ESTUDO DE CASO SOBRE SEGURANÇA DA INFORMAÇÃO NAS REDES SOCIAIS NA FAMETRO

CASE STUDY ON INFORMATION SECURITY IN SOCIAL NETWORKS ON FAMETRO

Daniele Souza de Araújo

Discente do curso de Sistemas de Informação (FAMETRO).

Luiz Otavio Ribeiro Afonso Ferreira

Docente do curso de Sistemas de Informação (FAMETRO).

Hortência Magalhães Ferreira

Discente do curso de Sistemas de Informação (FAMETRO).

Marcia Paula Chaves Vieira

Docente do curso de Sistemas de Informação (FAMETRO).

RESUMO

Esse trabalho tem por finalidade apresentar os resultados obtidos por meio da pesquisa exploratória aplicada que visa quantificar o comportamento das pessoas sobre a segurança da informação nas redes sociais. A pesquisa foi realizada durante o período de 15 a 30 de abril de 2014. Com base na análise dos dados recebidos, serão apresentadas sugestões de métodos de segurança nas mídias sociais a fim de conscientizar os usuários, orientando-os a utilizar tais meios cibernéticos de forma a preservar a sua identidade e privacidade contra ataques virtuais e pessoas mal intencionadas.

Palavras-chave: Segurança da informação. Redes sociais.

ABSTRACT

This work aims to show the results obtained through exploratory research applied with objective to quantify the user behavior about information security on social networks. The survey was conducted during the period 15 to 30 april 2014. Based on analysis received answers, we are going to suggest strategies of security on social networks to educate users and guide them in using of these systems with identity and privacy preserved against cyber-attacks and malicious people.

***Keywords**: Information security. Social networks.*

Recebido em: 31/05/2014
Aceito em : 08/08/2014

1 INTRODUÇÃO

As redes sociais se tornaram ferramentas do cotidiano das pessoas. Características como velocidade de propagação de informações, grande quantidade de pessoas que conseguem atingir, facilidade de acesso, riqueza de informações pessoais disponíveis, somado ao alto grau de confiança que os usuários depositam entre si, popularizaram as redes sociais, como também despertou o interesse de pessoas mal-intencionadas.

O Tema "estudo de caso sobre segurança da informação nas redes sociais na Fametro" foi cogitado com base na grande disseminação e repercussão deste tema atualmente na sociedade, em que usuários cometem exageros e se equivocam ao supor que estão protegidos ou imunes a qualquer tipo de vulnerabilidades, crimes ou golpes virtuais.

Do ponto de vista metodológico, a natureza desta pesquisa é essencialmente aplicada, possuindo uma abordagem quantitativa e fenomênica, sendo, portanto, uma pesquisa exploratória e descritiva, incluindo como atividades a pesquisa bibliográfica seguida de um levantamento de dados e estudo de caso, tendo ainda sido utilizada a ferramenta "Google Drive" como mecanismo para coleta de dados apresentadas aos usuários.

Este trabalho encontra-se dividido na introdução, impacto das redes sociais na segurança da informação, análise e interpretação dos dados, análise estatística dos dados, considerações finais e apêndices.

2 IMPACTO DAS REDES SOCIAIS NA SEGURANÇA DA INFORMAÇÃO

Os avanços tecnológicos ocorrem de maneira tão desenfreada que não fazer parte destes leva a uma marginalização do indivíduo. O surgimento da internet é, sem dúvida, um grande acontecimento quando falamos em evolução tecnológica, uma ferramenta de comunicação e fonte intensa de informações para todos os fins.

Além da internet, a sociedade moderna criou muitos meios para difundir a comunicação, esses modificaram as maneiras de interação e os relacionamentos entre as pessoas atualmente, de forma que atingiu um grau de agilidade e diversificou a escala e a dimensão da informação.

Com a evolução da internet e a necessidade de uma comunicação mais rápida entre os usuários, ocorreu o surgimento das redes sociais que, segundo Marteleto (2001, p.72) representam "um conjunto de participantes autônomos, unindo ideias e recursos em torno de valores e interesses compartilhados". Essas mídias tomaram grande proporção em nossa sociedade moderna, dos mais variados aspectos.

O acesso às redes sociais já faz parte do cotidiano de muitos usuários da internet. Por meio delas, você pode ter informação sobre os assuntos do momento, saber o que seus amigos estão fazendo, onde estão e o que estão pensando, também pode ver assuntos relacionados à seleção e vagas de empregos, pesquisas de opinião e mobilizações sociais.

As redes sociais acabaram atraindo também pessoas mal intencionadas. Os crimes cometidos por meio do computador e outras tecnologias alcançaram cada vez mais pessoas, o que nos leva a observar que os criminosos estão usando a tática de se esconderem "por trás" das tecnologias. Isso por acharem que estarão seguros, longe de ação judicial, haja vista a dificuldade da sua identificação, localização e captura.

Tais fatores tiveram como causa esse grande avanço tecnológico dos últimos anos, décadas, em que computadores e tecnologias com acesso à internet estão ao alcance de qualquer pessoa, pois ter acesso à *Web*, atualmente, não é mais privilégio para poucos, independe de faixa etária, gênero, classe social ou renda. O que faz com que mais pessoas se conectem e faça parte dessa sociedade virtual, e por conseguinte atraia novos criminosos para o mundo online.

E como não temos escolha se devemos usar ou não a mídia social, então temos a obri-

gação de obter as informações necessárias para a forma como vamos usá-la (QUALMAN, 2011). Portanto, para usar as redes sociais com segurança, é muito importante que você esteja ciente dos riscos que elas podem representar e possa, assim, tomar medidas preventivas para evitá-los, pois a questão comportamental pode afetar significativamente as demais medidas de segurança, por mais modernas que elas sejam. (SILVA; COSTA, 2009 *apud* QUALMAN, 2011).

3 ANÁLISE E INTERPRETAÇÃO DOS DADOS

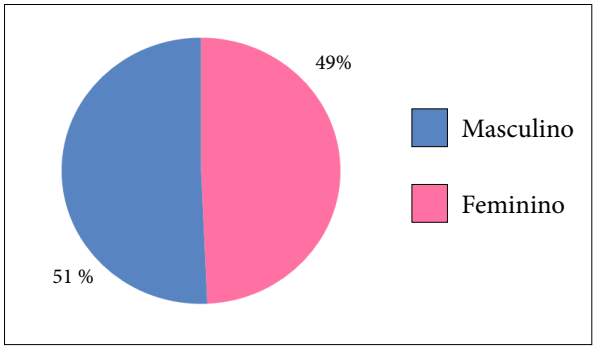
A pesquisa elaborada envolveu um questionário contendo 18 (dezoito) perguntas, agrupadas por 06 (seis) variáveis para que possamos ter uma análise mais organizada e estruturada, além de uma melhor compreensão sobre o assunto. A pesquisa obteve uma amostra equivalente a 140 questionários respondidos por usuários das mídias sociais.

