IX SINGEP
Simpósio Internacional de Gestão, Projetos, Inovação e Sustentabilidade
International Symposium on Management, Project, Innovation and Sustainability
ISSN: 2317-8302
CYRUS Institute of Knowledge MAKE A DIFFERENCE
9TH INTERNATIONAL CONFERENCE

ANALISE SOBRE A SEGURANÇA DIGITAL EM MEIO AS SMART CITIES

ANALYSIS ON DIGITAL SECURITY IN THE MIDDLE OF SMART CITIES

EVERTON MACHADO DO AMPARO
UNIVERSIDADE ESTADUAL DE CAMPINAS - UNICAMP

IEDA KANASHIRO MAKIYA
UNIVERSIDADE ESTADUAL DE CAMPINAS - UNICAMP

MURILO AUGUSTO OLIVEIRA SPARNS
UNIVERSIDADE ESTADUAL DE CAMPINAS - UNICAMP

LUCAS DE CARVALHO SOUZA FERREIRA

Nota de esclarecimento:
Comunicamos que devido à pandemia do Coronavírus (COVID 19), o IX SINGEP e a 9ª Conferência Internacional do CIK (CYRUS Institute of Knowledge) foram realizados de forma remota, nos dias **20, 21 e 22 de outubro de 2021.**

Agradecimento à orgão de fomento:
Agradecimento ao SBLAB (Laboratório de Negócios Sustentáveis/ Sustainable Business Laboratory)

IX SINGEP
Simpósio Internacional de Gestão, Projetos, Inovação e Sustentabilidade
International Symposium on Management, Project, Innovation and Sustainability
ISSN: 2317-8302
CYRUS Institute of Knowledge MAKE A DIFFERENCE
9TH INTERNATIONAL CONFERENCE

ANALISE SOBRE A SEGURANÇA DIGITAL EM MEIO AS SMART CITIES

Objetivo do estudo
Este trabalho visa questionar, por meio de um embasamento teórico conciso, a eficácia dos meios de seguranças em plataformas digitais, os perigos que sondam estes meios virtuais, juntamente com uma analise elaborada acerca da competência das plataformas em meio as Smart Cities.

Relevância/originalidade
A pesquisa realiza um paralelo não antes atríbuido acerca dos diferentes meios das plataformas digitais utilizadas no cotidiano com foco social e de governança, traçando os perigos voltados para cada canal dentro das smart cities através de uma filtragem dos dados apresentados.

Metodologia/abordagem
Pesquisa realizada a partir de estudos teóricos de caráter bibliográfico, tendo como finalidade o aprimoramento e atualização constantes do conhecimento, a qual é realizada por meio de uma investigação científica de obras já publicadas e a partir de uma analise documental.

Principais resultados
O uso de plataformas digitais em smart cities tem sido uma alternativa segura e confiável se tratando de transparência para fazer com que haja mais segurança nas informações que são compartilhadas através das mídias sociais e da internet.

Contribuições teóricas/metodológicas
A pesquisa contribui com a conceitualização e levatamento de questões da segurança digital em meio as smart cities, traçando um caminho entre a relação dos perigos cibernéticos com o compartilhamento de dados dentro das midias digitais.

Contribuições sociais/para a gestão
Os resultados da pesquisa contribuem para o aprimoramento da segurança no meio social e digital, e colabora para um melhor entedimento acerca do tema, através de uma filtragem das possíveis ameaças que rondam os meios virtuais.

Palavras-chave: Smart City, Cibersegurança, Segurança Digital, Governança

IX SINGEP
Simpósio Internacional de Gestão, Projetos, Inovação e Sustentabilidade
International Symposium on Management, Project, Innovation and Sustainability
ISSN: 2317-8302
CYRUS Institute of Knowledge MAKE A DIFFERENCE
9TH INTERNATIONAL CONFERENCE

ANALYSIS ON DIGITAL SECURITY IN THE MIDDLE OF SMART CITIES

Study purpose
This article aims to question, through a concise theoretical basis, the effectiveness of security means in digital platforms, the dangers that probe these virtual means, along with an elaborate analysis of the competence of platforms in the midst of Smart Cities.

Relevance / originality
The research draws a parallel not previously attributed to the different means of digital platforms used in everyday life with a social and governance focus, outlining the dangers facing each channel within smart cities through filtering the data presented.

Methodology / approach
Research carried out from theoretical studies of bibliographic character, with the purpose of constantly improving and updating knowledge, which is carried out through a scientific investigation of published works and through a documental analysis.

Main results
The use of digital platforms in smart cities has been a safe and reliable alternative when it comes to transparency for make the information that is shared through the media more secure social and internet.

