PONTIFÍCIA UNIVERSIDADE CATÓLICA DE CAMPINAS

CENTRO DE CIÊNCIAS EXATAS, AMBIENTAIS E DE TECNOLOGIAS

SILVANA BORDINI COCA MACHADO

PROPOSTA METODOLÓGICA PARA DIVULGAÇÃO DE DADOS PRIVADOS NAS CIDADES INTELIGENTES

CAMPINAS

2016

SILVANA BORDINI COCA MACHADO

PROPOSTA METODOLÓGICA PARA DIVULGAÇÃO DE DADOS PRIVADOS NAS CIDADES INTELIGENTES

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia Elétrica do Centro de Ciências Exatas, Ambientais e de Tecnologias da Pontifícia Universidade Católica de Campinas como requisito parcial para obtenção do título de Mestre em Gest!ao de Redes de Telecomunicações.
Área de Concentração: Sistemas de Telecomunicações e Informática – Gestão de Redes e Serviços.

Orientador: Prof. Dr. David Bianchini

PUC-CAMPINAS

2016

Ficha Catalográfica

Elaborada pelo Sistema de Bibliotecas e

Informação - SBI - PUC-Campinas

t005.8
M149P

Machado, Silvana Bordini Coca.
Proposta metodológica para divulgação de dados privados nas cidades inteligentes / Silvana Bordini Coca. - Campinas: PUC-Campinas, 2016.
84P.

Orientador: David Bianchini.
Dissertação (mestrado) – Pontifícia Universidade Católica de Campinas, Centro de Ciências Exatas, Ambientais e de Tecnologias, Pós-Graduação em Gestão de Redes de Telecomunicações.
Inclui anexo e bibliografia.

1. Banco de dados - Medidas de segurança. 2. Proteção de dados. 3. Crescimento urbano. 4. Tecnologia da informação - Sistemas de segurança. 5. Direito a privacidade. I. Bianchini, David. II. Pontifícia Universidade Católica de Campinas. Centro de Ciências Exatas, Ambientais e de Tecnologias. Pós-Graduação em Gestão de Redes de Telecomunicações. III. Título.

20.ed. CDD – t005.8

Pontifícia Universidade Católica de Campinas
Centro de Ciências Exatas, Ambientais e de Tecnologias
Programa de Pós-Graduação Stricto Sensu em Engenharia Elétrica

Autor (a): Machado, Silvana Bordini Coca

Dissertação de Mestrado em Gest!ao de Redes de Telecomunicações.

BANCA EXAMINADORA

Presidente e Orientador Prof. Dr. David Bianchini

1º Examinador Prof.(a) Dr.(a) Eliane Maria Grigoletto

2º Examinador Prof.(a) Dr.(a) Lia Toledo Moreira Mota

Campinas, 28 de Novembro de 2016.

Dedico este trabalho a toda minha família, em especial à minha mãe, Apparecida Geny, um exemplo de vida e dedicação, que sempre esteve presente ao meu lado, me incentivando e possibilitando que eu tornasse meus sonhos realidade, sonhando comigo.

Ao meu marido, Carlos Fernando, companheiro e incentivador de minhas conquistas e parceiro nos desafios.

E ao meu filho, Arthur, minha grande fonte de energia e inspiração.

AGRADECIMENTOS

Ao Prof. Dr. David Bianchini,
Incentivador, guia, mestre e parceiro, sempre atento e cuidadoso na minha formação profissional e amigo sincero em todos os momentos desta empreitada.

Aos Profs. Drs. Eric Alberto de Mello Fagotto, Lia Toledo Moreira Mota, Marcelo Luís Francisco Abbade, Marcius Fabius Henriques de Carvalho e Omar Carvalho Branquinho,
Por todos os esforços e por toda dedicação oferecida aos alunos do programa de pôs-graduação, pelo exemplo de condução para a criação de valores intelectuais e pesquisas orientadas.

À Pontifícia Universidade Católica de Campinas,
Pela conceção da bolsa no Programa de Mestrado, sem o qual este trabalho não poderia ter sido concretizado.

Aos colegas e companheiros da turma,
Pelo companheirismo, apoio, solidariedade e parceria.

Á Prefeitura de Limeira,
Pela acolhida e abertura para discussão sobre o tema, participando, respondendo os diversos questionários e contribuindo com dados.

“Devemos aprender durante toda a vida, sem imaginar que a sabedoria vem com a velhice.”
(Platão)

RESUMO

MACHADO, Silvana Bordini Coca. Proposta metodológica para divulgação de dados privados nas Cidades Inteligentes. 2016. Dissertação (Mestrado em Engenharia Elétrica) - Programa de Pós-Graduação em Engenharia Elétrica, Curso de Gestão de Redes de Telecomunicações, do Centro de Ciências Exatas, Ambientais e de Tecnologias. Pontifícia Universidade Católica de Campinas. Campinas. 2016.

Segundo relatório da ONU, Organização das Nações Unidas, de 2014, pela primeira vez na história, a maior parte da população mundial está vivendo em centros urbanos. O movimento de urbanização, desde 1950 até os dias atuais, apresentou uma imigração da área rural para a urbana quase dobrando a realidade daquela época, a qual era de 30%, e até 2050, espera-se uma população urbana superior a 66%. A infra-estrutura e os serviços oferecidos deverão estar dimensionados para atender a este aumento populacional. A informação destes cidadãos, necessária para provimento de atendimentos não apenas da saúde, educação, transporte e segurança são armazenadas nos mais diversos sistemas, sem que haja obrigatoriamente uma centralização e padronização destes dados. Muitos dados caracterizam informações pessoais, como registros nacionais, endereços, que devem ser salvo-guardados adequadamente, caso contrário, podem ser uma porta para o vazamento e mal-uso dos mesmos. As tecnologias utilizadas para coleta e armazenamento dos dados podem afetar sensivelmente a vida da população surgindo então os problemas com a segurança e a privacidade de dados. A norma ISO 27001 define o tripé da segurança da informação por meio da confidencialidade, integridade e disponibilidade, buscando contextualizar a emergência das Cidades Inteligentes, que se fundamentam na oferta de serviços via infovias de comunicação e pelas quais são disponibilizadas informações a órgãos governamentais, instituições em geral e a todo cidadão. Este trabalho tem por objetivo apreender como fazer o uso adequado de dados pessoais nas instituições, perante esta ótica de proteção, ao mesmo tempo em que, principalmente, com relação aos órgãos públicos se exige transparência. Nesse contexto em que se busca transparência e agilidade por meio das tecnologias da informação e comunicação, se observará no decorrer desta pesquisa que efetivos cuidados com a confidencialidade exigem ainda maior atenção dos gestores e responsáveis pela coleta, processamento e distribuição da informação. O resultado obtido foi a proposição de uma metodologia para o tratamento de dados e informações privadas pelas instituições públicas, utilizando-se modelo de apoio a decisão *Analytical Hierachical Process* (AHP) e avaliação de subconjuntos de dados.

Palavras-chave: segurança da informação, privacidade, AHP, confidencialidade de dados.

ABSTRACT

MACHADO, Silvana Bordini Coca. Methodological proposal for disclosure of private data in smart cities. 2016. Dissertation (Master degree in Electrical Engineer) - Programa de Pós-Graduação em Engenharia Elétrica, Curso de Gestão de Redes de Telecomunicações, do Centro de Ciências Exatas, Ambientais e de Tecnologias. Pontifícia Universidade Católica de Campinas. Campinas. 2016.

According to the United Nations report, 2014, for the first time in history, most of the world's population is living in urban centers. The urbanization movement, from 1950 to the present day, presented a migration from rural areas to urban almost doubling the reality of that time, which was 30%. And by 2050, it is expected that to be over 66% urban population. That is, the available infrastructure and services should be sized to meet this rapid growth and in less than a century. The information from these citizens, requiring for services provision of care for health, education, transportation and security, are stored in various systems, which may not part of any data centralization and standardization. Many data feature personal information, such as national registers, addresses, and others, which are not well safeguarded and can be a door to the leakage and misuse. The technologies used for the collection and storage of data can affect significantly the lives of people by emerging problems with security and data privacy. The ISO 27001 standard defines the triple constraint for information security through confidentiality, integrity and availability. In order to take the emergence of Smart Cities in the context, which are based on the provision of services via communication highways and by which provide information to governmental agencies, institutions in general and to every citizen. This study aims to learn how to make proper use of data personal institutions under security protection. In this context, they are seeking transparency and agility through ICT, which can be seen during this study that effective confidentiality requires even greater attention from managers and any team responsible for collecting, processing and distributing information. This result for this research is the proposition of a method for public organizations on how to handle data and information related to privacy, using a method based on decision making with the Analytic Hierarchy Process (AHP) and data subsets evaluation.

Indexing Terms: information security, privacy, AHP, data confidentiality.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AHP	=	*Analytical Hierarchical Process*
AMP	=	Apoio Multicritério à Decisão
APP	=	*Australian Privacy Principles*
CI	=	Índice de Consistência
CIA	=	*Confidenciality, Integrity and Availability*
CID	=	Confidencialidade, Integridade e Disponibilidade
CR	=	Taxa de Consistência
DDOS	=	*Distributed Denial of Service*
DHS	=	*Department of Homeland Security*
DLP	=	*Data Loss Prevention*
DOS	=	*Denial of Service*
FTC	=	*Federal Trade Commission*
HIPPA	=	*Health Insurance Portability and Accountability Act*
ICO	=	*Information Commissioner's Office*
IoT	=	*Internet of Things – Internet das Coisas*
LAI	=	Lei de Acesso à Informação
PI	=	Personal Information
PMI	=	*Project Management Institute*
PSI	=	*Personal Sensitive Information*
RI	=	Índice de Consistência Aleatória
ROI	=	*Return on Investment/Retorno ao Investimento*
SGSI	=	Sistema de Gestão de Segurança da Informação
SSN	=	*Social Security Number*
TIC	=	Tecnologia da Informação e Comunicação
VPL	=	Valor Presente Líquido

SUMÁRIO

INTRODUÇÃO

Desde a Revolução Industrial, iniciada em meados do século XVIII, com a invenção da máquina a vapor, por James Watt, até os dias atuais, a humanidade vivenciou diversas e significativas transformações (BRESSER-PEREIRA, 2016). Duas grandes guerras aconteceram, e depois da última delas, o impulso no sentido de investimentos em tecnologias e industrialização agilizaram o processo de transformação.

Uma reorganização mundial tomou conta dos países após a Segunda Guerra, onde muitos buscaram inserção em um novo modelo de sociedade. Modelos de indústrias orientadas para processos repetitivos e em série foram surgindo em todos os continentes, sobretudo, na Europa, América do Norte e Ásia. Neste momento, a Revolução Industrial acenou para os cidadãos como uma alternativa de vida que oferecia, além de um progresso financeiro, a oportunidade de ganho cultural e social (VIANNA et al., 2008).

A busca por maior produtividade impulsionou o processo de globalização mundial e alavancou a era da informação. Com a informação, os dados das empresas, as quais eram formadas por pessoas, eram coletados e armazenados em sistemas ou planilhas manuais ou automatizadas por sistemas computacionais.

Da necessidade de se interligar os computadores derivou a rede de comunicação de dados, simultaneamente, com as grandes redes de telecomunicações. A tecnologia nesta área se diversificou. Surgiram as redes de comutação de mensagens, de quadros ou *frames* (quadros), pacotes ou datagramas e, ainda, as redes de comutação de células. Dentro deste contexto tecnológico, então, surgiu a integração de diversas redes, alcançando uma amplitude mundial, denominada *Internet* e desta forma, todos os computadores, conectados a qualquer tipo de rede, passaram a se comunicar. A *Internet* permitiu a interconexão entre computadores localizados em residências, empresas, instituições, organizações, e outros. Os dados dos sistemas que foram coletados para processos específicos estavam todos na

rede. A rede mundial, ao permitir a comunicação, tornou-se um espaço para discussão, troca de informações, e um lugar para armazenamento de dados. As infovias de informação são ubíquas, com facilidade de acesso a todos os pontos. Com os novos dispositivos disponibilizados pela IoT (*Internet of Things* – Internet das Coisas) esta característica de disponibilidade das informações está ainda mais presente (OVIDIU VERMESAN, 2013).

Dentro deste contexto de comunicação e acesso a informações disponibilizadas por instituições nem sempre muito éticas, certos problemas começaram a preocupar a sociedade (TECHNOLOGY; MAGAZINE, 2014). Devido a população urbana crescente de forma exponencial nas recentes décadas, os espaços e soluções urbanas precisaram ser repensados. Além de infraestruturas para novas soluções em transportes, saúde, educação e serviços públicos, a discussão sobre a Tecnologia da Informação e Comunicação (TIC) e estas soluções estão sendo tratadas pelo termo “Cidades Digitais” e/ou “Cidades Inteligentes” (*smart cities*).

Quando os serviços das TICs fazem o tratamento de dados, uma situação de risco emerge para os contribuintes e usuários dos serviços: a privacidade de dados pessoais.

O tratamento de dados pessoais sensíveis (*Personal Sensitive Information - PSI*) está sendo discutido em diversos países desde o final do século XX. Alguns países, como Inglaterra, Estados Unidos e Austrália, possuem leis e regras que protegem seus cidadãos e não permitem que qualquer um deles corra o risco de ter sua privacidade divulgada indevidamente. Outros países, como Brasil, por exemplo, estão discutindo leis que regulem e normatizem a utilização, pelas empresas e organizações, dos dados de seus clientes e usuários.

Cabe salientar que a Norma ISO 27001 (ABNT, 2013), em sua segunda revisão de 01/10/2013, trata-se de diretriz para a implementação de um Sistema de Gestão de Segurança da Informação (S.G.S.I.), também discute a questão da segurança de dados nas organizações, traçando diretrizes para a proteção dos mesmos (ABNT, 2013).

A questão vem sendo estudada cada vez mais, na medida em que os meios tecnológicos vêm facilitando o acesso aos dados privativos das pessoas. Como tratado por (GUTWIRTH et all, 2014), o conceito de privacidade surgiu quando a violação de privacidade de celebridades e pessoas públicas foram levadas pela rede e jornais com dados de situações que os deixavam envergonhados ou sem explicações. De acordo com (RODOTÀ, 2008), ocorreu uma redefinição da privacidade no século XX, já que outros conceitos foram introduzidos, como a transparência e o controle de dados pessoais, em detrimento da privacidade e do direito de confidencialidade. Surge**,** então**,** a necessidade de se discutir a proteção de dados de maneira mais ampla.

O direito à privacidade deve ser garantido a todos os cidadãos, todo o tempo, como discutido por (MARTINEZ-BALLESTE et all, 2013). Com este foco, os sistemas que incorporam as TICs das Cidades Digitais precisam estar preparados para o manuseio e o armazenamento adequado e seguro, mas sobretudo**,** para a coleta dos dados.

Dentro deste contexto, surgem questões de fundamental importância, como: Quais dados definem o indivíduo, quantos e quais são os dados importantes e que o distingue dos demais, onde estes dados devem e podem estar armazenados, quem são as pessoas que podem requisitar informações sobre este indivíduo?

É fundamental que a legislação forneça bases para que as empresas e organizações civis procedam adequadamente com o manuseio de dados pessoais. Estes dados não podem e não devem ser comercializados, mesmo que entre setores de uma mesma entidade, sem que os indivíduos detentores destas informações sejam advertidos desta possibilidade. Estas entidades não podem explorar os dados de seus clientes de forma silenciosa e obscura. Para tanto, uma definição específica de quais são os dados, quais são as informações que devem ser declaradas como de privacidade pessoal necessita estar claramente definida nos processos e nos formulários, no momento da coleta das informações.

A discussão sobre a ética no tratamento destes dados deve estar plenamente inserida no dia a dia das organizações. A ética com a não prática de farejadores (*sniffers*) nas redes de comunicação, com o cuidado do sigilo de dados evitando a transferência de informações entre entidades (a exemplo do que aconteceu no Brasil quando o setor de telefonia foi privatizado – as empresas forneceram suas listas de assinantes para outras empresas, de outros segmentos mercadológicos). A ética no manuseio das informações, como dados de saúde pessoal. No entanto, os dados de saúde que podem contribuir para uma ação de prevenção, devem estar dentro da transparência abordada anteriormente. E onde está este limite?

Como disponibilizar a informação correta sem ferir o direito à privacidade, mantendo-se o cuidado da segurança da informação (confidencialidade, integridade e disponibilidade), ética e a transparência do setor público?

Este trabalho está centrado no problema que orienta esta pesquisa, o qual pode ser explicitado com a seguinte questão: pode-se elaborar um modelo de tratamento de dados que permita aos gestores públicos das Cidades Inteligentes avaliar a possibilidade ou não de disponibilização de dados dos contribuintes?

O objetivo deste trabalho é conceituar o estado da arte no campo da segurança de informações privadas e desenvolver uma metodologia para uso das mesmas, de modo que possa ser apresentada aos gestores das instituições públicas, com ênfase nas Cidades Inteligentes, que buscam operar como governo transparente, bem como todas as demais organizações governamentais que também devem utilizar adequadamente os dados pessoais dos contribuintes. O foco está na confidencialidade, que requer uma atenção maior dos responsáveis em orgãos públicos, desde a coleta até a disponibilização dos dados.

Com o foco nestas questões, a partir da introdução onde está justificada a relevância do tema, objetivos e problema de pesquisa, este trabalho se inicia com as motivações explicidatas no capítulo 0. Neste capítulo,

está em avaliação a mudança da sociedade com o advindo da industrialização, o impacto da segurança na sociedade atual, como uma introdução para a discussão da segurança da informação e como a segurança da informação e tratamento de dados pessoais estão sendo regulamentados em diversos países, bem como no Brasil.

No capítulo 0 é iniciada a discussão da metodologia de gestão de projetos e o tratamento da mesma pelo setor público, discutindo-se o modelo de apoio a decisão multicritério, com foco no modelo AHP e um algoritmo de exclusão com base em classificação de subconjuntos apresentado no item 0.

O capítulo 4 discorre sobre como os elementos discutidos nos capítulos anteriores serão utilizados para tratar as informações pessoais de contribuintes pelas organizações públicas. Um modelo de decisão utilizando múltiplos critérios será apresentado como uma possível solução para a definição de quais áreas da segurança deverão ser priorizadas, e como o algoritmo de exclusão deverá ser aplicado aos dados que podem ou não ser disponibilizados pelo setor público, dentro do modelo de Cidades Inteligentes.

Um estudo de caso será apresentado no capítulo 0.

O capítulo 6 consiste de conclusões e recomendações, com discussão de tópicos complementares, além da exposição de resultados gerais, resumo conclusivo do capítulo, contribuições do trabalho, novos problemas que poderão se desenvolver e futuros estudos a serem realizados com base em oportunidades da metodologia.

MOTIVAÇÕES

As motivações que conduziram este estudo estão fundamentadas no processo de modernização e industrialização das organizações civis, a padronização das normativas do tratamento de informações, e as legislações existentes em alguns países. Estes temas serão discutidos nas sessões seguintes.

Histórico da organização civil

A organização mundial foi alterada sensivelmente após a Revolução Industrial, que se iniciou em meados do século XVIII, mas teve sua concretização em meados do século XX. Foi um grande marco para toda a humanidade, alterando o processo produtivo de manufaturado (feito com as mãos), para a produção em grande escala, com o auxilio de máquinas e equipamentos (CAVALCANTE; DA SILVA, 2011).

A oportunidade de trabalhar em grandes indústrias seduziu milhares de pessoas que viviam em áreas rurais, levando-as a abandonar a vida no campo para buscar vivenciar o eldorado industrial. O êxodo rural foi um dos primeiros impactos negativos da Revolução Industrial, mudando o eixo da civilização para a área urbana (BRANCO, 2006).