O primeiro grupo de perguntas está relacionado com o perfil do usuário das redes sociais, onde buscamos traçar uma descrição das pessoas que mais fazem uso dessas ferramentas tecnológicas.

3.1 Grupo perfil (01 a 05)

Com base no gráfico abaixo é possível concluir que da amostra coletada, 51% são homens e 49% são mulheres. Analisando os dados, observamos que há uma diferença mínima com relação ao gênero dos usuários das mídias sociais. O que pode ser comprovado por pesquisas do IBGE, em que revelou: "o percentual de homens que acessam a internet na população masculina situou-se em 22,0%, um pouco acima do indicador referente ao contingente feminino (20,1%)".

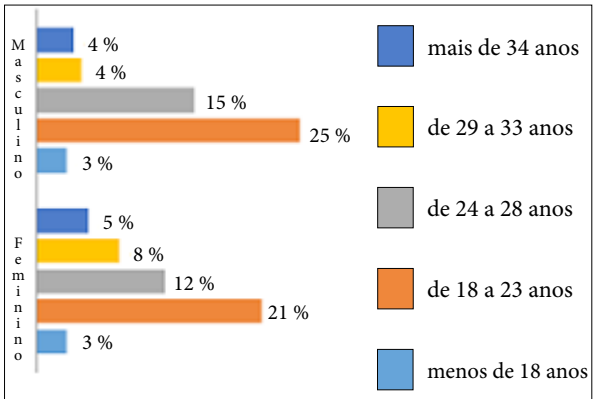
Gráfico 01 - Percentual do gênero que mais faz uso das redes sociais.



Fonte: Dados da pesquisa.

Dentre eles, a faixa etária predominante é de 18 a 23 anos (46%), seguido da faixa etária de 24 a 28 anos (27%), para ambos os gêneros. Como é possível observar no gráfico 02 a seguir, o público masculino é maior na idade entre 18 e 23 anos, já entre 29 a 33 anos o público predominante é o feminino.

Gráfico 02 - Análise do perfil.



Geral

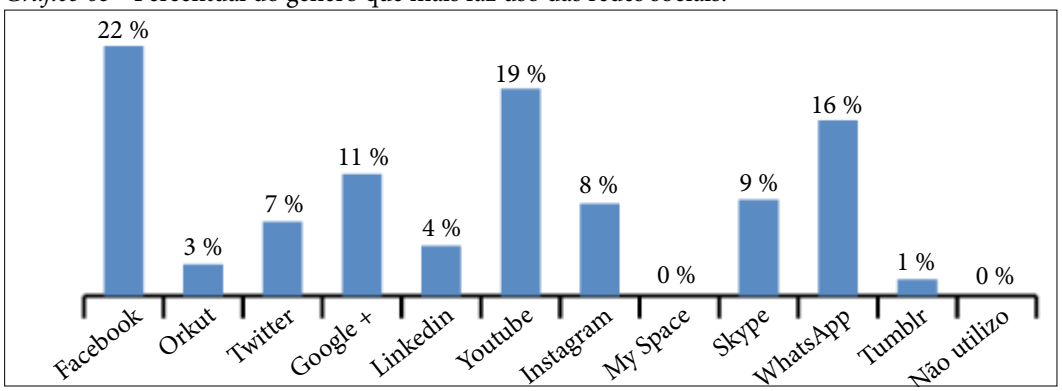
Idade	Feminino	Masculino	Total	Total (%)
menos de 18 anos	4	4	8	6%
de 18 a 23 anos	30	35	65	46%
de 24 a 28 anos	17	21	38	27%
de 18 a 23 anos	11	6	17	12%
mais de 34 anos	7	5	12	9%
Total	**69**	**71**	**140**	**100%**

Fonte: Dados da pesquisa.

Nota-se por outro lado que o uso das redes sociais está presente em todas as gerações, desde os mais novos aos mais velhos. O que nos faz refletir sobre as mudanças de paradigmas: usuários com idades superiores a 34 anos em que muitas vezes a resiliência é um pon-

to crítico e a adaptação a novas tecnologias é dificultada; inclusão social e as rápidas transformações trazidas pela globalização - em que hoje é possível, praticamente, "nascer conectado" (GIDDENS, 2012).

Gráfico 03 - Percentual do gênero que mais faz uso das redes sociais.



Fonte: Dados da pesquisa.

Segundo Aristóteles (III a.C.), "o homem é um ser social" , ou seja, ele tem a necessidade de interagir, comunicar-se e manter relacionamentos, conforme o gráfico acima, percebemos estas características bem presentes.

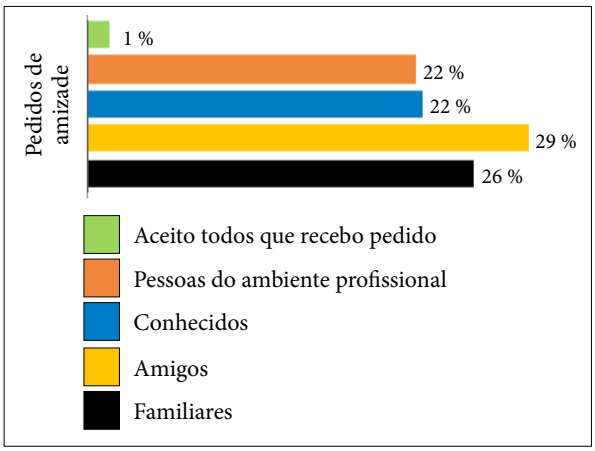
Todos os usuários estão conectados por algum tipo de mídia social, muitas vezes por mais de uma, haja vista a multiplicidade de escolha na resposta ao questionário. Nota-se também que a rede social mais utilizada é o Facebook (22%), seguido pelo YouTube (19%) e WhatsApp (16%). Dentre eles o que apresenta maior risco e vulnerabilidade é o Facebook, a rede social mais utilizada no mundo, com um expressivo número de usuários. Este possui dados pessoais dos usuários, ferramentas para localização e espaços de armazenagem de fotos e vídeos. Além da instigante pergunta "O que você está pensando?", fazendo com que os usuários dividam sua vida pessoal em público, tornando algo que antes era somente "seu" visível a todos por meio de um clique.

