REVISTA INTERDISCIPLINAR ENCONTRO DAS CIÊNCIAS
V.1, N.2. 2018

ANÁLISE DO CONHECIMENTO DE SEGURANÇA E PRIVACIDADE DA INFORMAÇÃO

ANALYSIS OF KNOWLEDGE OF INFORMATION SECURITY AND PRIVACY

Isaac Teixeira de Souza[1] | Ívina Pereira dos Santos[2] | Charles Duarte Barbosa[3] | Sávio de Brito Fontenele[4]

RESUMO
O presente trabalho é um estudo descritivo de campo com foco quantitativo, em que foi verificado o conhecimento sobre segurança e privacidade na internet e a transparência das empresas fornecedoras desses serviços. A população do estudo foi composta por usuários de serviços de aplicativos de redes sociais e internet banking, e a amostra composta por 366 sujeitos, selecionados de forma aleatória e por conveniência. Como instrumento para a coleta dos dados utilizou-se um questionário desenvolvido pelo autor, disponibilizado na internet, compartilhado por meio de redes sociais e aplicativos de mensagens. Os resultados apresentam que 71,6% os usuários não alteram as senhas com frequência e 53,6% não se sentem seguros na utilização dos sistemas e a maior parte 72,7%, não fazem a leitura das normas dos sistemas que utilizam. Sobre a navegação anônima de segurança de dados, 37,7% conhecem esse tipo de navegação, mas não utilizam, 32,2% conhecem e utilizam e 30,1% pesquisados não conhecem. Nessas perspectivas podemos considerar que as pessoas conhecem a segurança da informação, mas não utilizam meios como navegação privada e não tem hábito de alteração de senhas após um período para tornarem seus acessos mais seguros e confiáveis; e que falta conhecimento e educação para a utilização das tecnologias, o que pode gerar transtornos e problemas graves, como a violação de seu perfil em alguma rede social e/ou acesso aos seus dados bancários. Fazendo necessário que todos possam ter maiores conhecimentos sobre segurança e privacidade de dados, bem como colocar em prática no seu cotidiano ações de prevenção como alteração das senhas periodicamente e uso da navegação anônima em computadores de uso em comum.

PALAVRAS-CHAVE
Informação. Segurança. Privacidade. Vulnerabilidade.

ABSTRACT
The present work is a descriptive field study with a quantitative focus, in which the knowledge about security and privacy in the internet was verified and the transparency of the companies that provide these services. The study population consisted of users of social networking and internet banking application services, and the sample comprised of 366 subjects, selected at random and for convenience. A questionnaire developed by the author, made available on the internet, shared through social networks and messaging applications was used as a tool for data collection. The results show that 71.6% of users do not change passwords frequently and 53.6% do not feel secure in using the systems and most of them 72.7% do not read the standards of the systems they use. About anonymous data security, 37.7% know this type of navigation, but do not use it, 32.2% know and use it and 30.1% do not know it. In these perspectives we may consider that people know the security of information, but do not use means such as private browsing and have no habit of changing passwords after a period to make their access more secure and reliable; and lack of knowledge and education to use the technologies, which can generate serious problems and problems, such as the violation of your profile on some social network and / or access to your banking data. Making it necessary for everyone to have more knowledge about data security and privacy, as well as put into practice in their daily prevention actions such as change of passwords periodically and use of anonymous browsing on computers of common use.

KEYWORDS
Information. Safety. Privacy. Vulnerability.

INTRODUÇÃO

A busca pelo poder nos persegue desde os primórdios. Ante o fato de se ter algo a mais que dinheiro, imóveis e entre outros, era a forma de se obter a autoridade necessária para coagir os outros. No entanto, essa realidade foi modificada quando as pessoas começaram a busca pelo conhecimento, ou seja, a necessidade de aprender ese qualificar. A partir desses processos de transformação e ideais civilizatórios, o poder deixou de estar atrelado aos bens materiais e passou a estar inteiramente ligado a informação. Assim, se o indivíduo possui a mesma, logo possui o poder (CARVALHO; KANISKI, 2000).

Junto a essas modificações, houve um aumento potencial nos meios de disseminação dos dados, sejam eles pessoais ou de cunho público (LARA; CONTI, 2003). Dessa forma, as pessoas passam a estar vulneráveis aos detentores do poder, uma vez que esses podem manipular essas informações. Diante desse contexto, o segmento de segurança da informação vem ganhando espaço em todos os âmbitos do mercado.