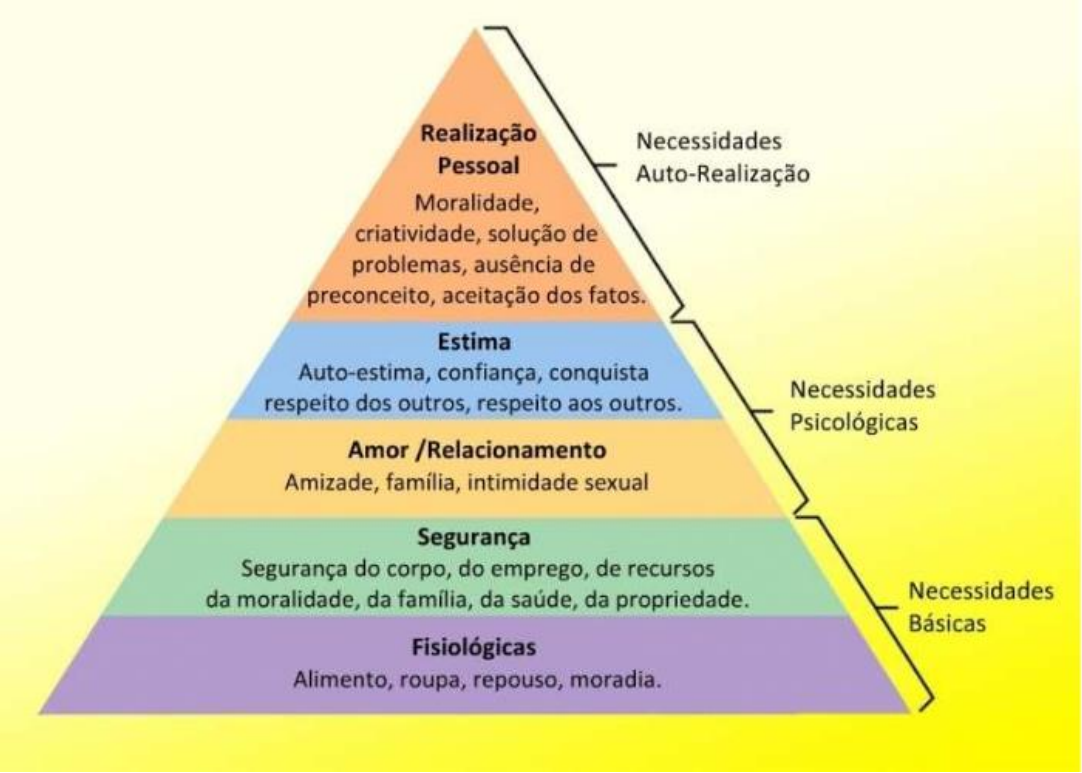
Até a metade do século XX, a população rural era superior a 70% da população mundial. A maioria dessas pessoas viviam do que produziam com o seu próprio esforço: plantação, alimentos caseiros, artesanatos, produtos artesanais. A industrialização provocou a substituição de produtos fabricados de forma artesanal e caseira por produtos resultantes de linhas de fabricação em larga escala, o que caracterizou o progresso deste período (UNITED NATIONS DEPARTMENT OF ECONOMIC AND SOCIAL AFFAIRS, 2014).

Da industrialização à tecnologia da informação

Com a industrialização, novas formas de produtos e serviços foram reinventados buscando agregar valores e inovação. Impactos sociais surgiram como resultados desta revolução, transformando a estrutura social existente. Mudanças de ordem econômica, social, política e cultural, permanecem até hoje, foram introduzidas de forma irreversível à sociedade (PEIXOTO; OLIVEIRA; MAIO, [s.d.]).

No início do século XX, com a maioria das pessoas vivendo no campo, com sua subsistência sendo fornecida pela agricultura ou agropecuária, e sem grandes desenvolvimentos tecnológicos, o nível de informação requerido era muito inferior aos atuais, e as necessidades, dentro da pirâmide de *Maslow*, Figura 1, estavam restritas aos 2 níveis: Fisiológico e Segurança.

Figura 1. Representação da Pirâmide de Maslow



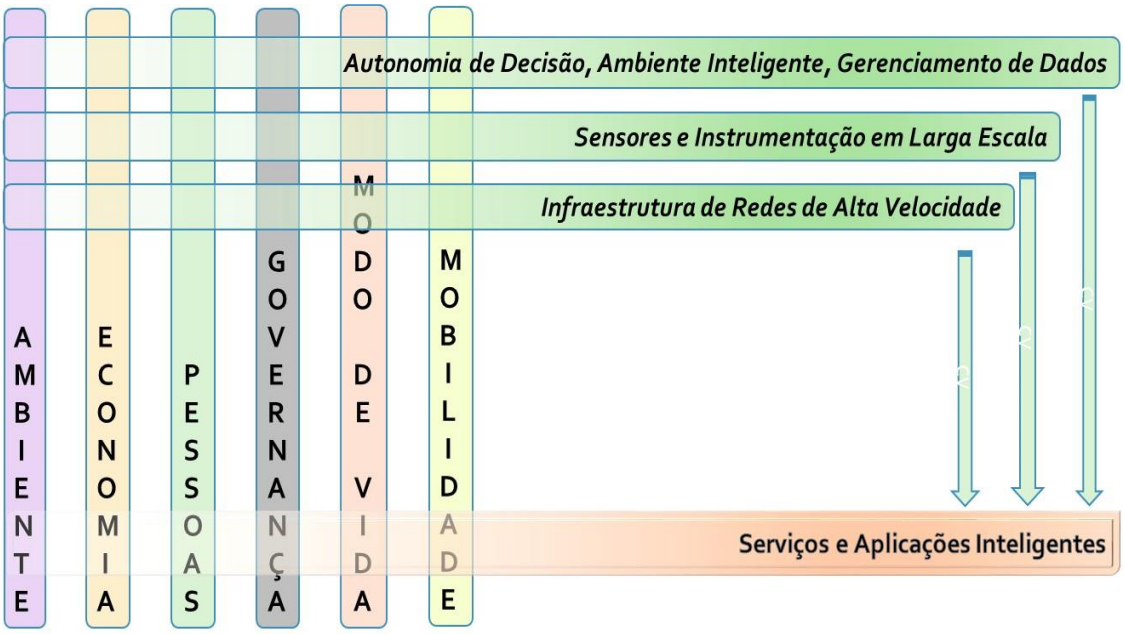
Fonte: Jornal Brasileiro (2014)

Segundo o relatório da Organização das Nações Unidas (ONU), de 2014, a população mundial que vive em centros urbanos é superior a 50%

(NATIONS, 2014). Essa população requer que serviços e produtos oferecidos nestes centros, principalmente relacionados com os 2 níveis descritos anteriormente, sejam fornecidos adequadamente: saúde, transporte e segurança. Além destes, com a maior socialização e convivência em sociedades próximas, surgiram as necessidades sociais: educação e cultura, que se tornaram essenciais em termos de serviços.

Novos serviços e novos produtos nos centros urbanos desencadearam a modernização, impulsionando empresas e centros urbanos a buscar novas tecnologias. Estas tecnologias, quando aplicadas aos processos produtivos existentes, alavancavam produtividade e novos processos e produtos. Conforme (BALAKRISHNA, 2012), uma nova arquitetura de blocos foi proposta para atender às necessidades de Cidades Inteligentes, como indica a Figura 2.

Figura 2. Arquitetura de Blocos de Cidades Digitais



Fonte: Elaboração própria, adaptado de BALAKRISHNA, 2012.

Esta arquitetura considera que uma definiçao aceitável para Cidades Inteligentes é qauela onde os investimentos em capital humano e social, bem como em infraestrutura e comunicações são combustíveis essenciais para um desenvolvimento econômico sustentável e com alta qualidade de vida, através

do gerenciamento sensato dos recursos naturais e com uma governança participativa. Fundamentado nesta definição, definiu-se 6 dimensões inteligentes, as quais são apresentadas verticalmente na Figura 2:

Ambiente: Trata dos assuntos de sustentabilidade e recursos naturais;

Economia: Preocupada com a inovaçao e incentivo ao emprededorismo;

Pessoas: Com foco no nível de educação e escolaridade da população;

Governança: Fornecimento de serviços ao cidadão;

Modo de vida: Relacionado à qualidade da saúde, acesso à cultura, segurança, moradia, transportes e outros.

Mobilidade: Tanto refere-se ao acesso ao transporte público, físico, como à comunicação de dados.

Um dos requisitos fundamentais é a instrumentação da infraestrutura em larga escala, representada na Figura 2 como uma das barras na horizontal, a qual inclui serviços públicos, ransporte, gestões ambientais, industriais e governamentais, através de sensores, leitores e outros dispositivos de detecção. Atualmente, muitos dos sensores presentes dentro dos dispositivos móveis podem ser utlizados em todo o parque da infraestutura, como elementos captores.

A infra-estrutura de redes é necessaria para facilitar a mobilidade, a conexão e a transmissào das informações para as 6 dimensões verticais discutidas anteriormente, distribuindo serviços e produtos aos usuários finais.

Um terceiro elemento é o gerenciamente eficiente dos dados que chegam das dimensões verticais, fornecendo a capacidade de transformação de dados em informações inteligentes, as quais podem ser espalhadas através

de aplicações e serviços, fundamentais para que se alcance eficiência e precisão na operação deste complexo ecosistema.

Para tanto, são requisitados profissionais com qualificação adequada. Esta busca constante por profissionais qualificados, bem como a produção global, fez com que o mundo se abrisse para a globalização.

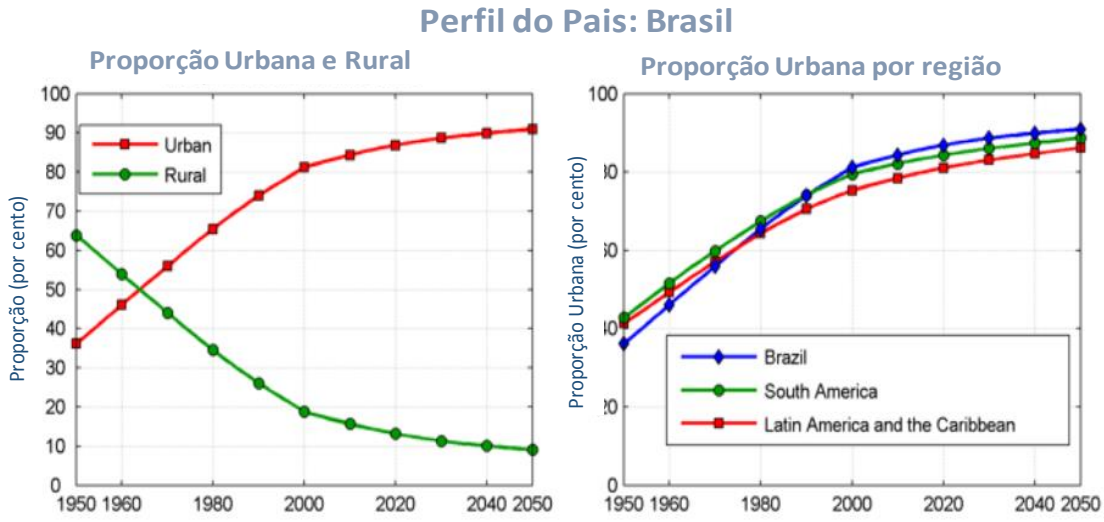
Para que a globalização se concretizasse, a informação passou a ser o grande bem do mercado. Dados de empresas, indivíduos e comunidades passaram a ser os dados sistêmicos e fonte de informação. Consequentemente, estes mesmos dados dos indivíduos passaram a ser importantes para as transações econômicas e sociais.

Dados que podem ser transferidos pela rede física sem obstáculos, sem barreiras, completamente disponíveis. E com a IoT, estes dados podem ser disponibilizados instantaneamente nos mais diversos dispositivos, móveis ou residenciais, disponíveis ou a serem disponibilizados. Não existindo mias limites para o acesso à informação. Fatos que acontecem em um momento, podem ser disponibilizados na *internet* em poucos minutos.

Cenário atual brasileiro

No Brasil, de 1950 até os dias atuais, ocorreu um grande êxodo rural. Naqueles anos, somente perto de 30% da população vivia em área urbana, e a grande maioria estava concentrada no campo. Em menos de 100 anos, a população urbana aumentou para 85%, como mostra a Figura 3. A projeção apresentada no relatório da ONU prevê que até 2050 mais de 90% da população brasileira estará vivendo em centros urbanos (NATIONS, 2014).

Figura 3. Dados da ONU sobre planejamento de centros urbanos no Brasil



Fonte: Nations, 2014.

A Revolução Industrial também atingiu o Brasil, com a chegada das montadoras automotivas e outros gêneros. Como o Brasil é um país primeiramente agrícola, devido a sua vasta extensão territorial e um clima predominantemente tropical, parte da industrialização se deu por meio do setor alimentício. Esta Revolução Industrial foi a grande responsável por esse aumento na população urbana em detrimento do trabalho no campo (GATTÁS, 1982).

No ritmo de mudança e das correntes mundiais, o Brasil também fez seu movimento dentro do processo de globalização, com transformações nas estruturas econômica, social, geopolíticas, devido à sua integração neste movimento. Empresas brasileiras ganharam dimensão transcontinental e muitas se instalaram no território brasileiro, tornando-o a nona economia mundial (NAKAGAWA, 2016)

O Brasil passou a fazer parte dos países emergentes, sendo a primeira letra da sigla BRICS, que congrega Brasil, Rússia, Índia, China e África do Sul. Foram trazidos para o país investimentos externos expressivos, e chamou a atenção do mundo por ser o maior país da América do Sul e possuir uma democracia sustentável (BAUMANN et al., 2015).

Dentro da perspectiva de Tecnologia da Informação, no período em que se chamou de proteção de mercado, entre as décadas de 1970 e 1990, houve um grande investimento das empresas de tecnologia no Brasil. As que pretendiam colocar seus produtos no território nacional precisavam garantir que uma alta porcentagem do produto estivesse sendo fabricado em território brasileiro e muitas empresas criaram equipes com conhecimento e competência para produção de computadores e periféricos.

No Brasil**,** em meados da década de 1990**,** as empresas de telecomunicações nacionais foram privatizadas e um grande aporte tecnológico se sucedeu, e foi um grande benefício para o país a renovação do parque instalado. Novas tecnologias que estavam sendo implantadas nos países da América do Norte, Ásia e Europa foram trazidas para o Brasil, tanto para produção de equipamentos como para a fabricação de dispositivos móveis. O conhecimento técnico em empresas de tecnologia e o potencial de clientes no território propiciaram uma explosão tecnológica em todo o país.

A *Internet* e banda larga, em se tratando de transmissão de dados, são fundamentais para a divulgação de tecnologia em todo o país. Nos programas nacionais para fomentação de *internet* inclusiva, as Cidades Inteligentes e a disponibilização das informações para todos estão na pauta do momento.

Cenário da Segurança da Informação

Informação é um dos bens mais importantes da sociedade moderna. Em um mundo globalizado, onde as mais diversas regiões buscam conexão e troca de dados por redes, as organizações fazem uso intenso da TIC na condução de seus negócios. Consequentemente, a proteção da informação tornou-se um item essencial para o bem-estar organizacional.

1.1.1 Segurança da Informação e possíveis ameaças

Como cita Emiliio Daddario (1991), sobre as relações de ignorância de governos para com indivíduos:

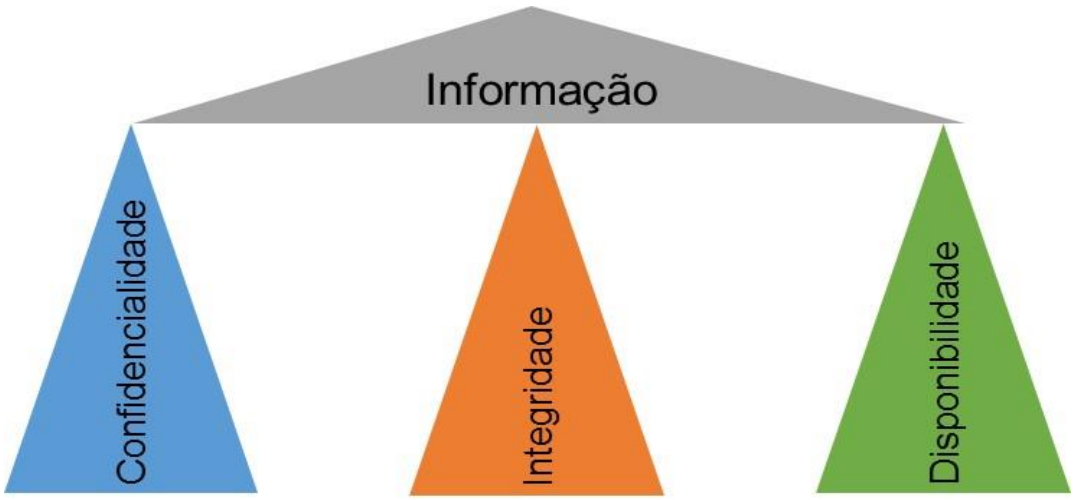
> “Devido às incertezas das decisões poíticas, a sociedade nao age à altura de suas capacidades técnicas... Até que o processo político tenha oferecido uma lista clara de prioridades, as contribuições da ciência e da tecnologia a problemas específicos de bem-estar público provavelmente permanecerão erráticos e sem sistemática ...Os tomadores de decisões políticas devem cuidar para que, ao adotar uma abordagem sistemática de classificação de prioridades, não abdiquem de sua função básica de defesa dos valores humanos...” (Emilio Daddario, Ventures, Magazine of the Yale Graduate School, Primavera de 1971 apud SAATY, 1991)

Cabe destacar que, privacidade de dados é parte dos valores humanos, assunto este que foi amplamente divulgado em 2013, por Edward Snowden, o qual denunciou a existência de programa de vigilância global, utilizado pela *National Security Agency* (NSA), documentado por (POITRAS, 2014).

A segurança das redes, da informação e de dados se tornou vital para muitas organizações e não se restringe apenas a sistemas de informação, mas também a proteção de dados e informações que possam ter algum valor às organizações e ou a qualquer cidadão.

A segurança da informação se baseia em três pilares, referenciados como tripé: confidencialidade; integridade; e disponibilidade (CID) ou, então, para descrição em inglês de *confidentiality*, *integrity* and *availability* (CIA), como exemplificado na Figura 4.

Figura 4. Tripé da Segurança da Informação



Fonte: (ABNT, 2013)

A confidencialidade diz respeito ao acesso às informações a serem fornecidas somente a quem, de fato, possa ter autorização para tal. A integridade diz respeito à proteção contra alterações indevidas de dados, e exatidão dos mesmos. A disponibilidade é a propriedade que garante que a informação esteja disponível sempre que se fizer necessário (VON SOLMS & VAN NIEKERK, 2013).

Dentro do tema segurança apresentam-se diversos aspectos que merecem especial atenção. O termo segurança, na tradução para o inglês, leva a dois verbetes distintos: *safety and security*.

Segurança tratado pelo termo *safety* refere-se à proteção em relação ao perigo para a vida das pessoas, prevenção de situações de riscos (FLEETS, 2014). Segurança da informação, dentro do termo em inglês *security*, versa sobre a segurança patrimonial, militar, a estabilidade de uma organização ou país. Como informação é um bem das empresas, então também está neste contexto, junto com a segurança dos sistemas de comunicação. A palavra de ordem é prevenção de ataques aos sistemas de segurança, como *malwares*, vulnerabilidades, vírus e ataques cibernéticos. O termo inglês *malware* está associado com *malicious software*, ou seja, programas de computador que quando infiltrados em um sistema computacional de forma ilícita podem causar danos como roubos de informações, confidenciais ou pessoais. Já os casos de *Denial of Service (DOS)* e *Distributed Denial of Service* (DDoS) se dão quando um computador (único ou mestre, respectivamente), por ação de *hacker* ou atacante, inicia uma série intensa de acessos a determinado *site*, sobrecarregando o tráfego, fazendo com que o serviço e/ou *site* caia e saia de operação. Vulnerabilidades se referem às falhas no *software* de forma a deixar espaço para um acesso não autorizado ou a um comportamento malicioso, como vírus e outras formas de *malware*.