Um projeto de mestrado de análise do comportamento humano no ambiente virtual constatou por meio de experimentos que o ser humano se comporta no mundo virtual como se comportaria no mundo real (informação verbal)[1]. O problema é que mais de 2/3 da população faz uso da internet, segundo dados estatísticos da Associação Brasileira de Telecomunicações (Telebrasil), e o que antes era um ambiente somente virtual passa a ser um ambiente como qualquer outro na vida real e isso nos faz perceber que o cuidado com a privacidade online é uma questão de responsabilidade social (YOUTUBE, 2012).

3.2 Grupo divulgação e restrição (06 a 09)

No gráfico 04, percebemos os percentuais coletados em relação à aceitação dos pedidos de amizade. Essa resposta, assim como a das redes sociais, permitia a multiplicidade, em que o usuário poderia escolher várias opções.

Gráfico 04 - Quais pedidos de amizade você costuma aceitar.

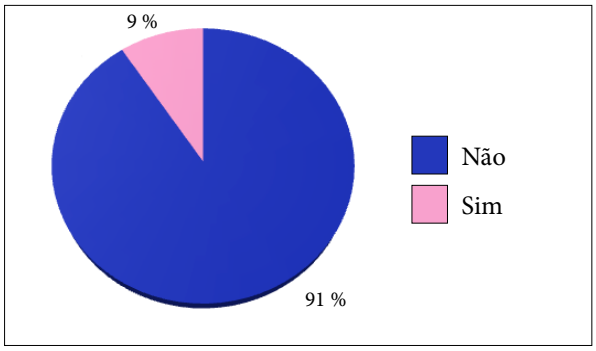


Fonte: Dados da pesquisa.

[1] Palestra com Nelson Novaes Neto, gerente geral de segurança do UOL/UOLDiveo. Disponível em: <https://www.youtube.com/watch?v=Q4FQyIlgZ9k>. Acesso em: 11 maio 2014.

Diante dos dados coletados, 1% dos usuários afirmou aceitar todas as solicitações de pedido que recebem. E 29% disseram aceitar pedidos de amigos. O que não descarta a hipótese de termos um usuário que aceita ambos os pedidos de amizades, conforme explicado anteriormente. Uma equipe de pesquisadores da Universidade da Columbia Britânica, no Canadá, divulgou um estudo que mostra que 1 em cada 5 usuários do Facebook aceita ser amigo de estranhos. Desse total, 60% o fizeram por ver que o *socialbot* (falso perfil) era amigo de um amigo seu[2]. Adicionar algum perfil ("*amigo*") sem checar se é verdadeiro traz uma grande ameaça para o usuário. Não se sabe qual a real intenção de tal pessoa ao enviar um pedido de amizade, por isso é preciso se certificar de todos os meios para se prevenir de um possível ataque virtual.

Gráfico 05 - Você disponibiliza seus dados pessoais nas redes sociais.

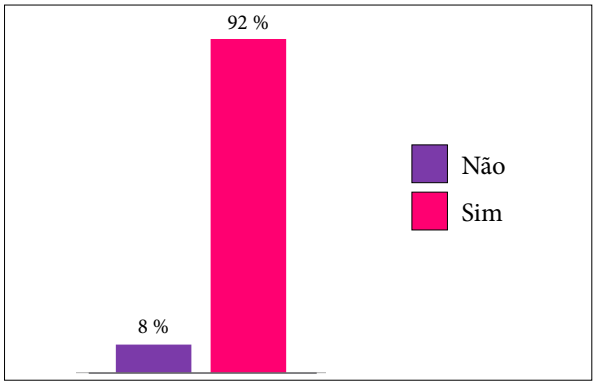


Fonte: Dados da pesquisa.

No gráfico 05, relata sobre a divulgação pública de dados pessoais nas mídias sociais, 91% responderam não, contra 9% que disponibilizam seus dados publicamente. Porém, observamos que tais dados analisados vão de encontro ao que foi comprovado na pesquisa feita pela Intel e a Ipsos Observer realizada em oito países, inclusive o Brasil. A pesquisa revelou, entre outras temáticas, os maus comportamentos dos usuários na hora de compartilhar informações pela internet. O estudo aponta que o excesso de compartilhamento foi um dos maus hábitos identificados – com pelo menos 6 entre 10 adultos e adolescentes dizendo acreditar que algumas pessoas divulgam informações além do necessário nas redes sociais. Entretanto, 40% dos entrevistados admitiu compartilhar informações pessoais diversas vezes ao longo do dia. No Brasil, mais da metade dos adolescentes informaram que passam o dia inteiro compartilhando informações online, principalmente fotos – conteúdo compartilhado com frequência por 78% dos adolescentes entre 13 e 17 anos[3]. Tal divergência pode ter sido provocada pelo fato de nossa pesquisa ter o tema segurança da informação, o que acreditamos ter, de certa forma, induzido as respostas dos usuários.

A preservação de sua privacidade pode ajudá-lo a se proteger dos golpes e ataques aplicados na internet. A divulgação e a coleta indevida de informações pessoais podem ocasionar fatores como: comprometer a sua privacidade, de seus amigos e familiares; facilitar o furto de sua identidade; facilitar a invasão de suas contas de usuário (por exemplo, de *e-mail* ou de rede social); fazer com que propagandas direcionadas sejam apresentadas; causar perdas financeiras, perda de reputação e falta de crédito; colocar em risco a sua segurança física e favorecer o recebimento de *spam*.

Gráfico 06 - Você se preocupa com a divulgação de suas fotos e/ou vídeos.



Fonte: Dados da pesquisa.

