

FUNDAÇÃO UNIVERSIDADE DO TOCANTINS
CURSO DE SISTEMAS DE INFORMAÇÃO

Brunno Sales Cunha

**Desenvolvimento de aplicações móveis para o apoio às atividades
dos agentes de segurança pública.**

Palmas/TO
2016

FUNDAÇÃO UNIVERSIDADE DO TOCANTINS
CURSO DE SISTEMAS DE INFORMAÇÃO

Brunno Sales Cunha

**Desenvolvimento de aplicações móveis para o apoio às atividades
dos agentes de segurança pública.**

Trabalho de Conclusão de Curso de Sistemas de Informação da Fundação Universidade do Tocantins, apresentado como parte dos requisitos para obtenção do título de Bacharel em Sistemas de Informação.

Orientador: Msc. Alex Coelho.

Palmas-TO, maio de 2016

DEDICATÓRIA

Primeiro a Deus por todos os ensinamentos e bênçãos alcançadas e por poder estar onde estou hoje. A toda minha família em especial minha esposa, que sempre me apoiou e sempre se empenhou a jamais me deixar desistir e sempre buscar o meu melhor.

AGRADECIMENTOS

Agradeço em primeiro lugar a Deus por toda força, graça e esperança que me foram dadas para atingir meus objetivos.

A minha esposa e minha mãe que sempre viram a necessidade da conclusão deste processo acadêmico e me incentivaram para obter os resultados esperados.

Aos meus filhos que mesmo não entendendo ainda o que tudo isto representa, serviram para alimentar minhas forças mesmo com o todo o cansaço e falta de tempo para me dedicar as atividades acadêmicas.

Ao Coronel QOPM Felizardo Ramos dos Santos da Polícia Militar do Tocantins por todo apoio que me deu e por entender que a minha capacitação e especialização será útil na corporação no combate a criminalidade.

Aos meus colegas Thales e Taivan por contribuírem na busca de melhorias no resultado deste trabalho.

“Ser o homem mais rico do cemitério não importa para mim... Ir para a cama à noite dizendo que fizemos algo maravilhoso... Isso é o que importa para mim”

Steve Jobs

SUMÁRIO

1 INTRODUÇÃO	6
2.1 SISTEMAS OPERACIONAIS PARA DISPOSITIVOS MÓVEIS	11
2.1.1 ANDROID	12
3 METODOLOGIA	24
4 DESENVOLVIMENTO	30
4.1 SISTEMA OPERACIONAL.....	30
4.2 SEGURANÇA DA INFORMAÇÃO	33
4.2.1 AUTENTICAÇÃO	33
4.2.2 CRIPTOGRAFIA.....	35
4.3 SERVIDOR WEBSERVICE	35
4.4 MODELAGEM DA SOLUÇÃO.....	37
4.4.1 MODELO CONCEITUAL.....	38
4.4.2 MODELAGEM DE TELAS	38
4.4.3 MODELAGEM DE CLASSES.....	40
.....	41
4.4.4 MODELAGEM DE BANCO DE DADOS	43
4.5 INSTALAÇÃO DO CERTIFICADO DIGITAL AUTO-ASSINADO NO SERVIDOR	45
4.6 COMPROVANDO A EFICÁCIA DO CERTIFICADO DIGITAL	Erro! Indicador não definido.
4.7 O PROBLEMAS ENCONTRADOS.....	47
5 DIFÍCULDADES	48
6 RESULTADOS	49
5. SUGESTÕES PARA TRABALHOS FUTUROS	50
6. CONCLUSÃO.....	50
REFERÊNCIAS	52

1 INTRODUÇÃO

É comum que na estrutura de governo dos estados brasileiros exista uma autarquia pública que integre as forças de segurança estaduais e municipais. No estado do Tocantins esta autarquia chama-se SIOP (Sistema Integrado de Operações), é subordinada diretamente pela Secretaria de Segurança Pública do estado e é constituída pelos seguintes entes públicos mediante convênio: Polícia Militar do Estado do Tocantins, Polícia Civil, Polícia Técnica Científica, Corpo de Bombeiros Militar, Guarda Metropolitana Municipal, Secretaria de Acessibilidade Trânsito e Transporte Municipal e Detran.

As principais atividades do SIOP são: atender as chamadas de emergências da população pelos canais telefônicos 190, 193 e 153, despachar recursos operacionais para o atendimento dos chamados e apoiar os agentes de segurança pública no empenho de suas tarefas em campo.

A segurança pública busca diuturnamente oferecer tranquilidade e paz social aos cidadãos. A produção de dados estatísticos neste cenário deve ser rápida e confiável pois a tendência criminal de agora pode não refletir a mesma de horas atrás.

A implantação de tecnologia em órgãos que culturalmente possuem regras de administração rígidas precisa ser tratada para oferecer o mínimo de desgaste cultural àquela corporação.

1.1. PROBLEMA

A falta de informações em tempo hábil prejudica a qualidade do serviço na segurança pública, incentivando a prática de crimes e colocando em risco os agentes de segurança que, por não deterem de informações apropriadas podem subestimar o nível de alerta necessário para execução de suas ações.

Em uma estrutura governamental a falha no planejamento da previsão orçamentaria do ano pode prejudicar a implantação de qualquer tipo de projeto. Portanto, na condição do estado não adquirir aparelhos smartphones para o uso de

aplicativos móveis: será que os agentes de segurança pública utilizariam de aparelhos smartphones e plano de dados particulares para o uso de uma ferramenta de aplicação estritamente profissional?

A qualidade da internet 3G pode comprometer a busca de informações em rotinas vinculadas a aplicações móveis?

A resposta destas perguntas, a busca do desenvolvimento de uma aplicação relevante para a segurança pública, as pesquisas científicas que colaboram com objetivo lançado, a arquitetura e os pontos de interesses que levam a conclusão deste tema serão expostos neste trabalho acadêmico.

1.2. OBJETIVO

Este trabalho tem como objetivo principal implantar uma solução que apoie os agentes de segurança pública nas execuções das rotinas operacionais utilizando dispositivos móveis.

1.2.1. OBJETIVOS ESPECÍFICOS

- Realizar um estudo sobre o uso de aplicações móveis em autarquias públicas de governo.
- Pesquisar sobre a lei que regula a contratação de empresas para a aquisição de produtos.
- Estudar sobre as principais plataformas móveis do mercado e compará-las.
- Definir qual a melhor tecnologia de webservice para comunicação entre aparelhos móveis e servidores.
- Identificar uma necessidade comum e relevante entre os agentes de segurança pública.
- Planejar e Codificar a necessidade levantada;
- Realizar comparativo entre o antes e o depois da implantação do aplicativo.

1.3. ORGANIZAÇÃO DO DOCUMENTO

O trabalho está estruturado da seguinte forma:

- Capítulo 1 – Introdução;
- Capítulo 2 – Revisão de Literatura;
- Capítulo 3 – Metodologia;
- Capítulo 4 – Desenvolvimento;
- Capítulo 5 – Conclusões;
- Capítulo 6 – Referências.

A Revisão Literária está segmentada em quatro partes: O uso de tecnologias em processos governamentais, Sistemas operacionais para dispositivos móveis, Licitações e Princípio da economicidade, Segurança da Informação e WebService

O capítulo 3 aborda a metodologia usada, as tecnologias envolvidas na busca dos resultados e a definição da aplicação que será desenvolvida para subsidiar estes estudos.

O desenvolvimento apresenta as etapas mais importantes para se obter os resultados do estudo proposto.

Capítulo 5, demonstra a finalização do trabalho e as sugestões de outros estudos no mesmo segmento aqui apresentado.

O capítulo referências discrimina as obras utilizadas para fomentar este trabalho sem as quais não haveria embasamento teórico na qualidade que o autor almeja.

2 REVISÃO DE LITERATURA

Esta etapa atinge conceitos importantes sobre assuntos que sustentam a base para o desenvolvimento deste estudo.

2.1 O USO DE TECNOLOGIA EM PROCESSOS GOVERNAMENTAIS

As estruturas governamentais buscam mais eficiência para cumprir suas burocracias estatais que, segundo Abrucio (1997), tais burocracias têm como particularidade um tamanho muito grande correspondente ao enorme volume de atribuições herdadas pelo modelo do bem-estar social e a severidade na gestão trazida

pelo modelo burocrático weberiano. Abrucio cita Les Metcalfe & Sue Richards e complementa:

“[...] o setor público não está numa situação em que as velhas verdades possam ser reafirmadas. É uma situação que requer o desenvolvimento de novos princípios. A administração pública deve enfrentar o desafio da inovação mais do que confiar na imitação. A melhora da gerência pública não só é uma questão de pôr-se em dia com o que está ocorrendo na iniciativa privada: significa também abrir novos caminhos. (LES METCALFE e SUE RICHARDS apud ABRUCIO, 1997, p. 6).”

Na busca da melhoria e inovação dos processos governamentais e o avanço paralelo da tecnologia, surge o termo “Governo Eletrônico” que Ruediger (2002) define como o uso de novas tecnologias de informação e comunicação aplicadas nas funções de governo e em especial nas relações do governo com a sociedade. Ruediger, afirma que na teoria o “Governo Eletrônico” além de dinâmico promove mais eficiência, transparência e desenvolvimento sendo naturalmente encarado como ferramenta de gestão pública.

Portanto, é importante observar que por se tratar de gestão pública haverá interesses políticos atrelados às ações de governança eletrônica. Como descrito por Kettl em seus estudos referentes às relações públicas e políticas:

“Public management is inevitably about politics. Thus management reform is also about political reform.” [Kettl: 2000, p.68]

Martins (2004) classifica os principais tipos de relações que se encontram na estrutura do Governo Eletrônico. O primeiro tipo existente de relação é entre o governo e as empresas, onde permite ao Estado realizar compras diretas, licitações e empenhos como também administrar a comercialização de produtos e serviços, para este tipo de relação dar-se o nome de G2B (Governo para Empresas). O segundo tipo de relação é entre o governo e o cidadão, que figura como cliente, sendo consumidor dos seus serviços, inclusive na transparência e colabora no aumento da participação da sociedade nas contas públicas e nas políticas de estado, este modelo Martins define como G2C (Governo para Clientes). A terceira e última relação é a intragovernamental, onde a tecnologia é utilizada para aumentar a eficácia e a eficiência nas atividades governamentais proporcionando o aumento na arrecadação, a melhoria na prestação

de serviços e elevando a qualidade de vida dos agentes de governo. Para esta relação Martins define o G2G (Governo para Governo).

2.1.1 O USO DE TECNOLOGIA MÓVEIS EM PROCESSOS GOVERNAMENTAIS

O notável uso de tecnologias para reduzir gastos e para garantir a celeridade nos processos empresariais estimulam o poder público para a adoção de informatização nas autarquias de governo. Allazo, Sablón e Iano (2009), defende que “o uso estratégico do governo para prover serviços e aplicações utilizando celulares, computadores portáteis, assistentes digitais pessoais (PDAs) e dispositivos similares torna-se algo realmente atrativo”.

Em agosto de 2015 o Brasil registrou, segundo a ANATEL, cerca de 280 milhões de linhas ativas no SMP (Serviço Móvel Pessoal). Aliado ao crescente número de dispositivos móveis e a necessidade de inovação no setor público surge o conceito *mobile government* também descrito com por alguns autores como *m-government*. Kushchu e Kuscu (2012) descrevem sobre o conceito:

“Advances in E-government oriented technologies and services are taking place with a considerable speed around the world. E-government efforts aim to benefit from the use of most innovative forms of information technologies, particularly web-based Internet applications, in improving governments’ fundamental functions. These functions are now spreading the use of mobile and wireless technologies and creating a new direction: mobile government (m-government).” (Kushchu e Kuscu, 2012, p.01)

Allazo, Sablón e Iano (2009) destacam que “o m-government é um subconjunto do e-government, onde o uso de informação e tecnologias modernas permite melhorar as atividades de organizações voltadas para o setor público” (ALLAZO, SABLÓN e IANO, 2009, p. 123).

O planejamento para a execução de projetos de aplicações móveis governamentais voltadas à segurança pública, devem levar em consideração peculiaridades brasileiras. A evolução no desenvolvimento de aplicações do tipo G2G para o uso pelos agentes de segurança pública no desempenho de suas tarefas será exposto neste estudo.

2.2 SISTEMAS OPERACIONAIS PARA DISPOSITIVOS MÓVEIS

Fling (2009) explica que o requisito primordial dos dispositivos móveis para executar softwares e serviços é possuir uma plataforma ou um núcleo de programação que pode ser dividido em 3 categorias: licenciada, proprietária e código aberto.

Para Fling (2009) as plataformas licenciadas são vendidas a fabricantes de aparelhos para a distribuição exclusiva em dispositivos. Os objetivos é criar interfaces (APIs) que funcionam de forma semelhante em vários dispositivos com o mínimo de esforço necessário para se adaptar às diferenças de cada dispositivo, embora isso não seja uma total realidade. Já as aplicações proprietárias são projetadas e desenvolvidas por fabricantes para uso exclusivo em seus dispositivos. Estas aplicações não estão disponíveis para o uso por fabricantes de dispositivos concorrentes.

Ganhando cada vez mais força, as plataformas *open source* são plataformas de código aberto que permitem gratuitamente a utilização e a modificação pelos seus usuários.

Milhões	2009	2010	2011	2012	2013	2014
Android	12	69,6	243,5	500,1	790,8	1055,1
iPhone OS	20,3	46,8	93,1	135,9	153,1	191,7
W.Phone	14,7	12,2	9	17,5	33,9	34,7
Blackberry	34,5	47,5	51,1	32,5	19,3	6,1
Symbian	80	109,9	81,5	23,9	3,9	-
linux	6,4	5,2	14,5	13	1,7	-
Other OSs	3,4	5,7	1,8	2,4	10,5	7,2
TOTAL	172,3	296,9	494,5	725,3	1013,2	1294,8

Tabela 1: Resultados Anuais do quantitativo de aparelhos com plataformas móveis no mundo, expressos em milhões.

Fonte: IDC

A Tabela 1 deixa explícita a variação na aceitação do mercado em relação as principais plataformas de sistemas operacionais para dispositivos móveis, ao longo de 6 anos.

	Android	iOS	Windows Phone
Market Share (Global)	84,7%	11,7%	2,5 %
Usuários Ativos	1 Bilhão	800 milhões	60 milhões
Número de APPs	1,3 Milhão	1,2 milhão	300 mil

Tabela 2: Resultados Anuais do quantitativo de aparelhos com plataformas móveis no mundo

Fonte: IDC

A Tabela 2 ilustra em conformidade com o estudo realizado pela IDC (provedora de inteligência de mercado de Tecnologia da Informação e Telecomunicações), realizado em maio de 2015 os sistemas operacionais Android e iOS foram responsáveis por mais que 96% de todos os embarques de smartphones em todo o mundo.

2.1.1 ANDROID

Liderado pelo Google, o Android é uma plataforma de código aberto criado para utilização em dispositivos móveis e pertence a Open Handset Alliance.

O Android adota a linguagem de programação JAVA, GARGENTA 2011 descreve, dentre algumas diferenças, o processo de compilação e execução de aplicativos desenvolvido para Android:

“You still write the Java source file, and you still compile it to Java byte code using the same Java compiler. But at that point, you recompile it once again using the Dalvik compiler to Dalvik byte code. It is this Dalvik byte code that is then executed on the Dalvik VM.” (Gargenta 2011, p. 10)

Gargenta (2011) descreve que o Android foi criado a partir de módulos de baixo nível do Linux, portanto todo o código das bibliotecas e da estrutura das aplicações nativas são totalmente acessíveis. Mais ainda, o Android está licenciado sob lincenças (Apache/MIT) para que outros possam estendê-lo livremente e utiliza-lo para diversos fins.