Theoretical / methodological contributions
The research contributes to the conceptualization and raising of issues of digital security in the midst of smart cities, tracing a path between the relationship between cyber dangers and data sharing within digital media.

Social / management contributions
The research results contribute to the improvement of security in the social and digital environment, and contribute to a better understanding of the subject, through a filtering of possible threats that surround the virtual media.

Keywords: Smart City, cybersecurity, Digital Security, Governance

1 Introdução

A ampliação desenfreada dos meios cibernéticos nos últimos anos vem sendo a maior influência para o desenvolvimento e avanço de novas tecnologias, conhecimentos e informações em extensão global. É inegável a importância que cada dia mais, o espaço cibernético venha evoluindo e explorando territórios antes desconhecidos em questões tecnológicas. Atualmente, as empresas se embasam totalmente, confiantemente nos meios virtuais para reger os meios administrativos, logísticos e judiciais, o que obviamente não deixa de ser um avanço para estes meios, já que o meio cibernético possibilitou uma padronização mais concisa e organizada. Porém, conforme foi se ampliando as qualidades e bonificações acerca deste meio, foi também ampliando-se as diversas formas de burlar, atacar e extorquir informações por meio do espaço virtual.

Diversos estudos vêm sendo realizados a fim de ampliar o conhecimento acerca dos diversos cyber ataques que estão se tornando cada vez mais recorrente desde o desenvolvimento amplificado das redes sociais como por exemplo o Facebook. As brechas de segurança existentes nas plataformas midiáticas, assim como nos sistemas de administração empresariais vem causando prejuízos datados em bilhões. Dentro deste cenário há ainda uma gama muito reduzida de pessoas que são qualificadas para enfrentar de forma adequada esta onda de ataques a sistemas na rede mundial de computadores.

Conforme será analisado neste estudo, o paralelo entre a segurança digital e as plataformas digitais possibilita a correlação com a área de desenvolvimento conhecida como "smart city"; que são plataformas que subsidiam a qualificação do desenvolvimento de diversas áreas de uma cidade a fim de ampliar a habitabilidade deste espaço. Fundando-se nos questionamentos levantados por diversos teóricos sobre a cybercultural e o eminente risco de segurança evidenciado, será realizado um mapeamento das múltiplas abordagens empregados pelas mídias sociais, assim como um levantamento de dados a fim de exemplificar, associar e investigar a cultura digital e suas funcionalidades.

A partir desta sondagem de dados e abordagens relacionados tanto as "smart cities", quanto a própria segurança digital, este trabalho visa questionar, por meio de um embasamento teórico conciso, a eficácia dos meios de seguranças nestas plataformas digitais, os perigos que sondam estes meios virtuais, juntamente com uma analise elaborada acerca da competência das plataformas digitais com relação aos termos de segurança impostos, buscando soluções para estes questionamentos que se tornam cada dia mais pertinentes.

2 Referencial Teórico

De acordo com o Relatório da Segurança Digital no Brasil (Simoni, 2018) desenvolvido pela empresa dfndr lab em análise quantitativa entre os períodos de janeiro e março de 2018 o Brasil sofreu por volta de 56,9 milhões de ciberataques tendo 7,9 milhões de pessoas impactadas. Em termos de comparação, segundo o artigo Brasil em números (IBGE, 2010) em 2010 o Brasil tinha por volta de 190 milhões de habitantes, ou seja, 4,15% da população brasileira teria sofrido com ciberataques dentro de 3 meses.

Além disso, segundo o artigo "Trends in Cybersecurity Breach Disclosures" (Audit Analytics, 2020) que apresenta um relatório geral sobre cibersegurança, é demonstrado que em setembro de 2017 a empresa Equifax teve uma perda de 1.7 bilhões de dólares devido a brechas de segurança.

Tem-se, portanto, dentro deste cenário um sinal alarmante de perigo para a população, a invasão de privacidade e o compartilhamento de dados têm se tornado cada vez mais recorrentes com o evoluir da tecnologia, um levantamento feito em 2020 diz que o número de usuários de internet subiu em 7% totalizando agora 4,54 bilhões de usuários no mundo, 59% da população global (GSMA, 2020). E é certo afirmar que são poucos aqueles que entendem e estão preparados para os perigos da rede mundial de computadores.

