FALTA DE SEGURANÇA E O CRESCIMENTO DOS CYBERS CRIMES NO BRASIL

Lillyanne Karolline de Melo Silva [1]

Leonardo Mèrcher [2]

RESUMO

Atualmente os crimes cibernéticos no Brasil cresce de forma exponencial e descontrolada em consequência do avanço tecnológico e de uma economia moderna, rápida e dinâmica introduzida através dos benefícios da era digital. Com o objetivo de divulgar e desempenhar um papel sócio educativo ressaltando o crescimento dos incidentes de segurança no país, mostrando que através de técnicas simples e funcionais pessoas e organizações passaram a ter conhecimento sobre os riscos em que estão expostas e de como se proteger de inúmeras ameaças existentes no mundo digital, onde pessoas e organizações precisam se relacionar, interagir e estabelecer relações comerciais e institucionais de forma segura através da aplicação de boas práticas de segurança e colhendo bons resultados se livrando de serem vitimas de ataques digitais, pois a conscientização é o melhor caminho em decorrência das leis no país serem brandas e ineficientes, todos devem fazer o seu papel para que se tenha um mundo digital melhor e seguro.

Palavras chave: Crimes cibernéticos. Boas práticas. Conscientização.

[1] Lillyanne Karoline de Melo Silva bacharelado no curso de Relações Internacionais pela UNINTER - Centro Universitário Internacional.

[2] Leonardo Mèrcher doutor em Ciência Política pela UFPR – Universidade Federal do Paraná.

INTRODUÇÃO

O forte crescimento e avanço tecnológico no Brasil e no mundo, tem proporcionado para as pessoas e organizações um novo horizonte em suas relações, seja ela comercial, pessoal ou institucional, tudo isso se tornou possível porque a tecnologia se faz presente praticamente em todas as ações em nosso cotidiano. Atualmente em muitos segmentos tornou-se impossível realizar qualquer atividade por mais simples que seja, sem o apoio da tecnologia tanto em eficiência como em produtividade.

Este artigo destaca o crescimento do número de cyber crimes e cyber ataques no Brasil, porque pessoas e organizações estão sendo vítimas de crimes relacionados à segurança digital, não apenas relacionados a prejuízos financeiros mas também a exposição social e cultural, por não se preocuparem com as ameaças presentes no mundo digital, este artigo tem o objetivo de divulgar não apenas números informativos tem também um papel sócio educativo, onde através da aplicação de boas práticas de segurança possibilita que as pessoas e organizações entendem de que forma estão sendo expostas aos riscos, tornando-se possíveis vítimas, se protegendo e fazendo o uso consciente de todos os benefícios oferecidos pela era digital.

Através das novas formas de se relacionar com o mundo as informações passaram a ter um valor incalculável, pois através delas movimenta-se a economia do país, aproxima investidores e pessoas de todos os lugares estimulando e aquecendo as relações comerciais e pessoais, sabendo disso cracks e organizações mal intencionadas aproveitam dessas vulnerabilidades fazendo delas um alvo fácil para os cyber ataques no Brasil. Aproveitando as fragilidades das lei em nosso país, esses grupos criminosos tem feito do Brasil o alvo favorito em um esquema de segurança digital, tais como: sequestro de dados, exposição de conteúdo indevido, movimentando um negócio multe milionário no mercado negro.

Solicitar a criação de novas leis e melhorar as já existentes com o objetivo de coibir essas ações criminosas deve ser o papel realizado pelos órgãos de segurança competentes em nosso país, apoiando uma reforma imediata nas questões de políticas de segurança pública afim de prover segurança e confiabilidade em um mundo digital melhor.

2 PORQUE CRESCE O NÚMERO DE CYBERS CRIMES NO BRASIL?

Nas últimas duas décadas o Brasil propagou um crescimento exponencial quanto ao número de pessoas que passaram a fazer uso da internet no seu dia a dia, seja para trabalho onde as empresas estão cada vez mais informatizadas, graças ao avanço da tecnologia onde todos os processos passaram a ser cada vez mais digitais, tais como: transações bancárias, emissões de documentos eletrônicos ou para o uso pessoal através das redes sociais e canais de entreterimento como como jogos online e serviços de *streaming*, mas em contra partida da mesma maneira que cresce o número de pessoas cresce também os riscos de realizar essas operações através das mídias digitais, isso ocorre por uma série de fatores principalmente no Brasil seja ele sócio econômico, cultural, falta de conhecimento tecnológico de como se proteger e fazer o uso dessas ferramentas de forma segura.