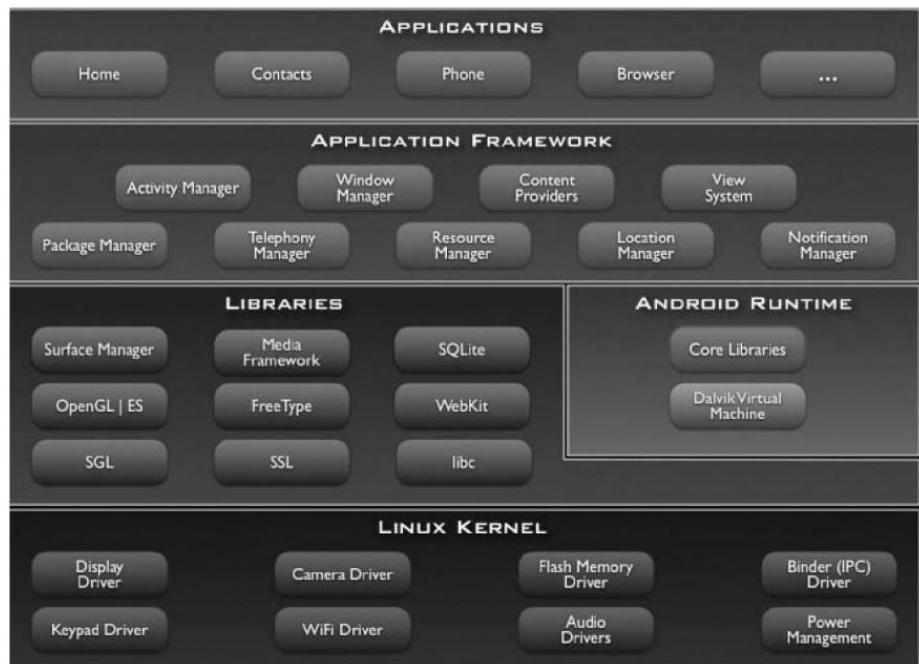


Figura 1: Arquitetura Android

Fonte: Livro Android para Desenvolvedores

Segundo MICHEL e PEREIRA (2009) a Figura 1 demonstra a camada Aplicações, que é a mais superficial das camadas e que concentram os aplicativos básicos desenvolvidos em Java, por exemplo os clientes de e-mail, navegadores, programas SMS, entre outros desenvolvidos pela comunidade. A segunda camada, Framework, encontra-se todos os acesso necessários para se desenvolver aplicativos. Dispõe de APIs e gerenciamento aos recursos disponíveis. A terceira camada, Bibliotecas, inclui um conjunto de bibliotecas desenvolvidas em C/C++ e que a plataforma utiliza para carregar funcionalidades de mais baixo nível e que são acessada pelo desenvolvedor por intermédio da camada de Framework. E por fim a camada Linux Kernel que figura como a camada que realiza a abstração do hardware e a pilha de software, além de desempenhar funções importantes como o gerenciamento de energia desligando dispositivos que não estão sendo utilizados por aplicações.

2.1.2 IOS

O iOS foi desenvolvido originalmente para ser concebido por dispositivos móveis da Apple. Mas tornou-se também uma plataforma para outros tipos de dispositivos: iPods, iPads e Apple TV.

MILANI (2012) afirma que a Apple desenvolveu o iOS para a execução restrita aos hardwares construídos por ela. Portanto, apenas produtos da Apple conseguem executar com sucesso a plataforma iOS.

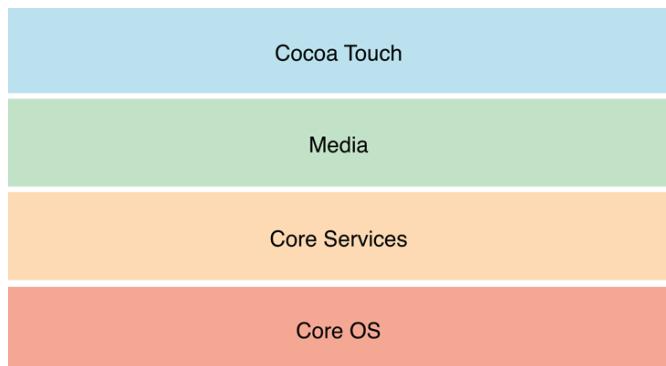


Figura 2: Arquitetura iOS

Fonte: Apple

A arquitetura do iOS, ilustrada pela Figura 2, é subdividida em 4 partes, segundo MILANI (2012). A primeira parte e mais alto nível é a Cocoa Touch, que o desenvolvedor necessita para se interligar às funções dos dispositivos ela é uma API que possibilita ao programador o controle de vários recursos como multi toque, interface gráfica, transferência de arquivos e gestos de interação com usuário, entre outros recursos. Abaixo da camada de Cocoa Touch está a chamada Media, que possui a atribuição do gerenciamento dos efeitos de tela, audiovisual, e tecnologias como a OpenGL ES e Quartz, ambas utilizadas no desenvolvimento de aplicações que exigem maior recurso gráfico. A terceira camada é a Core Services, que oferece alguns dos principais serviços da plataforma para o desenvolvedor, como por exemplo, o de manipulação de arquivos, acesso ao SQLite, entre outros serviços. Por fim, a camada de mais básica e elementar, o Core OS, considerado o núcleo de todo o sistema operacional. Esta camada é a que gerencia os sockets, certificados, a parte de segurança e da comunicação dos sistemas interligados a uma rede de dados.

Para desenvolver atualmente para iOS o profissional deverá deter de conhecimentos da linguagem de programação Swift 2 e/ou Objective C. Porém a Apple encoraja os desenvolvedores a migarem totalmente para o Swift 2 tendo em vista a descontinuidade do Objective C.

2.1.3 WINDOWS PHONE

Em terceiro lugar no ranking de plataformas móveis em uso da atualidade, a Microsoft oferece o Windows Phone como uma plataforma licenciada para uma das maiores fabricantes de aparelhos celulares de todo mundo, a Nokia.

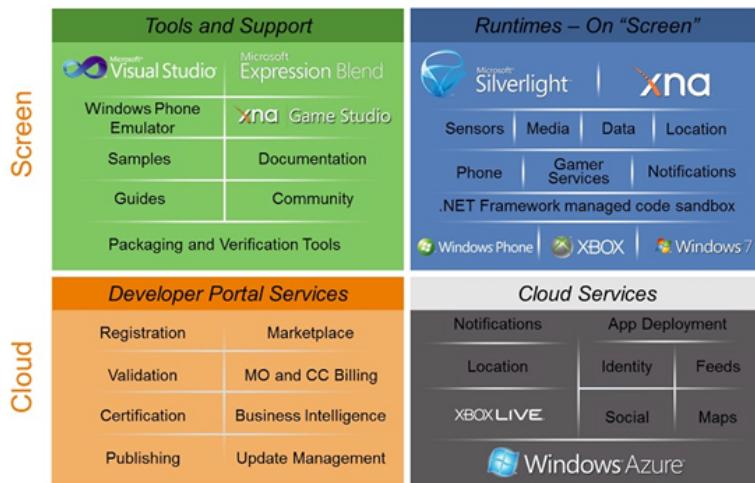


Figura 3: Arquitetura Windows Phone

Fonte: Livro Desenvolvendo Aplicações para Windows Phone

Diferente das plataformas Android e iOS, o Windows Phone conta com um modelo arquitetural diferente com módulos hierarquicamente equivalentes, conforme descrito por Mônaco e Carmo (2012) e exibido na Figura 3: Runtime, Tools, CloudServices e Portal Services. No acesso Runtime o Windows Phone promove segurança para a plataforma isolando todas as aplicações individualmente, não permitindo qualquer tipo de integração entre elas ou com qualquer nível inferior do sistema operacional. O acesso a características nativas dos aparelhos se dá pelo uso de APIs. No módulo Tools o desenvolvedor conta com suporte para o desenvolvimento de aplicações com nas principais IDEs, o Visual Studio e o Expression Blend, a primeira mais voltada para a linguagem de programação C++ e a segunda com foco na criação de animações e interfaces com visuais ricos. Cloud Services é o canal de comunicação com os serviços externos na nuvem e como por exemplo o Azure, mapas, serviços de publicidade, webservices de terceiros e etc., oferecendo uma maior possibilidade de escalabilidade e maior disponibilidade. O Portal Services engloba os bastidores da homologação, validação, certificação e inteligência de negócios dos aplicativos oferecidos pelo Windows Phone Marketplace.

2.1.4 COMPARATIVO ENTRE PLATAFORMAS MÓVEIS

Em uma análise mundial a IDC (2014) demonstra um considerável avanço na venda de aparelhos Android frente as concorrentes Apple iOS e a Microsoft Windows desde o terceiro quadrimestre de 2009.

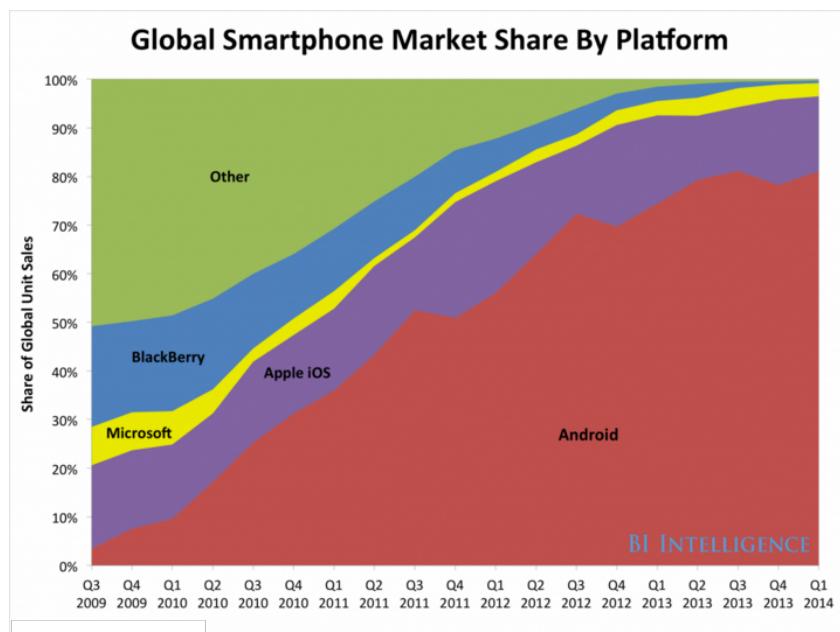


Grafico 1: Participação da plataforma no mercado global

Fonte: IDC, Strategy Analytics

A Apple ainda detém de uma fatia grande do mercado porém o Android está ficando com quase todo o resto. A qualidade de telefones Android está ficando cada vez melhor, afirma a IDC, e oferece um desafio a longo prazo para a Apple.

Sistema Operacional	2014		2018 (Previsão)	
	Volume de Vendas (em milhões)	Oferta de aparelhos na loja virtual	Volume de Vendas (em milhões)	Oferta de aparelhos na loja virtual
Android	997,7	80,20%	1.401,30	77,60%
iOS	184,1	14,80%	247,4	13,70%
Windows Phone	43,3	3,50%	115,3	6,40%
BlackBerry	9,7	0,80%	4,6	0,30%
Outros	9,3	0,70%	37,7	2,10%
Total	1.244,10	100%	1.806,30	100%

Tabela 3: Previsão de cota no mercado de plataforma móveis em 2018. Volumes nominais expressos em milhões.

Fonte: IDC

O que demonstra o resultado da análise da IDC na Tabela 3 é que em 2018 o iOS perderá o atual segundo lugar para o Windows Phone que tende a ganhar mercado, mas ainda ficará distante do Android que injetará até lá mais 403 milhões de aparelhos com sua plataforma.

Outro fator relevante na comparação entre plataformas é o custo médio dos aparelhos.

Sistema Operacional	Preço médio de aparelhos smartphones	
	2014	2018
Android	\$254	\$215
iOS	\$657	\$604
Windows Phone	\$265	\$214
BlackBerry	\$339	\$252
Outros	\$154	\$173
Total	\$314	\$267

Tabela 4: Previsão de preço médio de aparelhos com sistemas operacionais.

Fonte: IDC, Strategy Analytics

É possível reparar na Tabela 4 que o preço médio do aparelho Android está indo em direção a U\$ 200 e que o preço médio do iPhone está chegando a quase U\$ 600. Demonstra-se que a previsão para o mercado de 2018 é que os valores médios de smartphones sofram um redução de 4,9% enquanto os aparelhos smartphones com os sistemas operacionais iOS devem diminuir apenas 1,4% do valor atual.

2.2 LICITAÇÕES E O PRINCÍPIO DA ECONOMICIDADE

O art. 3º da Lei 8.666/93, que regulamenta as práticas de licitações e contratos administrativos, interpõe uma série de princípios a serem considerados pela Administração na realização da probidade administrativa:

“Art. 3º. A licitação destina-se a garantir a observância do princípio constitucional da isonomia e a selecionar a proposta mais vantajosa para a Administração e será processada e julgada em estrita conformidade com os princípios básicos da legalidade, da imparcialidade, da moralidade, da igualdade, da publicidade, da probidade administrativa, da vinculação ao instrumento convocatório, do julgamento objetivo e dos que lhe são correlatos.” (Constituição Federal do Brasil)

Para Maria Sílvia Zannela Di Pietro a “A própria licitação constitui um princípio a que se vincula a Administração Pública. Ela é decorrência do princípio da indisponibilidade do interesse público e que se constitui em uma restrição à liberdade administrativa na escolha do contratante; a Administração terá que escolher aquele cuja proposta melhor atenda ao interesse público.” (Di Pietro, 1999, p.294).

Entre os princípios da licitação está o princípio da economicidade que é interpretado em seu aspecto conceitual por várias doutrinas:

- a) OLIVEIRA (1990) argumenta que a “economicidade diz respeito a se saber se foi obtida a melhor proposta para a efetuação da despesa pública, isto é, se o caminho perseguido foi o melhor e mais amplo, para chegar-se à despesa e se ela fez-se com modicidade, dentro da equação custo-benefício.”
- b) TORRES (1991) afirma que o “conceito de economicidade, originário da linguagem dos economistas, corresponde, no discurso jurídico, ao de justiça.” Implica “na eficiência na gestão financeira e na execução orçamentária, consubstanciada na minimização de custos e gastos públicos e na maximização da receita e da arrecadação”.
- c) REZENDE (1980) traduz que “além da quantificação dos recursos aplicados em cada programa, subprograma ou projeto, a efetiva implantação do orçamento-

programa depende, ainda, da aplicação de métodos apropriados para a identificação de custos e resultados, tendo em vista uma correta avaliação de alternativas. No caso de empreendimentos executados pelo setor privado, a escolha entre alternativas para atingimento dos objetivos do grupo é, normalmente, feita mediante comparações entre taxas de retorno estimadas para cada projeto, com a finalidade de estabelecer qual a alternativa que oferece os melhores índices de lucratividade. No caso de programas governamentais, o raciocínio é semelhante, recomendando-se, apenas, substituir a ótica privada de avaliação de custos e resultados (lucros) por uma abordagem que procure revelar os custos e benefícios sociais de cada projeto.