> As tecnologias da informação e comunicação tendem a encontrar formas mais ágeis de expressar conteúdo, com informações mais concisas e orientadas para públicos específicos. Essa é a técnica da aceleração, motivada pelo advento da internetização. A inserção de informações na mídia digital provoca uma maneira de comunicar diferenciada. Ela é extensiva, mais global e dificilmente poderá ser totalmente monitorada (SIMEÃO; MIRANDA, 2003, p. 35).

É bastante perceptível o avanço da informação e de sua divulgação, antes tínhamos somente dados de pessoas/empresas que exercia algum tipo de atividade governamental ou de grande exibição por meio de jornais, revistas e panfletos, atualmente podemos ter alguns dados de qualquer pessoa/empresas através da internet e os serviços oriundos da mesma.

> Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio (ISO/IEC 27002, 2007, p.16).

Onde é voltado totalmente para o meio empresarial porem Sêmola (2003, p.43) oferta uma definição de segurança da informação mais imparcial em relação à pessoa física/jurídica, que é a seguinte: “uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade". Então podemos definir segurança da informação como uma área do conhecimento que visa primordialmente proteger os ativos contra qualquer tipo de alteração, indisponibilidade e acesso não autorizado.

Em qualquer sistema seja ele *web* ou *mobile* para sua utilização é sempre necessário que os usuários ao criarem suas contas ler e aceitar os termos de uso, que nada mais é um contrato entre a empresa fornecedora do sistema e o usuária, este tem a funcionalidade de delimitar o que se pode e

o que não pode fazer dentro da plataforma, sendo assim uma garantia para a empresa de que todos estão cientes das suas ações, atrelado ao termo de uso essas mesmas empresas adotam também as políticas de privacidade que informa aos clientes o que serão feitos com seus dados durante o uso e até mesmo depois do uso do sistema.

É de responsabilidade da empresa fornecer de maneira facilitada os termos para que o usuário se sinta seguros e confiáveis ao utilizar seus serviços (BRASIL, 2014), mesmo com todos os serviços disponibilizando as normas de privacidade e os termos de uso durante o cadastro do usuário.

A prerrogativa do estudo vem de experiências pessoais e profissionais dos autores, em que os usuários possuem pouco conhecimento acerca da segurança da informação, possuem pouca privacidade dos dados e não conhecem as políticas de segurança dos meios de comunicação que utilizam. E que as empresas disponibilizam as políticas de segurança, tentam facilitar ao máximo o acesso a essas políticas e incentivam a leitura do mesmo para se ter um bom uso da plataforma.

Sabendo que os meios de comunicação fazem cada vez mais parte do cotidiano das pessoas físicas e jurídicas, esta pesquisa tem como principal objetivo verificar o conhecimento das pessoas com relação a segurança e privacidade dos dados ao utilizar aplicativos de redes sociais e internet banking e verificar-se-á como as empresas transparecem suas normas de segurança para seus usuários.

O presente trabalho é um estudo descritivo de campo com foco quantitativo, onde foi verificado o conhecimento de usuários com relação a sua segurança e privacidade nos inúmeros meios de disseminação das diversas informações pessoais e/ou públicas e a transparência das empresas fornecedoras desses serviços.

A população do estudo foi composta por usuários de serviços de aplicativos de redes sociais e internet banking, e a amostra composta por 366 sujeitos de ambos os sexos, selecionados de forma aleatória e por conveniência.

Como instrumento para a coleta dos dados utilizou-se um questionário desenvolvido pelo autor do estudo, disponibilizado pela internet, onde o link do mesmo foi compartilhado por meio de redes sociais e aplicativos de mensagens. Foi definido como critério de inclusão para participação da pesquisa a) ser usuário de rede sociais e/ou internet banking; b) acordar com os termos da pesquisa apresentados no termo de consentimento livre e esclarecido-TCLE; c) ter o questionário totalmente preenchido. E como critério de exclusão, não apresentar pelo menos um dos critérios de inclusão. A presente pesquisa segue de acordo com as normas do conselho nacional de saúde 466/12 para pesquisas com seres humanos.

