O MAU USO DA INFORMAÇÃO: COMO NOS PROTEGER DE MÁS INTENÇÕES

Bruna Coelho Temer[1], Andréia Almeida Mendes[2], Luciana Rocha Cardoso[3].

[1] Graduanda em Tecnologia em Análise e Desenvolvimento de Sistemas, FACIG/Manhuaçu/MG, btemer@sempre.facig.edu.br
[2] Doutora em Linguística (UFMG/MG), FACIG/Manhuaçu/MG, andreialetras@yahoo.com.br
[3] Mestre em Ciência da Computação (UFV-Viçosa-MG), FACIG/Manhuaçu/MG, luroca@sempre.facig.edu.br

Resumo- A popularização da computação e da *Internet* é apontada por uma série de analistas de segurança internacional como um espaço no qual certa periculosidade colocaria em risco sistemas dos Estados nacionais. A partir disso, o espaço virtual das redes de computadores vem sendo progressivamente militarizado. O fundamento para essa militarização baseia-se na teoria em que o mundo virtual viria a ser o novo aspecto da guerra, guerra que viria a ser centrada na preocupação de elaboração de ataques a infraestruturas inimigas e, ao mesmo tempo, preocupar-se-ia com a necessidade de proteção dos ativos nacionais virtuais de valor estratégico. Esse princípio definido pelo nome “guerra cibernética”, é desprovido de uma base técnica sólida e sugere uma insegurança artificial cuidadosamente fabricada e difundida para a segurança na *internet*.

Palavras-chave: Informação; Guerra cibernética; Segurança; Formas de proteção.

Área do Conhecimento: Ciências Exatas e da Terra

1 INTRODUÇÃO

E se uma pessoa fizer mau uso de alguma informação obtida? Nos dias de hoje, vivemos em estado de desconfiança. A cada dia surgem novas ferramentas que permitem facilidade para acesso a bancos, dados acadêmicos e redes sociais, por exemplo. Ainda não sabemos a qualidade da segurança, nem se estamos propensos a ataques por meios de informação. Quase todos os processos que realizamos online geram informações; essas informações são armazenadas e disponibilizadas a certas pessoas.

A partir daí, informações deixam de ser sigilosas; imagine isso a nível governamental: informações de estratégias militares armazenadas em computadores, assim como informações confidenciais. Segundo o código de ética profissional do administrador (2008), o profissional deve “manter sigilo sobre tudo o que souber em função de sua atividade profissional”. O artigo 154 do Código Penal (1940) prevê que “revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a alguém”. A pena aplicada nesse tipo de crime é detenção, de três meses a um ano, ou multa.

Atualmente, o mundo está repleto de competitividade, seja ela nos comércios, religiões ou, simplesmente, para opressão. Com a informação certa, é possível atingir pessoas e grupos de pessoas de forma arrasadora. Segundo Clarke e Knake (2010), as pessoas com más intenções na web podem roubar todas as suas informações ou mandar instruções para movimentar dinheiro, derramar petróleo, espalhar gás, explodir geradores, descarrilar trens, colidir aviões, enviar um pelotão para uma emboscada ou, até mesmo, fazer com que um míssil exploda em um lugar errado. Isso não são hipóteses. Os autores ainda afirmam que coisas assim já aconteceram, experimentalmente, por engano ou, até mesmo, como resultado de algum crime cibernético.

Mostra-se, neste artigo, a possibilidade de se evitar que alguém faça mau uso de suas informações, mas não é possível que você mesmo possa evitar que informações sejam absorvidas para mau uso, afetando muito além de apenas um indivíduo.

1.1 REFERENCIAL TEÓRICO

Recentemente, podemos observar o uso de *drones* controlados por militares para bombardeios e ataques, não precisando arriscar nenhuma vida. Acontece também uma série de *hackers* que derrubam *sites* para expor informações: *Anonymous*. Segundo BENKLER (2012), os EUA consideram o grupo uma ameaça à segurança nacional, porém, segundo o autor, o *Anonymous* desempenha o papel de provocador audacioso, abrangendo as fronteiras entre destrutivo, perturbador, e instrutivo. Em novembro de 2015, o grupo declarou que iria *hackear* e derrubar o Estado Islâmico, que vem cometendo atos de terrorismo por todo o mundo. Se o *Anonymous*, por exemplo, pode derrubar um grupo terrorista, derrubar um estado é tarefa simples.