Mas a ameaça não é iminente somente de cibercriminosos, em 2018, foi noticiado pelos meios de comunicação um vazamento de dados envolvendo a rede social Facebook, tendo sido envolvida a divulgação e utilização indevida de dados pessoais de milhares de usuários, essas informações teriam sido utilizadas pela empresa britânica Cambridge Analytica para auxiliar a campanha presidencial de Donald Trump. O vazamento de dados ocorreu no ano de 2013 após a empresa ter disponibilizado um aplicativo vinculado ao facebook com a finalidade de mapear um perfil de usuário de rede, através de um quiz de perguntas. Após coletadas as informações era possível traçar um perfil de pensamento do usuário. (Júnior, Ehrhardt, & Silva, 2019)

Tendo essas ideias em mente, pode-se estabelecer uma relação entre segurança digital e plataformas digitais, a partir disto, pode-se somar as áreas de desenvolvimento das "smart cities". Segundo Perez, Huerta e Lopez:

> Uma Smart City pode ser determinada como um espaço geográfico capaz de administrar recursos (naturais, humanos, equipamentos, construções e infraestrutura), assim como os desperdícios gerados pelo estilo de vida, ela deve ser sustentável e não deve ser prejudicial ao meio ambiente (Pérez, Huerta, & Lopez, 2014).

Uma plataforma smart city se apropria das tecnologias de informações e comunicações (ICT) a fim de melhorar a qualidade do habitar, assim como os métodos de empregabilidade e amplificar a capacidade de sustentabilidade de uma cidade (Smart Cities Council 2014). Monitorando uma localidade com a intenção de integrar uma infraestrutura propicia a avanços sociais, sendo assim, corrobora com todas as áreas, tanto estruturais, como administrativas e culturais, planejando um melhor desempenho dos aspectos de segurança maximizando os serviços ao uso do cidadão (US Office Technical and Scientific Information)

Sendo o uso das plataformas digitais recorrentes nas smart cities, têm-se como exemplos os aplicativos Decidim, que foi implementado em Barcelona e Consul em Madrid para fazer uma maior inclusão de sua população em meio as decisões sociais, governamentais e de cunho sociopolítico (Smith & Martín, 2021). Isso amplia as possibilidades de interação da população com as escolhas a serem tomadas em sua cidade. Em 2016 a plataforma Decidim foi adotada por 31 cidades, 13 regiões e 23 organizações enquanto o Consul foi por mais de 130 instituições em 33 países. Entretanto, há detalhes que precisam ser trabalhados e desenvolvidos em meio a isso, quanto maior é a liberdade e o acesso que a população tem aos meios digitais, maiores se tornam os perigos na rede como pode ser visto no caso do facebook.

Contudo, é necessário ter em mente que a empregabilidade das plataformas citadas tem diferentes contextos de uso, o facebook por ser uma rede social tem como principal proposta o lazer de seus usuários, entretanto isso não o impede de adicionar sistemas e funções voltados para o meio participativo e de governança como as opções de criar grupos e definir eventos ou então realizar a divulgação dos mesmos, como por exemplo doação de sangue que é amplamente empregado pela rede social. Tendo isso em mente é possível relacionar a função da governança entre redes sociais e sistemas participativo empregados nas smart cities, como o Decidim e então pode-se associar a segurança do uso de dados entre ambos os exemplos.

Dentro do contexto levantado é plausível então traçar um análogo entre os modelos de governança citados anteriormente, dividindo-os em duas categorias, *bottom up* e *top down*, estes sendo definidos como: Abordagem participativa envolvendo a participação dos funcionários na implementação da gestão de competências, também conhecida como abordagem bottom-up (Jerzy Rosinski, 2014). E a Abordagem diretiva (ou abordagem especializada) em que a implementação de competências é dirigida do topo da organização e habilitada por consultores externos (Rządkowska, 2006, 31-32; Filipowicz, 2004, 53), também conhecida como abordagem de top-down.

Além disso, para melhor compreensão de como funciona uma abordagem de ciberataque Krombholz, Hobel, Huber, e Weippl (2014) levantaram uma análise taxonômica da Engenharia Social a partir de três principais categorias, sendo elas **channel (canal), operator (operador)** e **type (tipo):**