- d) A Fundação Getúlio Vargas (1989) concluiu que “economicidade tem a ver com avaliação das decisões públicas, sob o prisma da análise de seus custos e benefícios para a sociedade, ou comunidade a que se refere”

2.3 SEGURANÇA DA INFORMAÇÃO

A segurança é aguardada por qualquer usuário quando se trata de informações. Para uma organização pública ou privada, é necessário garantir que as informações armazenadas em seus bancos de dados não sejam acessadas, alteradas ou corrompidas por algum intruso (SILVA, 2008).

De acordo com a norma NBR ISSO/IEC 27002:2013 da ABNT a segurança da informação deve ser construída a partir de um grupo de controles que incluem política, processo, procedimento, estrutura organizacional e funções de software e hardware. ABNT (2013) detalha que estes controles devem ser “estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário, para assegurar que os objetivos do negócio e a segurança da informação da organização são atendidos.” (ABNT, 2013, p. 4).

Dentre os mecanismos de controles está a autenticação e autorização que é o meio confiável de se ter garantia que o usuário ou o serviço remoto de terceiro possuem credenciais para obter as informações requisitadas.

Atualmente existem 3 modos distintos para a realização de autenticação usuário:

Acesso Positivo: é aquele que requer do usuário um conhecimento específico, por exemplo uma palavra-chave que será utilizada no processo de autenticação.

Acesso Proprietário: o usuário possui um objeto físico único que é utilizado no processo de autenticação, como por exemplo, um *smartcard*.

Acesso Biométrico: onde o requerente possui uma característica pessoal e única para acesso exclusivo como, por exemplo, o reconhecimento facial.

A criptografia é uma das principais ferramentas de segurança digital pois “é o conjunto de conceitos e técnicas, que visa codificar uma informação de forma que somente o emissor e o receptor possam acessá-la, evitando que um terceiro consiga interpretá-la. É o disfarce das informações. É a técnica de transformar dados em códigos indecifráveis para serem transportados de um ponto a outro sigilosamente. A chave (pública ou privada) é o que permite decodificar estes dados. Há várias utilidades para a criptografia, tais como proteger documentos secretos, transmitir informações confidenciais pela Internet ou por uma rede local, etc.” (RESENDE, 2009 , p. 111).

2.3.1 ASSINATURA DIGITAL E CERTIFICADO DIGITAL

Assinatura feita à mão é uma representação gráfica pessoal feita de próprio punho para atestar a veracidade de um documento indicando sua aprovação e/ou autoria. Assinatura digitalizada é meramente uma imagem digital de uma assinatura manuscrita (PEREIRA, 2008).

Segundo definição do Professor Luiz Gustavo Cordeiro da Silva:

Certificação Digital é um conjunto de técnicas e processos que propiciam mais segurança às comunicações e transações eletrônicas, permitindo também a guarda segura de documentos. Permite que informações transitem pela Internet com maior segurança. É baseada na existência de Certificados Digitais emitidos por uma Autoridade Certificadora (AC), considerada confiável pelas partes envolvidas. (Silva, 2008 p.10) Garantindo o conteúdo de mensagens ou textos, sua autoria e data em que foi assinada. Baseia-se no princípio da terceira parte confiável, que oferece confiabilidade entre partes que se utilizem de Certificados Digitais. Para isso

utiliza-se de uma Infra-estrutura de chaves públicas, cuja principal função é definir técnicas e procedimentos. A Medida Provisória 2.200-2, de agosto de 2001 estabelece a Infra-estrutura de Chaves públicas Brasileira – ICP-Brasil. (Silva, 2008, p.12)

A certificação digital garante a autenticidade da assinatura digital aliando valores legais e tecnológicos. Ela está sendo usada no Brasil para agregar valores jurídicos a documentos eletrônicos e para assegurar sua eficácia probatória (PEREIRA, 2008).

AMADEU (2004) explica que o certificado digital se apresenta como opção para assegurar que as informações sejam acessadas unicamente pelo próprio interessado ou para possibilitar que informações críticas trafeguem codificadas pelo ambiente digital conquistando um grau mínimo de privacidade e segurança das informações. AMADEU (2004) defende que o poder público deve participar nas relações entre o cidadão e a internet, desmitificando o receio da invasão de privacidade e esclarecendo quanto às ferramentas existentes, inserindo o cidadão em serviços virtuais oferecidos pelo poder público.

A pessoa física ou jurídica que adquirir um certificado digital junto a uma Autoridade de Registro, contará com todos os mecanismos de assinatura digital, criptografia e outros itens que envolvem a produção de um documento eletrônico com segurança e confidencialidade segundo o que expõe TRAIN (2005).

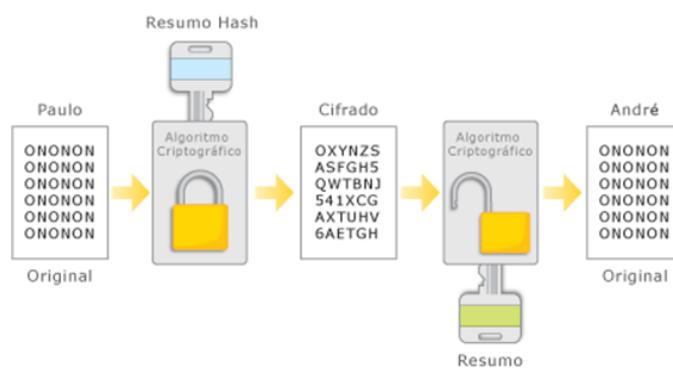


Imagen 1: Assinatura Digital

Fonte: <http://static.hsw.com.br/gif/certificado-digital-assinatura.gif>

O carro chefe das implementações aliado aos certificados digitais é o protocolo Secure Sockets Layer (SSL).

2.3.1.1 SSL

Quando em 1995, o mundo começo utilizar a internet para realizar transações financeiras a Netscape Communicattions Corp. que era a principal fornecedora de navegadores da época introduziu o um pacote de segurança chamado SSL (Secure Sockets Layer) a fim de atender essa demanda. Com o advento de novos navegadores o SSL ganhou mais força passando por algumas reformulações de versões.

Basicamente a SSL cria uma conexão segura entre dois soquetes promovendo, segundo TANEBAUM (2003) a transferência de parâmetros entre cliente e servidor, autenticação mútua de cliente e servidor, comunicação criptografada e garantia da integridade dos dados.

Quando em 1995, o mundo começou a utilizar a internet para realizar transações financeiras a Netscape Communicattions Corp. que era a principal fornecedora de navegadores da época introduziu um pacote de segurança chamado SSL (Secure Sockets Layer) a fim de atender essa demanda. Com o advento de novos navegadores o SSL ganhou mais força passando por algumas reformulações de versões.

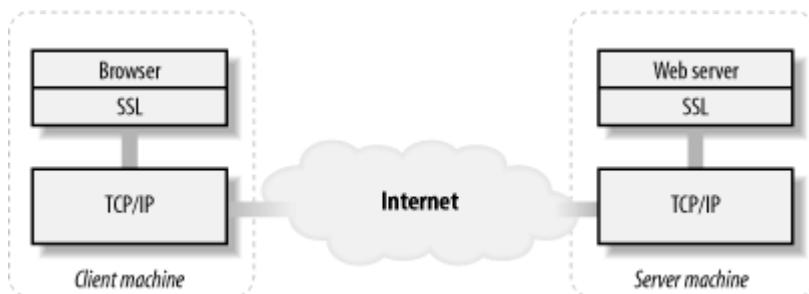


Figura 4: Representação da comunicação SSL

Fonte: Livro Rede de Computadores.

Conforme a Figura 4 demonstra o SSL opera nas duas pontas da comunicação, ele basicamente cria uma conexão segura entre dois soquetes promovendo, segundo TANEBAUM (2003) a transferência de parâmetros entre cliente

e servidor, autenticação mútua de cliente e servidor, comunicação criptografada e garantia da integridade dos dados.

2.4 WEB SERVICE

Segundo Abinader Neto e Lins (2006), diversas tecnologias surgiram nos últimos anos destinadas ao desenvolvimento de aplicações para a Internet. A variedade de linguagens e protocolos internos tornava inviável a integração de modo automatizado. Com base nesta problemática, foi desenvolvida a linguagem XML (Extended Markup Language) e o conceito de Web Service. A partir de então, não importava a tecnologia envolvida no processo que a comunicação entre elas poderia ser realizada utilizando o formato XML. Entre as vantagens de comunicação utilizando a linguagem XML está no tráfego suave do pacote pelo *firewall* tendo em vista que é um protocolo baseado apenas em texto.

De acordo com a [W3C] - Word Wide Web Consortium – Organização internacional que orienta e administra os padrões e protocolos utilizados na internet, *Web Service* é um software projetado para suportar interação máquina-a-máquina interoperáveis sobre uma rede. Utilizando uma interface de formato processável.

Atualmente a arquitetura SOAP (Simple Object Data Protocol) e REST (Representational State Transfer) são as mais utilizadas para desenvolvimento de softwares *Web Services* de acordo com a W3C.

2.4.1 DIFERENÇAS ENTRE A ARQUITETURA SOAP E REST

Apesar de possuírem aspectos distintos são capazes de oferecer os mesmos serviços. Portanto o estudo de caso é fator determinante para a adoção da arquitetura mais adequada ao projeto.

Segundo FERREIRA e MOTA (2014) uma das vantagens do SOAP é o uso de um método de transporte “genérico”. Enquanto que o REST faz uso de HTTP/HTTPS, o SOAP pode usar qualquer meio de transporte existente para enviar suas requisições. A tecnologia REST, se sai bem em situações em que há limitação de recursos e de largura de banda, e em operações que não precisa de estado, já se uma operação precisa ser continuada a tecnologia SOAP é a indicada.

3 METODOLOGIA

Este estudo foi produzido utilizando-se de inúmeras referências bibliográficas que correspondessem ao objetivo deste trabalho. Assim, foram considerados artigos de pesquisadores sobre os temas, trabalhos de conclusão de curso e *sites* especializados no assunto.

Para o desenvolvimento da aplicação, produção de modelagens necessárias para o planejamento e para a realização de testes foram utilizados os seguintes itens:

- Notebook, Intel (R) Core (TM) i7-6500U PCU @ 2.50GHz 2.60GHz com 16 GB de memória
- Celular Samsung Galaxy S3;
- Celular LG Prime;
- Eclipse Java EE IDE for Web Developers - Versão: Mars.2 Release (4.5.2) - Build id: 20160218-0600;
- Apache TomCat 8.0;
- Android Studio 2.1.1;
- Java 1.8.0;
- JDK 1.7.0;
- Wireshark 2.0.4 64Bits;
- Lucid chart;
- Oracle 9i;
- OpenSSL v1.0.2g Light Win64;
- Firewall Firewaker;
- DETRANET;
- PHP 7.0;
- PhpStorm 10.0.1;
- Apache 2.4.17.

Os itens acima foram adotados por apresentarem um bom suporte pela comunidade ou pela empresa fabricante e por serem estáveis para a produção da solução proposta.

Os estudos referentes aos webservices demonstram uma paridade entre a capacidade do Webservice REST e o Webservice SOAP, porém um fator que não agrada na escolha de um servidor SOAP é o consumo elevado de dados, tendo em vista que a maioria das requisições que serão realizadas proverão da internet de dados móveis. O oferecimento de um esquema explícito nas requisições de um servidor WSDL é importante, principalmente para grandes projetos, porém o uso limitado à poucos métodos convidam a convencionar o esquema em uma estrutura REST.

A seguir uma comparação entre as estruturas e os tamanhos de uma mesma mensagem no formato XML e JSON:

JSON	XML
<pre>{ nome:"Brunno", idade:32, veiculos:["city", "hrv"], parentes:{ mae:"Anna Maria", pai:"Kleber" } }</pre>	<pre><root> <nome>Brunno</nome> <idade>32</idade> <veiculos> <veiculo>city</veiculo> <veiculo>hrv</veiculo> </veiculos> <parentes> <mae>AnnaMaria</mae> <pai>Kleber</pai> </parentes> </root></pre>
Tamanho: 159 bytes	Tamanho: 300 bytes

Tabela 4: Comparativo entre XML e JSON.

Analizando a tabela acima é fácil entender o porquê o formato JSON foi 47% menor que o tamanho de um formato XML, respalda a ideia que o formato JSON proporcionado por servidores webservice com a tecnologia REST proporciona uma maior probabilidade de acesso a informação em lugares com a internet limitada em termos de velocidade e conectividade estável.

Como já mencionado neste estudo, a linguagem de programação utilizada para se desenvolver aplicativos nativos para o Android é o Java, portanto a escolha da mesma linguagem para o desenvolvimento da solução WebService REST necessária para a conectividade com as informações é prudente pois irá homogeneizar a linguagem do projeto em relações mais dinâmicas.

A especificação JAX-RS normatiza a implementação de um WebService com arquitetura RESTful. Ela utilizada anotações em sua API, que facilitam as configurações dos serviços que serão oferecidos. O JAX-RS faz parte atualmente do Java EE. Portanto é necessário escolher uma implementação. Uma opção *open source* popularmente utilizada é o Jersey mantido pela empresa Oracle. Para este estudo será utilizado a versão 1.15 do Jersey.

O local utilizado para o desenvolvimento desta solução foi o SIOP (Sistema Integrado de Operações) que é uma autarquia de governo subordinada diretamente à Secretaria de Segurança Pública do estado do Tocantins e é constituída pelos seguintes entes públicos mediante convênio: Polícia Militar do Estado do Tocantins, Polícia Civil, Polícia Técnica Científica, Corpo de Bombeiros Militar, Guarda Metropolitana Municipal, Secretaria de Acessibilidade Trânsito e Transporte Municipal e Detran.

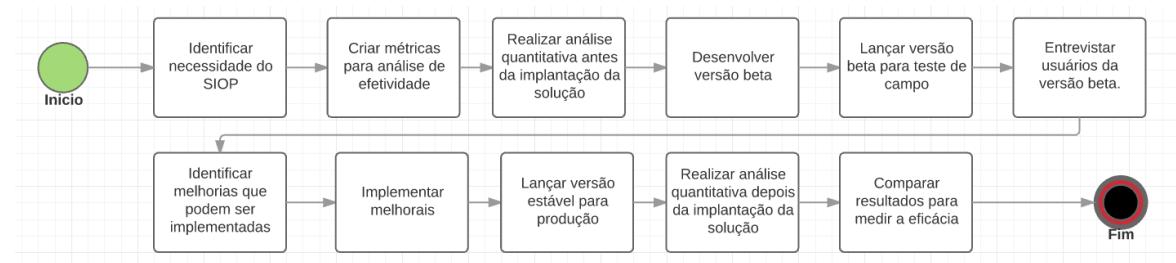


Figura 5: Representação dos passos para o desenvolvimento da solução.

Fonte: Elaborado pelo autor, 2016.

A Figura 5 descreve graficamente a sequência de passos que serão utilizados neste estudo que visa empregar melhorias nas rotinas operacionais do SIOP com o uso de aplicativos móveis no apoio às ações dos agentes de segurança pública aplicando o conceito de G2G explicado neste estudo como uma relação de Governo e Governo onde a tecnologia é utilizada para aumentar a eficácia e a eficiência nas

atividades governamentais proporcionando o aumento na arrecadação, a melhoria na prestação de serviços e elevando a qualidade de vida dos agentes de governo.