A guerra cibernética é definida no livro *Cyberwar* (2010), de Clarke e Knake, como determinadas ações conduzidas por Estados para penetrar computadores, ou redes de computadores, de outros países, com o objetivo de causar algum dano. Os teóricos chamam a atenção para a hipótese de que uma guerra cibernética tenha potencial de mudar o balanço militar e, em tese, isso alteraria as relações políticas e econômicas, gerando o caos. O ambiente digital está em transição a cada momento e, enquanto essa transição seja positiva acerca de um ponto de vista econômico, interfere de forma negativa trazendo certos riscos. Esse grande crescimento do uso da *internet* aumenta as chances de pessoas e/ou "atores" estatais lançarem ataques *online*, além de poderem esconder sua identidade, podendo proteger-se por trás das estruturas sociais que ainda não estão plenamente na *internet*.

O melhor ocasionador de uma guerra cibernética, do ponto de vista de Canabarro (2011), seria um país com uma baixa dependência de sistemas informatizados, e, também, a capacidade de desconectar as poucas conexões existentes entre o plano real e o plano virtual do país, como seria o caso da Coreia do Norte. Ainda segundo o autor, o país mais vulnerável a sofrer uma guerra cibernética seria os Estados Unidos, devido à grande parte de seus recursos críticos estarem fora do controle direto do governo.

Segundo a revista eletrônica Exame (2012), o governo dos Estados Unidos derrubou um famoso *site* de *download* de arquivos, *MegaUpload*, e, em seguida, foi atacado pelo grupo *Anonymous* com a queda de *sites* importantíssimos, como o *site* do Departamento de Justiça, MPAA, FBI, entre outros de grande importância. Naquele dia, segundo o *blog* de entretenimento "Jovem *Nerd*"[1], várias hipóteses de que uma guerra cibernética poderia ser iniciada começaram a surgir, chegando a ser uns dos assuntos mais comentados no *twitter*. A frase "Se o seu governo desligar a *internet*, fique calmo e desligue o seu governo" ganhou notório reconhecimento naquele dia. Pouco depois dos ataques os *sites* foram recuperados e voltaram ao ar, sem menção alguma à queda. Visto de um lado mais teórico, supomos que o *Anonymous* seja o Estado Islâmico dos dias de hoje. Da mesma forma que o ISIS ataca com atentados terroristas, o grupo *Anonymous* poderia atacar de forma cibernética; começaria então um ciclo de ataques *online*, não estaríamos seguros. Da mesma forma que o grupo poderia realizar um ataque terrorista digital, grandes empresas usufruem de *hackers* para obter informações valiosas de seus concorrentes e do governo. Não só as informações estariam nas mãos de pessoas erradas, mas também outras pessoas estariam "nas mãos" daquelas.

Segundo o sociólogo Machado Neto (1987), a guerra é efeito da convergência de várias causas (política, psicológica, religiosa, econômica, demográfica, geográfica etc.), mas também é a causa de alterações substanciais em praticamente todos os quadrantes da vida social. Segundo o autor, por exemplo: a guerra pode levar à consolidação de impérios e à centralização do poder (efeitos políticos); à sobrevivência de uma sociedade e ao definhamento de outra numa situação geral de escassez (efeitos econômicos); ao desenvolvimento de novas técnicas para uso militar e civil, tornando obsoletas as técnicas anteriores (efeitos tecnológicos); à evasão de pessoas dos territórios em conflito para outros que ofereçam condições de paz (efeitos demográficos).

Ainda em 2013, veio à tona notícias de que o governo americano opera sistemas de monitoramento e vigilância dos meios de comunicação do mundo todo, confome notícia divulgada pelo portal "G1", em 02 de julho de 2013. Edward Snowden, antes empregado da Agência de Segurança Nacional (NSA), trouxe à tona documentos que comprovavam espionagem do governo dos Estados Unidos. Por essa razão, Snowden foi exilado e mantido em segurança devido a ameaças feitas a ele.

Para nos proteger, foram inventados *softwares* que auxiliam nessa função. Segundo o *site* "JusBrasil", o Exército Brasileiro já adotou o uso de um *software* da Decatron que simula uma guerra

[1] *Blog* Jovem *Nerd*. Disponível em https://jovemnerd.com.br/nerdnews/guerra-cibernetica-fbi-derruba-megaupload-e-anonymous-se-vinga/

cibernética, provendo suporte para especialização de recursos humanos em análise de vulnerabilidades de redes, permitindo a execução de ações, em ambiente controlado, de proteção cibernética e defesa ativa, além do treinamento baseado em cenários reais de catástrofes e comprometimentos de infraestruturas críticas nacionais. Devemos visar o sigilo de nossos dados que acabamos compartilhando em meios que utilizam a tecnologia da informação.