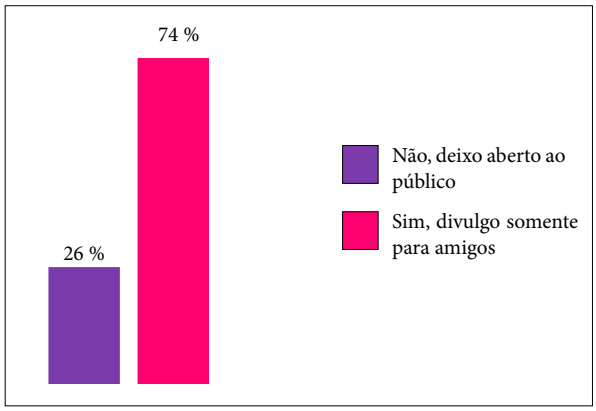
Outra preocupação é a divulgação de fotos e vídeos nas redes, como exposto no gráfi-

[2] Disponível em: <http://blogs.estadao.com.br/radar-tecnologico/2011/10/28/1-em-cada-5-usuarios-do-facebook-aceita-ser-amigo-de-estranho-diz-estudo> Acessado em 14/05/2014

[3] Site Fenainfo. Disponível em: <http://www.fenainfo.org.br/info_ler.php?id=42947> Acessado em 10/09/2014

co 06. De acordo com a amostra, 92% afirmam se preocupar e 8% não se importam. Porém, analisando o gráfico 07, logo abaixo, podemos perceber que apesar da preocupação há uma mudança no percentual, em que dos 92% preocupados somente 74% protegem ou restringem seu álbum de fotografias, divulgando-o somente para a lista de amigos.

Gráfico 07 - Você protege ou restringe seu álbum de fotos.



Fonte: Dados da pesquisa.

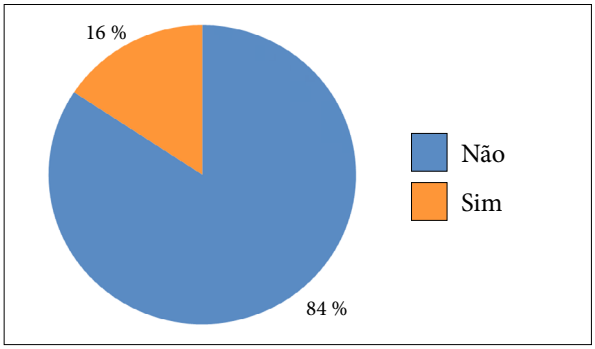
Analisando os dois gráficos, conclui-se que há uma pequena divergência e falta de coerência nas respostas dos usuários. Isso nos mostra que os usuários podem até ter a preocupação ao divulgar as suas fotos, mas não tem a consciência de limitar o acesso ao seu álbum de fotografias, deixando-o visíveis ao público. Com isso uma pessoa mal intencionada pode com um único clique copiar a foto e divulgar em locais impróprios ou mesmo utilizá-la em algo ilegal. Sempre pense antes de fazer publicações, assim como qualquer outra coisa que você publica na internet ou envia por *e-mail*, as informações que você compartilha no Facebook podem ser copiadas ou recompartilhadas por qualquer pessoa que possa vê-las[4].

3.3 Grupo aplicativos maliciosos (10 e 11)

De acordo com o gráfico 08, podemos analisar que em relação ao uso de aplicativos de geolocalização, 84% dos usuários não utilizam estas ferramentas, enquanto 16% afirmam fazer uso destes.

[4] Termo de privacidade e segurança da rede social Facebook.

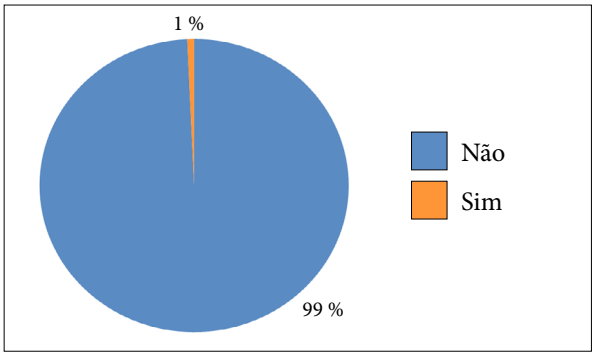
Gráfico 08 - Você faz uso constante de aplicativos que apontam sua localização geográfica.



Fonte: Dados da pesquisa.

A função de localização, presente em inúmeros aplicativos é algo perigoso, pois o compartilhamento do local onde você está, desperta o interesse de criminosos. Segundo o especialista em segurança da informação, José Milagres[5], isso é algo muito perigoso. Hoje o crime utiliza essa informação para poder roubar uma residência, assaltar, sequestrar. Não são raros os casos em que pessoas são semanalmente identificadas por criminosos por meio da geolocalização. (OLHAR DIGITAL, 2012)

Gráfico 09- Você permite que aplicativos não solicitados por você acessem seus dados pessoais.



Fonte: Dados da pesquisa.

O assunto exposto no gráfico 09 acima, relata a questão de aplicativos acessarem seus dados pessoais sem seu consentimento, 99% dos usuários dizem não permitir, e apenas 1% aceita.

Aplicativos que funcionam dentro das

[5] Disponível em: <http://olhardigital.uol.com.br/video/seguranca-nas-redes-sociais/31583>. Acessado em: 12 maio 2014.

redes sociais (por exemplo, jogos e agendas) se tornam cada vez mais comuns, o que muitas pessoas não têm conhecimento, é que ao baixá-los, você garante o acesso destas aplicações a seus dados pessoais e, normalmente, permite também que o aplicativo faça "*posts*" em seu nome e até tenha acesso a todos os seus contatos.

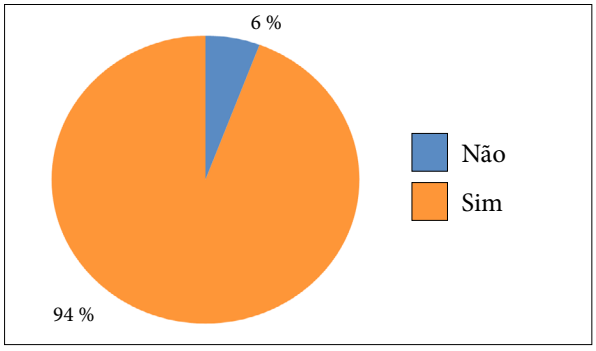
Um grande problema são os aplicativos maliciosos que, por trás de um simples jogo ou um "app", escondem um código sujo para, por exemplo, roubar seus dados, ter controle sobre tudo o que você faz na rede e até fazer com que seu perfil aja de determinado modo.

É preciso tomar cuidado, cheque todos os aplicativos cadastrados nos seus perfis em redes sociais e certifique-se que foram realmente autorizados por você e ainda lhe interessam.

3.4 Grupo veracidade e persistência dos conteúdos (12 e 13)

O gráfico 10 nos mostra a porcentagem de usuários que se dizem preocupados em verificar se uma informação é verídica antes de postá-la ou compartilhá-la nas redes sociais.

Gráfico 10 - Você se preocupa com a divulgação de suas fotos e/ou vídeos.