Após entrevistas com funcionários do SIOP analisou-se que as solicitações de pesquisa de veículos e condutores pelos agentes de campo demandavam tempo e recursos, e prejudicavam as ações de prioridade mais elevada principalmente pelo consumo de tempo necessário para a realização da rotina. Após levantamento da rotina em questão, identificou-se que o agente de segurança pública realizava o contato pelo canal de rádio e o funcionário do SIOP consultava a informação no sistema (DETRANET), que pertence ao Detran estadual, para responder pelo rádio os dados requeridos pelo agente de segurança pública. Este processo ocupa a rede de rádio por completo pois esta comunicação é transmitida para todos os rádios que estão na mesma frequência e que não necessitam saber da informação, não sendo possível outra comunicação paralela. O risco do ruído da informação neste ambiente é considerado alto ainda mais nos congestionamentos do canal de rádio.

O volume de pesquisas e o tempo de resposta das consultas podem servir de métrica para se medir a aceitação e qualidade, visto que o uso do software reflete as ações de segurança pública para fiscalização e combate à criminalidade e o tempo de resposta curto permite ações mais rápidas, otimizando o tempo de serviço do agente de segurança.

Após 30 dias de monitoramento em pesquisas realizadas no sistema DETRANET, utilizando relatórios de auditorias do firewall da rede do SIOP, identificou-se a frequência de pesquisas realizadas pelo método convencional.

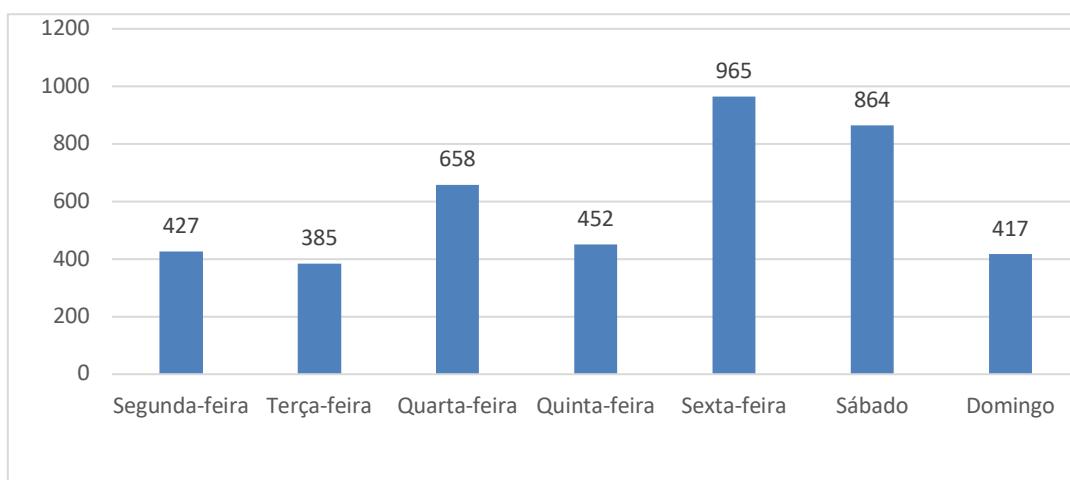


Gráfico 2: Quantitativo de consultas realizadas no sistema DETRANET durante 30 dias.

Fonte: Elaborado pelo autor, 2016.

O Gráfico 2 exibe o fluxo de consultas que em 30 dias chegou ao total de 4.168 consultas à condutores e veículos. Durante os mesmos 30 dias foram cronometrados os tempos que levavam algumas pesquisas por um processo de amostragem em diferentes horários e dias da semana. Identificou-se que o tempo de resposta para as solicitações variavam entre 3 à 9 minutos.

Identificou-se que as consultas de condutores realizadas são para verificar a pontuação na carteira do condutor, a categoria de condução do pesquisado e, em caso de acidente que precisa ser acionada a família da vítima, o endereço.

Identificou-se que as consultas de veículos possuem foco na fiscalização tributária e no combate ao roubo e furto de veículos automotores, sendo importante para o agente de segurança pública informações como a numeração do chassi, marca, modelo, cor, RENAVAM, nome do proprietário, data do vencimento do licenciamento, débito de licenciamento, débito de IPVA, débito de multas, restrições de roubos e restrições administrativas.

Para casos de verificações de roubo e furto do veículo uma quantidade considerável de agentes de segurança pública faz uso do aplicativo Sinesp Cidadão que é um módulo do Sistema Nacional de Informações de Segurança Pública, Prisionais e sobre Drogas que permite ao cidadão consultar a situação de roubo ou furto de qualquer automóvel registrado no Brasil. Os dados são pesquisados no banco de dados do Departamento Nacional de Trânsito (DENATRAN), foi idealizado pela SENASP, órgão do Ministério da Justiça e criado juntamente com o Serviço Federal de Processamento de Dados (SERPRO).



Figura 6: Fluxo de telas para consulta de veículos do aplicativo Sinesp Cidadão.

Fonte: Elaborado pelo autor com telas do aplicativo, 2016.

O aplicativo exposto na Figura 6 possui versões para Android, iOS e Windows Phone, porém o uso deste aplicativo é voltado para o cidadão e o mantenedor deste aplicativo recomenda em seu site que:

O aplicativo é voltado para o uso do cidadão, neste modo, os profissionais de segurança pública não podem restringir suas pesquisas somente ao aplicativo. Sugerimos confirmar as informações em outras fontes, como Detrans, Infoseg, Tribunais de Justiça e etc...

A recomendação incentiva o uso de outras fontes pois a base de consulta das informações prestadas pelo aplicativo não são alimentadas com a celeridade necessária, podendo um veículo roubado ou furtado ser incluído somente 4 dias após o fato ocorrido, tempo que pode levar para o processo correr por todo o rito burocrático necessário para sua inclusão desta informação na base de consulta. Sendo assim se vê a necessidade de um banco de dados mais confiável para a fomentar a pesquisa pelos agentes de segurança.

Diante do exposto, o desenvolvimento de aplicações móveis para o apoio às atividades dos agentes de segurança pública demonstra ser uma alternativa viável para oferecer melhor tempo de resposta nas consultas de dados e diminuir o tráfego na rede de rádio comunicação dos órgãos de segurança pública.

O objeto do desenvolvimento deste estudo será um aplicativo para consulta de condutores e veículos que fornecerá dados necessários para o desempenho das funções de fiscalização de trânsito e afins.

Para obter o resultado esperado é necessária uma interface de comunicação com a entidade que possui os dados esperados nas consultas. Para isso foi firmado um convênio com o DETRAN do Tocantins que forneceu um webservice para realização das consultas.

A seguinte arquitetura foi utilizada para desenvolver a solução deste estudo:

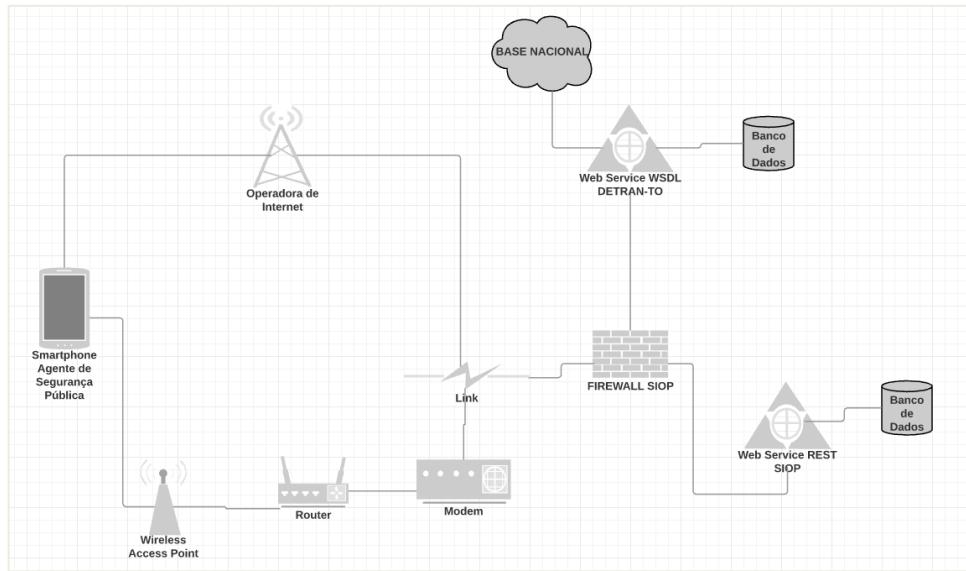


Figura 7: Arquitetura para a solução.

Fonte: Elaborado pelo autor, 2016.

A modelagem da arquitetura (Figura 7) define que o uso da solução poderá ser mediante a conexão *wireless* ou rede dados móveis 2G/3G/4G para acesso ao *webservice* do SIOP que conterá a regra de negócio necessária para validar a requisição e efetivar a consulta no *webservice* do DETRAN – TO, realizando a inclusão das requisições em uma base de dados para garantia de auditorias e estatísticas sobre a utilização da ferramenta.

4 DESENVOLVIMENTO

A partir do estudo teórico levantado neste trabalho e com base na necessidade de adequação a uma estrutura governamental de cultura tradicional, as seções seguintes demonstram como cada decisão foi tomada para o desenvolvimento da temática proposta.

4.1 SISTEMA OPERACIONAL

Entende-se que as principais plataformas existentes no mercado possuem todos os requisitos necessários para a implementação da solução, o que faz necessário questionar se existe a necessidade de criar um aplicativo para cada sistema operacional ou escolher apenas um.

Notavelmente a escolha de implantar em cada uma das 3 principais plataformas operacionais exigiria uma equipe de desenvolvimento diversificada e numerosa ou um tempo de desenvolvimento maior para uma equipe reduzida. A manutenção do software poderia ser tornar lenta e onerosa. Portanto, se as quantidades de usuários de cada uma das plataformas estiverem em faixas aproximadas de utilização é inevitável o desenvolvimento para cada um dos sistemas operacionais ou considerar o uso de tecnologias hibridas.

Para estimar a proporção de cada plataforma foi desenvolvido um algoritmo para reconhecimento do sistema operacional utilizado pelos agentes de segurança pública. O algoritmo foi implantado em um sistema intranet que seria executado após a autenticação do usuário. Tal sistema condensa rotinas administrativas e hospeda informações relevantes e restritas aos agentes de segurança pública do Tocantins.

```
1 <?php
2
3 // Abre ou cria o arquivo identifica_so.tcc
4 // "a" -> Abre o arquivo somente para escrita; coloca o ponteiro no fim do arquivo. Se o arquivo não existir, tentar criá-lo
5 $fp = fopen("identifica_so.tcc", "a");
6
7 // Cria variável que recebe o valor de uma string denotando o agente de usuário pelo qual a página é acessada
8 $useragent = $_SERVER['HTTP_USER_AGENT'];
9
10 // Concatena a variável $useragent com a quebra de linha, se usa servidor linux utilizar \n
11 $useragent = str_replace($useragent) . "\r\n";
12
13 // Escreve o valor do parâmetro $useragent no identifica_so.tcc
14 $escreve = fwrite($fp, $useragent);
15
16 // Fecha o arquivo
17 fclose($fp);
18
19 ?>
```

Figura 8: Algoritmo para quantificar utilização de sistemas operacionais.

Fonte: Elaborado pelo autor, 2016.

O algoritmo da Figura 8 produz resultados relevantes para esta tomada de decisão visto que ele não fornece o número de agentes X sistema operacional e sim requisição de serviço X sistema operacional, considerando qual sistema operacional é mais atuante em serviços para os agentes de segurança pública.

```

mozilla/5.0 (windows nt 10.0; win64; x64) applewebkit/537.36 (khtml, like gecko) chrome/49.0.2623.112 safari
mozilla/5.0 (windows nt 10.0; win64; x64) applewebkit/537.36 (khtml, like gecko) chrome/49.0.2623.112 safari
mozilla/5.0 (linux; android 5.0.2; lg-d337 build/lrx22g) applewebkit/537.36 (khtml, like gecko) chrome/49.0.
mozilla/5.0 (linux; android 5.0.2; lg-d337 build/lrx22g) applewebkit/537.36 (khtml, like gecko) chrome/49.0.
mozilla/5.0 (linux; android 5.0.2; lg-d337 build/lrx22g) applewebkit/537.36 (khtml, like gecko) chrome/49.0.
mozilla/5.0 (linux; android 5.0.2; lg-d337 build/lrx22g) applewebkit/537.36 (khtml, like gecko) chrome/49.0.
mozilla/5.0 (linux; android 5.0.2; lg-d337 build/lrx22g) applewebkit/537.36 (khtml, like gecko) chrome/49.0.
mozilla/5.0 (linux; android 5.0.2; lg-d337 build/lrx22g) applewebkit/537.36 (khtml, like gecko) chrome/49.0.
mozilla/5.0 (linux; android 4.3; gt-i9300 build/jss15j) applewebkit/537.36 (khtml, like gecko) chrome/50.0.2
mozilla/5.0 (linux; android 4.3; gt-i9300 build/jss15j) applewebkit/537.36 (khtml, like gecko) chrome/50.0.2
mozilla/5.0 (linux; android 4.3; gt-i9300 build/jss15j) applewebkit/537.36 (khtml, like gecko) chrome/50.0.2
mozilla/5.0 (linux; android 4.3; gt-i9300 build/jss15j) applewebkit/537.36 (khtml, like gecko) chrome/50.0.2
mozilla/5.0 (linux; android 4.3; gt-i9300 build/jss15j) applewebkit/537.36 (khtml, like gecko) chrome/50.0.2
mozilla/5.0 (linux; android 4.3; gt-i9300 build/jss15j) applewebkit/537.36 (khtml, like gecko) chrome/50.0.2
mozilla/5.0 (linux; android 4.3; gt-i9300 build/jss15j) applewebkit/537.36 (khtml, like gecko) chrome/50.0.2
mozilla/5.0 (linux; android 4.3; gt-i9300 build/jss15j) applewebkit/537.36 (khtml, like gecko) chrome/50.0.2
mozilla/5.0 (linux; android 4.3; gt-i9300 build/jss15j) applewebkit/537.36 (khtml, like gecko) chrome/50.0.2
mozilla/5.0 (linux; android 4.3; gt-i9300 build/jss15j) applewebkit/537.36 (khtml, like gecko) chrome/50.0.2
mozilla/5.0 (linux; u; android 2.3.5; es-sa; lg-p920h build/grj90) applewebkit/533.1 (khtml, like gecko) ver
mozilla/5.0 (linux; u; android 2.3.5; es-sa; lg-p920h build/grj90) applewebkit/533.1 (khtml, like gecko) ver
mozilla/5.0 (linux; u; android 2.3.5; es-sa; lg-p920h build/grj90) applewebkit/533.1 (khtml, like gecko) ver
mozilla/5.0 (linux; u; android 2.3.5; es-sa; lg-p920h build/grj90) applewebkit/533.1 (khtml, like gecko) ver
mozilla/5.0 (linux; u; android 2.3.5; es-sa; lg-p920h build/grj90) applewebkit/533.1 (khtml, like gecko) ver
mozilla/5.0 (linux; u; android 2.3.5; es-sa; lg-p920h build/grj90) applewebkit/533.1 (khtml, like gecko) ver
mozilla/5.0 (linux; u; android 2.3.5; es-sa; lg-p920h build/grj90) applewebkit/533.1 (khtml, like gecko) ver
mozilla/5.0 (linux; u; android 2.3.5; es-sa; lg-p920h build/grj90) applewebkit/533.1 (khtml, like gecko) ver
mozilla/5.0 (linux; u; android 2.3.5; es-sa; lg-p920h build/grj90) applewebkit/533.1 (khtml, like gecko) ver
mozilla/5.0 (linux; u; android 2.3.5; es-sa; lg-p920h build/grj90) applewebkit/533.1 (khtml, like gecko) ver
mozilla/5.0 (linux; u; android 2.3.5; es-sa; lg-p920h build/grj90) applewebkit/533.1 (khtml, like gecko) ver
mozilla/5.0 (linux; u; android 4.4.2; d5106 build/18.1.a.1.21) applewebkit/537.36 (khtml, like gecko) chrome/50
mozilla/5.0 (linux; android 4.4.2; d5106 build/18.1.a.1.21) applewebkit/537.36 (khtml, like gecko) chrome/50
mozilla/5.0 (linux; android 4.4.2; d5106 build/18.1.a.1.21) applewebkit/537.36 (khtml, like gecko) chrome/50
mozilla/5.0 (linux; android 4.4.2; d5106 build/18.1.a.1.21) applewebkit/537.36 (khtml, like gecko) chrome/50
mozilla/5.0 (linux; android 4.4.2; d5106 build/18.1.a.1.21) applewebkit/537.36 (khtml, like gecko) chrome/50
mozilla/5.0 (linux; android 4.4.2; d5106 build/18.1.a.1.21) applewebkit/537.36 (khtml, like gecko) chrome/50

```

Figura 9: Resultado gerado pelo algoritmo de identificação do sistema operacional.