Dilma Rousseff disse em 2013, segundo o portal de notícias "BBC", em meio às revelações de que o Brasil é alvo de espionagem, que o nosso país sabe proteger-se de uma guerra cibernética, mas não é isso que apontam os dados. Poucos métodos foram adotados para garantir segurança contra ataques, embora o termo já tenha sido prioridade na Estratégia Nacional de Defesa.

Individualmente, cada um pode (e deve) fazer sua parte no processo de proteção à informação. Temos grandes antivírus e *antispywares* reconhecidos e gratuitos à disposição de todos. Podemos evitar o envio de informações sempre que possível, para não ocasionar possível mau uso dos dados que enviamos usualmente online. Senhas de bancos, dados pessoais, tudo isso fica armazenado na rede. Quanto mais seguros estivermos, menores são as chances de estarmos vulneráveis à algum ataque.

2 METODOLOGIA

Este artigo foi escrito com base em uma pesquisa que pode ser assim classificada:

Qualitativa, pois a abordagem busca o motivo do lançamento de uma nova forma de guerra: a cibernética. O objetivo do uso da pesquisa qualitativa foi, nesse caso, produzir informações aprofundadas no tema.

Básica, pois o objetivo foi para gerar novo aprendizado útil para nos defendermos de novas ameaças que estão a surgir e, também, envolve algumas "verdades" universais.

Explicativa, pois procura-se explicar o porquê da existência das ameaças de ataques cibernéticos através dos resultados oferecidos.

Survey, pois, para que fosse possível analisar a ideia de que a população tem diante de alguma guerra cibernética ou segurança de seus dados, foi aplicado um questionário *online*.

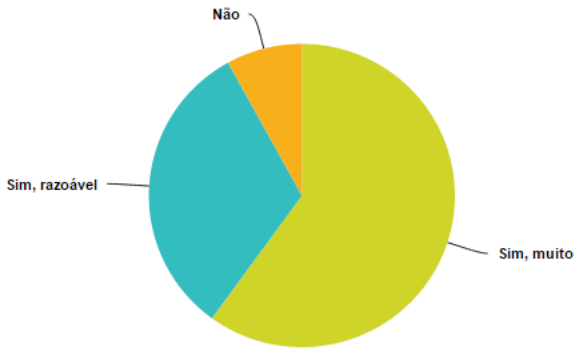
O questionário foi composto por 6 perguntas que envolviam ações do cotidiano que envolvem a relação das pessoas com seus computadores e a *internet*. O questionário foi lançado aos alunos do curso de Análise e Desenvolvimento de Sistemas, da mesma instituição de ensino FACIG – Manhuaçu/MG que se encontra em Anexo A - *Survey* deste trabalho. O questionário foi enviado à 35 alunos da instituição e foi respondido por 25 alunos, gerando uma porcentagem acerca de 70% de respostas completas.

Após isso, os questionários foram analisados e tabulados pelo programa "*Survey Monkey*". Em seguida, foram confeccionados gráficos que são apresentados na próxima seção.

3 RESULTADOS E DISCUSSÃO

A seguir, serão apresentados os gráficos correspondentes à análise dos resultados. A primeira indagação do questionário diz respeito à preocupação quanto à segurança de dados na *internet*, o resultado obtido, pode ser observado no gráfico 1:

Gráfico 1 – Preocupação quanto à segurança de dados na *internet*.



Como se observa no gráfico, nenhum dos entrevistados se sente "Muito seguro" em relação à seus dados serem mantidos *online*. Segundo BREI e ROSSI (2005), a confiança que o cliente exerce sobre a companhia que lhe fornece o ambiente *online* para suas transações vem de quando os clientes enxergam que o custo/benefício de manter o relacionamento para realizar o que é necessário é bastante positivo. Isso explicaria os gráficos 2 e 3, apresentados abaixo:

Gráfico 2 – Nível de segurança no qual as pessoas se sentem por seus dados pessoais serem mantidos *online*