1.1.1 Segurança de dados privados

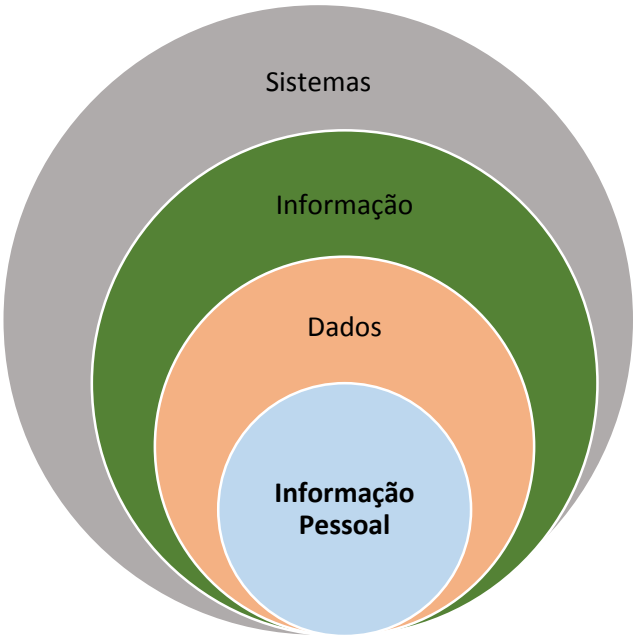
Neste cenário de privacidade, emergem as discussões sobre dados individuais: Informações Pessoais, ou em inglês, *Personal Information (PI)*. A informação pessoal diz respeito a qualquer informação identificável ou identificada. Dados pessoais incluem informações que dizem respeito ao indivíduo com relação aos seus dados pessoais (moradia, por exemplo) bem como seus dados profissionais. Inclui dados publicamente disponibilizados, como, por exemplo, informações em redes sociais na *internet* e englobando, ainda, os dados fornecidos durante cadastros por formulários de coletas de dados em empresas, escolas, bancos ou organizações públicas e privadas. Em alguns cadastros surge também a classificação de dados pessoais sensíveis, os quais requerem um tratamento mais controlado e regulamentado (KING & RAJA, 2012).

Com a disseminação de redes de comunicação, redes sociais, acesso às bases de dados públicas e privadas de diversas instituições, principalmente governamentais no ambiente das Cidades Inteligentes, o acesso inapropriado aos dados pessoais emerge como uma abertura nos sistemas de informação. Instituições trocam listas de dados de seus clientes com outras, parceiras e ou clientes, sem, contudo, possuírem, muitas vezes, a autorização explícita dos proprietários dos dados. De um modo espontâneo e livre, de forma geral, os bancos públicos, parceiros de instituições públicas, obtém dados pessoais de cidadãos com relação aos salários e pensões, e oferecem cartões de créditos, seguros, planos de saúde. Lojas virtuais compartilham dados de seus clientes com seus parceiros de negócios, como empresas de revistas, dentre outras. Tem-se um contrassenso em relação ao processo de mineração de dados (*data mining*), que busca fornecer dados analíticos às empresas de *marketing* para otimizar oferta de produtos e serviços se trabalhados sem as permissões devidas. Desde que os usuários estejam informados e cientes, concordando com a prática, estes serviços e novos conteúdos podem ser oferecidos, mas a privacidade deve estar sempre preservada. Como exemplo, teve-se a divulgação pública pela mídia, Bom Dia Brasil (GLOBO, 2016), sobre o compartilhamento de dados de aposentados pelo organismo federal com bancos não governamentais, no sentido de oferecer crédito consignado. Os

aposentados não foram instruídos desta possibilidade e poderiam acreditar que estavam sendo beneficiados, como amplamente divulgado pelo governo.

A Figura 5 mostra como estão inter-relacionados os diversos níveis de segurança detalhados neste capítulo. Segurança da Informação, como um item mais abrangente, possui em seu bojo a informação como item principal. Esta, por sua vez, é formada de dados que compõem determinado conteúdo que, quando processados, se transformam e produzem informação (ZINS et al., 2007). E dentre os dados que um cidadão pode deter, muitos são específicos sobre sua pessoa, os quais podem ser tratados como informação de natureza pessoal.

Figura 5. Níveis de Segurança da Informação.



Fonte: Elaboração Própria, 2016.

Este trabalho está focado em discutir os riscos e exposições que podem ser causados em um sistema de informação quando a atenção adequada não for dispendida para o tratamento das informações pessoais.

Na busca por soluções efetivas de segurança de dados pessoais, deve-se considerar a enorme quantidade de dados coletados e disponibilizados para processamento e manipulação, os quais podem afetar a segurança da privacidade, o que pode inviabilizar a implementação e adoção nas Cidades

Inteligentes. O controle da segurança da informação deve estar implementado de forma a assegurar que a informação registrada, seja por coleta coletiva ou expontânea, permaneça com tratamento confidencial, tenha integridade e esteja disponivel às devidas partes interessadas (CILLIERS & FLOWERDAY, 2014).

1.1.2 Segurança de dados

Neste ambiente de segurança da informação, não menos importante está a segurança de dados. Dados de transações comerciais entre empresas, negócios, faturamento, dentre outros são alvos de ataques por *hackers* em grande quantidade, diariamente. Por exemplo, *Data Loss Prevention* (DLP), dentro da segurança de dados, refere-se aos sistemas e metodologias que permitem a redução do risco de vazamento de informações confidenciais através da inspeção de conteúdos com um grau de sofisticação tal que ultrapassa a verificação de palavras e expressões triviais. As soluções existentes fazem parte de um pequeno número tecnologias de segurança da informação que estimulam os usuários a estarem informados e entendendo as relações das suas ações em relação à segurança (CALDWELL, 2011).

Proteção de dados e privacidade devem fazer parte do cotidiano de toda organização e sociedade e a integração entre segurança e privacidade deve estar presente em pesquisas futuras (BARTOLI, HERN, HERNÁNDEZ-SERRANO, & SORIANO, 2011). Em um mundo no qual os dados são facilmente coletados, armazenados e compartilhados, e considerações sobre a manipulação inadequada de dados é uma resultante, cada indivíduo deve agir com responsabilidade no manuseio destas informações, de acordo com as legislações e com os valores culturais vigentes em cada país.

Segurança de dados privados – análise de algumas legislações vigentes

Em termos gerais, em países com legislações já em vigência, quando comparados com aqueles em fase de desenvolvimento, percebe-se que um tratamento com maior critério é fornecido a toda e qualquer informação pessoal, tanto pelas mídias quanto TICs, quando dados individuais fizerem parte do contexto.

Com todo o desenvolvimento ocorrido no século XX, como apresentado nos capítulos anteriores, poucos, nos conceitos legais, foram tão transformadores quanto o direito à privacidade. Discussões sobre o intenso processamento de dados de milhões de pessoas por entidades públicas e privadas, com a utilização de modernos sistemas de tecnologia da informação e comunicação oferecem uma maior disponibilidade de informação, mas também há o risco da exposição inadequada. O conceito de privacidade foi reinventado neste século, visto que passou a envolver conceitos como transparências e controle de dados pessoais, culminando com o desenvolvimento do direito à proteção de dados (DONEDA, 2006).

A exposição não espontânea de uma pessoa a estranhos tem ocorrido com maior frequência, mais pela divulgação de dados pessoais do que pela invasão de sua habitação, divulgação de notícias pela imprensa ou violação de correspondências. Estes meios tradicionais de violação estão sendo suplantados por outra forma: a tecnologia da informação e comunicação (TIC). Os dados fornecidos pelos indivíduos a empresas públicas e privadas, durante algum relacionamento, são coletados e armazenados utilizando tecnologias de informação. A utilização dos dados para os fins coletados não se apresenta como um problema, mas, muitas vezes, visto a sua disponibilidade, eles são utilizados para outros fins. Faz-se necessário o estabelecimento de critérios de utilização dos mesmos, para que não ocorram vazamentos e má utilização.

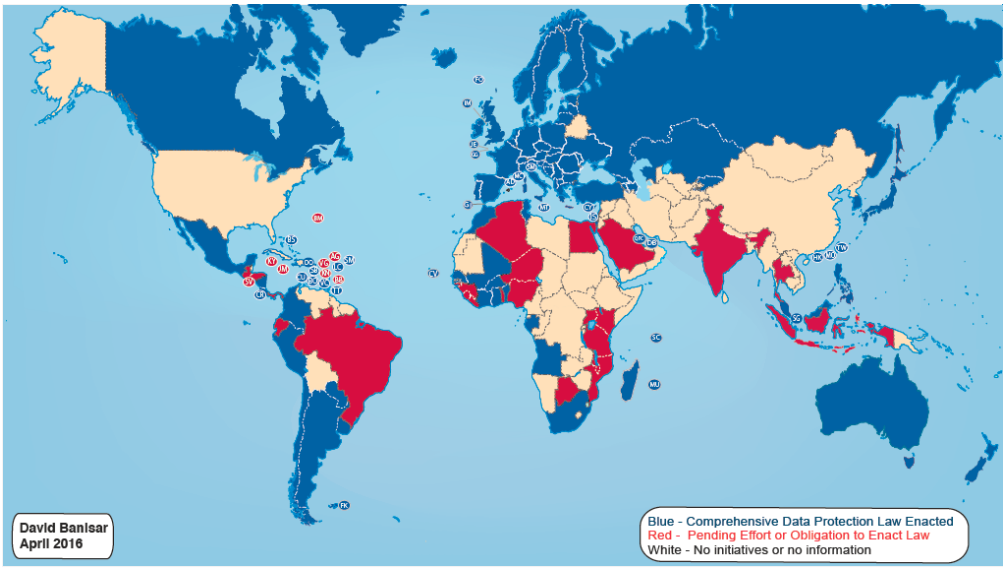
Os países da União Europeia estão discutindo legislações e regras que possam ser mais apropriadamente aplicadas de forma a garantir e salvaguardar as informações pessoais dos indivíduos, inclusive no trânsito e comércio entre os mesmos. No âmbito do serviço público, muitas das leis esbarram na controvérsia das definições: privacidade e transparência.

Enquanto são requisitados a terem transparência para com o cidadão, os órgãos públicos são contrapostos com o item da privacidade, a qual deve ser preservada e salvaguardada.

Estudando as regras e legislações existentes, é possível oferecer uma noção mais específica do momento atual. Desta forma, esta pesquisa buscará apreender a realidade sobre segurança privada procedendo a uma abordagem sobre os processos vigentes na União Europeia, Austrália Inglaterra e Estados Unidos. Por outro lado, os processos em andamento no Brasil e desafios para aplicação no serviço público, mais precisamente nas cidades que estão migrando para oferecer uma Cidade Inteligente, com gestão e dados integrados.

A Figura 6 apresenta uma visão de como estavam as implementações de proteção da privacidade no mundo, no final de 2014. Os países em azul são aqueles que possuem legislações e regras já estabelecidas e implementadas – a grande maioria na Europa, Ásia e América do Norte. Os países em vermelho ainda estão em processo de definição, mas sem regulamentação já estabelecida – alguns países da América do Sul, entre eles o Brasil. E os demais países não possuem iniciativa alguma no momento atual – países da África e a grande maioria dos países árabes (Banlsar, 2016)..

Figura 6. Mapa da proteção da privacidade



Fonte: BANLSAR, 2016

1.1.3 Proteção de Dados na Inglaterra

A legislação de todo o Reino Unido (Inglaterra, Irlanda do Norte, Escócia e País de Gales) é Ato de Proteção aos dados de 1998 (KINGDOM, 2005), o qual regulamenta o processamento de informações relativas aos indivíduos, incluindo coleta, manutenção, uso e divulgação de tais informações. Todos os dados pessoais só podem ser processados para o fim pelo qual foram coletados. Não podem ser utilizados para propostas que não sejam as coletas de origem. Esta lei trata da proteção das pessoas comuns, livres e à livre circulação dos dados entre países e fronteiras.

Como dados pessoais, esta legislação explicita ser relativa a qualquer indivíduo vivo, e que poderiam identificar a quem pertencem. Mais claramente é definido o conteúdo de informações pessoais sensíveis, como sendo qualquer uma dentro da seguinte lista, dentre outros: origem racial, origem étnica, opiniões políticas, religião, condições físicas e/ou mentais, sexo e vida sexual, por exemplo (MENDES, 2008).

No entanto, cabe ressaltar que esta lei não definiu, especificamente, os requisitos de segurança a serem implementados e nem tampouco as métricas de orientação. Este fato, porém, não ficou desassitido e, mais recentemente, foi criado o *Information Commissioner's Office* (ICO) – que equivale a uma agência de regulação e fiscalização, o qual recomenda que as organizações adotem a ISO 27001 como prática de implementação, controle e padronização (KATE & LUCENTE, 2015).

1.1.4 Proteção de Dados na Austrália

A proteção de dados na Austrália se apresenta como um conjunto de leis nos diversos níveis do governo: federal, estadual e por território. No entanto, o *Privacy ACT* 1988 (COMMONWEALTH GOVERNMENT OF AUSTRALIA, 2016) apresenta os princípios de privacidade que são aplicados para as organizações privadas e devem ser observadas por todas as

organizações governamentais. Além disso, a Austrália também possui 13 Princípios de Privacidade Australianos, ou 13 *Australian Privacy Principles* (APP) que são aplicadas por todas as organizações públicas (AUSTRALIAN GOVERNMENT, 2014), os quais estão divididos em 5 seções distintas, chamadas de partes, e as duas últimas referem-se à integridade e ao acesso às informações, o que remete a dois dos três critérios principais da norma de segurança da informação, ISO 27001, já discutida em 0.

Desde 2015, foi instituído o Escritório do Comissariado de Privacidade (*Office of Privacy Commissioner*), que possui a atribuição direta pela adoção e aplicação do *Privacy act* 1988. Existem, ainda, outras legislações próprias para setores como saúde e telecomunicações, todas com impacto à proteção de dados e privacidade.

A *Privacy Act 1988* deixa explícito que dados pessoais, comumente chamado de “informação pessoal” na Austrália, referem-se à informação ou qualquer opinião, sendo verdadeira ou falsa, sobre um indivíduo, cuja identidade esteja aparente e possa ser facilmente identificada.

Com relação à segurança da informação, toda organização deve possuir processos e políticas implementadas de forma a proteger a informação de mal-uso e perda, bem como de acessos não autorizados, modificações e revelação. Ainda, deve possuir processos para destruição permanente de informações pessoais que não sejam mais necessárias para a organização.

1.1.5 Proteção de Dados nos Estados Unidos

O *Department of Homeland Security (*DHS) *Privacy Office* é o primeiro orgão do governo Americano com a responsabilidade de centralizar as informações e regulamentações com relação a dados privados. Em 2012**,** foi editado um guia para tratamento de informação pessoal sensíveis (CALLAHAN, 2012). Nele são delineados os dados sensíveis que são tratados como subconjunto com tratamento diferenciado.

Dentro dos 50 estados da organização americana, cada um deles possui sua própria legislação para vários temas, inclusive para o tema de privacidade. Embora a *Health Insurance Portability and Accountability Act* (HIPAA), orgão que regulamenta o mercado de saúde neste país, tenha um tratamento mais específico para dados de sáude e seguridade, este não pode ser aplicado a todos os setores do mercado.

No âmbito dos dados pessoais sensíveis, um dos dados mais comumente tratados dentro dos estados é o *Social Security Number (SSN),* número de 9 dígitos, registrado também na carteira de motorista, o qual é tratado com um documento de identificação dentro de todo o território americano, e a data de nascimento, que em combinação com os demais documentos, poderia facilmente simplificar a identificação dos indivíduos. Ainda são considerados dados pessoais o número do passaporte e o número do registro de estrangeiro ou imigrante.

Um dos aspectos relevantes neste país é a existência de um órgão que ressalta e obriga as organizações a aplicarem a legislação: *Federal Trade Commission* (FTC), o qual tem autoridade para nao permitir que orgãos públicos ou privados se esquivem de implementar medidas mínimas de proteção de dados que possam criar furstrações aos cidadãos com relação à divulgação de dados.

1.1.6 Proteção de Dados no Brasil: Legislação e ações em curso

A partir de 2015, o governo brasileiro iniciou uma consulta pública para discussão da proteção de dados pessoais na *Internet*. Embora não exista uma lei específica para a proteção de dados, estão no conteúdo de algumas leis como a da Lei do Cadastro Positivo, de 2011 (BRASIL, 2011a), a Lei de Acesso à Informação conhecida com Marco Civil da *Internet*, de 2014 (BRASIL, 2014), além de alguns dispositivos constitucionais genéricos, como os artigos 5º, 10º e 12º da Constituição Federal Brasileira de 1988, na versão de 2012 (BRASIL, 2012a).

A Lei do Cadastro Positivo versa sobre a criação e consulta aos bancos de dados de pessoas físicas na formação de bancos de dados financeiros. Menciona a garantia de privacidade no tratamento de dados.

A Lei de Acesso à Informação, no artigo 31, também regulamenta como deverá ser feito o tratamento das informações pessoais. Nesta lei**,** estão mencionadas as necessidades de transparência, respeito à intimidade, além do direito à vida privada, bem como liberdades e garantias individuais. Existe a especificação de restrição de acesso por agentes públicos sem autorização específica que não seja:

1. Diagnóstico médico;
2. Estatísticas e pesquisas de interesse público;
3. Cumprimento de ordem judicial;
4. Proteção de direitos humanos; ou
5. Proteção do interesse público preponderante.

Esta legislação, popularizada como Marco Civil da *Internet*, trata de garantias gerais bastante satisfatórias para a privacidade. Encontra-se em consulta pública para aperfeiçoamento e complementação.

Cabe ressaltar que a Constituição Federal, primeiramente aprovada em 1988 e com várias emendas constitucionais, deixa explicito que:

a. A intimidade, vida privada, honra e imagem das pessoas é inviolável;
b. Confidencialidade de correspondências e comunicações eletrônicas são protegidas e todos possuem garantia de acesso à informação, no entanto a confidencialidade da fonte de origem dever ser garantida sempre que for necessário o exercício de atividade profissional.

A questão da transparência, dentro dos órgãos públicos brasileiros, é crucial para que toda informação governamental esteja disponível para a população (BRASIL, 2011b). No entanto, é necessário definir regras e diretrizes

que sejam adequadas com a privacidade. As cidades estão trabalhando este assunto individualmente. Contudo, com uma definição mais clara e objetiva poderia ter-se uma gestão mais adequada com os dados do cidadão, que não faz parte do programa de transparência, mas que deve ser preservado.

A legislação brasileira ainda tem muito a evoluir na direção de proteção de dados do seu cidadão e contribuinte. Não está claro o que deverá ser considerado como pessoal, como deverá ser feita a coleta – específica ou genérica. O Congresso Nacional tem vários projetos e leis para serem votados e aprovados, mas não existe um prazo para os mesmos. Também se faz necessário a existência de um órgão regulador e fiscalizador dedicado à aderência às legislações vigentes. E o direcionamento para implementação de políticas de segurança que sejam aderentes à família de normas ISO 27000.

Uma comparação das legislações apresentadas, tem-se como apresentado na Figura 7.

Figura 7. Comparação entre as legiislações vigentes

País	Lei	Orgão regulador	Específica?	Uso Multiplo?	Item
Inglaterra	ACT 1988	Information Commissioner's Office	Sim	Não	Qualquer informação pessoal
Austrália	Privacy ACT 1988	Office of Privacy Commissioner	Sim	Não	Qualquer informação pessoal
Estados Unidos	DHS Handbook (2012)	Federal Trade Commission	Sim	Não	SSN = Social Security Number
Brasil	Marco Civil, Cadastro Positivo Transparência (2011/2014)	_____	Não	Sem regulamentação	Sem regulamentação

Fonte: Elaboração Própria, 2016

Com isso, este trabalho poderá auxiliar principalmente as cidades mais informatizadas a estabelecer uma linha de corte entre o mínimo de dados a ser considerado privado, e o máximo de dados a ser disponibilizado nos portais de transparência. A discussão está centrada em dados pessoais de contribuintes.