Fonte: Elaborado pelo autor, 2016.

Os resultados gerados, conforme a figura 9, possibilitam a busca por sistemas operacionais que foram utilizados para requisitar os serviços do sistema intranet, após quantificar a presença dos argumentos “android”, “ios” e “windows phone” foi produzida a seguinte estatística:

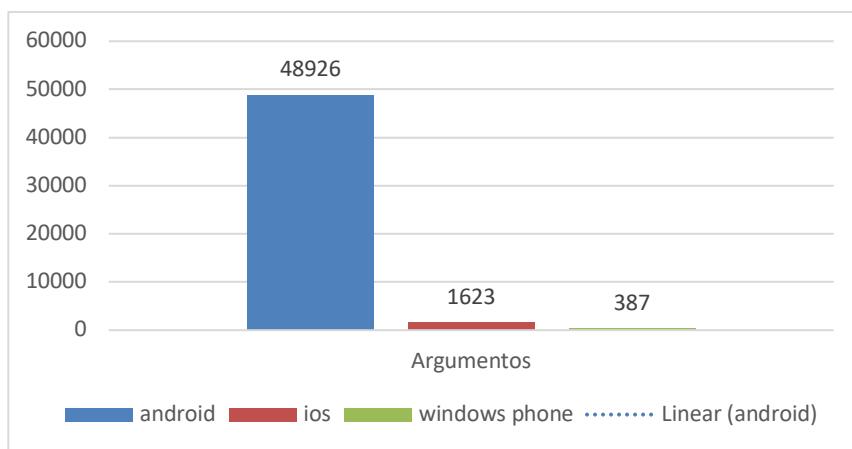


Gráfico 3: Quantitativo de argumentos na identificação de sistemas operacionais.

Fonte: Elaborado pelo autor, 2016.

O resultado obtido inclina o desenvolvimento para o sistema operacional Android visto que representa 96% dos sistemas operacionais pesquisados.

O acesso a solução proposta por este estudo pode ser realizado por *smartphones* particulares dos agentes de segurança pública ou por *smartphones* funcionais das instituições de segurança pública. Portanto é necessário saber qual sistema operacional comportaria a melhor opção de compra de *smartphones* pelo poder público, visto que existe uma legislação específica que regulamenta a aquisição deste tipo de produto.

A lei de licitação refletida no art. 3º da Lei 8.666/93 e o princípio da economicidade exposto neste estudo determina que o poder público deve optar pelo menor custo para obter o resultado que se espera. Portanto a análise de custo de mercado dos aparelhos com o sistema operacional embarcado, divulgado pela IDC, aponta o sistema operacional Android como menor custo em todas as categorias de *smartphones* e ainda com a previsão de apresentar um quadro ainda melhor frente aos seus concorrentes no futuro.

Por fim, tanto no prisma jurídico quanto na análise do público-alvo o Android apresenta a melhor opção para desenvolvimento desta solução.

4.2 SEGURANÇA DA INFORMAÇÃO

Os dados requisitados pelo aplicativo de consulta deste estudo são de extrema confidencialidade e deve ser restrita apenas aos agentes de segurança pública, portanto o uso de autenticação e criptografia dos dados é essencial neste processo.

4.2.1 AUTENTICAÇÃO

A restrição aos dados à aplicação para apenas os agentes de segurança pública é determinante para evitar que usuários indesejados obtenham o aplicativo e utilizem livremente. Porém a autenticação realizada por “Acesso Positivo” pode prejudicar a eficiência que se deseja obter. Pois se o agente necessitar consultar um veículo em trânsito (abordo de uma viatura) o processo de inclusão das credenciais de acesso neste modelo de autenticação pode elevar o tempo de resposta e

modificar o itinerário da equipe, prejudicando o bom andamento das rotinas operacionais.

A sigla IMEI é o acrônimo de *International Mobile Equipment Identity*, que em português significa “Identificação Internacional de Equipamento Móvel, este número é único em todo mundo segundo CONRAD SHEEHAN (2007).

Como o agente de segurança pública vai utilizar um aparelho *smartphone* para a realização da pesquisa este processo pode contar com um “Acesso Proprietário” que utilizará o número de IMEI para autenticação do usuário.

É necessário neste processo uma fonte de dados contendo os IMEI's autorizados para realização de consultas pelo aplicativo. Para este cadastro foi criado um processo de homologação de aparelhos que agrupa controles políticos, processuais, procedimentais e de estrutura organizacional:

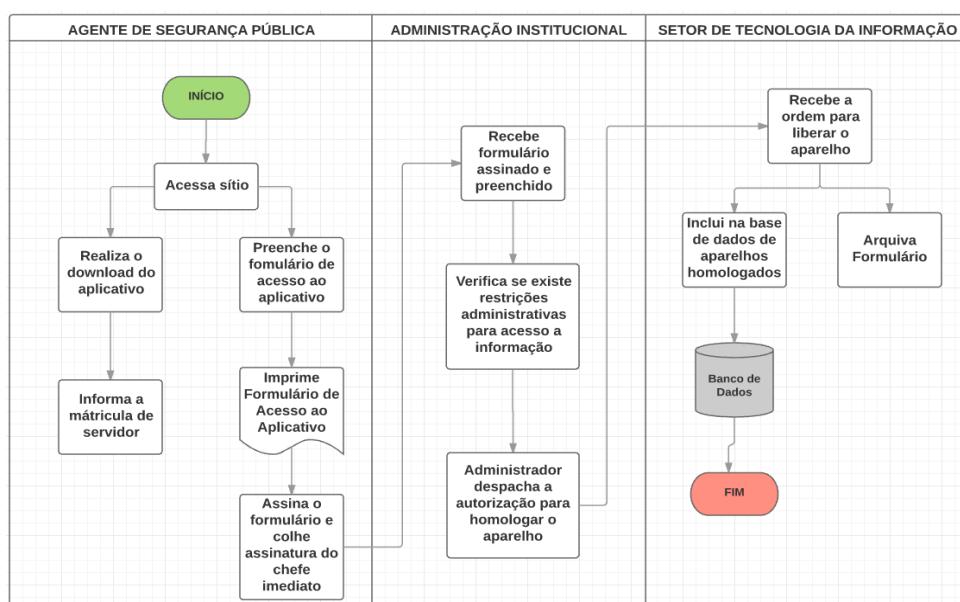


Figura 10: Fluxo de Atividades para a homologação de aparelhos.

Fonte: Elaborado pelo autor, 2016.

O fluxo apresentado pela Figura 10 contempla a inclusão da informação necessária para a autenticação dos aparelhos *smartphones* com respaldo administrativos e jurídicos.

O Formulário de acesso em anexo regulamenta a utilização do aplicativo e notifica os agentes de segurança pública das penalidades que podem ser aplicadas se os mesmos fizerem uso indevido da informação. O arquivamento dos formulários é imprescindível caso haja necessidade da realização de auditorias.

4.2.2 CRIPTOGRAFIA

A imagem 3 demonstra que as requisições de consultas e respostas podem estar sujeitas a vários nós de rede para alcançar os servidores do SIOP, então em qualquer um desses nós que a comunicação entre cliente-servidor for interceptada por terceiros estará sujeita a visualização, porém se esta comunicação estiver criptografada ficará ilegível para o interceptador.

Para conseguir criptografar a comunicação entre cliente e servidor foi criado um certificado auto-assinado que fica restrito apenas ao setor de tecnologia de informação. A criação do certificado digital é uma alternativa para o desenvolvimento de testes de aplicações. O certificado auto-assinado produz a criptografia da informação, porém não é reconhecido por qualquer Autoridade Certificadora.

No anexo I (Passos para a criação de um certificado autoassinado) é demonstrada uma alternativa para a criação do certificado auto assinado que é importante para a produção de testes de criptográfica.

4.3 SERVIDOR WEBSERVICE

Para obter os dados referentes a veículos e condutores é necessário realizar uma consulta em uma base de dados oficiais que respaldem a ação dos agentes de segurança pública em suas ações. Neste estudo foi realizado um convênio com o DETRAN do estado do Tocantins que ofereceu uma interface webservice do tipo SOAP para comunicação.

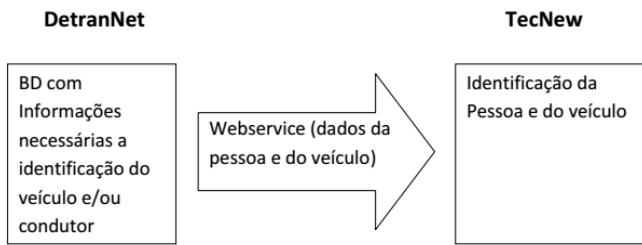


Figura 11: Conceito do webservice do DETRAN-TO.

Fonte: Elaborado pelo autor, 2016.

A documentação do WEBSERVICE do DETRAN oferece informações para conexão com o serviço e a especificação dos métodos: Consulta Veículo e Consulta Condutor, conforme o conceito da Figura 11, que serão necessários para a finalidade deste projeto.

- **Consulta informações de um veículo**
 - ✓ Nome do Serviço: `ConsultaVeiculo`
 - ✓ Tipo de Entrada: string (Placa ou Renavam)
 - ✓ Tipo de Saída: XML
 - ✓ Retorno:

```

<?xml version="1.0" encoding="utf-8" ?>
<NewDataSet>
<Table xmlns="http://wsto.detran.to.gov.br">
<Error></Error>
<Renavam>00600005046</Renavam>
<Chassi>9BGT0000STT00005</Chassi>
<Placa>NTT0010</Placa>
<Marca>GM/MONZA SL/E</Marca>
<Cor>GRENA</Cor>
<TipoVeiculo>AUTOMOVEL</TipoVeiculo>
<Especie>PASSAGEIRO</Especie>
<Categoria>PARTICULAR</Categoria>
<AnoFabricacao>1995</AnoFabricacao>
<AnoModelo>1995</AnoModelo>
<PlacaUf>TO</PlacaUf>
<NomeLocal>PALMAS</NomeLocal>
<NomeProprietario>CARLOS AGUILAR JUNIOR TESTE</NomeProprietario>
<NomeRestricao1>SEM RESTRIÇÃO</NomeRestricao1>
<NomeRestricao2>SEM RESTRIÇÃO</NomeRestricao2>
<NomeRestricao3>SEM RESTRIÇÃO</NomeRestricao3>
<NomeRestricao4>SEM RESTRIÇÃO</NomeRestricao4>
<TotalDebitoLicenciamiento>0.00</TotalDebitoLicenciamiento>
<TotalDebitoIPVA>0.00</TotalDebitoIPVA>
<TotalDebitoDPVAT>0.00</TotalDebitoDPVAT>
<TotalDebitoMultas>0.00</TotalDebitoMultas>
<TotalDebitoOutros>0.00</TotalDebitoOutros>
<DataUltimaAtualizacao>30/10/2012</DataUltimaAtualizacao>
</Table>
</NewDataSet>

```

Figura 12: Especificação da Consulta de Veículos no DETRAN-TO via Webservice. (Dados Fictícios)

Fonte: Elaborado pelo autor, 2016.

A consulta de veículos pelo Webservice do Detran, conforme a Figura 12, fornece todas as informações que poderiam ser obtidas na comunicação via rádio.

- Consulta informações de um Condutor
 - ✓ Nome do Serviço: ConsultaCondutor
 - ✓ Tipo de Entrada: String (CPF)
 - ✓ Tipo de Saída: XML
 - ✓ Retorno:

```
<?xml version="1.0" encoding="utf-8" ?>
<NewDataSet>
<Table xmlns="http://wsto.detran.to.gov.br">
<outNome>EUGENIA ALVES VIEIRA</outNome>
<outDocumentoIdentidadeNumero>702886</outDocumentoIdentidadeNumero>
<outDocumentoIdentidadeOrgaoEmissor>SSP</outDocumentoIdentidadeOrgaoEmissor>
<outDocumentoIdentidadeUF>TO</outDocumentoIdentidadeUF>
<outCPF>02991149108</outCPF>
<Categoria>AB</Categoria>
<outEnderecoLogradouro>407 NORTE ALAMEDA 12</outEnderecoLogradouro>
<Numero>20</Numero>
<Complemento>PLANO DIRETOR NORTE</Complemento>
<outEnderecoBairro>PLANO DIRETOR NORTE</outEnderecoBairro>
<MunicipioEndereco>PALMAS</MunicipioEndereco>
<outEnderecoCEP>77001546</outEnderecoCEP>
<UFEndereco>TO</UFEndereco>
<DataNascimento>19890728</DataNascimento>
<MunicipioNascimento>TOCANTINOPOLIS</MunicipioNascimento>
<UFNascimento>TO</UFNascimento>
<Sexo>2</Sexo>
<outNomeMae>REGINA ALVES VIEIRA</outNomeMae>
<Validade xml:space="preserve"></Validade>
<Observacoes xml:space="preserve"></Observacoes>
<Pontos>0</Pontos>
</Table>
</NewDataSet>
```

Figura 13: Especificação da Consulta de Condutores no DETRAN-TO via Webservice. (Dados Fictícios)

Fonte: Elaborado pelo autor, 2016.

A consulta de condutores pelo Webservice do Detran conforme a Figura 13 fornece todas as informações que poderiam ser obtidas na comunicação via rádio.

Identificadas as tecnologias Webservices envolvidas neste processo é importante definir como será o fluxo de atividades nas consultas pelas aplicações móveis, afim de subsidiar a modelagem de classes e de banco de dados necessários para a implementação da ferramenta.

4.4 MODELAGEM DA SOLUÇÃO

A estruturação do conceito da ferramenta leva em consideração todos os requisitos e decisões tomados até o momento. Aspectos de segurança e tecnológicos são primordiais para boa qualidade do software e para obtenção dos resultados esperados.