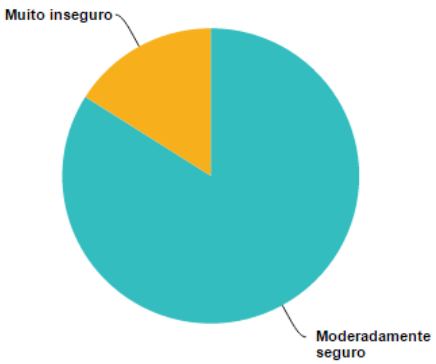
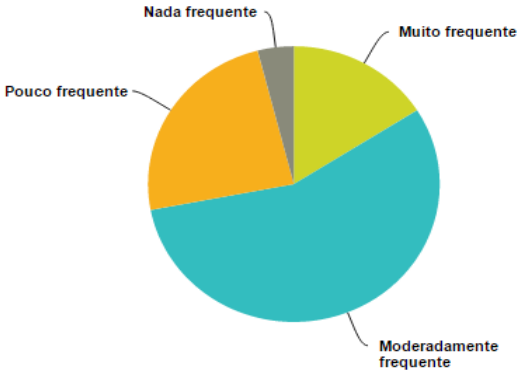


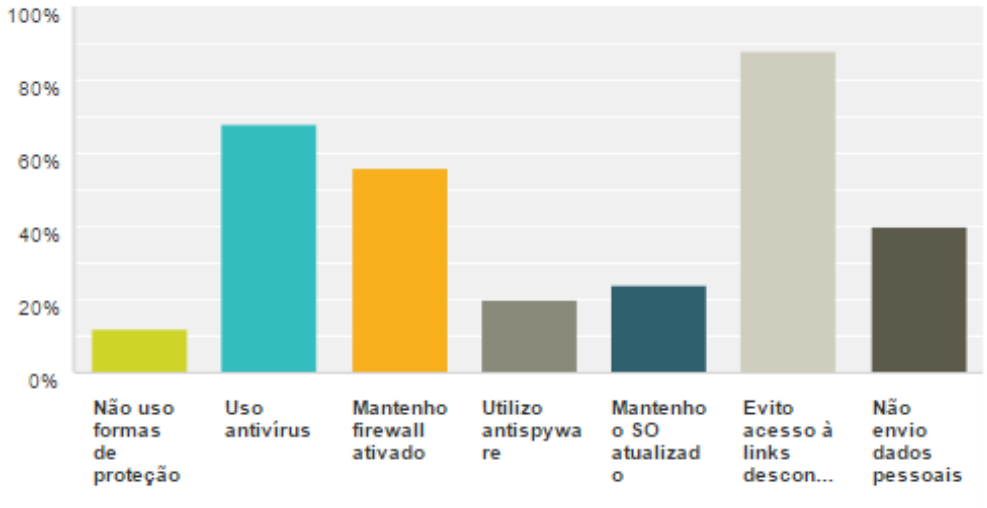
Gráfico 3 – Frequência na qual as pessoas se sentem seguras com as operações realizadas na *internet*



Pela análise dos gráficos 2 e 3, percebe-se que, aparentemente, os clientes que realizam operações na *internet* não são leais às empresas que fornecem os serviços. Ainda segundo BREI e ROSSI (2005), à curto prazo, os grandes fatores responsáveis pela lealdade são a confiança e o comprometimento, e não a satisfação, que seria a responsável pela lealdade de clientes com pouco tempo de relacionamento com a empresa. Para Oliver (1999) a satisfação é um estado pós-uso decorrente de uma situação de consumo única ou de experiências repetidas que refletem como um produto ou serviço supriu seu propósito. Embora tudo isso, segundo Albertin (2004) constatou-se a existência de um “senso comum” que considera a segurança na *Internet* como a maior restrição para o crescimento do comércio eletrônico, independentemente de estar baseada em fatos ou na percepção dos usuários.

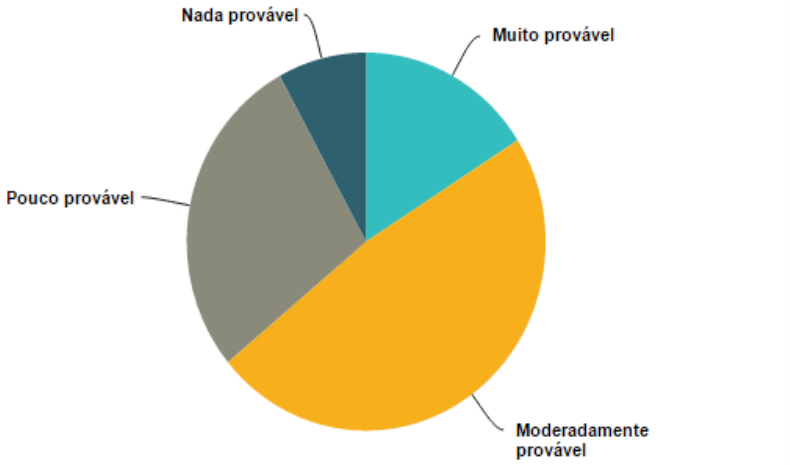
Podemos também observar, pelo resultado do Gráfico 4, que a maioria dos entrevistados procura alguma forma de se proteger de ameaças *online*. Para BERNSTEIN (1997), nenhuma solução de segurança deve ser considerada capaz de oferecer toda a proteção necessária. Segundo o autor, cada solução de segurança deve atender à característica pessoal da necessidade de cada um.