Inicialmente foi criado um e-mail teste através do google, que também foi avaliado, para realização dos preenchimentos de perfis testes de usuário nas seguintes plataformas: *Facebook*,

Instagram, *Snapchat*, *Likedin*, *Twitter* e *Tinder*, App da Caixa Econômica e Banco do Brasil para verificação do momento em que as políticas de segurança e privacidade são apresentadas no cadastro, posteriormente foi buscada o local onde as mesmas politicas estão disponibilizadas ao usuário, já dentro da plataforma. Essa etapa foi realizada através de prints das telas durante o cadastro nas plataformas e já na plataforma o caminho para encontra-las. Os dados foram tabulados e analisados no programa Excel 2013 do Windows Microsoft Corporation, por distribuição de frequências.

DESENVOLVIMENTO

A amostra da pesquisa é composta 366 pessoas sendo 162 (44,3%) do gênero masculino e 204 (55,7%) feminino com a faixa etária entre os 11 e 57 anos de idade, com uma média de idade de 26,6 anos, prevalecendo as idades entre 18 e 25 anos com 160 pessoas. As ocupações que mais se destacaram entre os pesquisados foram estudantes com 116 participantes sendo 32% do total e professor com 39 pessoas sendo 11% da amostra.

Tabela 01: Perfil dos usuários participantes do estudo.

		Quantidade	Porcentagem
Sexo	Masculino	162	44%
	Feminino	204	56%
Idade	11 – 18	41	11%
	18 – 25	160	44%
	26 – 33	103	28%
	34 – 41	30	8%
	42 – 49	20	5%
	50 – 57	12	3%
Profissões	Professor	39	11%
	Estudante	116	32%
	Não possui	12	3%
	Outras	199	54%

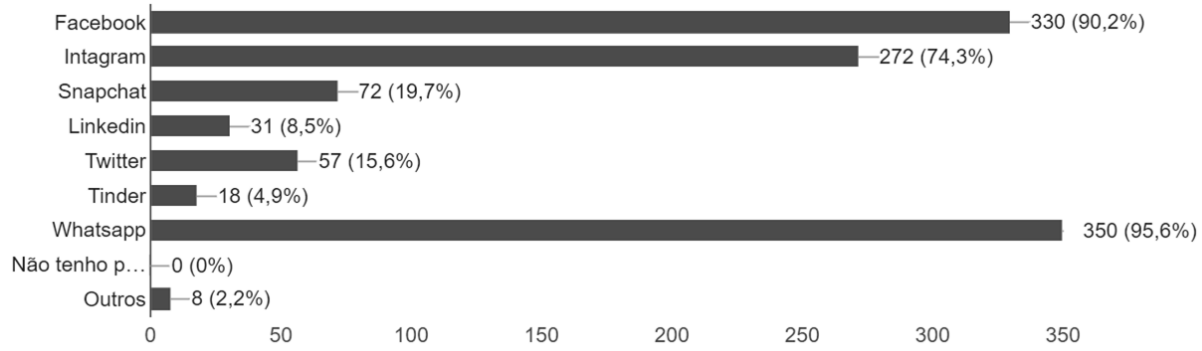
Fonte: Dados da pesquisa (2017)

Segundo os dados da pesquisa dos 366 participantes todos apresentam pelo menos uma rede social, o que implica dizer que todos possuem acesso de alguma forma a rede mundial de computadores que é um grande gerador de informações, uma vez que é necessária internet para se ter acesso as redes sociais presentes no gráfico 01, dessa forma todos os participantes podem gerar e acessar dados diversos.

Onde dos participantes 330 (90,2%) tem conta na rede social Facebook e 350 (95,6%) no aplicativo *Whatsapp* os quais são os dois principais meios de divulgação de informações da vida pessoal de seus usuários, estando nesses visíveis aos demais usuários os dados pessoais,

profissionais e localização. Assim caracterizando o primeiro pilar da segurança da informação que é o da disponibilidade que aborda o fato dos dados estar passiveis de acesso onde e quando o usuário necessitar.

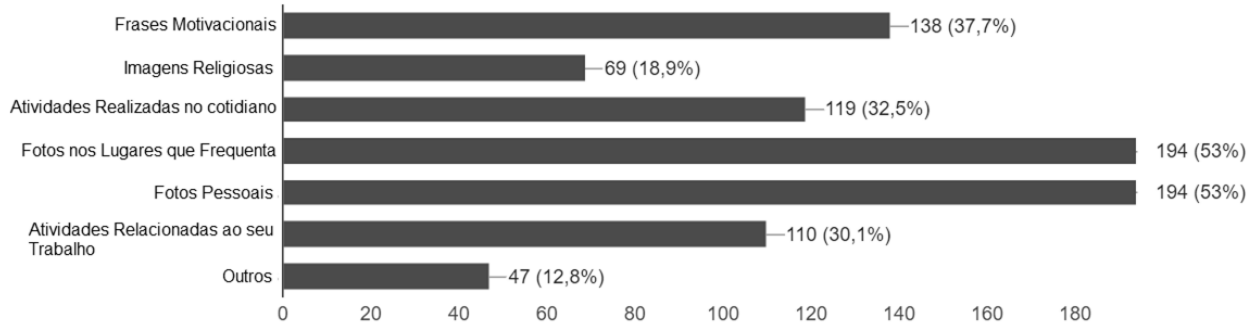
Gráfico 01: Redes sociais utilizadas pelos usuários.