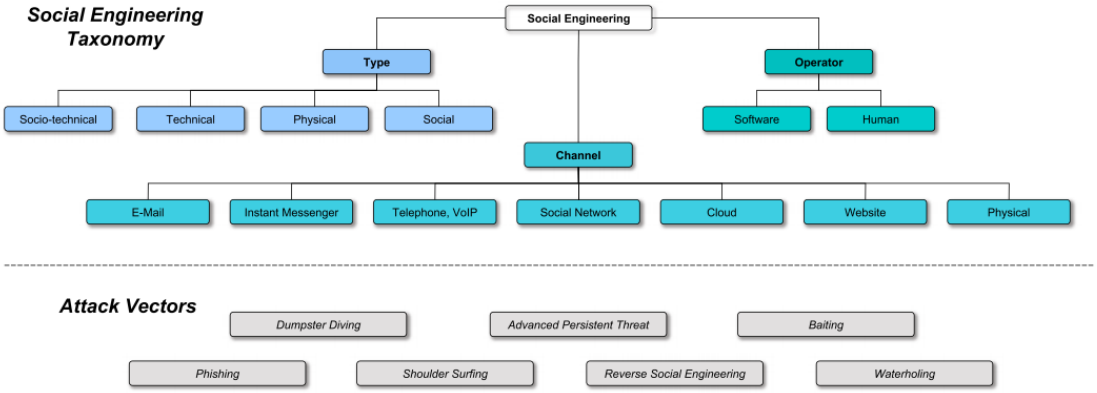

Figura 1 – Fluxograma taxonômico dos fatores que contribuem para um ataque de engenharia social. fonte: (Krombholz, Hobel, Huber, & Weippl, 2014)

Seguindo a linha **type,** tem-se as categorias que dividem as principais técnicas realizadas para o ataque, tendo então o ***social*** que se trata do uso de métodos sócio psicológicos como a persuasão para manipular as vítimas, como por exemplo a inferência de uma suposta autoridade e/ou curiosidade como indução.

O meio ***physical*** se trata do uso de abordagens diretas na qual o atacante realiza de algum modo uma ação física com o objetivo de coletar informações e induzir a vítima. O ***technical*** é caracterizado pelo uso das informações presentes na internet, que não é uma regra nas categorias anteriores, sendo assim o engenheiro social faz uso de mecanismos de pesquisa para obter senhas das vítimas podendo então utiliza-las no futuro. E por fim, o meio ***socio-technical*** se trata de uma fusão de parte, ou, de todos os métodos citados anteriormente, um exemplo de ataque desse gênero é o *"baiting attack"*. (Pérez, Huerta, & Lopez, 2014)

Classificando também o ataque pela linha **operator**, tem-se dois principais meios do mesmo ser realizado, sendo eles ***software*** que são ataques automatizados por programas o que permite múltiplos alvos e ***human*** que são ataques realizados diretamente por uma pessoa o que diminui o número de alvos por vez se comparado ao operador software.

E por fim em **channel** tem-se as principais vias de ataque que são usadas a partir da necessidade dada pelo tipo e pelo operador. Classificados por Krombholz, Hobel, Huber, e Weippl (2014) como:

E-mail é o mais comum dos canais para phishing e ataques de engenharia social reversa.

Mensagem Instântanea (Messenger, whatsapp, telegram...) - aplicativos que estão ganharam popularidade entre os engenheiros sociais como ferramentas para phishing e ataques de engenharia social reversa. Eles também podem ser usados facilmente para identificar exploit de roubo de maneira amigável;

Telefone, Voz através do IP - São canais de ataques comuns para engenheiros sociais para fazer com que suas vítimas passem informações sensíveis.

Redes Sociais - Oferece uma variedade de oportunidades para ataques de engenharia social. Dando o seu potencial para criar falsas identidades e seus modelos complexos de compartilhamento de informações, fazer deles fáceis para seus atacantes esconderem suas identidades e informações delicadas;

Nuvem - Serviços de nuvem podem ser usados para ganhar conhecimento situacional de um cenário colaborativo. Atacantes podem implantar um arquivo ou software em diretórios compartilhados para fazer as vítimas manterem a informação.

Websites - São comumente usados para ataques do tipo waterholing. Além disso, podem ser usados em combinação com e-mails para serem realizados ataques phishing.

A partir da compreensão técnica do funcionamento, dos tipos, dos operadores e dos canais usados em ciberataques Krombholz, Hobel, Huber, e Weippl (2014) desenvolveram uma matriz relacionando as informações aos vetores de ataques:

		Phishing	Shoulder surfing	Dumpster diving	Reverse social engineering	Waterholing	Advanced persistent threat	Baiting
Channel	E-mail	✓			✓		✓	
	Instant Messenger	✓			✓			
	Telephone, VoIP	✓			✓			
	Social Network	✓			✓			
	Cloud	✓						
	Website	✓				✓	✓	
	Physical	✓	✓	✓	✓			✓
Operator	Human	✓	✓	✓	✓			✓
	Software	✓		✓	✓	✓	✓	
Type	Physical		✓	✓				✓
	Technical					✓	✓	
	Social				✓			
	Socio-technical	✓			✓	✓	✓	✓

Figura 2 – Classificação de ataques de engenharia social de acordo com os dados levantados. fonte: (Krombholz, Hobel, Huber, & Weippl, 2014)