4.4.1 MODELO CONCEITUAL

A modelagem conceitual ordena as interações entre os entes da solução e configura um conceito que serve de artefato para a modelagem de classes, telas e de banco de dados.

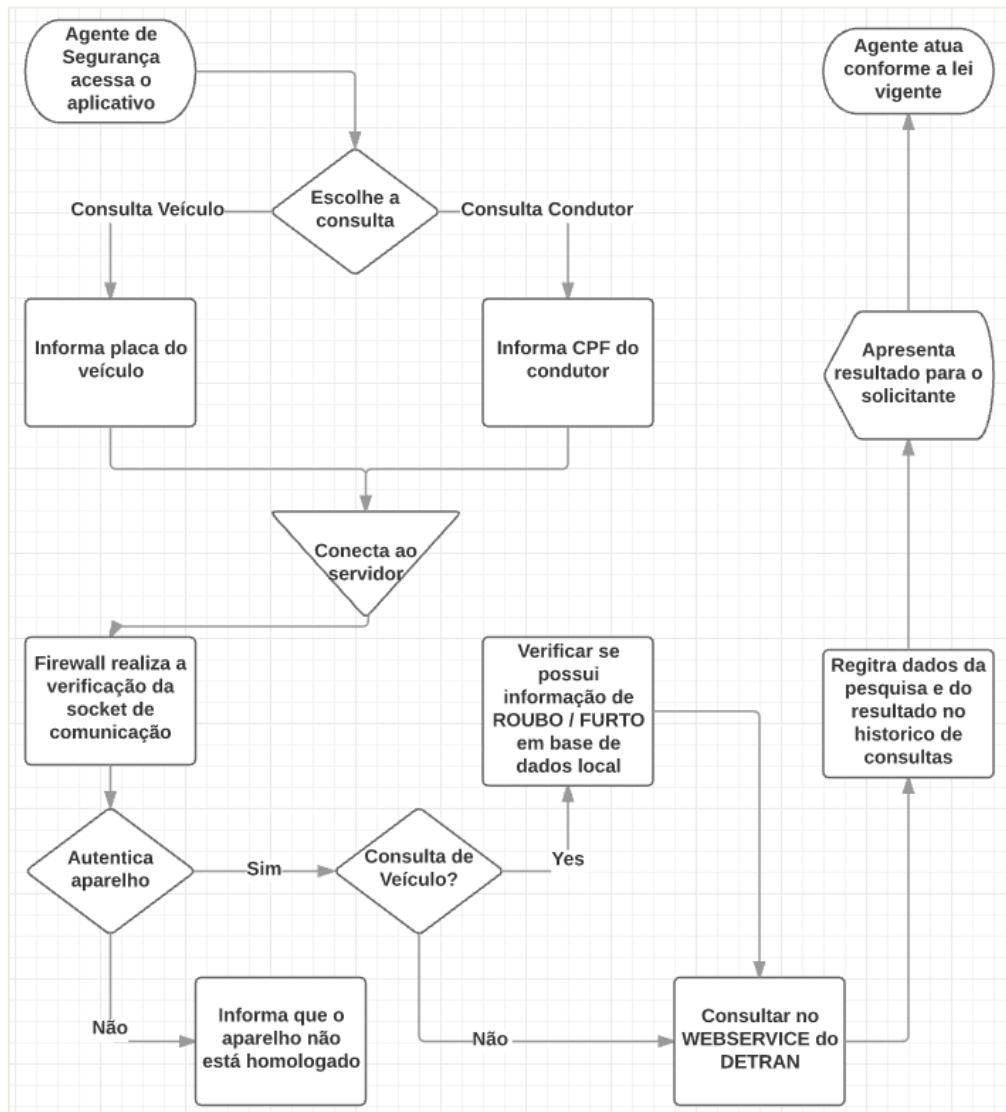


Imagen 9: Modelagem conceitual da solução.

A modelagem apresentada pode sofrer alterações durante o desenvolvimento da aplicação sendo otimizada ou ganhando novos recursos.

4.4.2 MODELAGEM DE TELAS

A usabilidade do sistema é importante para a experiência do usuário com o aplicativo. Considerando que o aplicativo Sinesp Cidadão possui uma adesão considerável entre o mesmo público alvo abordado neste estudo, servirá para a base de construção da navegação entre as telas do aplicativo.



Imagen 10: Modelagem de telas para consulta de veículos.

Fonte: Elaborado pelo autor, 2016.

A rotina de consulta de veículos necessita a entrada da placa do veículo, após o usuário submeter a tela 02 o sistema suprime o botão de pesquisa para evitar que o usuário submeta novamente a uma segunda consulta antes de retornar o resultado da primeira que foi realizada, congestionando a operação. A tela 03 é exibida com o componente *ProgressDialog* que demonstra ao usuário que uma ação ocorre no background do aplicativo e que a aplicação não está parada ou travada. Como se tratará muitas vezes de conexão de internet de dados móveis fica convencionado para este estudo que o aplicativo realizará 3 tentativas com o servidor remoto automaticamente.

A requisição à consulta pode não ser completada por diversos impedimentos técnicos ou administrativos. Entre eles são:

- Falha na comunicação com o servidor do SIOP;
- Falha na comunicação com o servidor do DETRAN;
- Falha na conexão com o banco de dados;

- d) Aparelho não cadastrado para realizar consultas;
- e) Aparelho bloqueado para realização de consultas.

As possibilidades de erros são retornadas para o usuário que será motivado a aguardar ou a entrar em contato com o suporte de TI para solução do problema. O erro é apresentado na tela 05 que possibilitará que o agente realize uma nova tentativa com o mesmo valor de entrada da tela 02.



Imagem 11: Modelagem de telas para consulta de condutores.

Fonte: Elaborado pelo autor, 2016.

A rotina para consulta de condutores necessita da entrada do CPF do condutor do veículo. Esta funcionalidade possui a mesma metodologia que a consulta de veículos. Esta requisição possui as mesmas possibilidades de erros e gerenciamento de exceções do qual foi apresentado para a consulta de veículos. Entretanto a entrada pelo CPF deve ser submetida a uma validação na regra de negócio da aplicação móvel visto que utilizar servidores remotos para esta verificação poderá comprometer o tempo de resposta desejado para a operação.

4.4.3 MODELAGEM DE CLASSES

A modelagem de classes deve atender os requisitos levantados neste estudo e construir a ideia do mecanismo lógico para a obtenção dos resultados esperados,

este estudo conceituará a modelagem de classes de dois sistemas necessários para a realização de consultas pelos aparelhos móveis a partir de um servidor webservice.

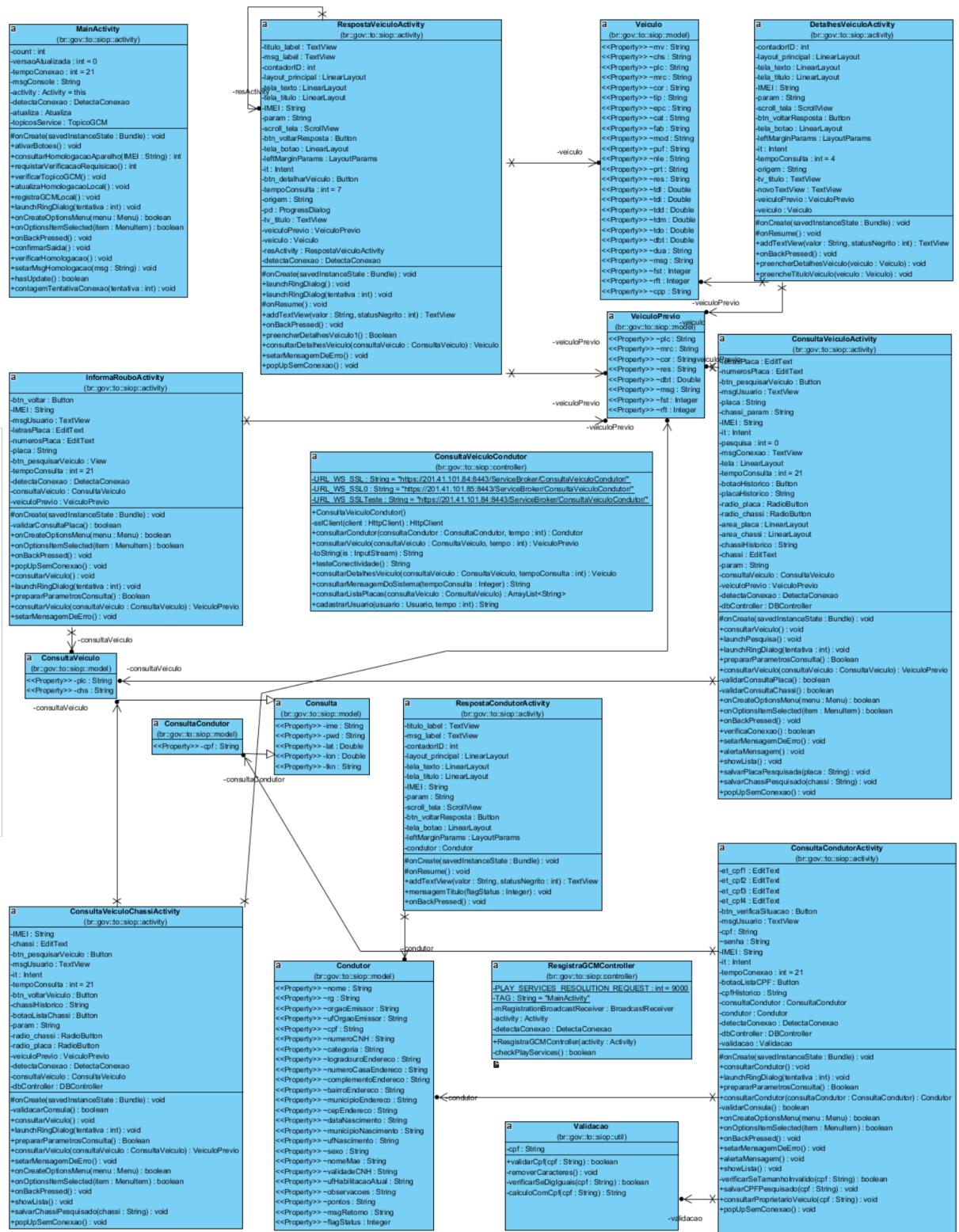


Imagen 11: Modelagem de classes do aplicativo móvel.

Fonte: Elaborado pelo autor, 2016.

A modelagem acima especifica rotinas fundamentais para a formatação da regra de negócio necessária para a comunicação com o servidor webservice REST.

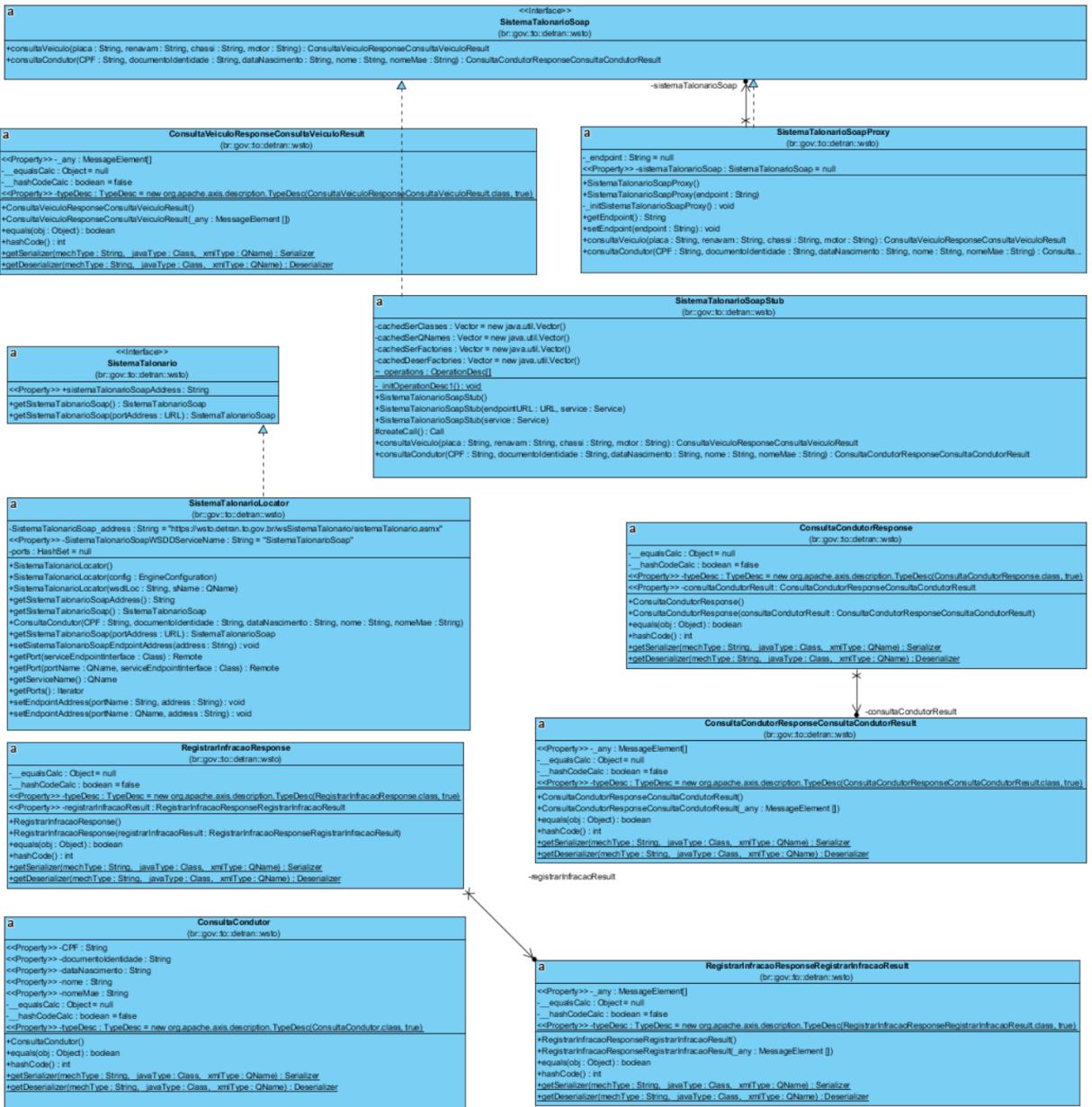


Imagen 12: Modelagem de classes do para conexão com o DETRAN -TO.

Fonte: Elaborado pelo autor, 2016.

A imagem 12 especifica a estrutura que pode realizar as consultas no webservice SOAP do DETRAN-TO, nesta modelagem o sistema requisita para uma fonte de dados oficial as informações que serão transmitidas ao solicitante da informação.