REFERENCIAL TEÓRICO

Como referencial teórico a ser aplicado a este estudo, estão sendo considerados elementos que subsidiem o processo de tomada de decisão com a segurança que se faz necessária, em um ambiente que se constituirá em um espaço crítico em que, tanto se disponibilizará informações, quanto se tratará da proteção ao contribuinte. Projetar este ambiente exige que se trabalhe com fundamentos desta área do conhecimento, considerando aspectos políticos, administrativos e estratégicos que se inserem na estruturação. Para estes gestores, em sua atividade diária, faz-se necessário uma ferramenta que lhes ofereça o devido suporte ao processo de tomada de decisão. Por fim, agrega-se a este contexto um procedimento lógico e coerente que classifique os conjuntos de dados a serem trabalhados dentro do quadro de solicitações advindas da comunidade que requerem a liberação e uma dada informação.

Com este objetivo, considerou-se adequados os seguintes modelos teóricos para o desenvolvimento deste trabalho:

- Os princípios da gestão de projetos, delineados pelo *Project Management Institute* (PMI), e aplicados para a gestão pública;
- A aplicação de um Método de Apoio à Tomada de Decisão como um instrumento de apoio; e
- Um processo de classificação de dados em subconjuntos, para estruturar corretamente a tomada de decisão.

Estes modelos serão detalhados nas sessões seguintes.

Gerência de Projetos

Nas últimas décadas, o setor público, de modo geral, também passou a vivenciar a pressão para uma melhoria no desempenho e resultados. Estas forças levam as insituições a avaliarem a necessidade de mudanças, as quais podem ser efetivadas por meio de projetos. Objetivando um aprimoramento do gerenciamento e do desempenho de projetos em suas organizações, o setor

busca um modelo de maturidade na gestão de projetos. No entanto, poucos estudos são apresentados para o setor público, com a utilização efetiva de ferramentas e técnicas adequadas (SANTOS, 2009).

A administração pública é um tema vigente que tem sido associado às necessidades políticas de seus administradores, através da implementação de políticas que demonstrem transparência e responsabilidade. Muitas iniciativas são geradas pela necessidade de melhoria de resultados organizacionais e capacidade de adaptação à mudança (CRAWFORD; HELM, 2009).

E é neste contexto que se tornam relevantes as contribuições oriundas da área de Gestão de Projetos.

1.1.7 Uma abordagem objetiva sobre gestão de Projeto

Projeto é um conjunto de atividades realizadas por um grupo de pessoas com objetivo de produção de um produto, serviço ou resultados únicos. Tem início e fim definidos no tempo, e com escopo e recursos específicos. Deve ser único no sentido de não ser uma operação de rotina, mas um conjunto de atividades com a finalidade de alcançar um objetivo específico (PMI, 2013).

A aplicação de conhecimentos, habilidades e técnicas para a condução de projetos com eficácia é uma atribuição da gestão de projetos. A gerência de projetos está delineada em cinco grupos de processos, de modo a garantir uma padronização: início, planejamento, execução, controle e encerramento. O conhecimento do gerenciamento de projetos é formado por dez áreas distintas: integração, escopo, custos, qualidade, aquisições, recursos humanos, comunicações, risco, tempo e partes interessadas. Gerência de projetos é, portanto, a disciplina que padroniza a forma como os projetos são planejados, executados, controlados e finalizados. Atualmente, com complexidades crescentes, há menos tolerância a erros. As disciplinas de gestão de projetos, delineadas pelo PMBoK, fornecem uma estruturação para o gerenciamento de problemas, objetivando uma maior utilização dos recursos, e uma minimização dos riscos.

Seja para a sobrevivência ou até mesmo a liderança no mercado, os projetos são as chaves para este mundo atual, onde a competição é mundial e estes podem afetar aspectos vitais de qualquer linha de atuação (FORSBERG, 1996).

Dentre os principais grupos de critérios para gestão de projetos, alguns são tratados por (VARGAS, 2010), como abaixo descritas.

Financeiros: visam capturar os principais benefícios financeiros dos projetos. Estão diretamente relacionados a custos, lucros, produtividade. Alguns exemplos são a taxa de Retorno ao Investimento (ROI), Lucro e Valor Presente Líquido (VPL), dentre outros nesta área.

Estratégicos: diretamente relacionados aos objetivos da organização. Estes critérios são determiandos por desdobramentos da estratégia da organização. Por exemplo, nas organizações públicas, consta a questão da transparência, bem como a melhoria da visibilidade junto aos contribuintes (melhora na satisfação).

Riscos (Ameaças): nível de risco da organização com a realização do projeto. Muitas vezes, as avaliações das oportunidades apresentadas pelo projeto estão tratadas pelos critérios estratégicos, citados anteriormente.

Urgência: determina quão urgente os projetos precisam ser executados, e qual a prioridade do mesmo com relação às demais alternativas.

Comprometimento das partes interessadas: avalia o comprometimento de todas as partes interessadas. Quanto mais comprometimento, mais prioritário é o projeto. Muitas podem ser as partes interessadas: organização, orgãos reguladores, comunidade, dentre outros.

Conhecimento técnico: necessário para se avaliar e executar o projeto. Quanto maior conhecimento técnico, maior a facilidade de realizá-lo e menor será o custo do mesmo.

Os critérios de gestão de projetos orientam as instituições para uma decisão sobre qual caminho selecionar quando deparados com várias alternativas, mas, sobretudo, no caso desta pesquisa, com os temas de seguridade e integridade, contrapostos com a urgência e transparência.

Observando-se o quesito de transparência no setor público, vale destacar que dentre as iniciativas relativas a este tema, consta a Lei da Transparência, alicerçada pela legislação brasileira com a Lei de Acesso à Informação – LAI já citadas em (1.1.6), as quais foram regulamentadas pelo Decreto 7.724 (BRASIL, 2012b). Este decreto estabele a forma como devem ser disponibilizadas as informações, obrigando todas as entidades públicas a fornecerem informações de interesse coletivo ou geral que tenham sido produzidas por eles ou fornecidas por outros e custodiadas a estas entidades.

Uma das formas de implementar essa disponibilização da informação foi através da criação de Ouvidorias nos órgãos públicos, conforme (SEMERARO; CARDOSO, 2010), para atuar no diálogo entre o cidadão e a administração pública. A gestão do portal da transparência está, na maioria dos orgãos públicos, sob a responsabilidade da ouvidoria. Este “Projeto de Ouvidoria” tem em seu bojo um escopo de disponibilização de dados, mas também de proteção do contribuinte.

Método de Apoio à Tomada de Decisão

Estando a qualidade da informação respaldada na importância (como leis e regras), o tratamento analítico também estará pautado na importância dos fatos. Dentro deste contexto, surge a necessidade de tomar-se uma decisão quanto à viabilidade ou não de se publicar ou informar a terceiros. Desta maneira, compreende-se aqui situações em que estão presentes diversas variáveis, compondo um ambiente aderente aos estudados por tomada de decisão em cenário multicritério.

No cenário de tomada de decisão multicritério há os conceitos de cultura e modelo. Para que um modelo possa ser definido, deve-se entender o papel da cultura nesta definição. A cultura sendo o conjunto de conhecimentos,

valores que não estão intrínsecos, mas aprendidos e, posteriormente, compartilhados. O conjunto de informações que um indivíduo acumula durante o seu aprendizado, caracterizando como experiência de vida. É um misto de informação, experiência e criatividade. Já o modelo é uma representação da realidade, analisado por recursos (cultura) dos envolvidos. No modelo, uma realidade de dados estará representada através da visão da cultura e experiência do indivíduo a tomar a decisão (GOMES, L.F.A.M.; GOMES, C.F.S.; ALMEIDA, 2006).

Um método dedicado ao ambiente de decisão multicritério, o método *Analytical Hierarchical Process* (AHP), criado pelo professor Dr. Thomas L. Saaty, na década de 1970, e muito estudado após esta data. É uma técnica estruturada utilizada para a tomada de decisão em ambientes e/ou problemas complexos, em que são considerados na definição das prioridades e seleção de alternativas os mais variados critérios. Em estudo realizado por (SALOMON & MONTEVECHI, 1999), o método AHP apresentou vantagens como pensar na decisão de maneira hierárquica, lógica, e a possibilidade de verificar-se a inconsistência dos julgamentos, comparando-se com o cérebro humano.

O uso do AHP começa com a decomposição do problema em uma hierquia de critérios excludentes, os quais podem ser comparados e analisados de forma indepedente. A partir da hierarquia lógica, os especialistas avaliam todas as alternativas por comparação, duas a duas, para cada critério. A comparação pode ser realizada utilizando dados reais das alternativas ou julgamentos humanos advindos da experiência dos especialistas (SAATY, 2008).

Modelos de Apoio à Decisão não visam apresentar ao indivíduo que necessita tomar uma decisão a solução para o problema, como uma única alternativa representada pela ação selecionada. Porém, objetiva ser parte do “processo decisório” através da recomendação de ações que permitam ao decisor tomar a ação com maior confiança.

Se a qualidade da informação for respaldada na importância (como leis e regras), o tratamento analítico também estará pautando na importância dos fatos.

1.1.8 Modelo AHP – princípios básicos

De acordo com GOMES, um modelo de apoio multicritério à decisão (AMD) é um conjunto de métodos e técnicas que apoiam as organizações e indivíduos na tomada de decisão, com foco em múltiplos critérios. Este modelo aceita que as subjetividades dos analistas possam estar inseridas nos processos decisórios.

Modelos de AMD possuem, em sua maioria, a seguinte estrutura, apresentada na Figura 8, onde tem-se os seguintes itens relatados:

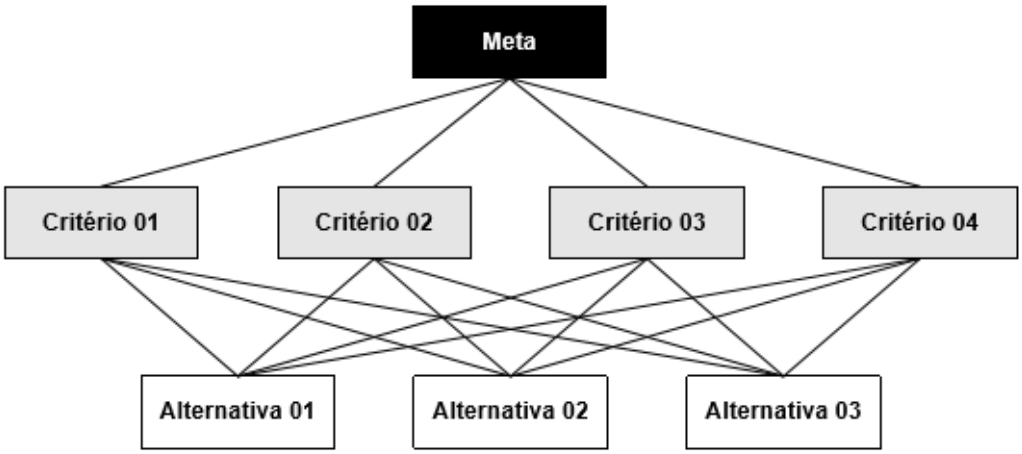
M: Meta e ou Objetivo do problema

C: Critérios para comparação

A: Conjunto de alternativas para solução do problema

P: Pesos dos critérios e/ou atributos, os quais estão representados pelos arcos entre as alternativas, critérios e meta.

Figura 8. Exemplo de hierarquia de alternativas, critérios e meta



Fonte: VARGAS, 2010

O modelo AHP é um dos modelos de apoio à decisão, o qual estrutura o problema da decisão em níveis hierárquicos, facilitando sua compreensão e avaliação. Busca oferecer uma abordagem quantitativa, por meio da conversão

de dados empíricos em modelos matemáticos. São definidos critérios, pelo menos dois, os quais conflitam entre si. A solução será dependente de um conjunto de especialistas, cada qual com sua experiência e vivência, muitas vezes se contrapondo um ao outro, avaliando os critérios, entre si, e as alternativas, em relação a cada critério, atribuindo pesos, com base em escala de relativa importância entre duas alternativas. O pesquisador Saaty (SAATY, 2005, 2008) propôs uma escala que determina a importância relativa de uma alternativa quando comparada com outra, amplamente utilizada e apresentada na Tabela 1.

Tabela 1. Escala de relativa importância de Saaty

Escala	Avaliação	Reciproco
Extremamente preferido	9	1/9
Muito forte a extremo	8	1/8
Muito fortemente preferido	7	1/7
Forte a muito forte	6	1/6
Fortemente preferido	5	1/5
Moderado a forte	4	1/4
Moderadamente preferido	3	1/3
Igual a moderado	2	1/2
Igualmente preferido	1	1

Fonte: SAATY, 2005

A tabela possui valores de 1 a 9, embora os mais utilizados estejam na escala dos números ímpares, os quais permitem uma distinção razoável entre os pontos de medição. Os números pares só devem ser considerados quando ocorrer a necessidade de negociação, ou distinção mais apurada, entre os avaliadores ou especialistas.

A partir da escala de Saaty (como será chamada a partir deste ponto), será construída uma matriz de comparação, primeiramente dos critérios, e depois das alternativas. Supondo que o Critério 1 tenha dominância sobre o Critério 2, a matriz para esta alternativa consta na Tabela 2.

Tabela 2. Matriz comparativa supondo X que sobressai sobre Y

	Critério ou Alternativa 1	Critério ou Alternativa 2
Critério ou Alternativa 1	1	Valor Opção da Tabela SAATY
Critério ou Alternativa 2	1 / Valor Opção da Tabela SAATY	1

Fonte: Elaboração própria, 2016.

O modelo AHP permite que o decisor possa pensar na decisão de forma lógica (hierárquica) e também verificar a inconsistência dos julgamentos, pelo cálculo das médias e pela equação (1) onde CI corresponde ao índice de consistência e n é o número de critérios, λ_{Max} é a média aritmética dos valores de cada um dos critérios, apresentada pelos pesos relativos entre os mesmos.

$$CI = \frac{\lambda_{Max} - n}{n-1} \quad (1)$$

Com o objetivo de verificar se o índice de consistência era adequado, (SAATY, 2005) propôs a taxa de consistência (CR), determinada pela razão entre o índice de consistência (CI) e o índice de consistência aleatória (RI), como na equação 2:

$$CR = \frac{CI}{RI} < 0.1 \sim 10\% \ (2)$$

O índice de consistência aleatória (RI) é um número fixo e dependente do número de critérios avaliados. A Tabela 3 apresenta os valores dos índices de consistência aleatória (RI):

Tabela 3. Índices de Consistência Aleatória (RI)

Número de Critérios	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Consistência Aleatória (RI)	**0**	**0**	**0.58**	**0.9**	**1.12**	**1.24**	**1.32**	**1.41**	**1.45**	**1.49**

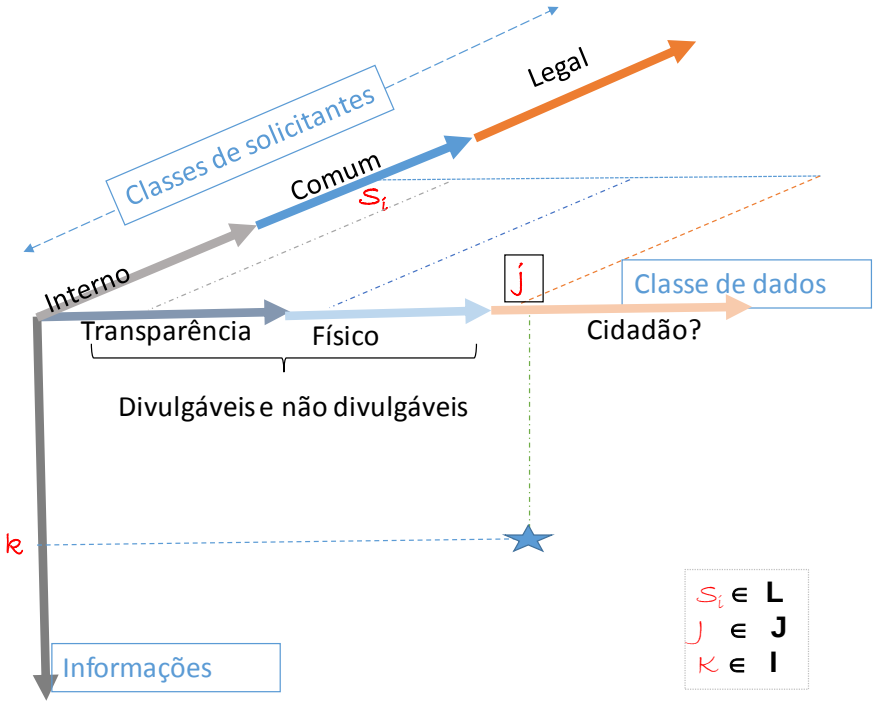
Fonte: Elaboração Própria, 2016.

Segundo Saaty, quando o CR for menor que 10%, é considerado que os valores atribuídos aos critérios constituem uma matriz consistente.

Classificação de dados de subconjuntos

A Figura 9 apresenta o modelo sugerido para fornecimento de acesso a dados, utilizando-se o Vetor Acesso = V(S_i, C_j, I_k), onde S_i refere-se ao pedido, solicitação em si, que pode ser feito por várias entidades, como consumidores, entidades legais, próprio orgão público. C_j corresponde às classes de dados, que podem ser consultadas, divulgadas ou não. I_k referencia às Informações, dados, que fazem parte do cadastro de cada indivíduo. Para uma solicitação i, a qual esta associada à uma classe de dados j, será ou nao fornecida uma informação k, dependendo da análise e da real necessidade do solicitante da i.

Figura 9. Entrada de pedido no orgão público



Fonte: Elaboração Própria, 2016.

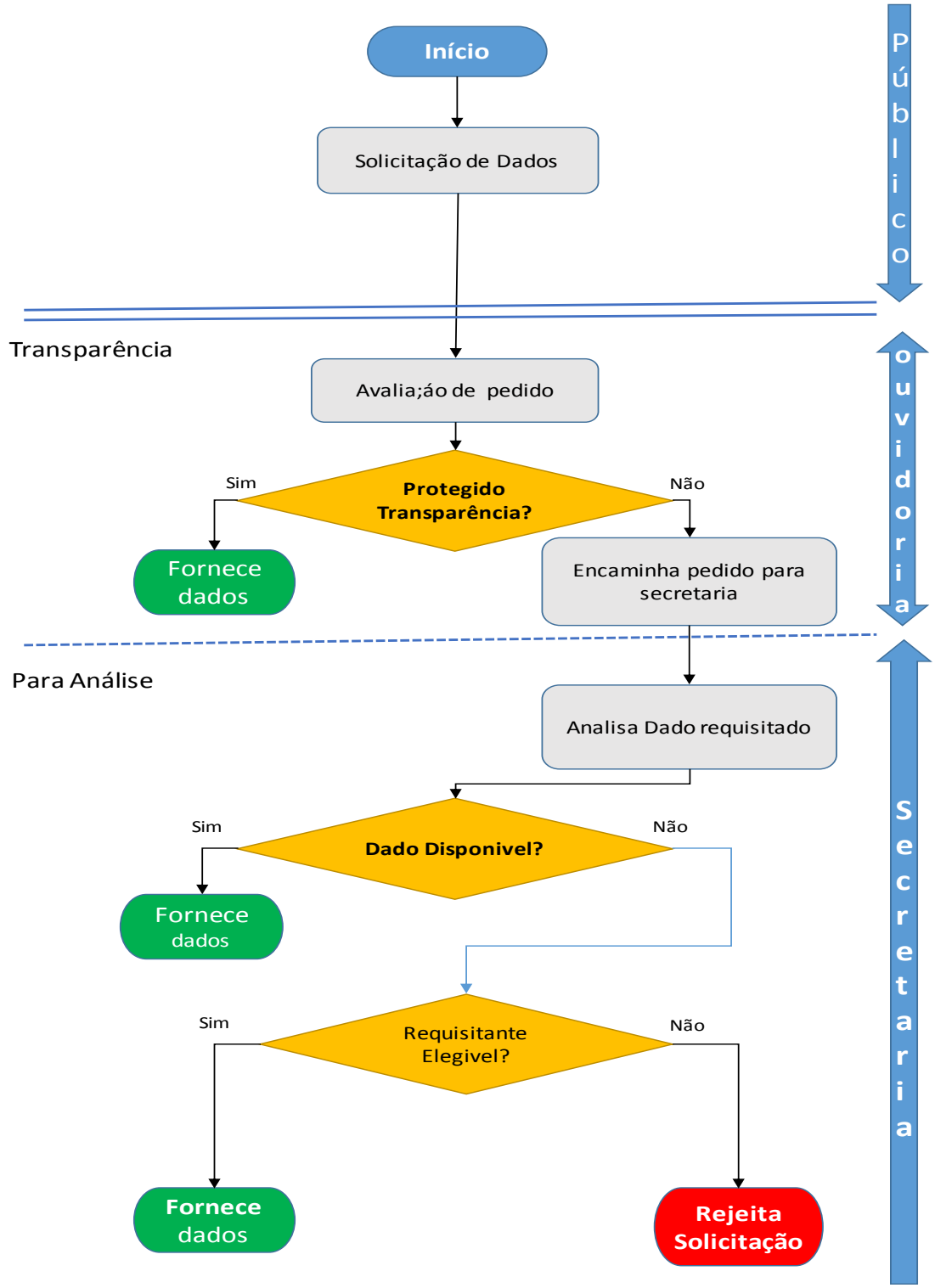
A busca pela informação deve ser feita utilizando um vetor X, com dados diversos que constroem uma informação específica sobre o cidadão. Dependendo de como o vetor for montado, e comparado com as matrizes

disponíveis para o orgão público, o acesso poderá ser dado, isto é, a informação será fornecida, ou negada.