Pode-se concluir a partir da matriz que o canal de websites é atingido por três principais ameaças, o *phishing*, o *waterholing* e o *advanced persistente threat*. Sendo o website um dos meios de inclusão de plataformas digitais em smart cities, como pode ser visto no caso do Decidim (Smith & Martín, 2021). Deve-se ser feito então como modelo de análise e solução para

a segurança dos meios digitais em smart cities o levantamento de métodos de segurança utilizados em websites com funções distintas em contramedida às principais ameaças apresentadas, que por definição são (Krombholz, Hobel, Huber, & Weippl, 2014):

> **Phishing** é a tentativa de obter informações confidenciais ou fazer alguém agir da maneira desejada mascarando como uma entidade confiável em uma comunicação eletrônica médio. Eles geralmente são direcionados a grandes grupos de pessoas. Ataques de phishing podem ser realizados em quase qualquer canal, da presença física do invasor a sites, redes sociais ou até mesmo serviços em nuvem. Ataques dirigidos a indivíduos ou empresas específicas são referidos como spear-phishing. O spear-phishing exige que o invasor primeiro coletar informações sobre as vítimas pretendidas, mas a taxa de sucesso é maior do que no phishing convencional. Se um O ataque de phishing visa alvos de alto perfil nas empresas, o ataque é conhecido como caça às baleias.
>
> **Waterholing** descreve um ataque direcionado em que os invasores comprometem um site que provavelmente seja de seu interesse para a vítima escolhida. Os atacantes então esperam no poço de água para sua vítima.
>
> **Advanced Persistent Threat** refere-se a longo prazo, principalmente Ataques de espionagem com base na Internet conduzidos por um invasor quem tem os recursos e a intenção de compor um sistema persistentemente.

Baseando primordialmente nas teorias e características apresentadas, esta pesquisa realizou um estudo com o intuito de ampliar a gama de instruções referentes a esta área, para assim assertivamente ampliar e evoluir gradativamente nestes aspectos.

3 Metodologia

A pesquisa foi realizada a partir de estudos teóricos de caráter bibliográfico, tendo como finalidade o aprimoramento e atualização constantes do conhecimento que se pretende adquirir, a qual é realizada por meio de uma investigação científica de obras já publicadas. Teve como referencias chaves estudos e definições sobre a cultura virtual, a utilização de plataformas digitais com a finalidade de entretenimento e meios cibernéticos corporativos. Através da teoria existente, buscou-se um maior conhecimento a respeito das plataformas digitais e seus meios de segurança, tanto em aplicativos de entretenimento e informação, como em aplicativos que são utilizados nos meios empresariais. Mitnick e Simon (2013) ressaltam que, para se obter uma maior segurança das informações não basta apenas ter mecanismos de defesa como antivírus e firewalls, afinal, normalmente, aquilo que mais se pretende proteger não será o alvo de hackers, mas sim o que menos se vê: o fator pessoal.

Sendo assim, por meio de uma busca em teorias já existentes sobre o tema em questão, o intuito desse estudo foi se aprofundar através da formação de um referencial teórico abrangente e explicativo para que pudesse haver uma maior e melhor compreensão dos fatos aqui expostos. Gil (2002) diz que a pesquisa é necessária quando há a necessidade de se obter maiores informações acerca de um determinado tema, visto que não se encontram em quantidade suficiente no meio externo para responder ao problema de pesquisa. Ou ainda quando os dados disponíveis se encontram em tal desordem que não podem ser adequadamente relacionados ao problema.

A partir de uma analise documental, buscou-se um aprofundamento maior do tema através de pesquisa em documentos, que, de acordo com Cellard (2008, p. 295) "[...] constitui uma fonte extremamente preciosa para todo pesquisador nas ciências sociais. Ele é, evidentemente, insubstituível em qualquer reconstituição referente a um passado relativamente distante [...]", fundando-se em artigos e livros e trabalhos na área de segurança de informação, buscando ampliar o repertorio teórico acerca da funcionalidade, formulação e implantação destes métodos utilizados pelas plataformas como forma de segurança. Estudiosos como Kevin D. Mitnick & William L. Simon e instituições como a PNUD que publicaram estudos na área foram utilizados como suporte para a realização desta pesquisa.

As etapas propostas para esta pesquisa tem por base a conceitualização de Sanders (1982) e seu caráter fenomenológico. Primeiramente se determinou os limites do que será investigado; escolhendo como problema chave a implantação dos métodos de segurança nas plataformas digitais tanto em seu caráter informativo, como corporativo. Posteriormente, há uma coleta de dados para análise, sendo realizado um amplo estudo de relatórios, artigos e livros, que tem por caraterização a denominação de estudo bibliográfico. Por fim, há uma realização de uma análise hermenêutica dos dados coletados sendo realizado durante todo o estudo, que também pode ser descrito como um método interpretativo para que se consiga compreender um determinado texto, documento, referencial. Seria, então, um método para explicar, em termos gerais, uma passagem textual em questão, tentando encontrar nela algum sentido (SANTANA, 2021).