Fonte: Dados da pesquisa (2017)

Nas redes sociais citadas 194 (53%) dos participantes afirmaram postar nelas fotos nos lugares que frequenta e fotos pessoais, 119 (32,5%) disseram que postam atividades relacionadas ao seu cotidiano 110 (30,1%) inserem na rede atividades relacionadas ao seu trabalho, 138 (37,7%) pessoas afirmam postar frases motivacionais e 69 (18,9%) compartilham imagens religiosas como demostra o gráfico a seguir:

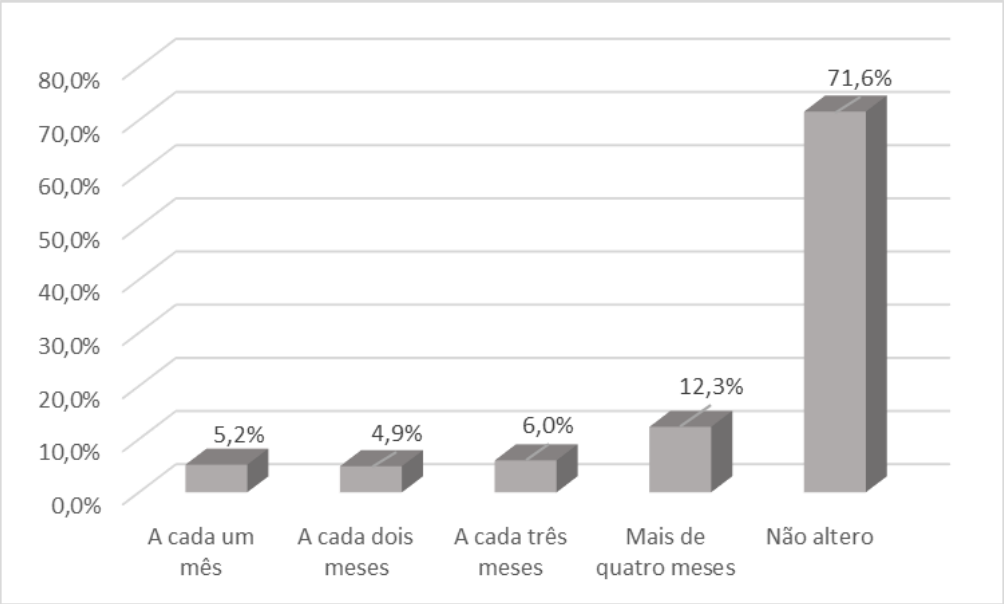
Gráfico 02: Postagens mais frequentes dos usuários nas redes



Fonte: Dados da pesquisa (2017)

O segundo pilar, que é o de integridade aborda o fato de uma informação só ser modificada pelas pessoas autorizadas podem ser garantidos por senhas que são atribuídas nos sistemas para que somente o usuário tenha acesso as suas informações. Porém somente o ato de se cadastrar a senha não basta, a senha precisa ser forte o bastante para que consiga suportar tentativas de invasões, outro ato de segurança para esse pilar está relacionado é a alteração de senhas entre o intervalo de tempo, este que não é bem aceito entre os usuários como relata os dados da pesquisa que dentre os participantes 71,6% não alteram as senhas utilizadas, 5,2% alteram a cada um mês, 4,9% alteram a cada dois meses, 6% a cada três meses e 12,3% alteram com mais de quatro meses.

Gráfico 03: Frequência de alteração de senhas pelos usuários



Fonte: Dados da pesquisa (2017)

O terceiro pilar que é o de confiabilidade está relacionado ao fato de as informações só poderem ser acessadas pelas pessoas autorizadas, está se parece um pouco com integridade, porém a diferença está em manipular e acessar os dados, onde na integridade não pode ocorrer à alteração do dado por terceiros e a confiabilidade os dados tem que estarem inacessíveis para as pessoas não autorizadas.