A simplicidade deste modelo está descrita acima, pois o que se está considerando é que os elementos serão testados contra padrões e liberados e/ou eliminados.

Dentro deste modelo, tem-se o seguinte fluxo de pedidos e informações da Figura 10, onde se considera dados dentro da diretriz de transparência, e tratamento com dados que do conjunto de dados não classificados para tratamento pelos orgãos apropriados dentro de estruturas públicas.

Figura 10. Fluxo de pedidos e dados



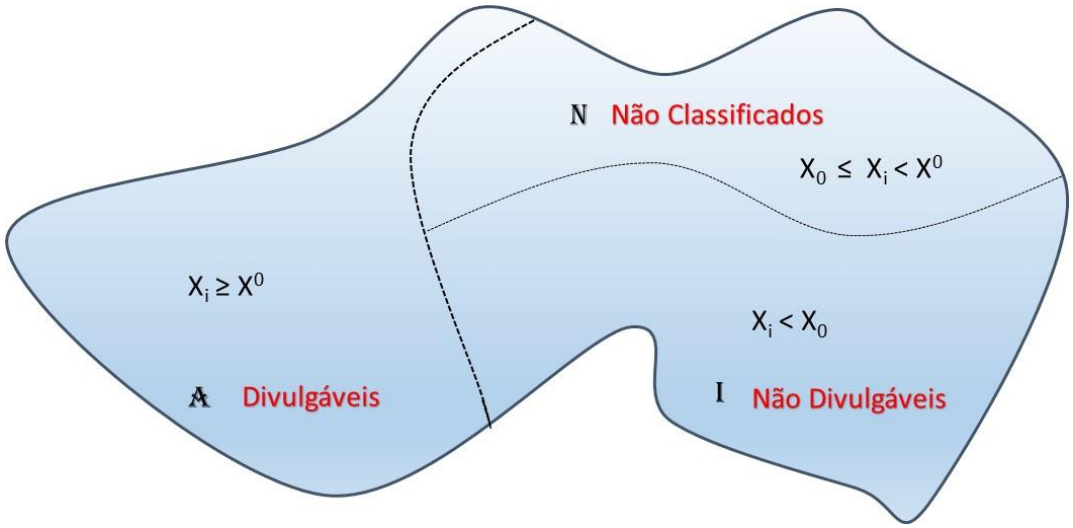
Fonte: Eaboração Própria, 2016.

Para uma análise de dados de conjuntos, onde cada registro corresponde aos dados pessoais de contribuintes, a proposta se baseia no algoritmo descrito na seção seguinte, que trata de dados em subconjuntos.

1.1.9 Classificação de Dados

A Figura 11 apresenta uma proposta para a classificação dos dados quanto à sua confidencialidade. Em um conjunto inicial, todos os dados são considerados não classificados. Utilizando-se o modelo sugerido por SULLIVAN (1977) propõe-se uma forma de identificar aqueles dados que são passíveis de ser divulgados e aqueles que não aceitáveis de serem divulgados.

Figura 11. Dados como estados de dados de um problema



Fonte: Elaboração Própria, 2016.

O objetivo é identificar quais dados X_i , sem análise no conjunto N (não classificados) são passíveis a divulgação dentro do subconjunto de não classificados. É preciso definir quais dados possuem mais capacidade e quais possuem menor capacidade (superiores a X^0 e dados inferiores, respectivamente, a X_0) de tal forma que dados X_i superiores a X^0 são aceitáveis e dados inferiores a X_0 não são aceitáveis. Dados que se encontrem entre X_0 e X^0 ($X_0 \leq X_i < X^0$) serão considerados como não classificados indicando que X^0 e X_0 não são suficientes para uma definição completa dos dados.

Enquanto houver dados indentificados como não classificados, deve-se trabalhar até que o conjunto “N” fique vazio.

1.1.10 Determinação dos dados de capacidade crítica X_0 e X^0

Aplicando o modelo acima para a avaliação de dados de contribuintes, tem-se a necessidade de se definir os valores X_0 e X^0, os quais são limites

críticos. Para cada dado de contribuinte, deverá se ter um vetor onde cada posição do vetor seja a caracterização de um dado (Nome, RG, CPF, Telefone, Endereço, Data de nascimento, e outros). Para cada um desses vetores:

a) Definir os limites pelo conjunto não classificado, introduzindo um Zero (“0”) em $\underline{X}$ (padrão inferior) ou um Hum (“1”) em $\bar{X}$, padrão superior, considerando que todos os dados estão no conjunto “N” (não classificados).

b) Se para β(t=1), houver um $\bar{X}$ (0,1,1,1,...1), o qual é considerado um conjunto de informações aceitáveis de serem fornecidas, então o pedido para liberação deverá ser aceito. Senão, t=t+1 e procede-se para o teste seguinte.

c) O resultado será X = (0, ...1, ...1, ...0, ...1) onde 1 representa o conjunto de dados liberado para divulgação e 0 para o conjunto não liberado para divulgação.

d) Ainda, deve-se levar em consideração quem é o emissor do pedido. Classes de solicitantes poderão direcionar ou não para a divulgação. Por exemplo, pedidos judiciais onde se tem o respaldo da lei, devem ter uma avaliação distinta de uma solicitação por contribuinte comum.

e) O Modelo proposto leva em consideração que a informação é um resultante de:

   i. Canal solicitante
   ii. Contribuinte ou orgão governamental
   iii. Informações liberadas pelo processo da máscara

f) Vetores com modelagens padrões para os diversos casos deverão estar disponíveis, considerando como informações básicas:

   i. CPF ou RG
   ii. Nome
   iii. Endereço
   iv. Telefone
   v. Data de Nascimento

vi. Filiação – nome da mãe

A Figura 12 ilustra um registro de dados:

Figura 12. Modelo de registro de dados Vetor X

X1	X2	X3	X4	X5	X6
CPF ou RG	**Nome**	**Data Nascimento**	**Endereço**	**Telefone**	**Filiação-Mãe**

Fonte: Elaboração Própria, 2016.

g) Um dado Xi, contraposto com os padrões X_0 e X^0, em operações de AND, e resultar valor 1 (Hum), este poderá ser divulgado. Do contrário, não poderá ser divulgado.

Um exemplo é o registro de dados de um contribuinte. Após análises, pode-se definir que um padrão inferior $\underline{X}$ contém todos os 6 campos como 0: (0,0,0,0,0,0), o que resultaria em não divulgação de dado algum. Já o padrão inferior poderia ser $\bar{X}$ = (0,1,1,0,0,0) o qual permite divulgação do nome e data de nascimento. Então, todo e qualquer Xi será comparado com estes padrões e somente serão fornecidos nome e data de nascimento, por exemplo.

A metodologia de apoio a esta pesquisa foi a análise de conteúdo (BARDIN, 2011), que permitiu efetuar um recorte de cada uma das proposições apresentadas para a proteção de dados em alguns países, à partir da elaboração de uma grelha que considerou elementos identificadores da proteção da privacidade dos cidadãos, com relação à manipulação e divulgação de dados pessoais sensíveis.

PERCURSO METODOLÓGICO

Com o objetivo de aplicar o modelo na gestão de dados pessoais dos contribuintes, fez-se um estudo, primeiramente, sobre a gestão de projetos, com base nos requisitos de projetos definidos na sessão 0, para definição dos critérios a serem adotados para a gestão pública. Com base nos critérios de projetos selecionados, consideram-se as alternativas de projetos os pilares da ISO 27001, descritos na sessão 0. Aplicando-se o método de apoio à decisão, AHP, sobre esses dois conjuntos: critérios e alternativas.

Para o tratamento de dados para a confidencialidade, considera-se a análise dos critérios de subconjuntos, o qual definirá ou não a possibilidade de divulgação dos dados.

Modelo da privacidade dentro da gestão pública

Sabe-se que a decisão estará centrada em valores e preferências dos gestores, onde um conjunto de critérios e objetivos serão utilizados para se dar prioridade a um projeto, buscando-se a relação favorável entre investimentos e benefícios.

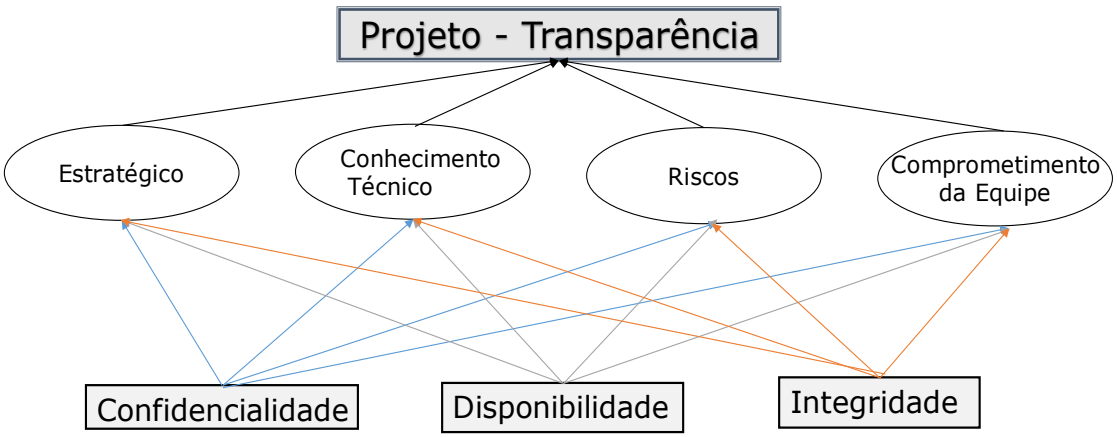
Como alternativas para este projeto, serão consideradas as bases da segurança da Informação: *Confidencialidade, Integridade e Disponibilidade (tripé).*

Para a avaliação das instituições públicas, estarão em foco os 4 critérios primários: *Estratégica, Conhecimento Técnico, Riscos e Comprometimento da Equipe.*

Num primeiro momento, a utilização do modelo AHP será para a definição de qual destas áreas é a prioridade, dentro da avaliação de segurança da informação com foco na privacidade de dados.

O diagrama, baseado no modelo AHP apresentado no capítulo 0 para esta proposta corresponde à Figura 13.

Figura 13. Modelo Hierárquico para seleçào do projeto de segurança



Fonte: Elaboração Própria, 2016.

Para o problema em estudo, o modelo deverá ser aplicado dentro da organização governamental, para apoio na definição de prioridades de segurança para os critérios de seleção de projetos:

Meta: Qual das bases da segurança da informação será priorizada? Por qual área iniciar as análises de dados?

A: Pilares da segurança da informação, baseados na norma ISO 27001 e apresentados no capítulo 3, que define 3 pilares para: confidencialidade, integridade e disponibilidade.

C: Critérios de projetos, os quais deverão ser definidos pelos orgãos governamentais, podendo se basear nas diversas áreas da gestão de projetos explicitados pelo PMI 2014, tais como: estratégico, conhecimento técnico, riscos, comprometimento da equipe, qualidade, custos, e outros.

P: Pesos e critérios definidos pelas instituições selecionadas

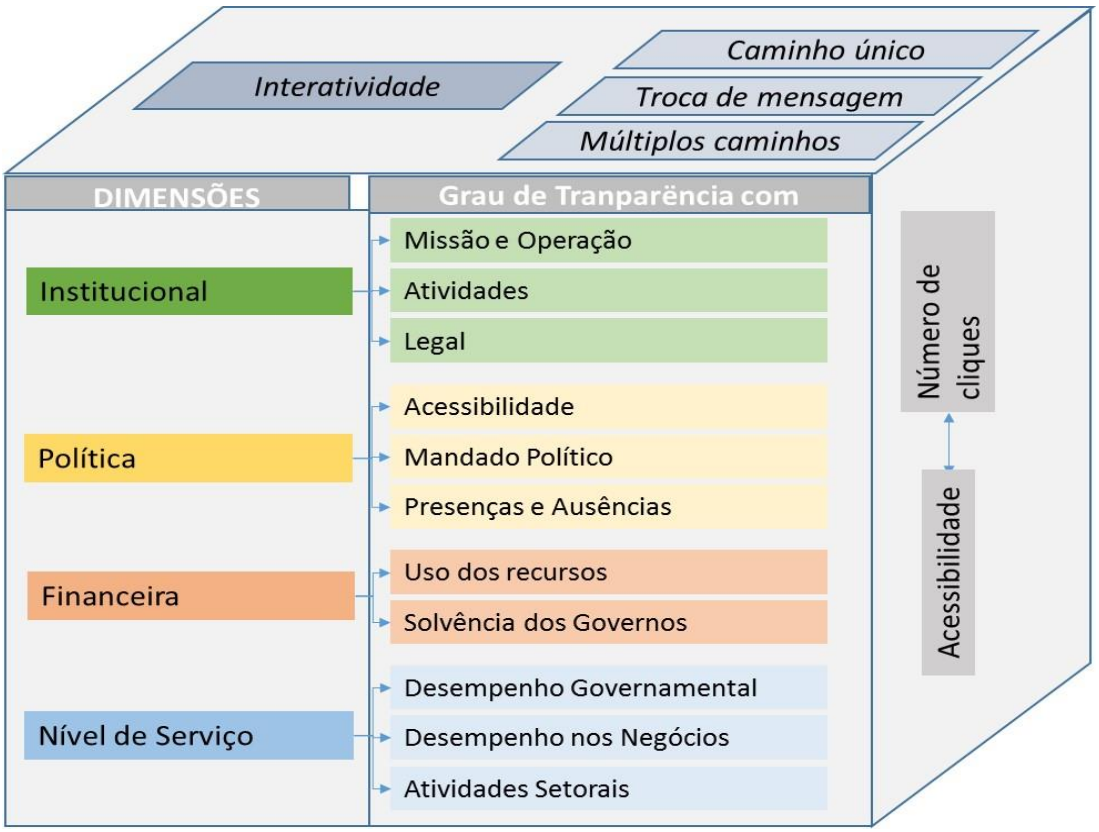
No caso deste estudo, o modelo a ser aplicado sobre o problema da identificação de qual área da segurança da informação, com o foco na divulgação de dados pessoais sensíveis a sererm disponibilizados por órgãos públicos será definido pela cultura do gestor/administrador público, que com sua experiência e conhecimento estará agregando no modelo questões do cotidiano.

Será avaliado um *software* para aplicação junto à instituição que tem interesse na implantação deste modelo. No estudo foi simulada uma aplicação do modelo AHP em *excel*, e os dados rodados encontram-se no Apêndice A.

Tratamento da Transparência

Por outro lado, não se pode desconsiderar um item extremamente importante dentro do setor público: a Transparência. Dentro do setor publico, considera-se a transparência como uma ferramenta de melhoria e demonstração de comprometimento de governantes para com o modelo democrático. Da mesma forma que foi definido em 1.1.9, um modelo de pedido de dados como exemplicado na Figura 9**,** na transparência pública também tem-se a definição de um quadro de avaliação, definido por (TOBERGTE; CURTIS, 2012), como observa-se na Figura 14.

Figura 14. Quadro de Avaliação da Transparëncia



Fonte: Elaboração Própria, 2016, adaptado de (TOBERGTE; CURTIS, 2012)

Este quadro apresenta 4 dimensões que devem ser consideradas quando da avaliação para a transparência no setor público: institucional,

política, financeira e nível dos serviços prestados. A dimensão institucional objetiva tratar do grau de transparência com relação à missão governamental, atividades institucionais e as informações que, obrigatoriamente, devem ser disponibilizadas por força da legislação vigente. Para o âmbito político, trata-se da acessibilidade da informação sobre os representantes e governantes políticos, bem como sua participação e trabalhos desenvolvidos. Quando se trata da dimensão financeira, o olhar estará voltado para o uso dos recursos públicos e nível de endividamento e/ou solvência governamental. A dimensão de nível de serviços está focada no grau de transparência relativo ao desempenho governamental com relação aos serviços prestados aos cidadãos.

Este modelo ainda explora o grau de transparência acoplado à medida de interatividade, que está dividida em três formas. O primeiro deles é o chamado acesso direto ou caminho único, o qual se refere ao acesso às informações e formulários disponibilizados pelos órgãos públicos, muitas vezes de forma estática e sem interação entre o contribuinte e os organismos provedores. O modo de troca de informação pode ser por meio de algum sistema de mensagens ou *e-mails*. E na outra forma de comunicação por múltiplos caminhos, onde um modelo dinâmico se faz presente com o propósito de fornecer uma troca externa para cada uma das 4 dimensões apresentadas.

Cada uma destas dimensões está dividida em diferentes itens, e são avaliadas utilizando-se medidas e questionários específicos. Neste estudo, as dimensões institucionais e de nível de serviços são as mais exploradas, quando são avaliados quesitos legais no fornecimento de informações pessoais, e a utilização de questionários para o tratamento dos pedidos recebidos pelos setores administrativos públicos, com orientação e gerenciamento das ouvidorias.

O tratamento da transparência, junto com análise de dados por subconjuntos, permitirá que os órgãos públicos possam disponibilizar dados sem ferir a privacidade pessoal dos contribuintes.

Alternativa: Confidencialidade – Análise de subconjunto de dados

Após a definição do projeto, ações apropriadas serão requeridas para cada alternativa. Estará em discussão a ação a ser considerada para a alternativa da confidencialidade.

Vetores com modelagens padrões para os diversos casos deverão estar disponíveis, considerando as informações básicas exemplificadas na Figura 12.

Na consideração de todos os dados sobre contribuintes, que uma instituição pública possa administrar (ou seja, é detentora e é requerida a salvaguardar estes dados), têm-se uma quantidade grande de dados que estão sujeitos às leis e regras de privacidade, e outro tanto que não estão classificados como tal. Como nos casos de:

a. Se considerar-se os 10 sobrenomes mais comuns segundo (PROCOB, [s.d.]), sem outro dado qualquer, este somente não poderá caracterizar um indivíduo, preservando a privacidade;
b. Dados requisitados com base em documentos legais serão sempre disponibilizados aos requerentes e somente aos requerentes.

Os dados de usuários e/ou contribuintes, utilizados por organizações públicas, são coletados quando o cidadão busca os serviços públicos, tais como: saúde, transporte, urbanismo, saneamento ou fiscal.

No momento do cadastro, são requisitados dados sobre os indivíduos, e de uma forma geral são requisitados dados como:

a. Nome
b. Data de nascimento
c. Cadastro de pessoa física ou registro geral, com data de expedição
d. Endereço

Por exemplo, para um cidadão requisitar o cartão de estacionamento de idoso ou deficiente físico, será requisitado que preencha um cadastro do setor de transporte fornecendo estes dados (SAO PAULO, 2015).

Como cadastro de contribuintes junto às organizações de água e saneamento básico não é diferente.

Na saúde, estes dados também são requisitados, não se limitando a eles. Muitas organizações também requisitam nome dos progenitores.