4 Análise dos resultados

Diante do cenário atual onde se vê um mundo cada vez mais inovador, com tecnologias cada vez mais avançadas, um tópico que tem chamado muito a atenção de todos é a segurança das informações que são compartilhadas nas plataformas digitais. As pessoas informam dados o tempo todo através desses mecanismos, acreditando que essas informações estão seguras, no entanto, não se pode ter absoluta certeza de que não estão sendo rastreados e tendo seus dados roubados. Desse modo, coloca-se em contexto a plataforma chamada de smart city, que tem como um dos objetivos se apropriar das tecnologias de informações e comunicações (ICT), de modo a melhorar a qualidade do habitar. Seu conceito estaria interligado a novas oportunidades dentro da revolução digital, principalmente devido a crescente difusão da capacidade de computação das novas tecnologias, inovação social e integração de mecanismos e ações de gestão e planejamento de espaços urbanos (CUNHA *et al.*, 2016).

Nesse sentido, o uso de plataformas digitais nas smart cities vem crescendo significativamente através de ferramentas como os aplicativos Decidim e Consul, usados para promover uma maior adesão da população em decisões sociais, governamentais e de cunho sociopolítico (SMITH; MARTIN, 2021). Através disso, há mais possibilidades de interação da população em relação às escolhas a serem tomadas em sua cidade, tornando sua participação mais efetiva e constante.

Importante salientar que a plataforma Decidim é uma tecnologia gratuita, garantindo uma real democracia nas decisões, ajudando os cidadãos, organizações e instituições públicas a se reorganizarem de maneira democrática em todas as escalas. Comparando com a tecnologia Consul, pode-se dizer que ambas possuem a mesma função em relação a questão da organização, não havendo grandes diferenças entre elas no que diz respeito à segurança de dados e tomada de decisões. No entanto, a diferença é que ambas realizam essa organização usando ferramentas diferentes, apresentando funções diferentes para esse propósito.

Logo, tem-se que o facebook e outras mídias sociais como twitter e instagram se aproximam mais do método de abordagem diretiva (top down) devido ao controle que as plataformas tem sobre as informações do público, enquanto que as plataformas Decidim e Decide Madrid estão voltadas para a abordagem participativa (bottom up), devido a inclusão dos cidadãos nas tarefas da cidade.

Após realizar um filtro com base nos aspectos de cada plataforma baseado nas informações apresentadas nas figuras 1 e 2, nos tipos de canais utilizados no Decidim e no facebook e na maneira como seus dados são utilizados, podemos traçar a diferença entre as ameaças apresentadas em ambos os meios (social e de governança):