Gráfico 4 – Formas de proteção utilizadas pelos entrevistados



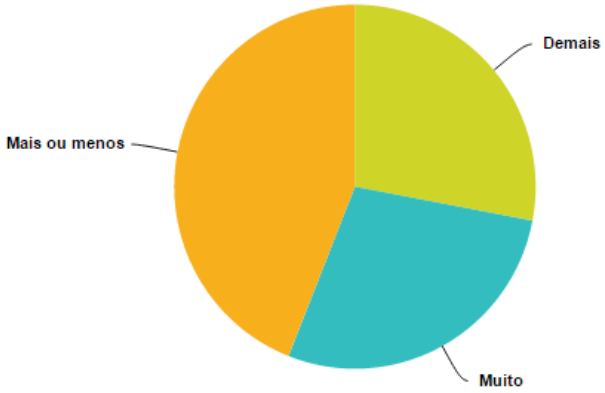
Segundo Johnson (2015), em relação à ameaça cibernética, as projeções de uma futura guerra são feitas com base em um padrão já estabelecido, o que explica por que aqueles que buscam demonstrar, com dados estatísticos, que haverá uma redução na frequência de guerras no futuro se sentem tão confiantes quanto os pessimistas. Isso explica o resultado do gráfico 5, no qual as pessoas acham que é "moderadamente provável" que ocorra uma guerra cibernética.

Gráfico 5 – Demonstrativo de probabilidade em relação a uma possível guerra cibernética



As pessoas se sentem intimidadas pelo fato de suas informações pessoais estarem disponibilizadas no meio *online,* como aponta o Gráfico 6. Segundo Krause e Tipton (1999) se evidencia que os negócios estão cada vez mais dependentes das tecnologias e estas precisam proporcionar confidencialidade, integridade e disponibilidade. Com a probabilidade de que isso não esteja mais disponível, a pessoa se sente menos segura e mais vulnerável.

Gráfico 6 – Presunção em relação à probabilidade de vulnerabilidade da perda de confidencialidade, integridade e disponibilidade de seus dados



Pode-se concluir a partir da análise desses gráficos que nenhuma pessoa se sente totalmente segura para realizar operações online. Foi constatado que é muito difícil se sentir seguro em relação à vulnerabilidade que é apresentada no meio online.

4 CONCLUSÃO

Com a descrição e limitação da segurança digital e os efeitos dos crimes digitais, a relação entre a segurança nacional torna-se difícil de justificar. Nesse sentido, a busca do governo pela consideração dos crimes digitais como ameaças militares não tem conexão com a realidade cotidiana da segurança de redes.

O que deve ser feito para evitar que seus dados sejam usados de forma negativa é exatamente o que foi descrito anteriormente, pois, se cada um fizer sua parte em relação à segurança, precisaremos focar apenas em áreas específicas para evitar que as informações sejam desviadas para mãos erradas.

5 REFERÊNCIAS

ALBERTIN, A. L. Comércio Eletrônico: Modelo, Aspectos e Contribuições de Sua Aplicação. São Paulo: Editora Atlas, 5ª edição, 2004

AMORIM, Celso. Defesa Nacional e Pensamento Estratégico Brasileiro.Política Hoje, Recife, v. 21, n. 2, p. . 06/2012. Disponível em: http://www.revista.ufpe.br/politicahoje. Acesso em: 01/12/2015

Anonymous derruba site do FBI após fechamento do Megaupload. 2012. Disponível em: http://exame.abril.com.br/tecnologia/noticias/anonymous-derruba-site-do-fbi-apos-fechamento-do-megaupload. Acesso em: 01/12/2015

BRASIL. Código Penal Brasileiro. Decreto-Lei n° 2848 de 07 de dezembro de 1940. Disponível em: <http://www.jusbrasil.com.br/topicos/10619917/artigo-154-do-decreto-lei-n-2848-de-07-de-dezembro-de-1940>. Acesso em: 01/12/2015.