Fonte: Dados da pesquisa.

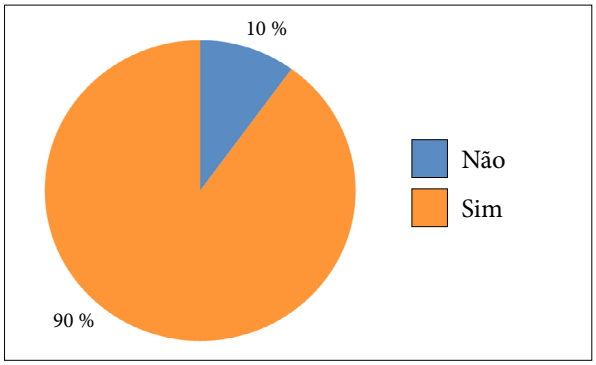
94% deles afirmaram que sim, checam a informação e caso a mesma tenha veracidade ela é passada adiante. Porém um caso recente que aconteceu no Brasil e que nos mostra uma contradição com os dados analisados é a trágica morte de uma mulher que foi espancada pela população ao ser confundida com uma foto divulgada nas redes sociais, onde a informação da imagem dizia que a mesma praticava rituais de magia negra com crianças. A questão é que essa informação compartilhada por muitos, era de 2002 e a mulher da foto não era a mesma que foi morta cruelmente[6].

Dessa triste realidade podemos concluir que a divulgação de boatos e inverdades é algo que pode comprometer até mesmo a segurança da própria vida. Por isso é necessário muito cautela e conscientização, pois as informações na Internet podem se propagar rapidamente e atingir um grande número de pessoas em curto período de tempo.

Enquanto isto é desejável em certos casos, em outros pode ser usado para a divulgação de informações falsas, que por ventura geram pânico e prejudicam pessoas, empresas e até mesmo comunidades inteiras.

O gráfico 11, apresentado abaixo, representa a quantidade de pessoas em porcentagem que tem ou não o conhecimento sobre a persistência dos dados e das informações nas redes sociais.

Gráfico 11 - Você tem conhecimento que, ao compartilhar conteúdos nas redes sociais, eles se propagam por inúmeras pessoas e que dificilmente poderão ser totalmente excluidos, por mais que sua conta seja removida.



Fonte: Dados da pesquisa.

Um percentual de 90% dos usuários disseram ter esse conhecimento, de que mesmo removendo a sua conta, as fotos, os vídeos, e outros dados, esses permaneceram na *Web*.

[6] Disponível em: <http://noticias.terra.com.br/brasil/policia/sp-morre-mulher-espancada-apos-boato-de-magia-negra,29b75d0892cc5410VgnVCM4000009bcceb0aRCRD.html>. Acessado em: 30/05/2014

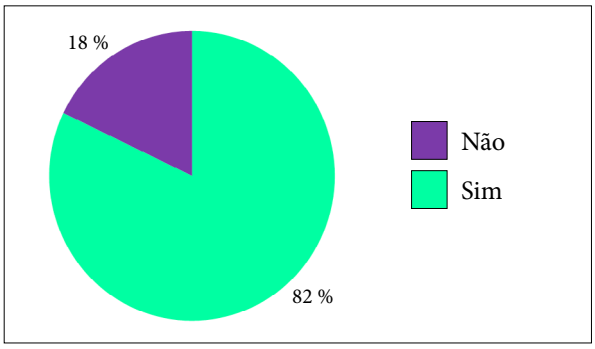
Os demais 10% afirmaram não ter esse conhecimento. Isso pode se tornar uma ameaça e consequentemente um grande problema para o usuário se usada com o auxílio de uma ferramenta de busca, como por exemplo, o Google.

Uma das principais ameaças à segurança e à privacidade dos usuários é proveniente do tipo de conteúdos e de informação que estes compartilham nas redes sociais. Portanto, é de suma importância que o usuário saiba fazer uso das redes sociais e principalmente das informações, fotos, vídeos, que publicam e/ou compartilham em tais mídias, causando constrangimento, danos morais e até contra a própria segurança.

3.5 Grupo segurança nas redes (14 a 17)

O gráfico 12 mostra a importância da utilização de mais de uma senha para as várias redes sociais, e-mails ou outro tipo de mídia que o usuário possa ter.

Gráfico 12 - Você utiliza mais de uma senha.



Fonte: Dados da pesquisa.

Com base na amostra coletada e nos dados apresentados, 82% dos usuários usam mais de uma senha e 18% não utilizam essa estratégia de segurança.

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), com o apoio do Comitê Gestor da Internet no Brasil (CGI.br, 2012), aconselha que nomes, sobrenomes, números de documentos, placas de carros e números de telefones estejam fora das senhas, além de apontar regras para a elaboração de senhas seguras.

O gráfico ao lado nos mostra que 37% dos usuários têm o costume de mudar de senha a cada seis meses , 9% mudam a cada ano e 54% não costumam mudar sua senha.

Gráfico 13 - Com que frequência você muda sua senha.

Fonte: Dados da pesquisa.

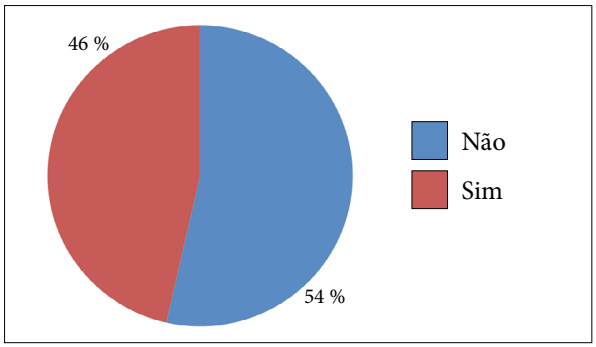
A frequência com que o usuário troca a sua senha é de elevada importância para a segurança de suas informações nas redes sociais. Especialistas defendem que o prazo máximo para garantir a segurança de uma senha é de 30 dias; outro fator importante é que essa palavra-chave deve ter, no mínimo 14 caracteres, entre letras, números e caracteres especiais.

Mudar a senha é essencial para prevenir e mitigar os riscos e vulnerabilidades envolvidos ao uso da internet. Portanto, mudá-la constantemente (de seis em seis meses, pelo menos) é crucial para diminuir as vulnerabilidades e as ameaças que o usuário está sujeito constantemente.

