dados-ocorrencia
[SIGEP] Iniciando simulador ...
[SIGEP] HTTP Server escutando na porta 3003.
[SIGEP] Enviando requisição de informações sobre a ocorrência de id '19fa9130d1'...
[SIGEP] Conectado ao serviço RabbitMQ.
[SIGEP] Resposta recebida:
{
  descricao: 'Possível homicídio por arma de fogo',
  local: {
    rua: 'Av. Duque de Caxias',
    numero: '97',
    cep: '59010-200',
    bairro: 'Ribeira',
    complemento: '',
    cidade: 'Natal',
    latitude: '-5.776712',
    longitude: '-35.204382'
  },
  dataHoraPrevista: '04:15 13/04/2021',
  relatos: [
    'Testemunha trafegava pelo local quando avistou o corpo caído no chão e acionou o 190.',
    'Segunda testemunha informou que ouviu dois tiros de arma de fogo por volta das 04:15 na regiã
o.'
  ]
}
```

Figura 9. Simulação de execução do SIGEP durante rotina de obtenção dos dados da ocorrência

6. Conclusão

O objetivo geral do trabalho proposto, conforme já exposto anteriormente, é a criação de uma plataforma para interoperabilidade dos órgãos de segurança pública. Para alcançar esse objetivo foram seguidas algumas etapas para o desenvolvimento da solução.

```
node index.js
[CAD-RN] Iniciando simulador ...
[CAD-RN] HTTP Server escutando na porta 3004.
[CAD-RN] Conectado ao serviço RabbitMQ.
[CAD-RN] Recebida requisição de dados da ocorrência de id '19fa9130d1'.
[CAD-RN] Enviando resposta:
{
  descricao: 'Possível homicídio por arma de fogo',
  local: {
    rua: 'Av. Duque de Caxias',
    numero: '97',
    cep: '59010-200',
    bairro: 'Ribeira',
    complemento: '',
    cidade: 'Natal',
    latitude: '-5.776712',
    longitude: '-35.204382'
  },
  dataHoraPrevista: '04:15 13/04/2021',
  relatos: [
    'Testemunha trafegava pelo local quando avistou o corpo caído no chão e acionou o 190.',
    'Segunda testemunha informou que ouviu dois tiros de arma de fogo por volta das 04:15 na região
.'
  ]
}
```

Figura 10. Simulação de execução do CAD-RN durante rotina de obtenção dos dados da ocorrência

Inicialmente, foi dada uma breve contextualização do escopo do projeto proposto, mostrando os problemas que motivaram a concepção do presente trabalho e os objetivos pretendidos. Em seguida, foi demonstrado como como funcionam os órgãos de segurança pública envolvidos na aplicação da plataforma proposta. Na sequência, foi apresentado os principais aspectos dos trabalhos relacionados ao tema abordado no presente trabalho.

Foi mostrado também projeto da arquitetura proposta, os requisitos estabelecidos para a aplicação a ser desenvolvida, os componentes que compõem a solução e o estudo de caso, isto é, como a solução proposta pode ser aplicada aos procedimentos normais de um dia de operações de CIOSP, ITEP e DHPP no atendimento a ocorrências resultantes de crimes contra a vida, além de mostrar também algumas das funcionalidades já implementadas até o momento.

A solução proposta está atualmente em fase de desenvolvimento e espera-se que, em breve, ela seja avaliada por membros das instituições envolvidas e, na sequência, utilizada na prática.

Referências

Alshawish, R. A., Alfagih, S. A., and Musbah, M. S. (2016). Big data applications in smart cities. In *2016 International Conference on Engineering & MIS (ICEMIS)*, pages 1–7. IEEE.

Bojadjievski, S., AnastasovaBojadjievska, N., Kalendar, M., and Tentov, A. (2018). Interoperability of emergency and mission critical iot data services. In *2018 26th Telecommunications Forum (TELFOR)*, pages 1–4. IEEE.

Cardoso, L., Marins, F., Quintas, C., Portela, F., Santos, M., Abelha, A., and Machado, J. (2018). Interoperability in healthcare. In *Health Care Delivery and Clinical Science: Concepts, Methodologies, Tools, and Applications*, pages 689–714. IGI Global.

Casey, E., Barnum, S., Griffith, R., Snyder, J., van Beek, H., and Nelson, A. (2017). Advancing coordinated cyber-investigations and tool interoperability using a community developed specification language. *Digital investigation*, 22:14–45.

Casey, E., Ribaux, O., and Roux, C. (2019). The kodak syndrome: risks and opportunities created by decentralization of forensic capabilities. *Journal of forensic sciences*, 64(1):127–136.

Cinque, M., Cotroneo, D., Esposito, C., and Fiorentino, M. (2017). Secure crisis information sharing through an interoperability framework among first responders: The sector practical experience. In *2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 316–323. IEEE.