Uma ação já mencionada que é a de atribuição de senhas nos sistemas, contudo essa também pode ser garantida por parte das empresas desenvolvedoras, uma vez que os mesmos podem utilizar técnicas para assegurar e transparecer a proteção dos dados de cada usuário. Contudo os mesmos em sua maioria não estão sentindo essa segurança, uma vez que segundo os dados da pesquisa 53,6% das pessoas entrevistadas não se sentem seguras em relação a utilização dos sistemas e 46,4% sentem-se seguras, como é mostrada na tabela a seguir que apresenta tais porcentagens e a quantidade de pessoas referentes a tais:

Tabela 02: Segurança em relação a utilização de softwares

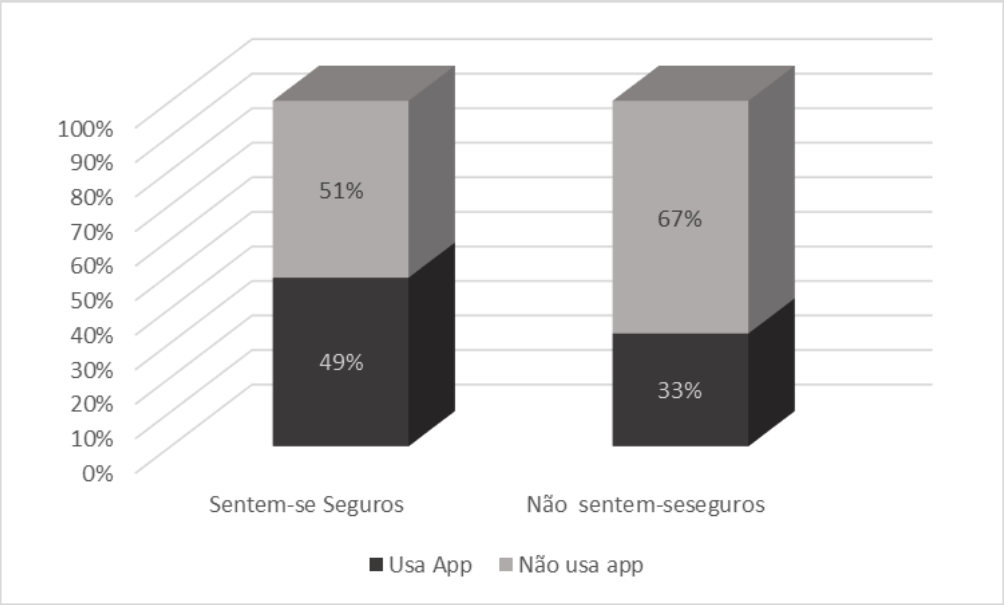
Segurança	Quantidade	Percentual %
Se sentem seguras	170	46,4%
Não se sentem seguras	196	53,6%
Total:	366	100,0%

Fonte: Dados da pesquisa (2017)

A confiabilidade é uma questão bastante delicada, uma vez que se os usuários não se sentem seguros os mesmos não utilizam as plataformas, como indica os dados da pesquisa que 67% dos participantes não sentem segurança a utilizar as plataformas e não usam essas para ações do dia a

dia, 49% se sentem seguros e os utilizam, 51% sentem-se seguros, entretanto não utilizam aplicativos e 33% não se sentem seguros porem utilizam aplicativos para ações do dia a dia.