BREI, Vinícius Andrade; ROSSI, Carlos Alberto Vargas. Confiança, valor percebido e lealdade em trocas relacionais de serviço: um estudo com usuários de Internet Banking no Brasil. **Rev. Adm.**

BENKLER, Yochai. Why Anonymous Is Not a Threat to National Security. Foreign Affairs, 2012. Disponível em: <http://www.foreignaffairs.com/articles/137382/yochai-benkler/hacks-of-valor?page=show>.

BERNSTEIN, Terry, BHIMANI, A. B., SHULTZ, Eugene, SIEGEL, Carol A.. Segurança na Internet. 1ª Ed.. Rio de Janeiro : Ed. Campus, 1997. 461p. (Tradução de *Internet Security for Business*).

BREI, Vinícius Andrade; ROSSI, Carlos Alberto Vargas. Confiança, valor percebido e lealdade em trocas relacionais de serviço: um estudo com usuários de internet banking no Brasil. **Revista de Administração Contemporânea**, v. 9, n. 2, p. 145-168, 2005.

CANABARRO, Diego Rafael. RESENHA DO LIVRO:" CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT". **Conjuntura Austral**, v. 2, n. 6, p. 145-151.

CÓDIGO DE ÉTICA PROFISSIONAL DO ADMINISTRADOR (Aprovado pela Resolução Normativa CFA nº 353, de 9 de abril de 2008)

CLARKE, Richard A.; KNAKE, Robert K.. Cyber War**:** The Next Threat to National Security and What to Do About It. New York: Harper Collins, 2010.

Exército Brasileiro recebe software simulador de guerra cibernética**.** 2013. Disponível em: http://internet-legal.jusbrasil.com.br/noticias/100306404/exercito-brasileiro-recebe-software-simulador-de-guerra-cibernetica. Acesso em: 01/12/2015

G1. Entenda o caso de Edward Snowden, que revelou espionagem dos EUA. **G1**, jul. 2013. Disponivel em: <http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>. Acesso em: 01 Dezembro 2015

JOHNSON, Robert A.. **Como Prever a Guerra do Futuro. Military Review**, Leavenworth County, v. 1, n. 2, p. 43-54. 07/2015. Disponível em: <http://usacac.army.mil/CAC2/MilitaryReview/Archives/Portuguese/MilitaryReview_20150831_art008POR.pdf>. Acesso em: 01/12/2015

KRAUSE, Micki e TIPTON, Harold F. 1999. **Handbook of Information Security Management.** Auerbach Publications.

MACHADO NETO, Antônio Luís. **Sociologia Jurídica**. 6. ed. São Paulo: Saraiva, 1987.

OLIVER, R. Satisfaction: a behavioral perspective on the consumer. New York: Irwin / McGraw-Hill, 1997. 1. ed. 432p

Anexo A - SURVEY

1. Você se preocupa com a segurança dos seus dados na *internet*?
    a. Sim, muito
    b. Sim, razoável
    c. Não
    d. Não sei responder/Não se aplica

2. Quão seguro você se sente de que seus dados pessoais são mantidos em confidencialidade quando faz compras, acessa *Internet Banking* ou realiza outras operações pela *Internet*?

    a. Muito seguro
    b. Moderadamente seguro
    c. Muito inseguro

3. Com que frequência as preocupações com a privacidade/segurança evitam que você efetue alguma operação envolvendo seus dados *online*?

    a. Muito frequente
    b. Moderadamente frequente
    c. Pouco frequente
    d. Nada frequente

4. Como aluno do curso de Análise e Desenvolvimento de Sistemas você tem aprendido a como se proteger de ameaças? Se sim, marque as formas que você usa para se proteger:

    a. Não uso formas de proteção
    b. Uso antivírus
    c. Mantenho *firewall* ativado
    d. Utilizo *antispyware*
    e. Mantenho o SO atualizado
    f. Evito acesso à *links* desconhecidos
    g. Não envio dados pessoais

5. Qual a probabilidade de que temos, como país, profissionais prontos para nos defender diante de algum ataque cibernético?

    a. Extremamente provável
    b. Muito provável
    c. Moderadamente provável
    d. Pouco provável
    e. Nada provável

6. Em sua opinião, estamos vulneráveis a perdemos confidencialidade, integridade e disponibilidade dos dados que são administrados por terceiros (ex.: bancos, escolas, comércio, redes sociais...)?

    a. Demais
    b. Muito
    c. Mais ou menos
    d. Pouco
    e. Nada