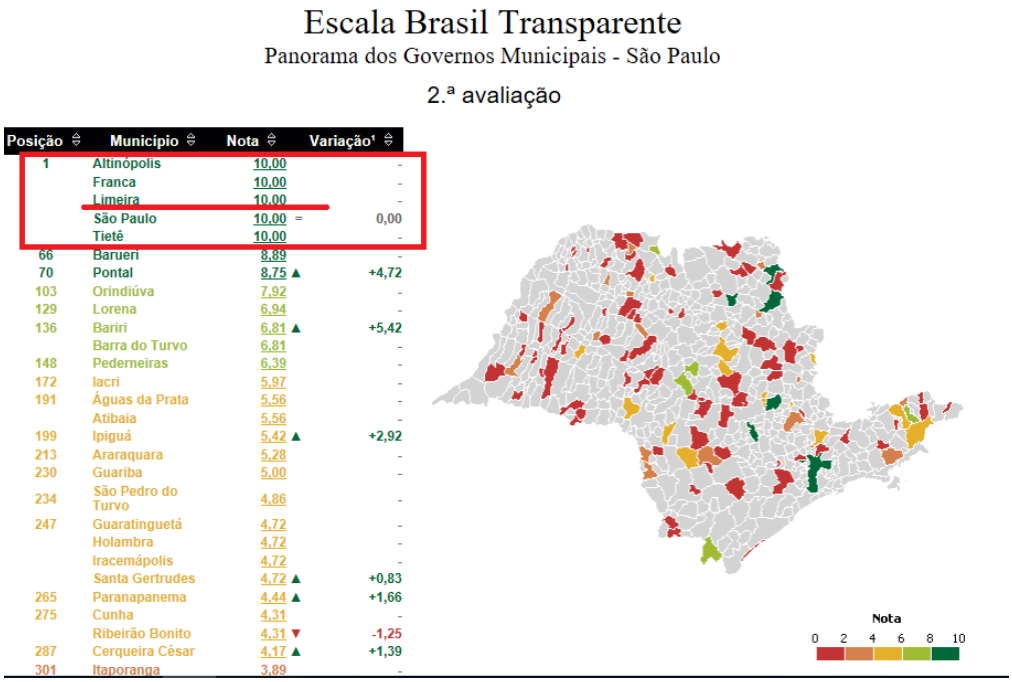
APLICAÇÃO POR MEIO DE ESTUDO DE CASO: DADOS UTILIZADOS PELOS SETORES PÚBLICOS

Esta pesquisa utiliza um estudo de caso para consolidar o processo de investigação e delimitar o universo a ser estudado. Para tanto, buscou-se, na região de Campinas, cidades que atendessem alguns critérios essenciais para aplicação dos procedimentos desenvolvidos. Basicamente, os elementos necessários para que a prefeitura pudesse participar do experimento foram:

a. Ter um processo de ouvidoria consciente da problemática estudada;
b. Grande número de solicitações para disponibilizar informações críticas;
c. Equipe proativa para estudo e aplicação de novos procedimentos na ouvidoria;
d. Execução do trabalho dentro do período do desenvolvimento desta pesquisa;
e. Constar da lista de municípios avaliados pelo Ministério da Transparência.

A partir destes critérios, buscou-se o contato com as prefeituras da Região Metropolitana de Campinas, e embora os interesses externados, a cidade de Limeira atendeu a todos os critérios e, também, os gestores se mostraram altamente interessados na proposta por terem já vivenciado situações nas quais um procedimento, conforme é a proposta deste trabalho, teria sido extremamente útil. Além disso, Limeira faz parte dos municípios com nota 10 (dez), dentro do *ranking* do Ministério da Transparência, Fiscalização e da Controladoria Geral da União (BRASIL, 2015), como apresentado na Figura 15.

Figura 15. *Ranking* de Transparëncia das cidades



Escala Brasil Transparente

Panorama dos Governos Municipais - São Paulo

2.ª avaliação

Posição	Município	Nota	Variação¹
1	Altinópolis	10,00	-
	Franca	10,00	-
	Limeira	10,00	-
	São Paulo	10,00 =	0,00
	Tietê	10,00	-
66	Barueri	8,89	-
70	Pontal	8,75 ▲	+4,72
103	Orindiúva	7,92	-
129	Lorena	6,94	-
136	Bariri	6,81 ▲	+5,42
	Barra do Turvo	6,81	-
148	Pederneiras	6,39	-
172	Iacri	5,97	-
191	Águas da Prata	5,56	-
	Atibaia	5,56	-
199	Ipiguá	5,42 ▲	+2,92
213	Araraquara	5,28	-
230	Guariba	5,00	-
234	São Pedro do Turvo	4,86	-
247	Guaratinguetá	4,72	-
	Holambra	4,72	-
	Iracemápolis	4,72	-
	Santa Gertrudes	4,72 ▲	+0,83
265	Paranapanema	4,44 ▲	+1,66
275	Cunha	4,31	-
	Ribeirão Bonito	4,31 ▼	-1,25
287	Cerqueira César	4,17 ▲	+1,39
301	Itaporanga	3,89	-

Fonte: (BRASIL, 2015)

Após discussões e apresentações junto aos diversos setores da prefeitura, com participação da pesquisadora em reuniões da Comissão Mista de Reavaliação de Informações, comandada pela Ouvidoria e com representação de todas as secretarias, foi apresentado o tema como assunto relevante.

Avaliando-se os dados dos relatórios de pedidos de informações, gerenciados pela Ouvidoria, constatou-se que a secretaria com maior número de pedidos é a de Obras e Urbanismo, como apresentado pela Figura 16, e, em sua maioria, os pedidos referem-se a dados pessoais de proprietários de terrenos e lotes, dentro do município.

Figura 16. Relatório da Ouvidoria para Março / 2016

- **Órgãos Mais Demandados e Número de Pedidos.**

Secretaria	Pedidos Enviados
Urbanismo	**16**
Ouvidoria	12
Administração	11
Fazenda	6
Serviços Públicos	5
Saúde	1
Obras	1
Mobilidade	1
SAAE	1
Meio Ambiente	1

Fonte: Portal Município de Limeira, 2016

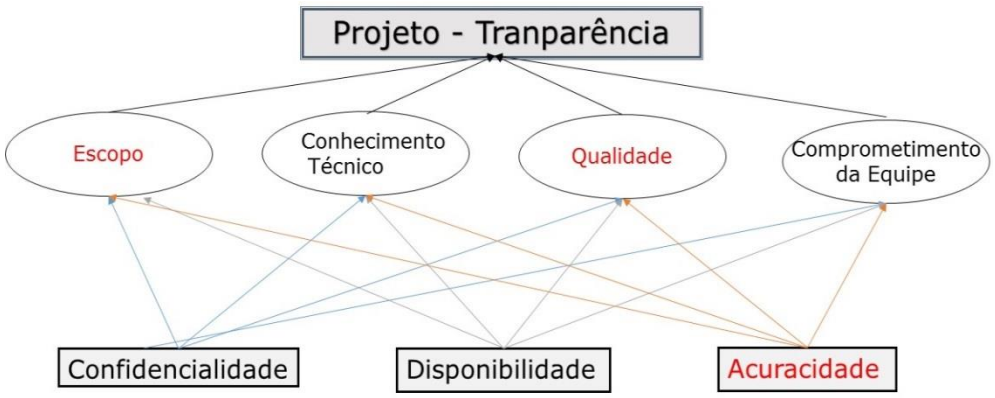
A concordância sobre a criticidade do tema privacidade era unânime, porém não se tinha o conhecimento de como tratar e quais as regras vigentes no mercado. Como os municípios possuem um direcionamento governamental para a transparência, eles tendem a disponibilizar toda e qualquer informação, sem perceber o risco da confidencialidade e privacidade.

Com este cenário, tiveram início os trabalhos fornecendo-se um seminário educativo a todos os integrantes da Comissão Mista, sobre todos os itens pesquisados: legislações em outros países, tripé da segurança de dados, como integrar com gestão de projetos, e tratamento das informações utilizando-se a teoria de conjuntos, assuntos já tratados no capítulo 0.

Estabeleceu-se um planejamento de trabalho, considerando o volume e diversidade de informações a serem trabalhadas. Assim, a coleta das informações a serem utilizadas pelo procedimento proposto neste trabalho foram coletas por meio de dois questionários apresentados aos gestores e oriundas de documentos específicos (ver Anexo).

O primeiro questionário apresentado no Anexo A tem o objetivo de colher, junto à Secretaria de Obras, quais áreas dos assuntos abordados são mais relevantes. Com base nas respostas fornecidas para a primeira pergunta, a qual está focada em elencar os diversos critérios da Gestão de Projetos, foi elaborado o modelo de hierarquia, como consta na Figura 17, em contraposição ao modelo original (Figura 13), onde os itens Escopo e Qualidade foram evidenciados pelos gestores, em detrimento de Estratégico e Riscos do modelo de estudo.

Figura 17. Modelo Hierárquico com dados da Secretaria de Obras e Urbanismos



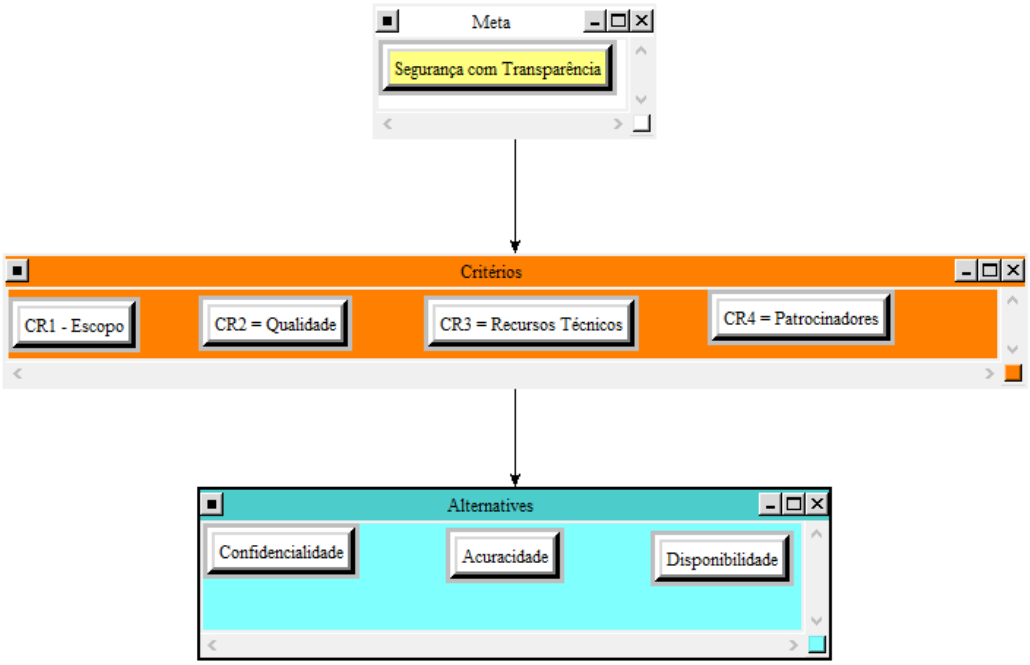
Fonte: Elaboração Própria, 2016.

A segunda pergunta do questionário apresentada no Anexo A tem como objetivo definir quais alternativas da segurança de dados são mais relevantes para o setor. Neste quesito, foram escolhidos 3 itens prioritários, e neste trabalho, também, o item integridade, do tripé da qualidade, foi substituído pelo item acuracidade (Figura 17).

A terceira e quarta questões buscam colher, junto aos gestores, quais informações são mais requisitadas e quais são mais relevantes para o município.

Após análise das respostas para estas quatro questões, foi elaborado um novo questionário, voltado para a coleta de informações de forma a ser utilizado o modelo de apoio à decisão, AHP, cujas respostas constam do Anexo B. Para estudo dos mesmos, escolheu-se o *Software SuperDecisions*, dentre os muitos existentes para aplicação do AHP, por ter sido ele desenvolvido pelo próprio criador do Método AHP, e também por ser disponibilizado gratuitamente, o que facilita o acesso ao mesmo pelos gestores da prefeitura sem envolver questões financeiras. Para tanto, o modelo de *clusters* do *SuperDecisions* para este caso, é como apresentado na Figura 18.

Figura 18. Modelo de *Clusters* do AHP, dentro do SuperDecisions

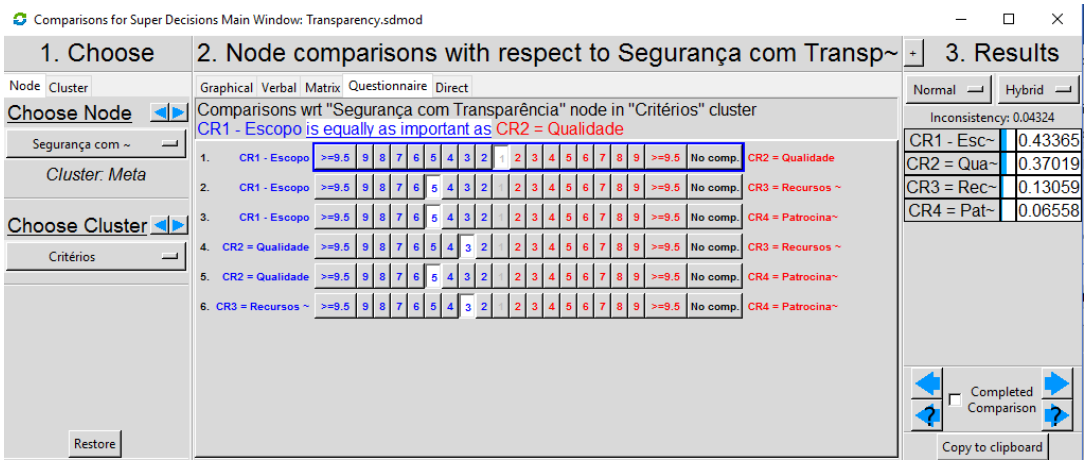


Fonte: Elaboração Própria, utilizando SuperDecisions (2016)

Esta ferramenta permite que o modelo seja dividido em *clusters*, desde meta, passando por critérios, e culminando com alternativas (no caso desde modelo, foi necessário criar esta última como *Alternatives,* do termo em inglês, para que os resultados pudessem ser avaliados).

Desta forma, foram atribuídos pesos aos critérios e alternativas, de acordo com os valores fornecidos no Anexo B, conforme ilustra a *Figura 19*.

Figura 19. Comparação dos Critérios em relação à Meta - Segurança com Transparência



Fonte: Resultado SuperDecisions (2016)

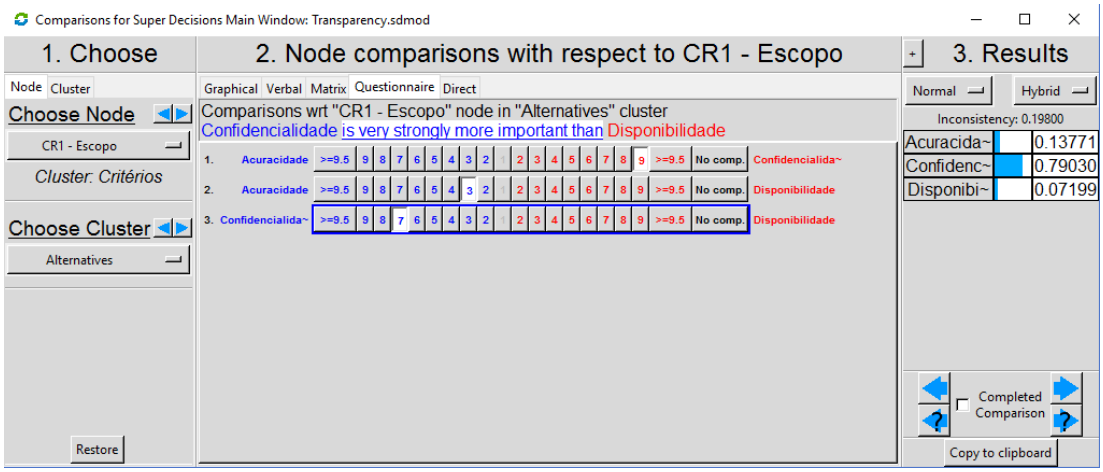
Nesta Figura 19, pode-se observar uma prevalência de Escopo sobre Qualidade, desta sobre Recursos Técnicos e Patrocinadores, e uma moderada importância de Recursos Técnicos sobre Patrocinadores.

Quando se avança com a análise das alternativas em relação aos critérios, observa-se figuras específicas, comparando-se cada uma das 3 alternativas, com relação a cada critério, utilizando-se a escala de SAATY, 2005, já discutida em 1.1.8.

A. Critério 1: Escopo

Na Figura 20, pode-se observar que Confidencialidade tem mais peso do que Acuracidade e Disponibilidade.

Figura 20. Pesos das alternativas para critério de Escopo

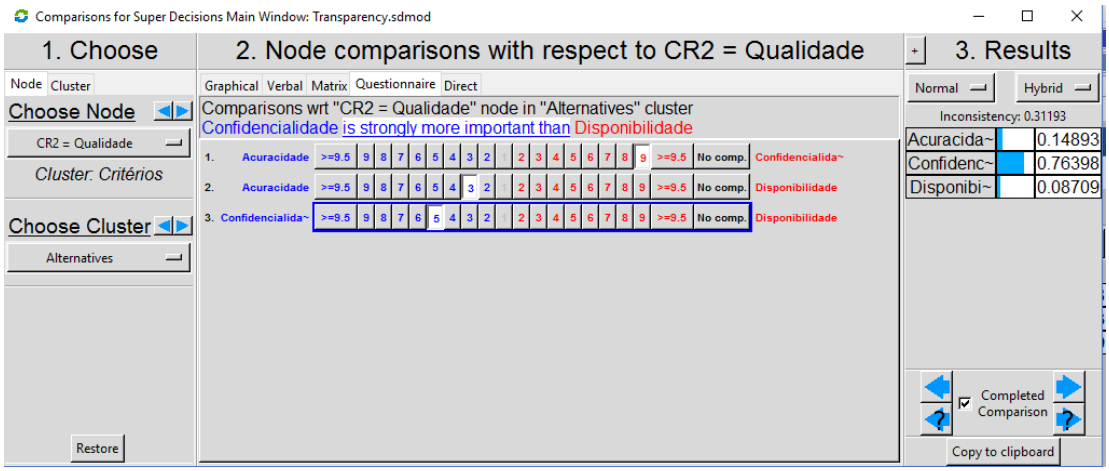


Fonte: Resultado da simulação com SuperDecisions (2016)

B. Critério 2: Qualidade

Observa-se, na Figura 21, que Confidencialidade também se sobrepõe a Acuracidade e Disponibilidade, mas que Acuracidade se sobressai moderadamente em relação à Disponibilidade, com mais veemência do que no critério Escopo.

Figura 21. Pesos das alternativas para critério de Qualidade

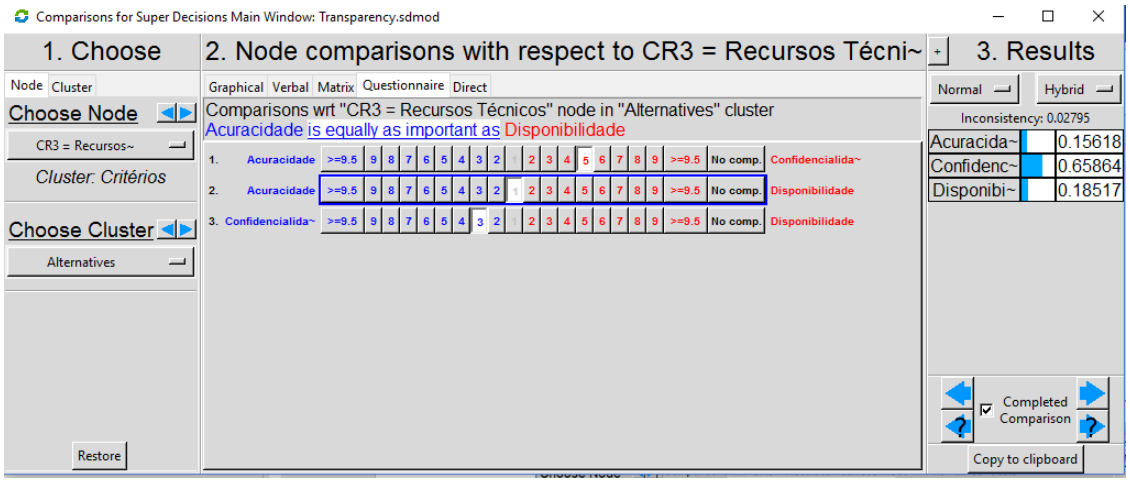


Fonte: Resultado da simulação com SuperDecisions (2016)

C. Critério 3: Recursos Técnicos

Na Figura 22 verifica-se que Confidencialidade continua como a mais forte das alternativas, para o critério Recursos Técnicos.