Gráfico 04: Sentimento de segurança X Utilização das plataformas

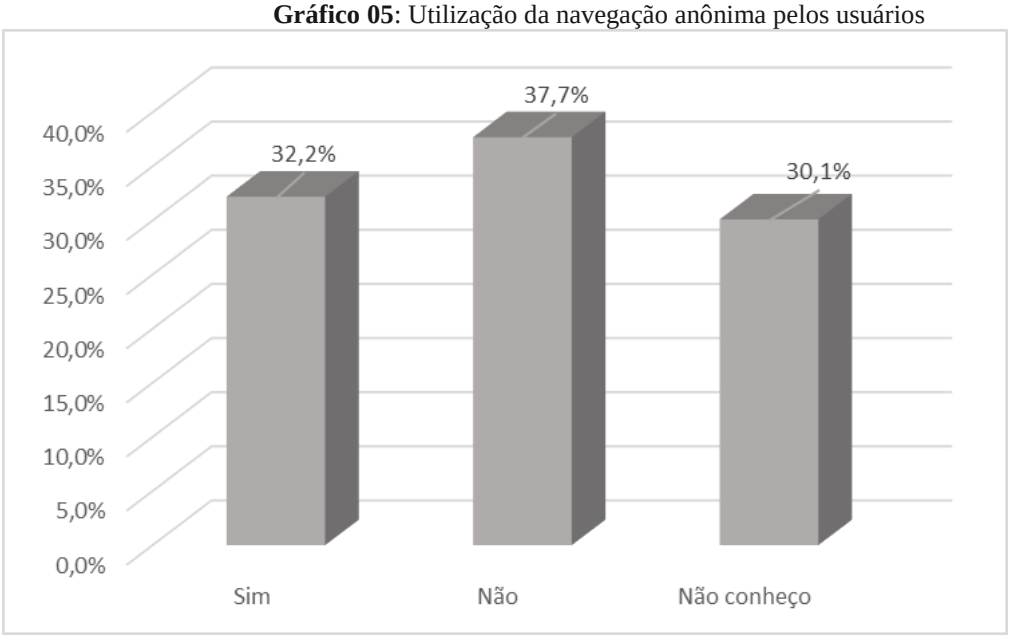


Fonte: Dados da pesquisa (2017)

Os pilares são a essência da segurança, uma vez que segundo Klettenberg (2016) qualquer falha relacionada à integridade, disponibilidade e a confidencialidade se tornam um risco a segurança da informação, podendo assim interferir na vida e nos processos do dia a dia das empresas/pessoas, então desta forma os mesmos precisam conhecer e aplicar a segurança para que os ricos não sejam gerados.

Além de alteração de senha como já foi citado outra forma simples de garantir a segurança é a utilização da navegação anônima dos navegadores, pois a mesma não armazena nem uma informação daquele acesso, por exemplo, se uma pessoa necessita acessar sua conta de e-mail em um computador público e essa o fizer na navegação normal e o navegador salvar seu e-mail e senha qualquer outra pessoa que tiver acesso aquela máquina poderá entrar na conta da mesma e então estará ferindo os três pilares, pois o e-mail se tornou disponível a pessoas não autorizadas, as informações ali contidas podem ter sido alteradas ferindo o pilar da integridade e as informações ali não serão mais confiáveis, de acordo com os dados da pesquisa 138 (37,7%) conhecem esse tipo de navegação porem não utiliza, 118 (32,2%) conhecem e utilizam e 110 (30,1%) pesquisados não conhecem tal forma de acesso.

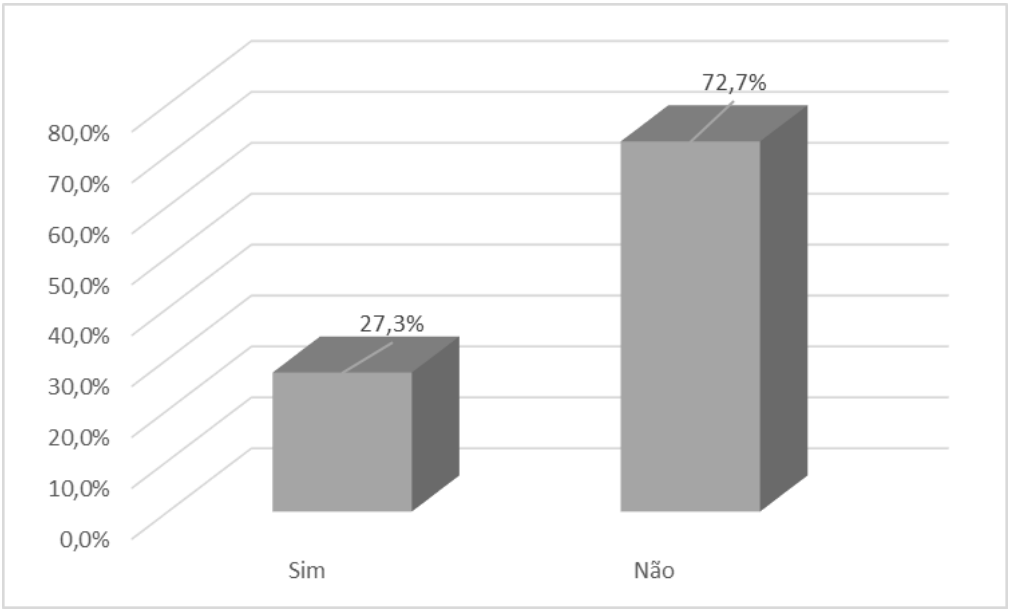
Gráfico 05: Utilização da navegação anônima pelos usuários