Segundo a companhia Norton Symantec “ao longo de 2016 foram registrados mais de 689 milhões de casos em todo mundo sendo 42,4 milhões no Brasil, isso corresponde a ¼ da polução nacional” (Norton, 2016) isso ocorreu pela facilidade e o crescimento da aquisição dos aparelhos *smartphones,* onde as pessoas começaram a substituir seus aparelhos telefônicos analógicos por dispositivos móveis com uma infinidade de novos recursos e aplicativos através do uso da internet.

Essa preocupação tem sido trabalhada a mais de 20 anos pela NIC.br Comitê Gestor da Internet no Brasil, ela responsável pela coordenação e integração dos serviços de internet em todo o País, em parceria com a CERT.br [2] criado incialmente com o objetivo de apoiar pessoas e organizações fazendo o uso de forma segura e consciente mais que com ao longo dos anos se firmou como um grande centro de pesquisas ao tratamento dos incidentes no Brasil através de um método de boas práticas cada pessoa ou organização pode notificar para CERT.br caso tenha sido vítima de um ataque com o intuído de ajudar e desenvolvido um trabalho relevante através materiais auto explicativos, treinamentos, cursos e palestras entendendo e capacitando pessoas e profissionais detectar possíveis ameaças, vale apenas destacar que esse trabalho não exige a necessidade de ser desenvolvido apenas por profissionais da área de TI podendo ser realizado por qualquer pessoa.

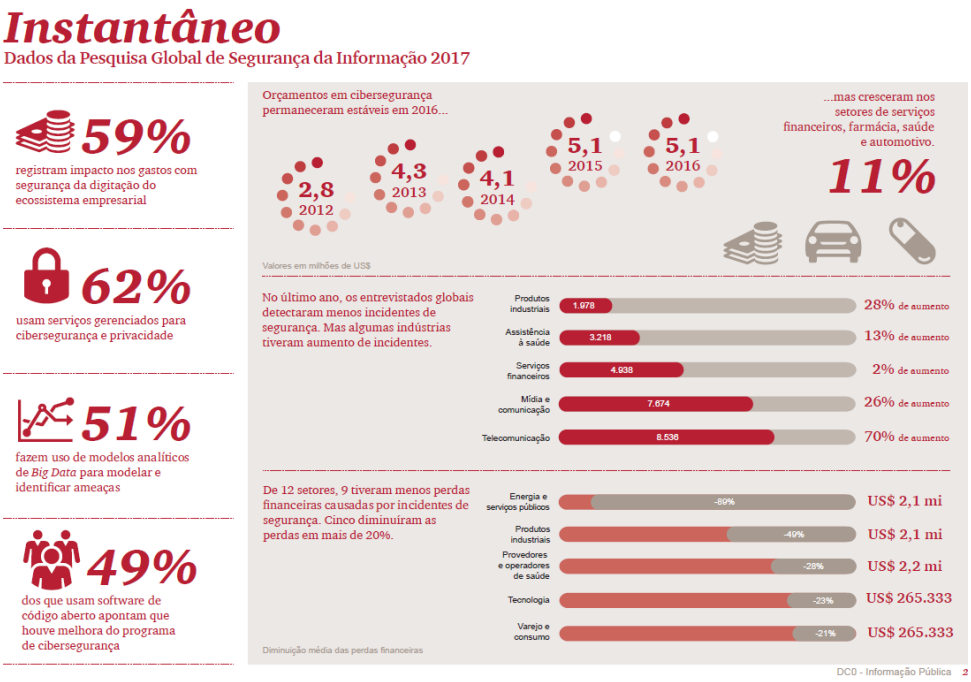
[1] NIC – Núcleo de Informação e Coordenação

[2] CERT – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

2.1 INFORMAÇÕES O BEM MAIS PRECIOSO DAS PESSOAS E ORGANIZAÇÕES.

No ano de 2017 o cyber ataque que popularizou não só no Brasil, mas em todo o mundo foi *Ransomware,* pois trata-se de um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento geralmente ocorre em servidores, usando criptografia, o atacante exige um resgate em dinheiro para restabelecer o acesso aos dados, geralmente o pagamento e feito através de moedas digitais como *bitcoins* pois desta forma dificulta o rastro do *cracker* uma vez que as leis para os crimes eletrônicos no Brasil são falhas, os atacantes aproveitam dessas vulnerabilidades explorando esses recursos a seu favor. Os *crackers* são pessoas com grande conhecimento em informática especialistas em quebrar códigos de segurança, diferente os *hackers* que são especialistas em segurança cibernética.

De acordo com a *Kaspersky Lab* durante o 7º congresso - Cúpula Latino Americana de Analistas de Segurança “o Brasil é o país latino americano mais afetado pela propagação do *ransomware*, onde sofreu 55% de todos os ataques em 2017 se comparando aos anos anteriores esse número representa um crescimento de 30%” (*Kaspersky Lab*, 2017). Depois de números alarmantes empresas no Brasil e no mundo começaram a se preocuparem com investimentos em ferramentas e soluções de segurança segundo o centro de pesquisas da PwC (2017, p.02) “em 2017 registrou o maior crescimento em investimentos em ativos de segurança”.