Figura 22. Pesos das alternativas para critério de Recursos Técnicos

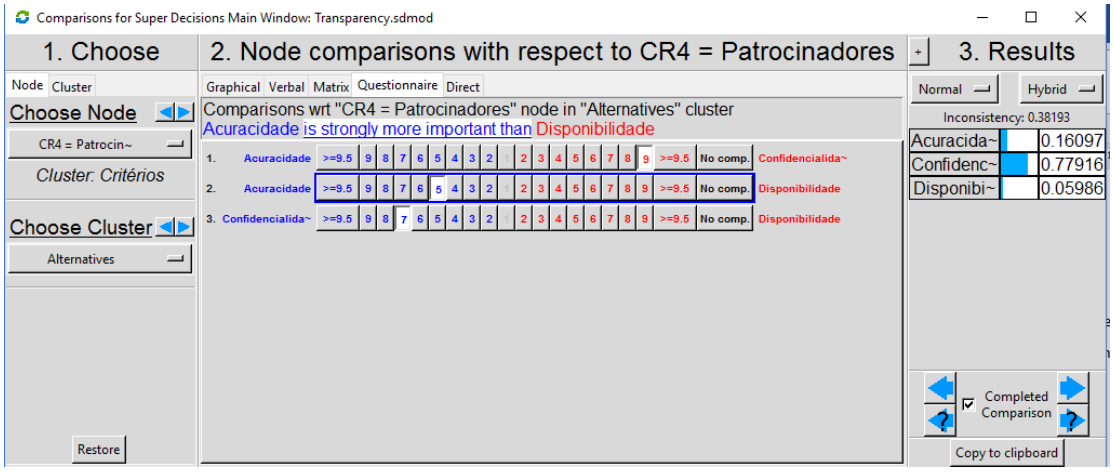


Fonte: Resultado da simulação com SuperDecisions (2016)

D. Critério 4: Patrocinadores

Neste critério, também a alternative de confidencialidade tem uma grande prevalescência sobre as demais alternativas, como apresentado na Figura 23.

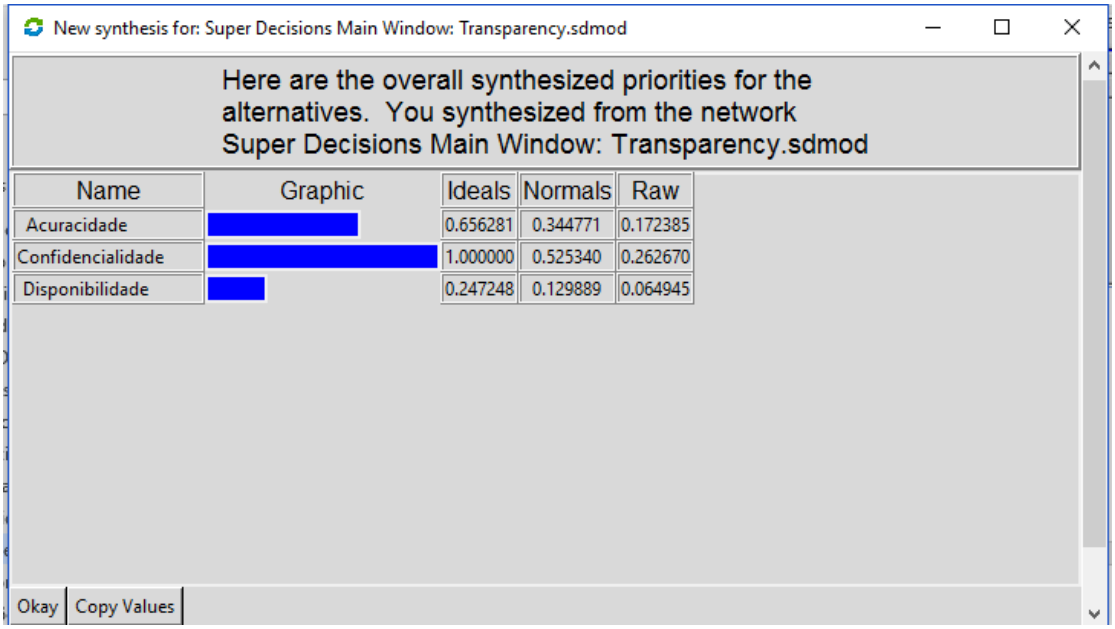
Figura 23. Pesos das alternativas para critério de Patrocinadores



Fonte: Resultado da simulação com SuperDecisions (2016)

O simulador *SuperDecisions* fornece várias análises de dados, entre elas a da Figura 24 , onde se pode observar a prevalecência da Confidencialidade, em relação às demais alternativas.

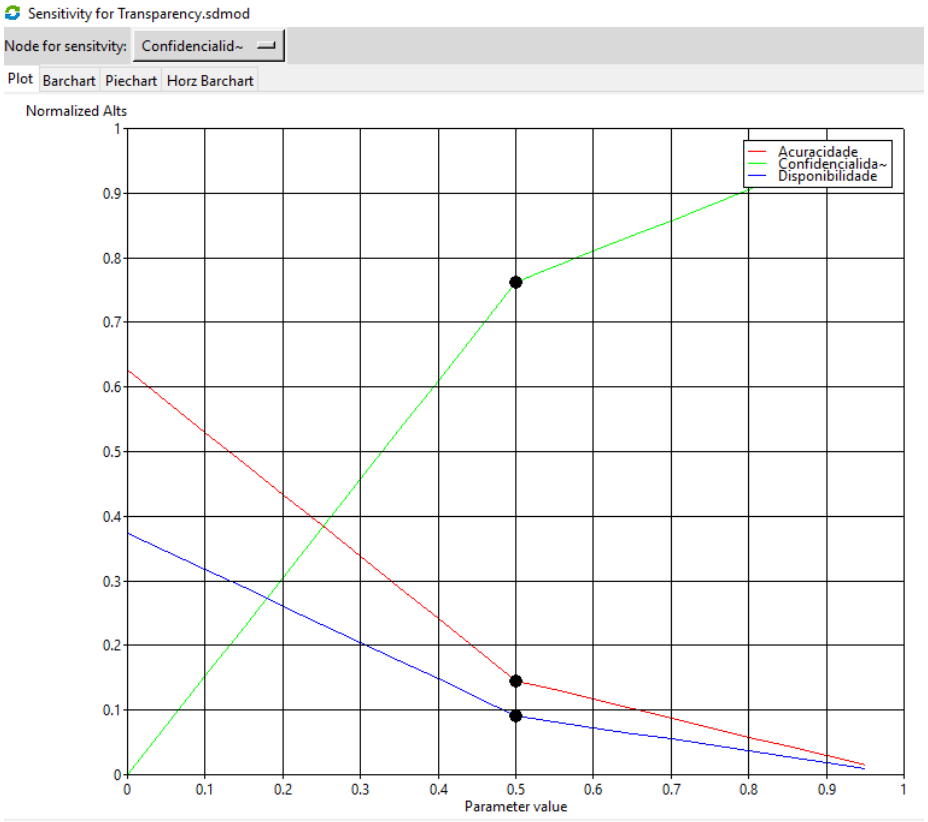
Figura 24. Análise das prioridades para alternativas apresentadas



Fonte: Resultado da simulação com SuperDecisions (2016)

Outra possibilidade é a análise da sensibilidade de uma alternativa para o modelo, como, por exemplo, a Confidencialidade, apresentada na ***Figura 25***.

Figura 25. Sensibilidade para Confidencialidade no Modelo de Segurança com Transparëncia



Fonte: Resultado da simulação com SuperDecisions (2016)

Esta figura apresenta a sensibilidade de todas as alternativas (acuracidade, confidencialidade e disponibilidade), em relação aos critérios e meta. Percebe-se umm valor da sensibilidade da confidencialidade muito superior às outras alternativas, a qual está representada pela linha verde.

Manuseio de informações pessoais dentro de secretarias

No dia a dia das instituições públicas, onde larga quantidade de dados e documentos é manuseada diariamente, faz-se necessário se estabelecer processos e procedimentos que agilizem no provimento das informações, mas que também garantam o cumprimento da legislação.

A Secretaria de Obras e Urbanismos da Prefeitura de Limeira utiliza um formulário padrão, eletrônico, para acesso às informações sobre os imóveis naquela localidade. Trata-se do Sistema de Imposto Predial e Territorial Urbano, conhecido também como CN-SIREM, como mostrado na Figura 27, no Anexo C. Este formulário está dividido em duas sessões, conhecidas como sessões A e

B. Na Sessâo B, constam informações técnicas do imóvel. Na Sessâo A, estão os dados do proprietário e/ou compromissário, que é um responsável pelo bem, mas sem estar devidamente registrado em cartório. Este formulário da prefeitura serve como fonte para diversos pedidos de informações.

Foi explicado e discutido com os responsáveis que:

1. O problema da privacidade pessoal consiste em preservar informações que dizem respeito às pessoas, e não a bens físicos. Desta forma, dados técnicos de imóveis e patrimônios físicos não fazem parte desta discussão. A Parte B do formulário CN-SIREM não está passível de proteção;
2. A regra para fornecimento de informação, a qual não esteja protegida pela Lei de Acesso à Informação (LAI) deve ser de não voluntariar e oferecer dados sobre pessoas físicas;
3. Está em discussão a preservação de dados pessoais, os quais permitam a outros identificar onde localizar o indivíduo, fisicamente. Sua residência, local de trabalho, telefones e outros dados pessoais.

Com informações sobre a importância da preservação de dados, e utilizando-se o modelo de classificação de dados de subconjuntos, foi requisitado que a secretaria classificasse os dados pessoais através de duas questões, constantes do Anexo A, questões 3 e 4. Com base neste questionário, tem-se este vetor real, como apresentado na Figura 26, onde somente 5 conteúdos foram considerados importantes, mas os 3 primeiros, Nome, CPF e Endereço são os mais requisitados

Figura 26. Modelo de registro de dados para Secretaria de Obras e Urbanismo de Limeira

X1	X2	X3	X4	X5
Nome	**CPF ou RG**	**Endereço**	**Data Nascimento**	**Telefone**

Fonte: Elaboração Própria, 2016.

Após analises e estudos, ficou concordado pelos responsáveis técnicos que:

1. O formulário CN-SIREM possui uma opção de impressão, como consta na Figura 28. As duas primeiras opções, como grifadas, não estarão mais sendo disponibilizadas como opções para impressão, voluntariamente, das fontes de dados, quando se tratar dos dados do proprietário;
2. O sistema de impressão foi alterado para não mais imprimir todo o registro de dados;
3. Não voluntariar a entrega de informações. Somente com pedido judicial será fornecida, ou com procuração em cartório;
4. Somente dados que não permitam a localização física podem ser disponibilizados (nome, data de nascimento).

CONCLUSÕES

Este trabalho abordou o tratamento da segurança da informação para dados pessoais, privados. O tratamento da transparência, junto com a análise de dados por subconjuntos, pode-se permitir que os órgãos públicos possam disponibilizar dados sem ferir a privacidade pessoal dos contribuintes.

Para a concretização deste estudo, utilizou-se conceitos de gestão de projetos, para definição de características da disciplina. A utilização de um mecanismo de segurança de dados pessoais proporciona uma confiabilidade almejada sobre as informações que podem ou não serem divulgadas. Com a estratégia de implementação adotada no modelo de análise hierárquica de dados, a definição de priorização da confidencialidade de dados, em detrimento de outras áreas do tripé de segurança, respalda o comprometimento das organizações, dentro do modelo de Cidades Inteligentes, a ser adotado.

Além disso, foi implementado um fluxograma dentro da organização para classificação de dados, o qual não disponibiliza, de modo voluntário, dados que possam identificar quem e onde se encontra qualquer indivíduo.

Diante da diversidade de dados e requisições impetradas junto aos escritórios de Ouvidoria, uma análise do canal de entrada, dos dados requisitados, e a disponibilização dos mesmos com medidas que indicam cautela e preservação dos dados se faz necessária. Os resultados dos testes mostraram uma disponibilidade e coerência com o tratamento dos dados.

Por fim, vale ressaltar os benefícios dos resultados práticos deste trabalho para as comunidades usuárias dentro do modelo de Cidades Inteligentes. Devido ao baixo custo da solução implementada, a qual não requer investimentos em tecnologia, mas em definição de processos, torna-se viável sua implantação no campo, aqui delimitado pelas secretarias das cidades informatizadas, inteligentes. Além disso, reforça a garantia da qualidade do serviço oferecido estar dentro dos padrões mínimos requeridos pela Lei da Transparência.

Resumidamente, as principais contribuições deste trabalho foram:

- Implementação e resultados das análises de modelo de Apoio à Tomada de Decisão, o qual respaldou a escolha da confidencialidade como quesito principal;
- Implementação de um fluxograma para manuseio de dados, dependendo do canal de entrada do pedido;
- Implementação e resultados das análises dos dados privados, fundamentada em legislações vigentes em outros países e sem ferir a transparência legislativa;

Sugestões para trabalhos futuros

Após a finalização desse trabalho, são apresentadas algumas sugestões para a continuidade do trabalho ora apresentado, conforme descrição a seguir.

- Desenvolvimento de um processo padronizado de coleta de dados, que garanta que somente dados pertinentes sejam realmente coletados.
- Desenvolvimento de processos mais robustos para Cidades Inteligentes, no que tange ao tratamento de informações e manuseio de dados.
- Apresentar aos órgãos públicos (Prefeituras e Municípios), alternativas com processos e sistemas robustos de coleta, proteção e divulgação de dados em todas as organizações.

REFERÊNCIAS

ABNT. **ABNT NBR ISO/IEC 27001:2013 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos**ABNT, , 2013.

AUSTRALIAN GOVERNMENT. Privacy fact sheet 17: Australian Privacy Principles. n. March, p. 1–11, 2014.

BALAKRISHNA, C. Enabling technologies for smart city services and applications. **Proceedings - 6th International Conference on Next Generation Mobile Applications, Services, and Technologies, NGMAST 2012**, p. 223–227, 2012.

BANLSAR, D. National Comprehensive Data Protection / Privacy Laws and Bills 2016. n. July, 2016.

BARDIN, L. **Análise de Conteúdo**. [s.l: s.n.].

BARTOLI, A. et al. Security and Privacy in your Smart City. **Cttc.Cat**, p. 1–6, 2011.

BAUMANN, R. et al. **BRICS Estudos e Documentos**BrasíliaFundação Alexandre de Gusmão, , 2015. Disponível em: <http://funag.gov.br/loja/download/1126-BRICS-Estudos_e_Documentos.pdf>

BRANCO, R. C. A “QUESTÃO SOCIAL” NA ORIGEM DO CAPITALISMO: pauperismo e luta operária na teoria social de Marx e Engels. p. 1–181, 2006.

BRASIL. Lei No. 12.414, de 9 de Julho de 2011. Lei do Cadastro Positivo. **Diário Oficial da União**, v. Brasilia, p. 2014–2017, 2011a.

BRASIL. **LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011. Lei da Transparência**, 2011b. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>

BRASIL. **Constituição Federal do Brasil (1988). Emendas Constitucionais no.s 1/1992 a 68/2011, pelo Decreto Legislativo no. 186/2008 e pelas Emendas Constitucionais de Revisão no.s 1 a 6/1994**. [s.l.] Biblioteca Digital Câmara dos Deputados, 2012a.

BRASIL. **DECRETO Nº 7.724, DE 16 DE MAIO DE 2012. Acesso à Informação**, 2012b.

BRASIL. Lei No. 12.965, de 23 de abril de 2014. Marco Civil da Internet. **Diário Oficial da União, Brasiília, DF**, p. 1–8, 2014.

BRASIL. **Ranking de cumprimento da Lei de Acesso à Informação - 2a. avaliação**, 2015.

BRESSER-PEREIRA, L. C. A Revolução Capitalista. 2016.

CALDWELL, T. Data loss prevention - Not yet a cure. **Computer Fraud and Security**, v. 2011, n. 9, p. 5–9, 2011.

CALLAHAN, M. E. U.S. DHS Handbook for Safeguarding Sensitive Personally Identifiable Information. n. March, 2012.

CAVALCANTE, Z. V.; DA SILVA, M. L. S. A Importância da Revolução Industrial no mundo da tecnologia. **VII Encontro Nacional de Produção Científica**, 2011.

CILLIERS, L.; FLOWERDAY, S. Information security in a public safety, participatory crowdsourcing smart city project. **2014 World Congress on Internet Security, WorldCIS 2014**, p. 36–41, 2014.

COMMONWEALTH GOVERNMENT OF AUSTRALIA. Privacy Act 1988. n. 119, 2016.

CRAWFORD, L. H.; HELM, J. Government and governance: The value of project management in the public sector. **Project Management Journal**, v. 40, n. 1, p. 73–87, 2009.

DONEDA, D. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: [s.n.].

FLEETS, T. B. **Top 100**. [s.l: s.n.].

FORSBERG, K. **Visualizing Project Management**. [s.l: s.n.].

GATTÁS, R. **A Indústria automobilística e a segunda revolução industrial no Brasil**, 1982. (Nota técnica).

GLOBO. **MPF apura vazamento de dados do INSS para uso de bancos e financeiras**, 2016. Disponível em: <http://g1.globo.com/bom-dia-brasil/noticia/2016/02/credito-consignado-e-oferecido-trabalhadores-antes-da-aposentadoria.html>

GOMES, L.F.A.M.; GOMES, C.F.S.; ALMEIDA, A. T. **Tomada de Decisão Gerencial - Enfoque Multicritério**. [s.l: s.n.].

GUTWIRTH, S; LEENES, R; DE HERT, P. **Reloading Data protection - Multidisciplinary Insights and Contemporary Challenges**. [s.l.] Springer Science-Business Media Dordrecht, 2014.

KATE; LUCENTE, J. C. **DATA PROTECTION LAWS OF THE WORLD**DLAPIPER, , 2015. Disponível em: <http://www.dlapiperdataprotection.com>

KING, N. J.; RAJA, V. T. Protecting the privacy and security of sensitive customer data in the cloud. **Computer Law and Security Review**, v. 28, n. 3, p. 308–319, 2012.

KINGDOM, U. **Data Protection Act 1998**TSO (The Stationary Office), , 2005. Disponível em: <http://www.legislation.gov.uk/ukpga/1998/29/contents>

MARTINEZ-BALLESTE, A.; PEREZ-MARTINEZ, P.; SOLANAS, A. The pursuit of citizens' privacy: A privacy-aware smart city is possible. **IEEE Communications Magazine**, v. 51, n. 6, p. 136–141, 2013.

MENDES, L. S. TRANSPARÊNCIA E PRIVACIDADE: VIOLAÇÃO E PROTEÇÃO DA INFORMAÇÃO PESSOAL NA SOCIEDADE DE CONSUMO.

UnB - Universidade de Brasília, 2008.

NAKAGAWA, F. **Brasil cai para a posição de 9ª economia do mundo**Exame.com, , 2016. Disponível em: <http://exame.abril.com.br/economia/pib-em-dolar-cai-25-e-brasil-cai-para-a-posicao-de-9a-economia-do-mundo/>

NATIONS, U. **World Urbanization Prospects: The 2014 Revision, Highlights (ST/ESA/SER.A/352)New York, United**. [s.l: s.n.]. Disponível em: <http://esa.un.org/unpd/wup/Highlights/WUP2014-Highlights.pdf>.

NATIONS, U. **World Urbanization Prospects, the 2014 revision**, 2014b. Disponível em: <http://esa.un.org/unpd/wup/Country-Profiles/>

OVIDIU VERMESAN, P. F. **Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems**. [s.l: s.n.].