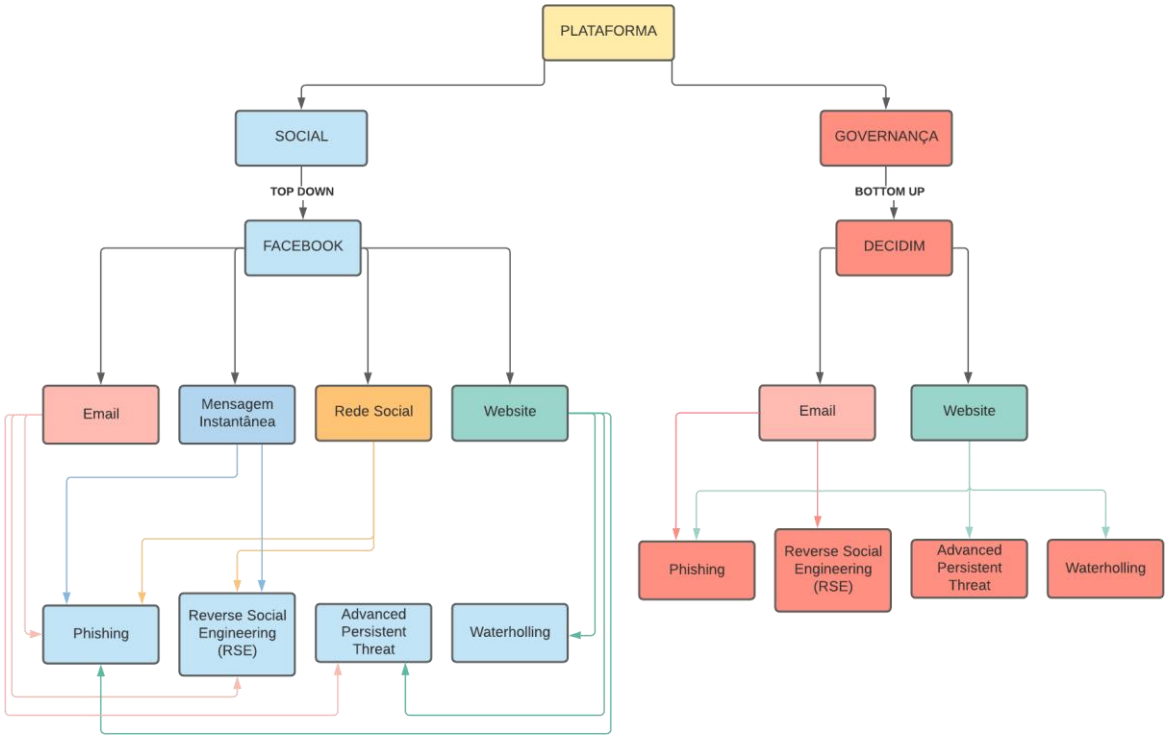

Figura 3 – Filtragem das plataformas de acordo com suas vulnerabilidades.

Pode ser notado então que as plataformas sociais detém de maiores riscos de segurança se tratando de vulnerabilidades considerando que as mesmas têm meios mais amplos de sofrerem ciberataques. Entretanto, através da filtragem realizada é possível verificar quais são os principais elementos da qual deve-se focar na segurança dentro das plataformas digitais dispostas nas smart cities na atualidade. Como apresentado anteriormente, riscos de vulnerabilidades permitiriam a manipulação de informações, o que seria um problema se tratando da governança de uma cidade, podendo acarretar em perigos ao meio social.

Enquanto que se tratando das informações usadas de maneira interna pelas empresas, realizando um comparativo, no caso ocorrido com o facebook houve falta de transparência das informações e de como elas estavam sendo utilizadas. Os dados dos usuários foram manipulados e colocados de modo indevido pela plataforma, fazendo assim uma manipulação através de engenharia social, que pode ser definida como (Mitnick, 2003):

> [..] usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não é, ou pela manipulação. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações [...].

Enquanto que acerca das plataformas utilizadas em Madrid e Barcelona (Smith & Martín, 2021) é possível visualizar que os usuários têm mais controle dado que dentro de um sistema bottom up, a transparência que a empresa criadora do software transmite é maior, como é propriamente dito no artigo "Going Beyond the Smart City? Implementing Technopolitical Platforms for Urban Democracy in Madrid and Barcelona" (Smith & Martín, 2021):

> [...]os desenvolvedores percebem que a tecnologia e os processos construídos em torno do desenvolvimento de tecnologia devem ser abertos e transparentes e disponíveis para análise - de modo que as suposições, valores, inclusões e exclusões da plataforma possam ser reconhecidos e tratados. A adaptabilidade não é importante apenas para a tecnologia da plataforma em si, mas também para os contextos institucionais de seu uso - estes também precisam se adaptar a fim de maximizar as possibilidades democráticas híbridas que se abrem online e off-line.

Tendo a transparência como uma medida de democratização da tecnologia, a inclusão de seus usuários além de mais segura se torna também um processo mais agradável, contribuindo para a inteligência coletiva. A segurança e confiança do público em suas plataformas colabora com avanços em seu meio social, como podemos ver nos casos abordados pelo Decidim, além da sua ferramenta principal com foco em governança, em segundo plano a proposta de transparência contribuiu para a segurança de seus usuários, que ao contrário do caso *top down* (facebook) em que os dados são usados de maneira diretiva, podendo ocorrer atos irresponsáveis, no *bottom up* eles são administrados pelos próprios participantes. Alguns dos atos levantados pelo Decidim e Consul em contribuição com o uso de plataformas digitais em smart cities foram (Smith & Martín, 2021):

	Smart City	Technopolitics
Technology	Engineering approach to managing urban processes Neutral tools for computation, communication, and control	Sociological approach to urban technologies Political artifacts configured for direct democratic participation
Politics	Technocratic management Non-political	Technological sovereignty Participatory
Governance	Public-private partnership Corporate protagonists	Civic-public dialogue Activist protagonists
Ownership	Proprietary Contracted services	Commons Free software communities
Citizenship	Passive or entrepreneurial Data point and tech user	Active subject Rights to the city
Democracy	A problem of legitimacy	A design principle
Urbanism	City as operating system Neoliberal strategy	City as social relations Democratic deliberation
Institutions	Closed services, client-oriented	Open processes, citizen-controlled

Tabela 1 – Estruturas tecnopolíticas e de Smart Cities levantadas pelas Plataformas Digitais Decidim e Consul.