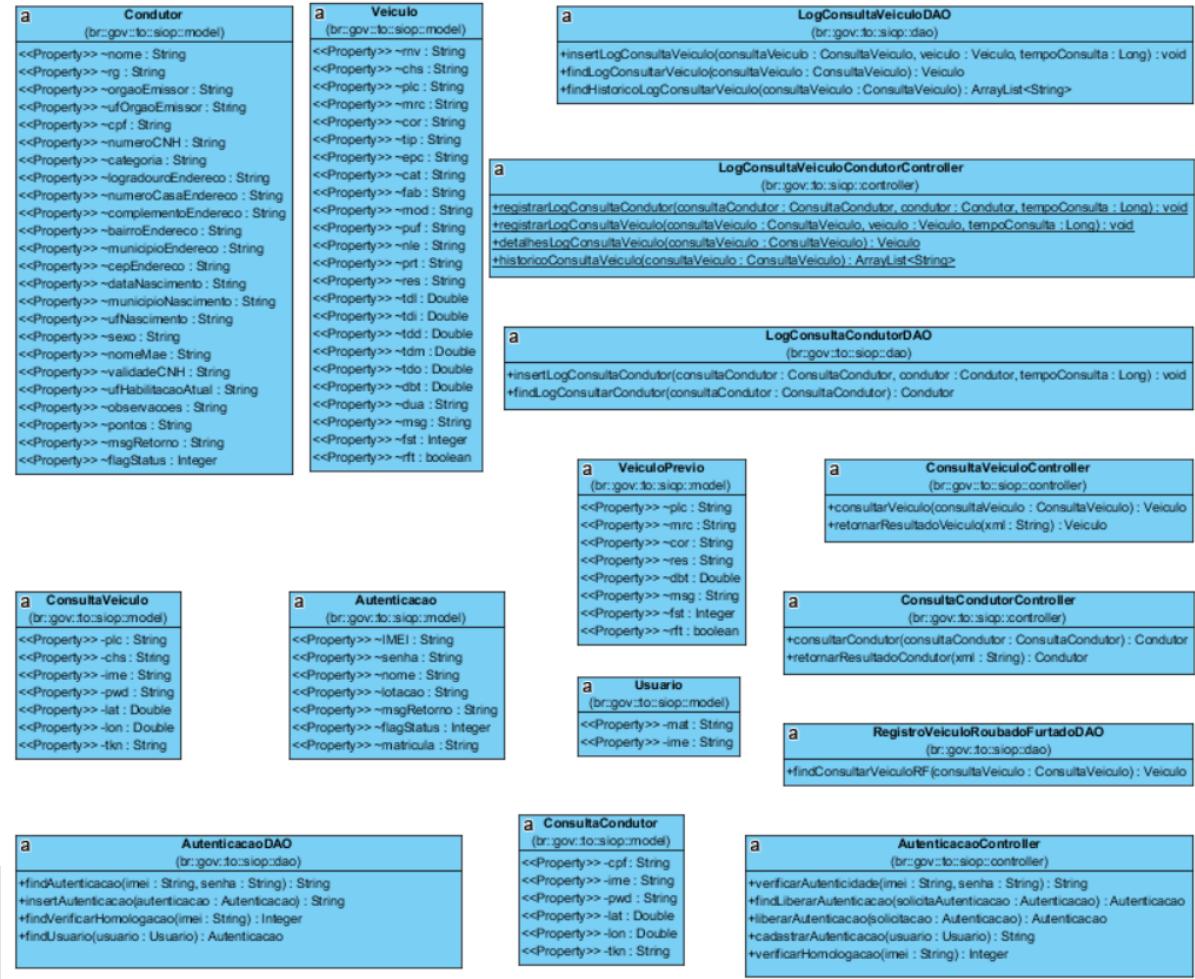


Imagen 13: Modelagem de classes do para conexão com o DETRAN -TO.

Fonte: Elaborado pelo autor, 2016.

A modelagem acima demonstra como será feito o intermédio da comunicação entre o servidor do DETRAN e a aplicação móvel, elencando fatores de verificação de homologação, cadastro de logs, consultas de condutores de veículos e condutores entre outros métodos.

As modelagens de classes exibidas nesta seção demonstram apenas as classes de maior importância técnica sendo suprimidas classes que são utilizadas para tarefas básicas como as utilizadas para conexão com o banco de dados.

4.4.4 MODELAGEM DE BANCO DE DADOS

A persistência de dados é fundamental para o processo de homologação, consultas e auditoria. A modelagem do banco de dados para este projeto atendeu a execução dos seguintes requisitos funcionais:

- a) Verificar se determinado IMEI está homologado para realizar consultas no aplicativo.
- b) Verificar status do IMEI. Pois eventualmente pode ter alguma restrição administrativa que impeça a realização de consultas.
- c) Buscar o histórico de consultas e seus respectivos resultados que determinado aparelho ou que determinado agente de segurança pública tenha praticado.
- d) Buscar a frequência de horários, dias ou meses referentes a utilização da solução.
- e) Considerar que o aparelho homologado pode ser em outro momento homologado para outro agente de segurança, considerando as relações comerciais existentes.

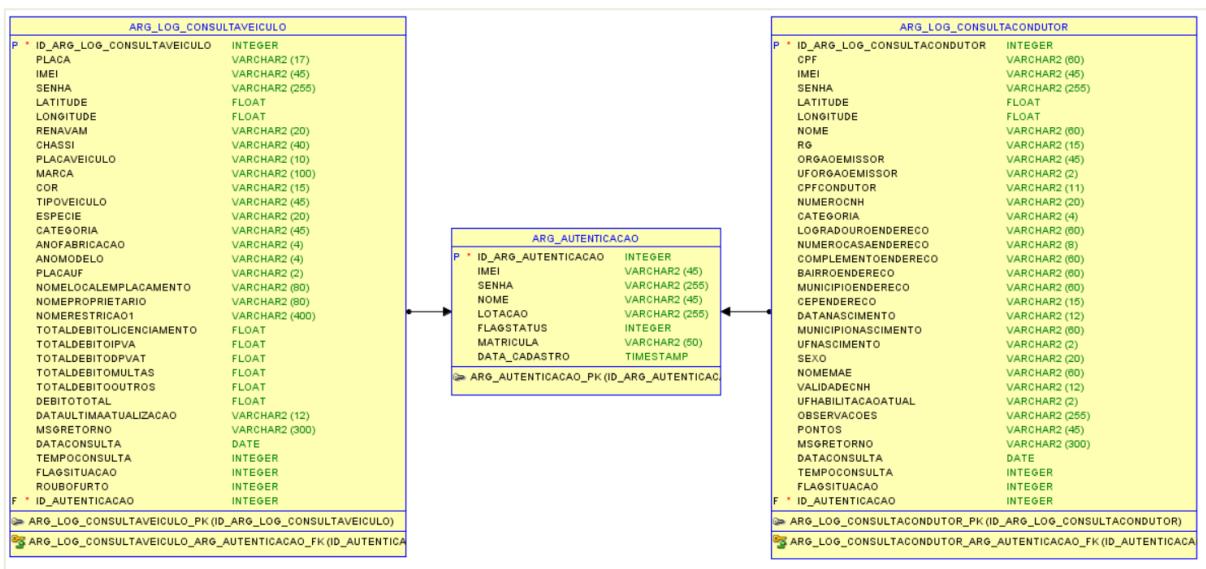


Imagen 12 Modelagem de banco de dados para a consulta de condutores.

Fonte: Elaborado pelo autor, 2016.

A imagem 12 reflete a uma modelagem simples e relacional que elenca todos os requisitos necessários para a estruturação de dados da solução. Para ser possível mensurar o tempo de resposta nas consultas com o DETRAN foi criada a coluna TEMPOCONSULTA que armazenará um dado importante para o estudo de gargalos na comunicação.

Para a coluna STATUS na tabela ARG_AUTENTICACAO que armazena todos os aparelhos homologados, foi convencionado o seguinte dicionário de dados:

- 0) Inativo;
- 1) Ativo.

Para a coluna FLAGSIITUACAO na tabela ARG_ARG_LOG_CONSULTACONDUTOR que armazena todas as consultas de condutores realizadas, foi convencionado o seguinte dicionário de dados:

- 0) CNH regular;
- 1) CNH irregular.

Para a coluna FLAGSIITUACAO na tabela ARG_ARG_LOG_CONSULTAVEICULO que armazena todas as consultas de veículos realizadas, foi convencionado o seguinte dicionário de dados:

- 0) Regular, não consta débitos e não possui restrições;
- 1) Irregular, possui débitos de Licenciamento/IPVA/DPVAT;
- 2) Restrição administrativa no veículo;
- 3) Possui a situação 1 e 2.

A adoção de dicionários contribui para a economia de tráfego na pesquisa. O aplicativo interpretará a codificação na mensagem de retorno e aplicará a convenção do dicionário para exibição ao usuário.

4.5 INSTALAÇÃO DO CERTIFICADO DIGITAL AUTO-ASSINADO NO SERVIDOR

Após a codificação da aplicação com base na regra de negócio modelada nas seções anteriores é necessária a instalação do certificado digital no servidor, esse processo irá garantir a criptografia das informações trafegadas e proporcionará maior segurança nos processos, os passos para a aplicação do certificado que foi criado na seção 4.1.2 são:

- 1) Localiza o arquivo web.xml na estrutura de pastas do projeto da aplicação webservice e abrir para a edição.

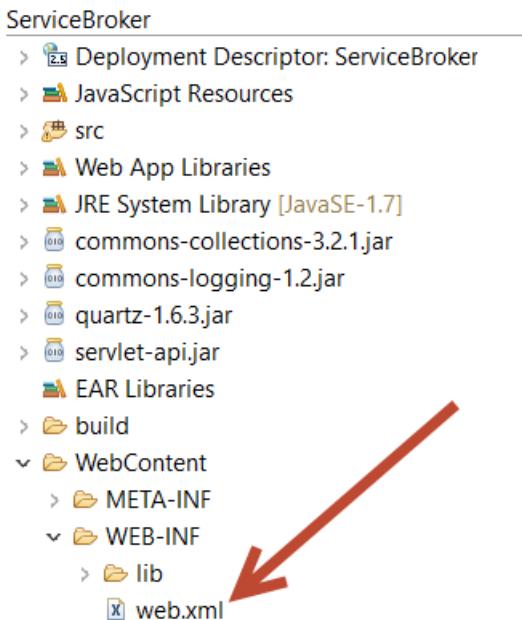


Imagen 13 Estrutura de pasta do ServiceBroker.

Fonte: Elaborado pelo autor, 2016.

No caso do desenvolvimento na IDE Eclipse o caminho padrão do arquivo é /WebContent/WEB-INF/web.xml.

2) Editar o arquivo web.xml e inserir o trecho abaixo:

```
<security-constraint>
    <web-resource-collection>
        <web-resource-name>securedapp</web-resource-name>
        <url-pattern>/*</url-pattern>
    </web-resource-collection>
    <user-data-constraint>
        <transport-guarantee>CONFIDENTIAL</transport-guarantee>
    </user-data-constraint>
</security-constraint>
```

Imagen 13 Trecho de configuração da aplicação webservice.

Fonte: Elaborado pelo autor, 2016.

O trecho acima deve ser incluído na tag <web-app>. Sua inclusão informa para o servidor de aplicação web que o tráfego de comunicação do projeto será oferecido pelo protocolo HTTPS e não mais pelo protocolo HTTP.

3) O arquivo server.xml presente no projeto do servidor deve ser editado para que o servidor de aplicação utilize o certificado que foi criado

anteriormente. É necessário informar em suas configurações os seguintes parâmetros:

```
<Connector SSLEnabled="true" acceptCount="100" clientAuth="false"
    disableUploadTimeout="true" enableLookups="false" maxThreads="25"
    port="8443" keystoreFile="C:\certificado\siop.jks" keystorePass="████████"
    protocol="org.apache.coyote.http11.Http11NioProtocol" scheme="https"
    secure="true" sslProtocol="TLS" />
```

Imagen 14 Trecho de configuração do arquivo server.xml.

Fonte: Elaborado pelo autor, 2016.

Após esta configuração a execução do projeto será redirecionada para o protocolo HTTPS.

4.6 O PROBLEMAS ENCONTRADOS

Após o lançamento da versão beta para utilização do aplicativo pelos agentes de segurança pública foram realizadas entrevistas por amostragem para conhecer a experiência do usuário perante as dificuldades, a qualidade do resultado e o tempo de resposta.

As principais queixas existentes na utilização da versão beta era o tempo de resposta na busca de informações de veículos.

Como a modelagem já previa a inserção do tempo de resposta na consulta entre SIOP e DETRAN, foi realizado nas 2.369 consultas á veículos e nas 1.815 consultas realizadas á condutores o cálculo da média do tempo de resposta e obtemos a marca de 1.7 segundos e 2.1 segundos respectivamente, levando a descartar a comunicação entre o SIOP e o DETRAN como gargalo na consulta, visto que não havia demora excessiva na requisição entre os dois órgãos.

Considerando que a rede móvel de dados contribui para o atraso da informação foram tomadas as seguintes medidas afim de otimizar o tempo de resposta da consulta de veículos:

- 1) Criação de uma tela intermediária de resposta que traz o resumo da situação do veículo contendo as seguintes informações: marca,

modelo, ano, cor e situação. A prévia desta consulta retorna um arquivo menor que a consulta integral, permitindo que o agente tome a decisão de buscar os dados analíticos clicando em “Buscar Detalhes” ou se satisfaça apenas com os dados já retornados.

- 2) Diminuição dos cabeçalhos dos dados retornados:

```
public class Veiculo {  
    String rnv;//renavam;  
    String chs;//chassi;  
    String plc;//placa;  
    String mrc;//marca;  
    String cor;  
    String tip;//tipoVeiculo;  
    String epc;//especie;  
    String cat;//categoria;  
    String fab;//anoFabricacao;  
    String mod;//anoModelo;  
    String puf;//placaUF;  
    String nle;//nomeLocalEmplacamento;  
    String prt;//nomeProprietario;  
    String res;//Restricao 1,2,3,4;  
    Double tdl;//totalDebitoLicenciamento;  
    Double tdi;//totalDebitoIPVA;  
    Double tdd;//totalDebitoDPVAT;  
    Double tdm;//totalDebitoMultas;  
    Double tdo;//totalDebitoOutros;  
    Double dbt;//debitoTotal;  
    String dua;//DataUltimaAtualizacao;  
    String msg;//msgRetorno;  
    Integer fst;//flagSituacao;  
    boolean rft;//rouboFurto
```

Imagen 15 Parte do código-fonte da classe Veículo.

Fonte: Elaborado pelo autor, 2016.

Com a refatoração dos atributos para o limite de 03 (três) letras a classe Veículo que é produzida para encapsular a mensagem de retorno fica consideravelmente menor, convencionado um dicionário de dados para a transação.

5 DIFICULDADES

A maior dificuldade encontrada foi a realização de convênio com o Departamento Estadual de Trânsito, DETRAN que precisou criar um webservice para viabilizar a consulta a uma fonte de dados oficiais. Os argumentos para o

deferimento do convênio foram o combate à criminalidade do estado e o aumento de arrecadação com os impostos visto que com a facilidade na busca da informação o agente de segurança pública vai atuar em maior volume.

6 RESULTADOS

Após o lançamento desta solução o aplicativo teve um total de 954 aparelhos homologados e realizou 73.785 consultas de veículos e condutores, identificando 234 veículos roubados nos primeiros 30 dias.

A consulta pelo aplicativo dura em média 4,5 segundos frente ao mínimo de 3 minutos de espera na consulta via rádio que era utilizada tradicionalmente pelos agentes de segurança pública.

O número de consultas aumentou mais de 1.770% diante a facilidade ao acesso da informação possibilitando consequentemente maior arrecadação e maior ações ao combate ao furto e roubo de veículos.

A utilização do aplicativo é feita com ônus integral ao agente de segurança pública justificada pela facilidade no acesso a informação. A mudança na cultura foi aceita pelos agentes que se adequaram ao processo rígido de homologação de aparelhos pessoais em busca da melhoria na qualidade individual de trabalho.