PEIXOTO, R.; OLIVEIRA, M. DE; MAIO, E. R. EDUCAÇÃO ESCOLAR: UMA NECESSIDADE A PARTIR DAS MUDANÇAS NAS RELAÇÕES DE TRABALHO. p. 1–18, [s.d.].

PMI. **A Guide to the Project Management Body of Knowledge (PMBOK® Guide)—Fifth Edition (ENGLISH)**. [s.l: s.n.].

POITRAS, L. **Citizenfour**, 2014. Disponível em: <https://citizenfourfilm.com/>

PROCOB. **Os Sobrenomes Mais Comuns Do Brasil**PROCOB, , [s.d.]. Disponível em: <https://www.procob.com/os-sobrenomes-mais-comuns-do-brasil/>

RODOTÀ, S. **A vida na sociedade da vigilância**. [s.l: s.n.].

SAATY, T. L. **Theory and Applications of the Analytic Network process: Decision Making with Benefits, Opportunities, Costs and Risks**. Pittsburgh: [s.n.].

SAATY, T. L. Relative Measurement and its Generalization in Decision Making: Why Pairwise Comparisons are Central in Mathematics for the Measurement of In¬tangible Factors - The Analytic Hierarchy/Network Process. **Review of the Royal Spanish Academy of Sciences, Series A. Mathematics**, 2008.

SALOMON, V.; MONTEVECHI, J. Justificativas Para Aplicação Do Método De Análise Hierárquica. **Anais do 19o ENEGEP**, 1999.

SANTOS, L. G. D. C. Análise Da Influência Da Evolução Na Maturidade Em Gerenciamento De Projetos No Desempenho Dos Projetos. p. 1–145, 2009.

SAO PAULO, P. **Cartão de Estacionamento para Idoso**, 2015. Disponível em: <http://www.prefeitura.sp.gov.br/cidade/secretarias/transportes/autorizacoes_especiais/index.php?p=21225>

SEMERARO, A.; CARDOSO, R. OUVIDORIA PÚBLICA COMO INSTRUMENTO DE MUDANÇA. **Instituto de Pesquisa Econômica Aplicada – ipea 2010**, 2010.

SULLIVAN, R. L. **Power System Planning**. [s.l: s.n.].

TECHNOLOGY, I.; MAGAZINE, S. David bianchini and ismael ávila. n. March, 2014.

TOBERGTE, D. R.; CURTIS, S. Assessing transparency in government: rhetoric, reality and desire. **2012 45th Hawaii International Conference on System Sciences**, v. 53, n. 9, p. 2451–2461, 2012.

UNITED NATIONS DEPARTMENT OF ECONOMIC AND SOCIAL AFFAIRS. **World Urbanization Prospects**. [s.l: s.n.].

VARGAS, R. V. Utilizando a programação multicritério (Analytic Hierarchy Process - AHP) para selecionar e priorizar projetos na gestão de portifólio. **PMI Global Congress 2010 - North America**, p. 1–22, 2010.

VIANNA, A. M. et al. Revolução Industrial : um breve ensaio crítico. n. c, 2008.

VON SOLMS, R.; VAN NIEKERK, J. From information security to cyber security. **Computers & Security**, v. 38, p. 97–102, 2013.

ZINS, C. et al. Mapa do conhecimento da ciência da informação implicações para o futuro da área. p. 3–32, 2007.

ANEXOS

A. Questionário sobre Gestão de Projetos, respondido pela Secretaria de Obras e Urbanismos, de Limeira.

Questões apresentadas para os gestores com relação aos critérios da Gestão de projetos, alternativas de Segurança da Informação, e dados pessoais.

1. Quais setores de projetos podem ser mais relevantes para o setor público?
   Atribuir números de 1 a 8, sendo 1 o mais importante e 8 o menos importante:

Escopo	(1)
Tempo	(3)
Custos	(3)
Qualidade	(1)
Recursos Técnicos	(2)
Comunicação	(4)
Riscos	(3)
Patrocinadores	(2)

2. Considerando o item de Segurança da Informação, quais fatores são mais relevantes para a informação no sistema público?
   Atribuir números de 1 a 8, sendo 1 o mais importante e 8 o menos importante:

Confidencialidade	(1)
Integridade	(3)
Disponibilidade	(2)
Acuracidade	(1)
Utilidade	(4)
Posse	(3)
Autenticidade	(4)

3. Considerando-se dados de contribuintes pessoa física, quais dados são mais relevantes sobre identificação do indivíduo?

Nome	(1)
Data nascimento	(3)
Filiação-mãe	(5)
Filiação-pai	(5)
CPF	(1)
RG	(2)
Endereço	(3)
Telefone	(4)
Trabalho	(5)
Outros (especificar)	

_____

4. Dentro deste mesmo contexto, quais dados são mais requisitados?

Nome	(1)
Data nascimento	(8)
Filiação-mãe	(7)
Filiação-pai	(7)
CPF	(2)
RG	(3)
Endereço	(2)
Telefone	(4)
Trabalho	(6)
Outros (especificar)	

_____

B. Questionário sobre pesos para os quesitos de projetos, respondido pela Secretaria de Obras e Urbanismos, de Limeira.

		Extremamente Preferido	Muito fortemente Preferido	Fortemente Preferido	Moderadamente Preferido	Igualmente Preferido
	#1 - Tendo em consideração **Segurança da Informação e Transparência, como você classificaria**	**9**	**7**	**5**	**3**	**1**
ESCOPO	Quanto Escopo é mais importante que **Qualidade?**					**XX**
	Quanto Escopo é mais importante que **Recursos Técnicos?**			**XX**		
	Quanto Escopo é mais importante que **Patrocinadores?**			**XX**		
Qualidade	Quanto Qualidade é mais importante que **Recursos Técnicos?**				**XX**	
	Quanto Qualidade é mais importante que **Patrocinadores?**			**XX**		
Recursos Técnicos	Quanto Recursos Técnicos é mais importante que **Patrocinadores?**				**XX**	

	#2 - Tendo em consideração **ESCOPO**	Extremamente Preferido	Muito fortemente Preferido	Fortemente Preferido	Moderadamente Preferido	Igualmente Preferido
		9	**7**	**5**	**3**	**1**
Confidencialidade	Quanto Confidencialidade é mais importante que **Acuracidade ?**	**XXX**				
	Quanto Confidencialidade é mais importante que **Disponibilidade ?**		**XXX**			
Acuracidade	Quanto Acuracidade é mais importante que **Disponibilidade?**				**XXX**	

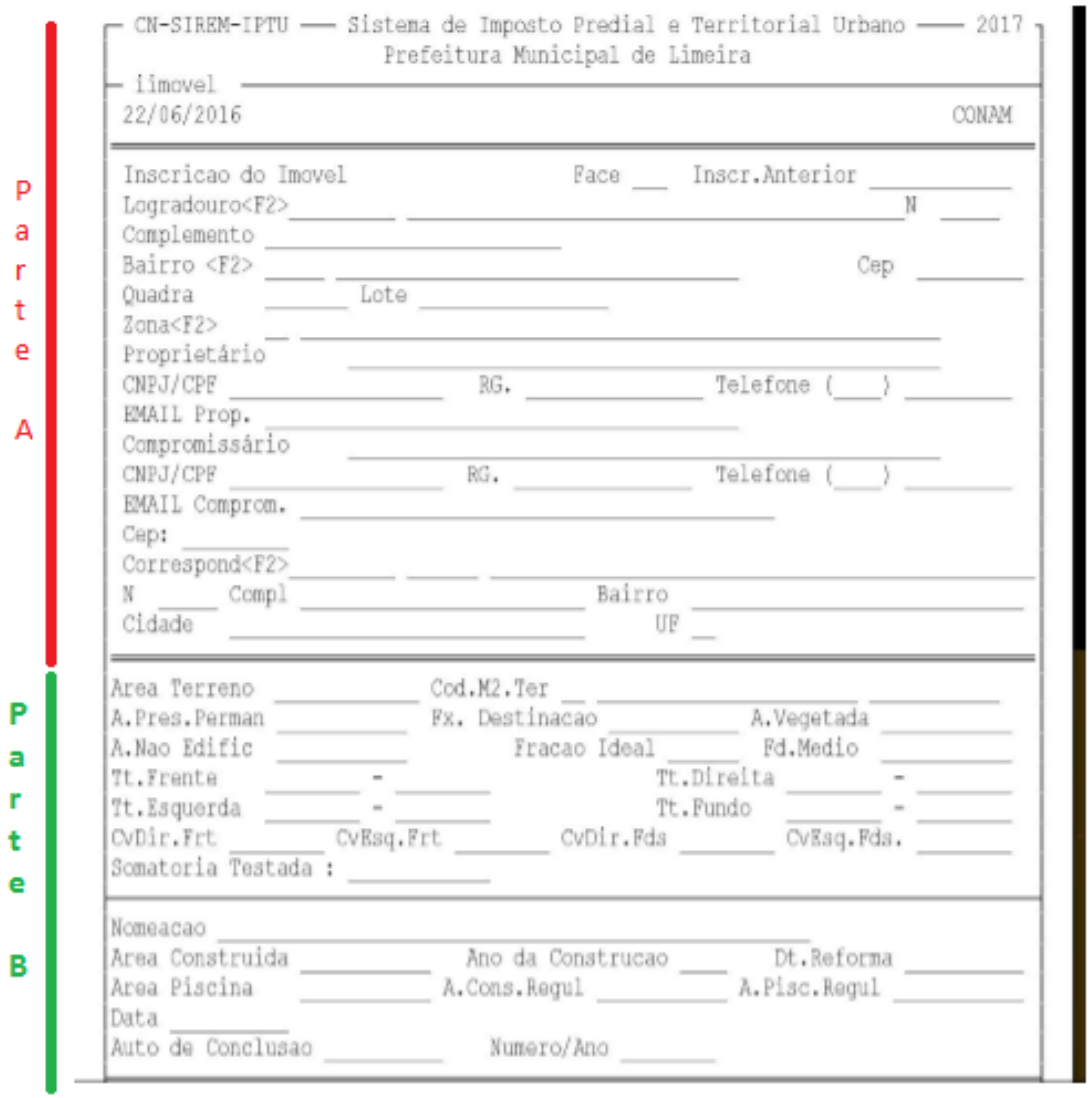
	# 3 - Tendo em consideração **QUALIDADE**	Extremamente Preferido	Muito fortemente Preferido	Fortemente Preferido	Moderadamente Preferido	Igualmente Preferido
		9	**7**	**5**	**3**	**1**
Confidencialidade	Quanto Confidencialidade é mais importante que **Acuracidade ?**	**XXX**				
	Quanto Confidencialidade é mais importante que **Disponibilidade ?**			**XXX**		
Acuracidade	Quanto Acuracidade é mais importante que **Disponibilidade?**				**XXX**	

	#4 - Tendo em consideração **RECURSOS TÉCNICOS**	Extremamente Preferido	Muito fortemente Preferido	Fortemente Preferido	Moderadamente Preferido	Igualmente Preferido
		9	7	5	3	1
Confidencialidade	Quanto Confidencialidade é mais importante que **Acuracidade ?**			XXX		
	Quanto Confidencialidade é mais importante que **Disponibilidade ?**				XXX	
Acuracidade	Quanto Acuracidade é mais importante que **Disponibilidade?**					XXX

	#5 - Tendo em consideração **PATROCINADORES**	Extremamente Preferido	Muito fortemente Preferido	Fortemente Preferido	Moderadamente Preferido	Igualmente Preferido
		9	7	5	3	1
Confidencialidade	Quanto Confidencialidade é mais importante que **Acuracidade ?**	XXX				
	Quanto Confidencialidade é mais importante que **Disponibilidade ?**		XXX			
Acuracidade	Quanto Acuracidade é mais importante que **Disponibilidade?**			XXX		

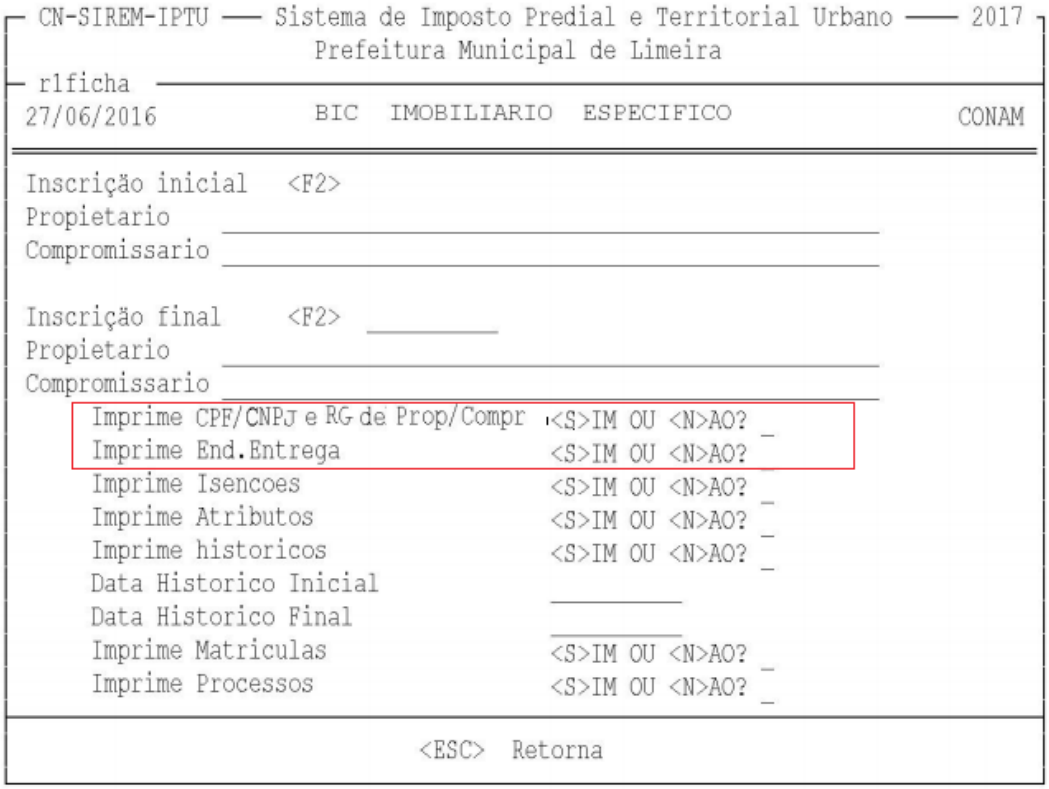
C. Formulários do Sistema de Imposto Predial e Territorial Urbano - CN-SIREM-IPTU

Figura 27. Formulário CN-SIREM-IPTU



Fonte: Fornecido pela Prefeitura de Limeira

Figura 28. Opção de Impressão do CN-SIREM-IPTU



Fonte: Fornecido pela Prefeitura de Limeira (2016)

APÊNDICES

A. Tabelas do Modelo AHP para o estudo hipotético

Na comparação dos Critérios, considerando Comprometimento em prevalência sobre outros; Recursos Técnicos sobre Qualidade, e Escopo sobre Qualidade, a tabela se mostrou como segue:

Tabela 4. Matriz AHP – Critérios

Matriz de Comparação - Entre Critérios									
	Escopo	Qualidade	Recursos T'ecnicos	Comprometimento	Matriz Normalizada				Vetor Médio
Escopo	1,00	5,00	1,00	0,20	0,14	0,25	0,19	0,12	**0,18**
Qualidade	0,20	1,00	0,14	0,14	0,03	0,05	0,03	0,09	**0,05**
Recursos T'ecnicos	1,00	7,00	1,00	0,33	0,14	0,35	0,19	0,20	**0,22**
Comprometimento	5,00	7,00	3,00	1,00	0,69	0,35	0,58	0,60	**0,56**
Soma	7,20	20,00	5,14	1,68					

Fonte: Elaboração Própria, 2016.

Aplicação do método AHP para cada alternativa, em relação aos critérios (3 alternativas para 4 critérios – 4 tabelas):

Tabela 5. Matriz AHP - Alternativas para Critério Escopo

CRITÉRIO: Escopo								
	Confidencialidade	Integridade	Disponibilidade	Matriz Normalizada			Vetor Médio	Vetor Objetivo
Confidencialidade	1,00	3,00	7,00	0,68	0,73	0,41	**0,61**	0,29
Integridade	0,33	1,00	9,00	0,23	0,24	0,53	**0,33**	0,13
Disponibilidade	0,14	0,11	1,00	0,10	0,03	0,06	**0,06**	0,21
Soma	1,48	4,11	17,00					

Fonte: Elaboração Própria, 2016.

Tabela 6. Matriz AHP - Alternativas para critério Qualidade

CRITÉRIO: Qualidade								
	Confidencialidade	Integridade	Disponibilidade	Matriz Normalizada			Vetor Médio	Vetor Objetivo
Confidencialidade	1,00	0,11	7,00	0,10	0,08	0,54	**0,24**	0,25
Integridade	9,00	1,00	5,00	0,89	0,76	0,38	**0,68**	0,35
Disponibilidade	0,14	0,20	1,00	0,01	0,15	0,08	**0,08**	0,15
Soma	10,14	1,31	13,00					

Fonte: Elaboração Própria, 2016.

Tabela 7. Matriz AHP - Alternativas para critério Recursos Têcnicos

CRITÉRIO: Recursos Técnicos								
	Confidencialidade	Integridade	Disponibilidade	Matriz Normalizada			Vetor Médio	Vetor Objetivo
Confidencialidade	1,00	3,00	7,00	0,68	0,33	0,85	**0,62**	0,38
Integridade	0,33	1,00	0,20	0,23	0,11	0,02	**0,12**	0,13
Disponibilidade	0,14	5,00	1,00	0,10	0,56	0,12	**0,26**	0,21
Soma	1,48	9,00	8,20					

Fonte: Elaboração Própria, 2016.

Tabela 8. Matriz AHP - Alternativas para critério Comprometimento

CRITÉRIO: Comprometimento								
	Confidencialidade	Integridade	Disponibilidade	Matriz Normalizada			Vetor Médio	Vetor Objetivo
Confidencialidade	1,00	7,00	9,00	0,80	0,85	0,60	**0,75**	0,32
Integridade	0,14	1,00	5,00	0,11	0,12	0,33	**0,19**	0,25
Disponibilidade	0,11	0,20	1,00	0,09	0,02	0,07	**0,06**	0,18
Soma	1,25	8,20	15,00					

Fonte: Elaboração Própria, 2016.

Comparando-se valores subjetivos constantes na Tabela 9, onde o valor total para cada critério é a média quadrática dos valores ponderados apurados durante a aplicação do modelo AHP, com os valores gerados pela aplicação do modelo em todos os dados, constantes na Tabela 10, tem-se que a escolha final pela Confidencialidade deu-se pelos dois modelos.

Tabela 9. Modelo subjetivo

Matriz de Decisão - Modelo Subjetivo						
	Escopo	Qualidade	Recursos T'ecnicos	Comprometimento	Total	
Confidencialidade	**0,61**	**0,24**	**0,62**	**0,75**	**0,67**	<<< Melhor opção
Integridade	**0,33**	**0,68**	**0,12**	**0,19**	**0,22**	
Disponibilidade	**0,06**	**0,08**	**0,26**	**0,06**	**0,10**	
Ponderação	0,18	0,05	0,22	0,56		

Fonte: Elaboração Própria, 2016.

Tabela 10. Resultado com a aplicação do modelo AHP

Matriz de Decisão - Modelo Objetivo						
	Escopo	Qualidade	Recursos T'ecnicos	Comprometimento	Total	
Confidencialidade	**0,29**	**0,25**	**0,38**	**0,32**	**0,32**	<<< Escolhido
Integridade	**0,13**	**0,35**	**0,13**	**0,25**	**0,21**	
Disponibilidade	**0,21**	**0,15**	**0,21**	**0,18**	**0,19**	
Ponderação	0,18	0,05	0,22	0,56		

Fonte: Elaboração Própria, 2016.

No cálculo do CI (Índice de Consistência), obteve-se o valor de CI=0,95, e para o CR (Taxa de Consistência) o valor de CR=0,10.