Pode-se concluir a partir dos tópicos levantados e dos dados apresentados, que a transparência das informações públicas em meio as mídias sociais contribui também para a

segurança do cidadão devido a liberdade de seus dados, sendo estes constantemente atualizados, assim evitando vazamentos ou uso indevido.

5 Considerações finais

Após a realização deste estudo foi possível verificar que o uso de plataformas digitais em smart cities tem sido uma alternativa segura e confiável se tratando de transparência para fazer com que haja mais segurança nas informações que são compartilhadas através das mídias sociais e da internet. Além disso, com esse conceito de ter informações abertas em meio a tecnologia, muitas localidades estão garantindo que os dados repassados aos seus usuários sejam mais confiáveis, claros e efetivos, promovendo uma maior participação dos mesmos em decisões políticas, sociais e econômicas.

As smart cities têm adotado essa metodologia como uma maneira de tornar acessível a todos o acesso a informações que são relevantes para o seu cotidiano, de maneira que a população se sinta parte integrante e sinta a importância de sua opinião. Também, nesse processo, uma garantia maior de que os dados compartilhados não serão usados para fins que não aqueles a que se propõem, fazendo com que esses recursos sejam usados somente em questões legais.

Nesse sentido, o uso das plataformas Decidim e Consul chegaram para tornar essas questões viáveis, de maneira que os dados não possam ser manipulados, roubados ou usados de maneira ilícita. Além disso, quando os dados são seguros, as pessoas se sentem mais confortáveis em participar, em expor suas ideias e opiniões, pois sabem que todas as informações que expuserem serão usadas de maneira legal e democrática.

Referências

Assunção, M. F. (2014). *Segredos do Hacker Ético.* Visual Books.

Audit Analytics. (2020). TRENDS IN CYBERSECURITY BREACH DISCLOSURES. *Audit Analytics*, 1-12.

Carvalho, C., & Galvão, A. (01 de 04 de 2016). ENGENHARIA SOCIAL: UMA ANÁLISE DE AMEAÇAS E CUIDADOS AOS FUNCIONÁRIOS DAS AGÊNCIAS BANCÁRIAS DE SANTARÉM E ITAITUBA – PARÁ. *Revista de Publicação Acadêmica da Pós-Graduação do IESPES*, pp. 1-15.

Chauhan, A., Puri, N., & Narekar, Y. (05 de 05 de 2019). Social Engineering. *International Journal of Advanced Research in Computer and Communication Engineering*, pp. 1-5.

Eremia, M., Toma, L., & Sanduleac, M. (19 de 12 de 2017). The Smart City Concept in the 21st Century. *ScienceDirect*, pp. 1-8.

GSMA. (2020). The State of Mobile Internet Connectivity 2020. *UKaid*, 1-61.

Happ, C., Melzer, A., & Steffgen, G. (2016). *Trick with treat - Reciprocity inscreases the willingness to communicate personal data.* Elsevier.

Irani, D., Balduzzi, M., Balzarotti, D., Kirda, E., & Pu, C. (10 de 03 de 2010). Reverse Social Engineering Attacks in Online Social Networks. *College of Computing, Georgia Institute of Technology*, pp. 1-20.

Jerzy Rosinski, J. K. (2014). Top-down and bottom-up approach to competence management implementation: A case of two central banks. *ResearchGate*, pp. 0-9.

Júnior, A. a., Ehrhardt, F. F., & Silva, R. L. (2019). *Sociedade em Rede: Caso cambridge analytica e a lei Nº13.709/2018 uma análise do seu potencial de proteção aos dados dos usuários.* Santa Maria: Universidade Federal de Santa Maria.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2014). *Advanced social engineering attacks.* Vienna: Elsevier.

Ministério do Planejamento, Desenvolvimento e Gestão. (2018). Brasil em Números. *IBGE*, 1-515.

Mitnick, K. D. (2003). *A arte de enganar.* Pearson Education.

Pérez, A., Huerta, A., & Lopez, D. (2014). *Network Achitecture based on Virtualized Networks for Smart Cities for the Foresight Future of Cities Project and Future Cities Catapult.* U.K: Governmment Office of Science.

Shenja Van der, G. (21 de 02 de 2020). The right to the city in the platform age: Child-friendly city and smart city premises in contention. *Information (Switzerland)*, pp. 1-16.

Simoni, E. (2018). Relatório da Segurança Digital no Brasil. *dfndr lab*, pp. 1-22.