> A displicência dos usuários que criam senhas fáceis de serem descobertas, que ficam longos períodos sem alterá-las, e ainda utilizam a mesma senha para acesso a várias contas, torna o ataque mais simples. Basta enviar um cadastro oferecendo um brinde ou a participação em um sorteio que solicite o nome e senha do usuário e pronto. O *hacker* terá a sua disposição tudo o que é necessário para um ataque, sem grande esforço. (GRANGER, 2001 *apud* POPPER; BRIGNOLI, 2003, p. 4-5).

O próximo gráfico nos mostra a proficiência do usuário, em que 54% deles nunca pararam para ler as dicas de segurança das redes sociais que mais frequentam, contra 46% que afirmam já ter visto pelo menos uma vez o manual de segurança da sua mídia favorita.

Gráfico 14 - Alguma vez você já parou para ler as dicas de segurança das redes que costuma frequentar.



Fonte: Dados da pesquisa.

Ler os manuais das redes sociais é essencial para a qualidade da vida virtual. Saber o que estão publicando e quais os direitos que a mídia faz das suas informações é de suma importância.

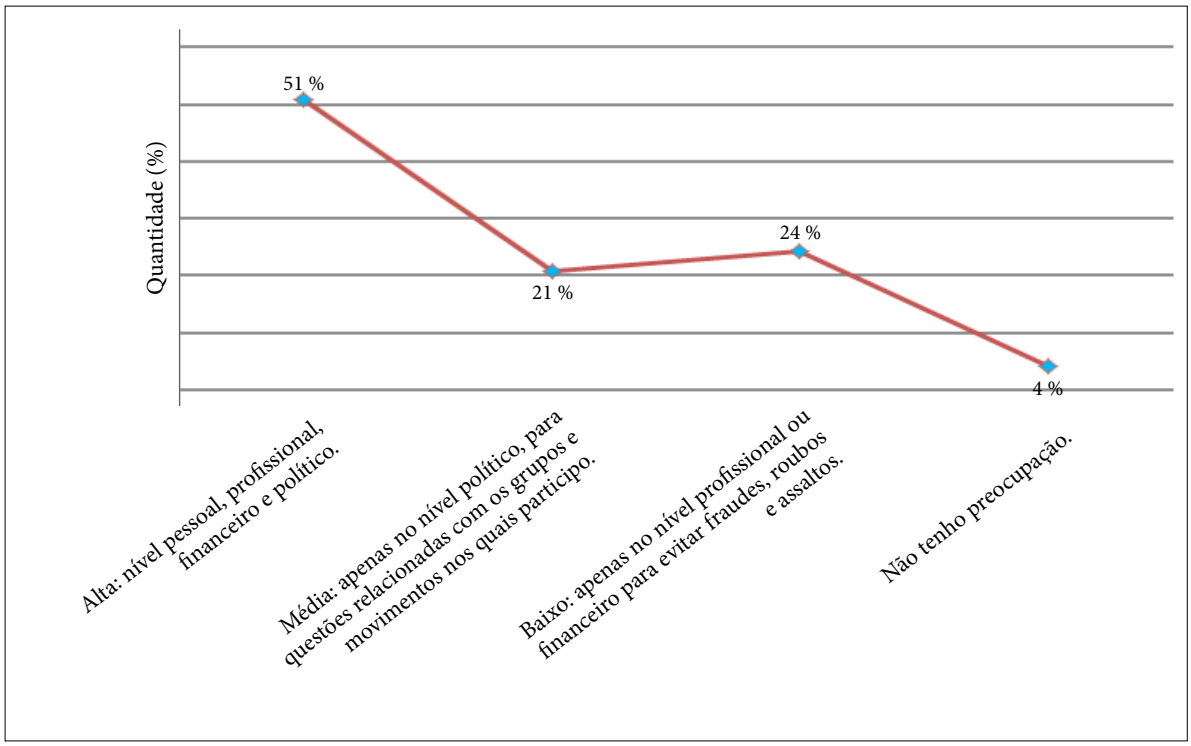
Hoje, as redes sociais oferecem configurações avançadas e detalhadas de segurança – principalmente para impedir o acesso indevido, o problema é que a maioria dos usuários não tem a devida preocupação com isso, ou então desconhece as possibilidades e ferramentas para aumentar a segurança e privacidade nesses canais.

> Existem recursos para troca de senhas, cadastro de equipamentos celular, cadastro de pergunta de segurança caso haja o esquecimento da senha, cadastro de segundo e-mail, alteração de dados, registrar o dispositivo que você está tentando conectar na rede social... há muitos recursos para tentar desencorajar o criminoso digital a acessar perfis indevidos [...] (OLHAR DIGITAL, 2012, Não paginado)

Você sabia que mesmo não cobrando nada pelo acesso, o Facebook capitaliza bilhões de dólares por ano? Isso só acontece porque você publica as suas informações na rede social e eles fazem uso delas para diversas finalidades e principalmente com publicidade, ou seja, uma empresa cria um anúncio e o Facebook é pago para exibir o anúncio. Os anúncios que você vê são selecionados com base nas coisas que você faz no Facebook, tais como curtir uma página ou comentar uma história, e nas informações que você compartilha, como sua cidade atual ou seu aniversário. Os anúncios também podem ser selecionados com base nas informações que você compartilha com os anunciantes ou sobre como você usa seus sites e aplicativos[7].

No gráfico 15, é analisado o grau de preocupação que as pessoas demonstram em re-

Gráfico 15 - Qual o seu nível de preocupação com a segurança.



Fonte: Dados da pesquisa.

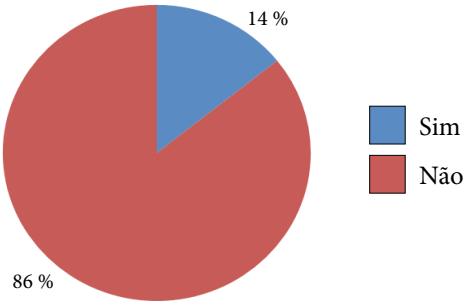
[7] Termo de privacidade e segurança da rede social Facebook

lação à segurança nas redes sociais. Faixa de 51% considera ter alta preocupação, enquanto que 21% e 24%, respectivamente, referem-se à média e baixa preocupação com a segurança, somente 4% dos usuários disseram não ter nenhuma preocupação com as suas informações divulgadas nas redes sociais e consequentemente com os problemas de segurança que possam acontecer. O que torna um dado preocupante, levando em consideração todas as informações até aqui descritas.