Fonte: Dados da pesquisa (2017)

Frente à questão sobre a leitura das normas de privacidade das plataformas, os participantes da pesquisa em sua maioria segundo os dados da presente pesquisa 72,7% não fazem a leitura dessas normas, 27,3% dos participantes relataram que fazem a leitura das normas dos sistemas que utilizam. Esse percentual podemos subentender que essa leitura das normas não é realizada por questões de não conhecimento sobre a sua funcionalidade ou por não estarem visíveis aos mesmos.

Gráfico 06: Leitura das normas de privacidade pelos usuários



Fonte: Dados da pesquisa (2017)

Foram analisadas nove plataformas, sendo elas de redes sociais, aplicativos de relacionamentos, computação em nuvem e internet banking, sendo elas Google, Facebook, Instagram, Snapchat, Linkedin, Twitter, Tinder, App Banco do Brasil e App Caixa Econômica, com

o intuito de verificar como as mesmas disponibilizam seus termos tanto no ato do cadastro do usuário quanto o mesmo já logado na plataforma.

Dos sistemas analisados apenas o Google que oferece serviços como e-mail (Gmail), computação em nuvem (Google Drive), rede social (Google +), entre outros, e o aplicativo da Caixa Econômica apresentaram os termos no ato do cadastro não como uma forma opcional, dessa forma se os usuários não efetuarem a leitura e concordarem com os mesmos o cadastro não é concluído e a conta não é criada.

Somente o aplicativo do Banco do Brasil não apresentou de nem uma forma os termos, nem no ato do cadastro, nem depois que os usuários estão logados na plataforma. Os demais deixam a leitura como uma opção para o usuário, geralmente é colocado um link para os termos de uso e privacidade em baixo dos campos para cadastro, que é direcionado para outra página que contém os termos, podendo assim ser uma possível justificativa do percentual atingido de não leitura.

A questão dos termos e a divulgação dos mesmos são discutidas na lei do marco civil da internet, de número 12.965, sancionada no dia 23 de abril de 2014 cujo objetivo é "Estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil", onde a mesma discorre no seu sétimo artigo, inciso seis que ao usuário é assegurado o direito de:

> Informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade. (BRASIL, 2014, p. 3, grifo nosso).

Percebe-se que as empresas em sua maioria estão agindo certo em disponibilizar tais informações e assim que os usuários concordam com tais, os mesmos assinam o contrato que também e abordado nesta lei no mesmo artigo, inciso oito: Consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais (BRASIL, 2014, p.3). Porem como os usuários em sua maioria não leem o contrato/termos, os mesmos ficam subjugados aos prestadores de serviço, uma vez que desconhecem seus direitos e deveres dentro dos sistemas e que não possuem o conhecimento de como seus dados estão sendo armazenados e processados por eles ou por terceiros.

CONSIDERAÇÕES FINAIS

Como apresentado o mundo da tecnologia está sempre em constante avanço porem esses avanços possuem dois lados o do bem que está relacionado aos benefícios que o mesmo trará para a vida das pessoas e o do mau que com esses avanços é aumentado equivalentemente o número de vulnerabilidades que o mesmo trará para a vida da empresa/pessoa, com isso podemos considerar

que os ataques a segurança estão diretamente relacionados aos avanços tecnológicos, formando um ciclo: Avanço, criação de ataques, resposta aos novos ataques, bem como falta de uma educação para a tecnologia. Dessa forma se faz essencial que todos não só conheçam a segurança da informação, mas que a mesma implemente esse comportamento no seu dia a dia na utilização dos meios tecnológicos da informação para minimizar os impactos que um ataque possa trazer para a sua vida.

Tendo como base os dados apresentados nesta pesquisa podemos concluir que as pessoas conhecem a segurança da informação porem não utilizam meios como navegação privada e alteração de senhas após um período para tornarem seus acessos mais seguros e confiáveis. Com relação à privacidade, tendo como base dos pesquisados postam fotos pessoais e fotos nos lugares que frequenta e postam atividades relacionadas ao seu trabalho, pode-se concluir que a privacidade se torna falha uma vez que todas as pessoas que tiverem acesso ao perfil dessas poderão saber o que essa pessoa faz, com quem anda e todas as questões de sua vida pessoal e profissional.