A qualidade da conexão de dados móveis é determinante para o sucesso de qualquer aplicativo móvel que necessite consultar dados em uma base de dados remota para a tomada de decisão em curto espaço de tempo. São necessárias ações de otimização para diminuir o volume de dados trafegados.

A consulta realizada pelo rádio não é mais frequente, sendo utilizada apenas em casos que o agente não dispõe de internet móvel ou de celular para realização da pesquisa pelo aplicativo.

5. SUGESTÕES PARA TRABALHOS FUTUROS

O aplicativo trabalhado neste estudo foi visto como canal de comunicação entre os agentes de segurança e o centro de comando de operações. A adesão de 90% de agentes ao aplicativo é considerada plenamente possível pelas expectativas. Portanto para não subutilizar esse canal de comunicação foi idealizada uma integração entre um sistema legado de registro de roubos e furto de veículos para que a partir da inclusão do registro todos os agentes recebessem um alerta com o detalhe do fato para que, de folga ou de serviço, pudessem contribuir para a localização do veículo roubado.

Como sugestão, um trabalho científico que estudasse boas práticas para viabilizar este serviço será de grande valor intelectual para os órgãos de segurança pública que se preocupam com o tempo de resposta ao cidadão.

6. CONCLUSÃO

É inevitável a adesão dos órgãos de segurança pública às ferramentas portáteis que flexibilizam suas ações operacionais e que integram a informação de maneira dinâmica e aproveitável.

A integração entre diferentes autarquias de governo não é tecnicamente um desafio que requer uma complexibilidade tecnológica e que seja exclusivamente praticada por empresas terceirizadas. O acesso público às tecnologias de hoje possibilita que um projeto como o que foi exposto neste estudo seja executado pelo funcionalismo público direto, garantindo melhor continuidade e manutenção do projeto. A integração entre autarquias está aliada ao consentimento dos gestores de pastas que definem o plano de governo que será adotado.

O uso de aplicativos móveis para apoio às ações de agentes de segurança pública traz benefícios que agrupa qualidade, velocidade e dinâmica em inúmeras frentes de serviço.

Na concepção inicial do escopo da solução foi vislumbrado apenas ações na fiscalização e ao combate ao furto e roubo de veículo, porém com a adesão em massa dos agentes de segurança surgiu a aplicabilidade em ações investigativas e de diligências policiais.

Uma nova era se inicia e a tecnologia é uma aliada que será utilizada tanto para o bem quanto para o mal.

REFERÊNCIAS

SILVA, Luiz Gustavo Cordeiro et al. Certificação Digital: Conceitos e Aplicações, Rio de Janeiro: Editora Ciência Moderna Ltda., 2008.

RESENDE, Dilma A. Artigo: CERTIFICAÇÃO DIGITAL, Revista Jurídica UNIGRAN V. 11 N. 22 Jul/Dez 2009

AMADEU, Sergio. Artigo: Certificação Digital, Criptografia e Privacidade. UNESCO,2004.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002:2005:

Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da Segurança da Informação. Rio de Janeiro: ABNT, 2005, 120p.

TANENBAUM, Andrew S. Redes de computadores. 4.ed. Campus,2003.

OLIVEIRA, Régis Fernandes de HORVATH, Estevão; e TAMBASCO, Teresa Cristina Castrucci. Manual de Direito Financeiro, São Paulo, Editora Revista dos Tribunais, 1990, p. 94.

REZENDE, Fernandes. Finanças Públicas, São Paulo, Atlas, 1980, pp. 111/112.
TORRES, Ricardo Lobo. “O Tribunal de Contas e o controle da legalidade, economicidade e legitimidade”. Rio de Janeiro, Revista do TCE/RJ, nº 22, jul/1991, pp. 37/44.

(4) Fundação opina sobre conceitos de economicidade e operacionalidade, revista do TCE/MT, nº 10, ago/1989, pp. 49/58.

TRAIN, Sheila. Identidade Digital. 1ª Edição – Especial FENACON, 2005

Kushchu, Kuscu H. M. “From e-Government to m-Government :Facing the Inevitable.” , 2003.

GARGENTA,Marko. Learning Android. Sebastopol: O'Reilly, 2011.

MILANI, André. Programando para iPhone e iPad. Novatec, 2012.

MÔNACO, Thiago e CARMO, Rodolpho Marques. Desenvolvendo Aplicações para Windows Phone. Brasport, 2012.

<http://www.idc.com/prodserv/smartphone-os-market-share.jsp>

<http://techcrunch.com/2014/05/06/android-still-growing-market-share-by-winning-first-time-smartphone-users/>

<http://www.businessinsider.com/iphone-v-android-market-share-2014-5>

Fling, Brian. Mobile Design and Development. Sebastopol: O'Reilly, 2009.

ALLAZO, Edwar Andres Velarde; SABLÓN, Vicente Idalberto Becerra Sablón; IANO, Yuzo. Aplicações Governamentais para TV Digital Móvel usando Ginga NCL. In: Revista de Radiodifusão, v. 3, n. 03, Setembro de 2009. Disponível em: <<http://www.set.com.br/revistaelectronica/radiodifusao/index.php/revistaderadiodifusaose/t/article/view/17/18>>. Acesso em: 29 abr. 2012.

MARTINS, Wolney Mendes. Classificação das atividades de governo eletrônico e as oportunidades de aperfeiçoamento das relações sociedade/Estado. In Ferrer e Santos orgs. E-goverment: o governo eletrônico no Brasil. São Paulo: Saraiva, 2004

Kettl, D. F. (2000): The Global Public Management Revolution, Brookings.

BRASIL, Constituição da República Federativa do Brasil/ colaboração de Antônio Luiz de Toledo Pinto e Márcia Cristina Vaz dos Santos Windt. São Paulo: Saraiva, 2000. 22^a ed.

http://www.anatel.gov.br/institucional/index.php?option=com_content&view=article&id=717

DI PIETRO. Maria Sílvia Zanella. **Direito Administrativo**. 11.ed. São Paulo: Atlas, 1999.

<https://developer.apple.com>

Albinader Neto, et al. (2006), Web Services em Java, Rio de Janeiro, Brasport.

http://www.teleco.com.br/sist_operacional.asp Acesso em 12/07/2015

Tecmundo: iOS, Android e Windows Phone: números dos gigantes comparados [infográfico] (2014) Disponível em:
<http://www.tecmundo.com.br/sistema-operacional/60596-ios-android-windows-phone-numeros-gigantes-comparados-infografico.htm>

[http://web.unipar.br/~seinpar/2014/artigos/pos/Cleber_de_F_Ferreira_Roberto_Dias_Mota%20\(1\).pdf](http://web.unipar.br/~seinpar/2014/artigos/pos/Cleber_de_F_Ferreira_Roberto_Dias_Mota%20(1).pdf) 2014

SECURE ELECTRONIC TRANSACTIONS BETWEEN A MOBILE DEVICE AND OTHER MOBILE, FIXED, or VIRTUAL DEVICES <https://www.google.com/patents/US20070011099> 2007, [Conrad Sheehan](#)

<https://tomcat.apache.org/tomcat-3.3-doc/tomcat-ssl-howto.html>

(<https://www.sinesp.gov.br/sinesp-cidadao>)

Pereira, Lúcio Camilo Oliva
Android para desenvolvedores / Lúcio Camilo Oliva Pereira, Michel Lourenço da Silva. -- Rio de Janeiro : Brasport, 2009.

ISBN 978-85-7452-405-4

1. **Android (Programa de computador)** 2. Aplicação de programa - Desenvolvimento 3. Computação móvel 4. Google 5. Internet sem fio 6. Telefones celulares I. Silva, Michel Lourenço da. II. Título.

09-06309

CDD-005.26



Formulário de Acesso ao Aplicativo
SIOP
PROTOCOLO: 65827

Código de Barras



Orgão Vinculado: POLÍCIA MILITAR	Unidade Lotação: SIOP	
Nome do Solicitante: BRUNNO SALES CUNHA		
Data de Nascimento: 30/03/1984		
Área de Atuação: <input checked="" type="checkbox"/> Operacional <input checked="" type="checkbox"/> Administrativo <input type="checkbox"/> Fiscalização de Trânsito		
CPF: 006.888.211-46	Cargo/Função: ANALISTA DE SISTEMAS	
Matrícula: 85125		
E-mail: TI.BRUNNO@GMAIL.COM		
Celular: (63) 8117-8838		
IMEI Autorizado (Para descobrir o IMEI disque *#06#):		
IMEI 1 351755078028665	IMEI 2 - Deixar em branco caso não possua 351755078028663	IMEI 3 - Deixar em branco caso não possua

• Para homologação do seu aparelho é necessário o envio deste formulário juntamente com cópia do RG funcional para o SIOP.

O usuário autorizado e homologado no Sistema Integrado de Operações (SIOP) deverá:

- Utilizar as informações disponíveis no SIOP somente nas atividades a que compete exercer, não podendo transferi-las a terceiros, seja a título oneroso ou gratuito, sendo monitoradas e acompanhadas suas consultas ao sistema do SIOP;
- Guardar o sigilo e a privacidade da informação, sendo responsável pelo uso indevido das informações constantes nos módulos do SIOP, sujeito às normas legais;
- Havendo troca, perda, extravio do aparelho portador do IMEI autorizado por este documento, o servidor deverá informar imediatamente a administração do SIOP para o bloqueio do referido aparelho.

O usuário incorre nos crimes descritos no Código Penal Brasileiro, sem prejuízo das sanções civis e administrativas pelo uso ou divulgações indevida das informações:

- Art. 153 - Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem: Pena - detenção, de 1 a 6 meses, ou multa. § 1º. A divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em Lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública: Pena - detenção de 1(um) a 4(quatro) anos e multa.
- Art. 299 - Omitir, em documento público ou particular, declaração que dele deva constituir, ou nele inserir, fazer inserir declaração falsa ou diversa da que deva ser escrita, com fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante. Pena - Reclusão de 01 (um) a 05 (cinco) anos e multa se o documento é público, e reclusão de 01 (um) a 03 (três) anos e multa se o documento é particular. Parágrafo único - Se o agente é funcionário público e comete o crime prevalecendo-se do cargo ou se a falsificação ou alteração é de assentamento de registro civil, aumenta-se a pena da sexta parte.
- Art. 313-A Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou banco de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: Pena - reclusão de 2 (dois) a 12 (doze) anos e multa.
- Art. 313-B. Modificar ou alterar, o funcionário, sistema de informação ou programa de informática sem autorização ou solicitação de autoria competente: Pena - detenção de 3(três) meses a 2(dois) anos e multa. Parágrafo único: As penas são aumentadas de um terço até a metade se a modificação ou alteração resulta dano para a Administração Pública ou para o administrado.
- Art. 325 - Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação: Pena: detenção, de seis meses a dois anos, ou multa, se o fato não constitui crime mais grave.

§ 1º - Nas mesmas penas deste artigo incorre quem: I - permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública; II - se utiliza, indevidamente, do acesso restrito.

§ 2º - Se da ação ou omissão resulta dano à Administração Pública ou a outrem: Pena - reclusão, de 2 (dois) a 6 (seis) anos, e multa.

- Art. 327 - Considera-se funcionário público para os efeitos penais, quem, embora transitoriamente ou sem remuneração, exerce cargo, emprego ou função pública.

§ 1º - Equipa-se a funcionário público quem exerce cargo, emprego ou função em entidade paraestatal, e quem trabalha para empresa prestadora de serviço contratada ou conveniada para execução de atividade típica da Administração Pública.

§ 2º - A pena será aumentada da terça parte quando os autores dos crimes previstos neste capítulo forem ocupantes de cargos em comissão ou de função de direção ou assessoramento de órgão da administração direta, sociedade de economia mista, empresa pública ou fundação instituída pelo poder público.

Ao assinar declaro, sob as penas da lei, verdadeiras as informações neste ato prestadas, compreendendo o que estabelecem os art. 153, 299, 313-a, 313-b, 325 e 327 do Código Penal Brasileiro, a legislação aplicada ao assunto e demais normas complementares do SIOP, aquiescendo com todas as responsabilidades inerentes ao uso das informações privilegiadas e de natureza de segurança pública nacional, bem como das implicações legais decorrentes do uso indevido das informações e do acesso, seja qual for à circunstância, e sujeito ao monitoramento e controle das ações realizadas no sistema SIOP.

BRUNNO SALES CUNHA	Assinatura do Chefe Imediato
--------------------	------------------------------

ANEXO I

PASSOS PARA A CRIAÇÃO DE UM CERTIFICADO AUTOASSINADO

Após a instalação do OpenSSL v1.0.2g Light Win64 os passos para criação de um certificado auto-assinado são:

- 1) Executar o OpenSSL como administrador;
- 2) Executar o comando:

```
genrsa -des3 -out ca.key 4096
```

Será gerada uma chave do tipo *rsa* de 4096 bits e armazenada no arquivo *ca.key*;

- 3) Será solicitada a digitação da chave *phrase* que deverá se memorizada, para a sua posterior utilização;
- 4) Confirmar a *phrase* digitada;
- 5) Após esses passos será criado o arquivo *ca.key* no mesmo diretório do executável do OpenSSL;
- 6) Para criar o certificado *ca.crt* do tipo x509 válido por 3650 dias que conterá a chave pública do arquivo *ca.key*, deve ser executado o seguinte comando:

```
req -new -x509 -days 3650 -key ca.key -out ca.crt
```

- 7) A senha *phrase* será solicitada para continuar;
- 8) Se a senha *phrase* for digitada corretamente o usuário deverá informar a sigla do país. Para este estudo digitamos “BR” referente ao Brasil. Outras informações são solicitadas para a criação do certificado, tais como: estado, cidade, nome da organização, nome da seção, nome do servidor ou nome do usuário que está criando e endereço de e-mail do usuário, respectivamente. Após a inclusão destes dados o certificado será criado na mesma pasta em que o OpenSSL foi instalado.

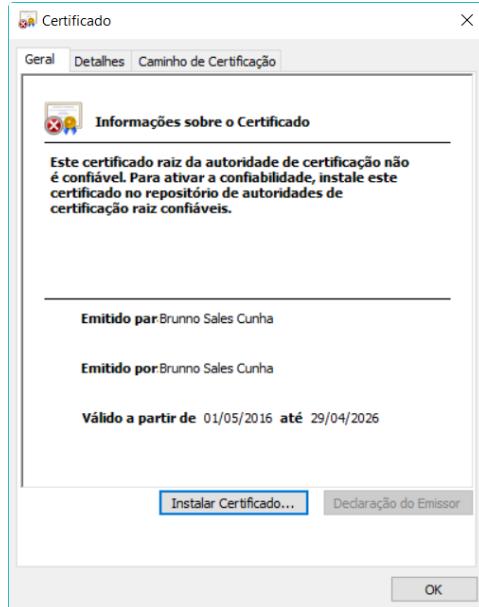


Imagen 5: Certificado Criado pelo OpenSSL.

Ao clicar duas vezes no arquivo ca.crt o usuário pode confirmar a criação do certificado com todas as informações inseridas no momento da sua geração.

- 9) Para utilizar o certificado em um servidor de serviço com a tecnologia java é aconselhável a importação do certificado .crt para .jks. Para isso o usuário pode executar o seguinte comando:

```
keytool -import -alias certificado_siop.cer -keystore  
C:\\certificado\\siop.jks -file C:\\OpenSSL-Win64\\bin\\ca.crt
```