3.6 Grupo golpe virtual (18)

E por fim, a pergunta que nos leva a reflexão para todas as questões levantadas até o momento. O gráfico 16 nos dá uma dimensão da porcentagem de pessoas que foram ou não vítimas de algum tipo de golpe virtual. 14% dos usuários já tiveram essa experiência, contra 86% que afirmaram não ter sido vítima do crime cibernético.

Gráfico 16 - Você já foi vítima de algum golpe virtual.



Respostas	Quantidade	Porcentagem (%)
Sim	20	14%
Não	120	86%
Total	**140**	**100%**

Fonte: Dados da pesquisa.

4 ANÁLISE ESTATÍSTICA DOS DADOS

Para a análise estatística dos dados foram consideradas somente as questões em que apresentavam variáveis com respostas simples, desconsiderando as de múltipla escolha.

Subdividimos as questões por grupos para relacioná-las, deste modo obtivemos como resultado 65 correlações. De acordo com Garson (2009 *apud* FUGUEIREDO FILHO; SILVA JÚNIOR, 2009), uma correlação é uma medida de associação bivariada (força) do grau de relacionamento entre duas variáveis. Enquanto que para Moore (2007 *apud* FUGUEIREDO FILHO; SILVA JÚNIOR, 2009), a correlação mensura a direção e o grau da relação linear entre duas variáveis quantitativas. Analisando as variáveis, encontramos o coeficiente de Pearson (r) de cada relação:

$$r = \frac{\sum x(X_1 - \bar{X})(Y_1 - \bar{Y})}{\sqrt{(\sum(X_1 - \bar{X})^2)(\sum(Y_1 - \bar{Y})^2)}}$$

Além disso, foram utilizados também os diagramas de dispersão para demonstração do grau de relacionamento entre as variáveis. Abaixo são apresentados os gráficos que demonstraram maior significância para o estudo.

Gráfico 17 - Diagramas de dispersão e tabela do Coeficiente de Pearson dos gráficos A e B.

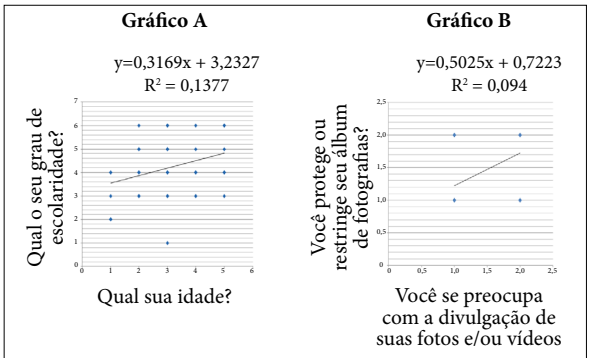


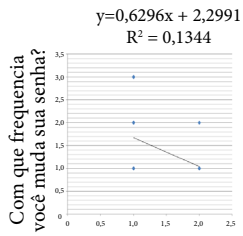
Gráfico D Troca de senha x Escolaridade	Gráfico N Renda x Troca de senha	Gráfico O Renda x Grau de preocupação
0,15	0,19	0,19

Fonte: dados da pesquisa.

Como pode ser observado nos gráficos A e B, há correlação linear positiva diretamente proporcional entre suas variáveis. O coeficiente de Pearson(r) encontrado foi A(0,37) e B(0,31). Segundo Cohen (1988), o valor representa uma classificação média, enquanto que na tabela 18, os coeficientes encontrados representariam uma classificação pequena.

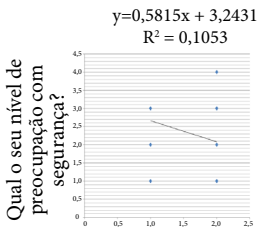
Gráfico 18 - Diagramas de dispersão e tabela do coeficiente de Pearson dos gráficos C e E.

Gráfico C



Você utiliza mais de uma senha?

Gráfico E



Alguma vez você já parou para ler as dicas de segurança das redes que costuma frequentar?

Gráfico F Idade x Grau de preocupação	Gráfico G Sexo x Troca de senha	Gráfico H Sexo x Grau de preocupação
-0,16	-0,16	-0,13

Gráfico I Escolaridade x Divulgação fotos/ videos	Gráfico J Escolaridade x Veracidade	Gráfico K Escolaridade x Propagação/persistência
-0,15	-0,20	-0,28

Gráfico L Escolaridade x Uso de senha	Gráfico M Escolaridade x Dicas de segurança
-0,22	-0,13

Fonte: dados da pesquisa.

Acima temos os gráficos C e E, onde há correlação linear negativa inversamente proporcional entre suas variáveis. O coeficiente de Pearson(r) encontrado foi C(-0,37) e E(-0,32). Segundo Cohen (1988), o valor representa uma classificação média, enquanto que os coeficientes de apresentados no gráfico 18, os valor representa uma classificação pequena.

5 CONSIDERAÇÕES FINAIS

De acordo com as análises e interpretações feitas, constatamos o quanto as redes sociais fazem parte do cotidiano do ser humano, ficando estes submetidos à influência de tais mídias. A popularização destas desencadeou vários benefícios, porém gerou grande preocupação em relação à segurança e à vulnerabilidade das informações que circulam no ambiente virtual.

Com base nas avaliações realizadas, foi possível verificar que uma maioria dos usuários se mostraram conscientes diante de ações e atividades a serem tomadas com o objetivo de manter seus dados em segurança. Porém ainda existem pessoas que cometem erros por simples ingenuidade, falta de informação ou mesmo desinteresse.

Por outro lado, constatamos que algumas pessoas responderam ao questionário não com base em suas ações e experiências, mas no que elas achariam o mais correto a se fazer, o que acreditamos ser ruim para a veracidade do nosso trabalho, entretanto esse risco é cabível a qualquer pesquisa científica. No entanto, o resultado final se mostrou satisfatório e nos deu um embasamento para outros trabalhos acadêmicos que por ventura ocorram futuramente.

Com isso, deixamos nossa mensagem de agradecimento e lembramos que estar bem informado e atualizado sobre métodos e meios de prevenção é crucial para um relacionamento saudável nas redes sociais.

REFERÊNCIAS

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de segurança para internet**: versão 4.0. 2 ed. São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em: <http://cartilha.cert.br/livro/>. Acesso em: 05 maio 2014.

COHEN, I. **Statistical power analisys for the behavioral sciences**. Hillsdale: Erlbaum, 1988

FIGUEIREDO FILHO, D. B.; SILVA JÚNIOR, J. A. Desvendando os mistérios do coeficiente de correlação de Pearson (r)*. **Revista Política Hoje**, Recife, v.18, n.1, p.115-146, 2009.