Os termos de uso e privacidade é a maneira que as empresas possuem de transmitir aos seus usuários o que é feito com os dados e ações realizadas dentro de suas plataformas, e como os mesmos podem utilizar seus serviços de forma segura, confiável e integra. Esses documentos representam de fato um contrato firmado entre empresa e usuário que apresenta o comportamento do mesmo ao utilizar a plataforma e quais as possíveis ações que poderão ser tomadas por parte das empresas fornecedoras desse serviço. Por isso é de suma importância efetuar a leitura de tais documentos, pois uma vez aceito você está sujeito as condições que empresa impõem para se utilizar seus serviços.

Os dados apresentados relacionados aos termos de uso e privacidade revelam que da parte dos usuários não realizada a leitura dos mesmos, isso pode ser um reflexo do posicionamento da empresa para essas questões tendo como base que das plataformas apresentadas somente duas apresentaram as políticas como uma etapa obrigatória onde só é possível passar para as demais e finalizar o cadastro somente se rolar a barra até o final e aceitar os termos, as demais apresentam os termos porem como uma opção, não sendo uma condição para a finalização do cadastro. Após o usuário está logado nas plataformas, a maioria deixa as políticas de fácil acesso para que se os usuários sentirem necessidade poder obtê-la.

A falta de conhecimento e educação para a tecnologia pode gerar aos usuários transtornos e problemas graves, como a violação de seu perfil em alguma rede social e/ou acesso aos seus dados bancários. Fazendo necessário que possam ter maiores conhecimentos sobre segurança e privacidade de dados, bem como colocar em pratica no seu cotidiano ações de prevenção como alteração das senhas periodicamente e uso da navegação anônima em computadores de uso em comum. A pesquisa foi realizada tendo como população todas as pessoas usuárias de redes sociais e

internet banking, sem delimitar uma localização especifica e não considerou o grau de instrução medido pelo nível de escolaridade o que pode influenciar nos resultados, sendo assim passível de pesquisas futuras para a obtenção de dados e comparação com os resultados aqui apresentados para tentar observar a relação de tais variáveis e se as mesmas possuem relação direta com as informações obtidas pela pesquisa.

REFERÊNCIAS

ABNT. Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 27002.** Tecnologia da informação — Técnicas de segurança - código de prática para a gestão da segurança da informação. Rio de Janeiro, ABNT, 2005.

BRASIL. Constituição (2014). Lei nº 12965, de 23 de abril de 2014. **Marco Civil da Internet**. Brasilia, Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 06 maio 2017.

CARVALHO I. C. L.; KANISKI A. L. **A sociedade do conhecimento e o acesso à informação: para que e para quem?**, Brasília. 2000, v. 29, n. 3, p. 33-39. Disponível em: http://www.scielo.br/pdf/ci/v29n3/a04v29n3. Acesso em: 21 mar. 2017.

KLETTENBERG, J. **Segurança da Informação:** Um estudo sobre o uso da engenharia social para obter informações sigilosas de usuários de Instituições Bancárias. Dissertação de mestrado - Programa de Pós-Graduação em Ciência da Informação. Centro de Ciências da Educação da Universidade Federal de Santa Catarina, 160p. Santa Catarina, 2016.

LARA M. L. G.; Conti V. L. **Disseminação da informação e usuários**, *São Paulo Perspec.* [online]. 2003, vol.17, n.3-4, pp.26-34. ISSN 0102-8839. Disponível em: http://dx.doi.org/10.1590/S0102-88392003000300004. Acesso em: 21 mar. 2017.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: uma visão executiva**. Rio de Janeiro: Campus, 2003.

SIMEÃO E.; MIRANDA, A. **O texto virtual e os sistemas de informação**. Brasília: Thesaurus, 2005.

Recebido em: 27 de Março de 2018
Aceito em: 25 de Abril de 2018

[1]Discente do Curso de Bacharelado em Sistemas de Informação da Faculdade Paraíso do Ceará (FAP). E-mail: isaacteixeiraa@gmail.com

[2]Discente do Curso de Bacharelado em Sistemas de Informação da Faculdade Paraíso do Ceará (FAP).

[3]Discente do Curso de Bacharelado em Sistemas de Informação da Faculdade Paraíso do Ceará (FAP).

[4]Docente do Curso de Bacharelado em Sistemas de Informação da Faculdade Paraíso do Ceará (FAP).