Cinque, M., Cotroneo, D., and Fiorentino, M. (2016). Facing reliability requirements for timely information sharing in future crisis management systems. In *Fast Abstract in the 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*.

Di Martino, B., Cretella, G., and Esposito, A. (2015). *Cloud Portability and Interoperability: Issues and Current Trends*. SpringerBriefs in Computer Science. Springer International Publishing.

Du, P., Chen, J., and Sun, Z. (2016). Resource management system for crisis response & management. In *ISCRAM*.

Elmhadhbi, L., Karray, M.-H., Archimède, B., Otte, J. N., and Smith, B. (2020). A semantics-based common operational command system for multiagency disaster response. *IEEE Transactions on Engineering Management*.

ENAP (2015). Introdução à interoperabilidade: Módulo 1.

Engelenburg, S. v., Janssen, M., and Klievink, B. (2017). Design of a software architecture supporting business-to-government information sharing to improve public safety and security. *Journal of Intelligent information systems*, 52(3):595–618.

Fernandes, J. and Machado, R. (2017). *Requisitos em projetos de software e de sistemas de informação*. Novatec Editora.

Fraga-Lamas, P., Fernández-Caramés, T. M., Suárez-Albela, M., Castedo, L., and González-López, M. (2016). A review on internet of things for defense and public safety. *Sensors*, 16(10):1644.

IEEE (1990). Ieee standard glossary of software engineering terminology.

Ivanc, B. and Blažič, B. J. (2016). Information security aspects of the public safety data interoperability network. In *2016 European Intelligence and Security Informatics Conference (EISIC)*, pages 88–91. IEEE.

Kapucu, N. and Haupt, B. (2016). Information communication technology use for public safety in the united states. *Frontiers in communication*, 1:8.

Kapucu, N., Haupt, B., and Yuksel, M. (2018). Spectrum sharing policy: Interoperable communication and information sharing for public safety. *Risk, Hazards & Crisis in Public Policy*, 9(1):39–59.

Kebande, V. R. and Ray, I. (2016). A generic digital forensic investigation framework for internet of things (iot). In *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, pages 356–362. IEEE.

Kożuch, B. and Sienkiewicz-Małyjurek, K. (2016). Inter-organisational coordination for sustainable local governance: Public safety management in poland. *Sustainability*, 8(2):123.

Liao, Y., Ramos, L. F. P., Saturno, M., Deschamps, F., Loures, E. d. F. R., and Szejka, A. L. (2017). The role of interoperability in the fourth industrial revolution era. *IFAC-PapersOnLine*, 50(1):12434–12439.

Mayer-Schönberger, V. (2005). The politics of public safety communication interoperability regulation. *Telecommunications Policy*, 29(11):831–842.

Pérez, F. J., Zambrano, M., Esteve, M., and Palau, C. (2017). A solution for interoperability in crisis management. *International Journal of Computers Communications & Control*, 12(4):550–561.

Puder, A., Römer, K., and Pilhofer, F. (2011). *Distributed Systems Architecture: A Middleware Approach*. The MK/OMG Press. Elsevier Science.

Ragazzo, C., Aguiar, J., Paixão, R., de Morais, A., Almeida, D., Badra, D., Cotosky, E., Estevam, G., Sousa, G., Mazarello, G., et al. (2021). *O Regulador Inovador: Banco Central e a agenda de incentivo à inovação*. Instituto Propague.

Rinjani, M. A., Adji, T. B., Permanasari, A. E., and Dzikrullah, F. (2017). Data service orchestration for law enforcement and open criminal justice data interoperability (national crime information center, indonesian national police case studies). In *2017 3rd International Conference on Science and Technology-Computer (ICST)*, pages 16–21. IEEE.

Rodrigues, E. (2008). *Curso de Engenharia de Software*. Universo dos Livros Editora.

Siemon, C., Rueckel, D., and Krumay, B. (2020). Blockchain technology for emergency response. In *Proceedings of the 53rd Hawaii International Conference on System Sciences*.

Xu, R., Nikouei, S. Y., Chen, Y., Blasch, E., and Aved, A. (2019). Blendmas: A blockchain-enabled decentralized microservices architecture for smart public safety. In *2019 IEEE International Conference on Blockchain (Blockchain)*, pages 564–571. IEEE.

Xu, R., Nikouei, S. Y., Nagothu, D., Fitwi, A., and Chen, Y. (2020). Blendsps: A blockchain-enabled decentralized smart public safety system. *Smart Cities*, 3(3):928–951.

Zacharewicz, G., Daclin, N., Doumeingts, G., and Haidar, H. (2020). Model driven interoperability for system engineering. *Modelling*, 1(2):94–121.

Zambrano-Vizuete, O. M., Pérez-Carrasco, F. J., Esteve Domingo, M., and Palau Salvador, C. E. (2018). Interoperability in emergency management. a solution based on distributed databases and p2p networks. *Computer Science and Information Systems*, 15(2):257–272.