GIDDENS, A. **Sociologia**. 6 ed. Porto Alegre: Penso, 2012.

MARTELETO, Regina Maria. Análise de redes sociais: aplicação nos estudos de transferência da informação. **Ciência da Informação**, Brasília, v. 30, n. 1, p. 71-81, jan./abr. 2001.

OLHAR DIGITAL. **Segurança nas redes sociais**. 2012. Disponível em: <http://olhardigital.uol.com.br/video/seguranca-nas-redes-sociais/31583> Acesso em: 12/05/2014.

POPPER, M. A.; BRIGNOLI, J. T. **Engenharia social**: um perigo eminente. [2003]. 11 f. Monografia

(Especialização em Gestão Empresarial e Estratégias de Informática) – Institutlo Catarinense de Pós-Graduação, [S.l], [2003].

QUALMAN, E. **Socialnomics**: como as mídias sociais estão transformando a forma como vivemos e fazemos negócios. São Paulo: Saraiva, 2011.

YOUTUBE. **Segurança da informação nas redes sociais**. Palestra com Nelson Novaes Neto, gerente geral de segurança do UOL/UOLDiveo. 2012. Disponível em: <https://www.youtube.com/watch?v=Q4FQyIlgZ9k> Acesso em: 11 maio 2014.

APÊNDICE A – INDICADORES ESTATÍSTICOS

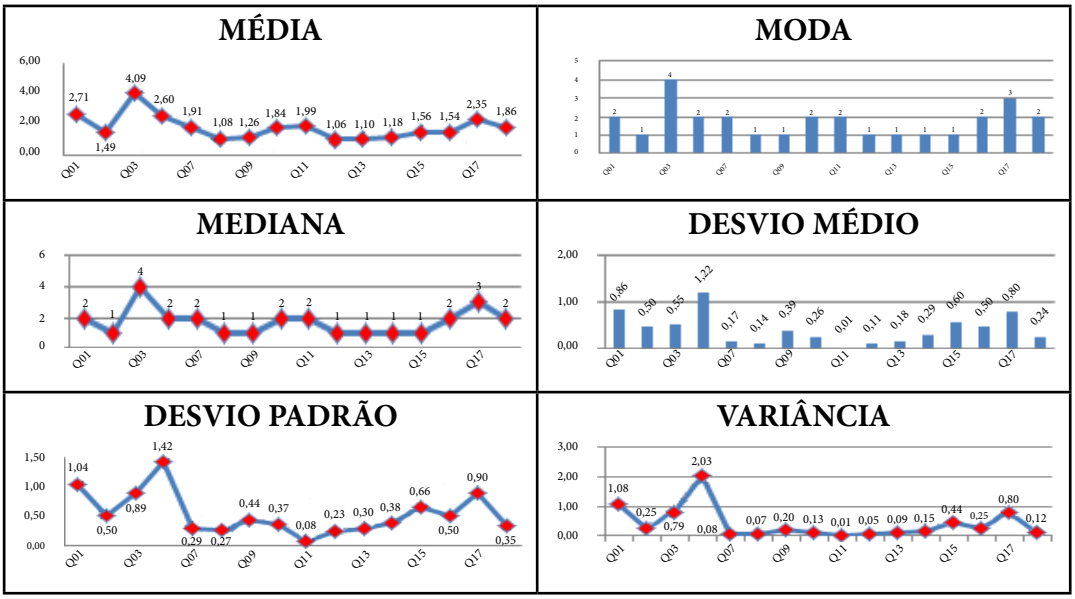
A seguir serão apresentados alguns dos principais indicadores da estatística que foram aplicados para cada questão. Não foram citadas as questões 5 e 6, por serem incompatíveis para a realização dos gráficos de dispersão, apresentados anteriormente, portanto não serão incluídas no passo a seguir. As variáveis estão representadas pela letra Q(Questão) junto ao número referente da mesma:

Tabela 01 - Indicadores estatísticos.

Variável	Média	Moda	Mediana	Desvio Médio	Desvio Padrão	Variância
Q01	2,71	2	2	0,86	1,04	1,08
Q02	1,49	1	1	0,50	0,50	0,25
Q03	4,09	4	4	0,55	0,89	0,79
Q04	2,60	2	2	1,22	1,42	2,03
Q07	1,91	2	2	0,17	0,29	0,08
Q08	1,08	1	1	0,14	0,27	0,07
Q09	1,26	1	1	0,39	0,44	0,20
Q10	1,84	2	2	0,26	0,37	0,13
Q11	1,99	2	2	0,01	0,08	0,01
Q12	1,06	1	1	0,11	0,23	0,05
Q13	1,10	1	1	0,18	0,30	0,09
Q14	1,18	1	1	0,29	0,38	0,15
Q15	1,56	1	1	0,60	0,66	0,44
Q16	1,54	2	2	0,50	0,50	0,25
Q17	2,35	3	3	0,80	0,90	0,80
Q18	1,86	2	2	0,24	0,35	0,12

Fonte: Dados da pesquisa.

Quadro 01 - Indicadores estatísticos.



Fonte: Dados da pesquisa.

- A média de cada pergunta foi encontrada com base na fórmula: M=S/n. Onde: S é a soma das respostas, e n é o número de respostas que se obteve nessa pergunta.
- A moda representa o valor mais frequente no conjunto de perguntas e respostas. Portanto, em cada questão foram obtidos aqueles valores que mais se repetiram. Não necessitando, pois, de fórmula.
- A mediana é uma medida de localização do centro da distribuição dos dados, definida do seguinte modo: Depois de ordenados os valores por ordem crescente ou decrescente, a mediana será o valor que ocupa a posição central, se a quantidade desses valores for impar ou será a média dos valores centrais, se a quantidade desses valores for par. O gráfico informa a mediana de cada questão.
- O desvio médio é uma medida de dispersão dos dados em relação à média de uma sequencia. Esta medida representa a média das distancia entre cada elemento da amostra e seu valor médio. O desvio médio é obtido a partir da fórmula:

$$S = \sqrt{s^2} = \sqrt{\sum_{i=1}^{n} \frac{(X_1 - \bar{X})^2}{n-1}}$$

- Para se chegar ao desvio padrão amostral foi preciso encontrar a variância amostral de cada questão. A fórmula da variância amostral é:

$$\theta^2 = \frac{\sum_{i=1}^{n}(X_1 - \bar{X})^2}{n-1}$$