Fonte: https://www.pwc.com.br/pt/10minutes/assets/2017/10min-cyber-privacidade-informacao-17.pdf

2.2 QUAIS OS IMPACTOS CAUSADOS NAS RELAÇÕES COMERCIAIS E INSTITUCIONAIS ATRAVÉS DO ACESSO DE INFORMAÇÕES SIGILOSAS?

O mundo vive um momento chamado de era da informação onde elementos que nas décadas passadas eram fator de grandes problemas como a distância geográfica e tempo de resposta nas operações comerciais, hoje não representam mais nenhum tipo de obstáculo para se estabelecer qualquer tipo de relação seja ela comercial ou não, pois a informação aliada ao conhecimento resultou em poderosas ferramentas nesse novo modelo de negócios chamado de economia moderna.

Segundo Eleuterio (2015, pag.23) “os efeitos da revolução da informação extrapolam as fronteiras das organizações e passaram a causar fortes impactos na economia mundial”. Onde pessoas e organizações trocam informações de forma simultânea a cada segundo, com isso informação tornou-se um bem de valor inestimável representando competitividade, eficiência e rapidez através da comunicação digital, organizações criminosas e crackers exploram esse segmento de mercado afim de ganharem vantagens financeiras comercializando informações sigilosas de pessoas e organizações no mercado negro da internet.

No segundo semestre de 2017 a empresa Uber líder no segmento de modelo de negócios disruptivos, trata-se da modernização de um serviço simples no caso transporte de passageiros por meio de aplicativos, onde os colaboradores têm a flexibilidade de horário, preços competitivos tudo isso através de aplicativos móveis pode alcançar crescimentos históricos graças a era da economia moderna. No entanto junto com o crescimento a empresa trouxe a exposição de todo esse sucesso quando sofreu um cyber ataque no segundo semestre de 2017, onde expôs aproximadamente cerca de 57 milhões de usuários, segundo seu site oficial o Uber está presente em mais de 108 países e 632 cidades do mundo, incluindo sua sede em San Francisco na Califórnia. Desde sua fundação em 2009 a empresa Uber foi sem dúvida um dos modelos de negócios que revolucionou de forma significativa a economia digital. Para Toffler (1980), apud Eleuterio (2015, pag. 23) “a revolução da informação, que sucedeu as duas primeiras revoluções a agrícola e a industrial, criou a economia digital, em que o capital intelectual e a tecnologia são os principais fatores de sucesso das organizações modernas”. Onde o Uber e outras organizações se tornaram uma referência nesse novo conceito de economia baseada nos avanços da tecnologia, conhecimento e informação os três pilares da economia na era digital.

2.3 COMO SE PREVENIR E SE LIVRAR DOS CYBER ATAQUES?

Realizar o procedimento ideal ou construir uma política de segurança infalível se tratando de segurança da informação e quase impossível, em virtude das diversas variáveis que precisam ser analisadas de forma criteriosa, para ser alcançado o que podemos classificar como cenário ideal, que seria através de políticas de boas práticas, conscientização e treinamento com toda equipe incluindo membros do corpo diretor da companhia, pois a maioria das ameaças estão sempre do lado de dentro da rede que acabam se tornando vítimas de ataques oportunistas que ficam hospedados em dispositivos na rede esperando o momento oportuno para entrar em ação classificados como: *fishing* usadas por *crackers* onde usuários são usados como iscas como o obtivo de interceptar mensagens eletrônicas, senhas e informações financeiras, então por esse motivo foi criando essa expressão *fishing* que significa pescar, esses aplicativos se instalam de forma oculta e são facilmente adquiridos através da utilização do uso de *software* crackeado. Os *cracks* exploram falhas de segurança e vulnerabilidades encontradas nos sistemas operacionais.

Portanto a maneira mais pratica, rápida e sem nenhum tipo de prejuízos financeiros sem dúvida e realizar backups regularmente em mídias externas e de forma que fiquem off-line, pois caso a pessoa ou organização seja vítima desse tipo de ataque uma vez que ela possui essa cópia de segurança, não será vítima dos absurdos valores que os *crackers* têm cobrado pelo resgate das informações.

Outro fator de extrema relevância é o uso de software pirata no Brasil, pessoas e organizações fazem uso dessa prática sem conhecimento dos riscos ligados a seu ramo de atividade e muito menos noção das multas que podem sofrer com a adoção dessa prática segundo a ABES (2017), “47% dos programas de computadores no Brasil chamados de software, são piratas” ou seja não se pagou para uso dessas ferramentas ferindo os direitos autorais da empresa desenvolvedora do produto.

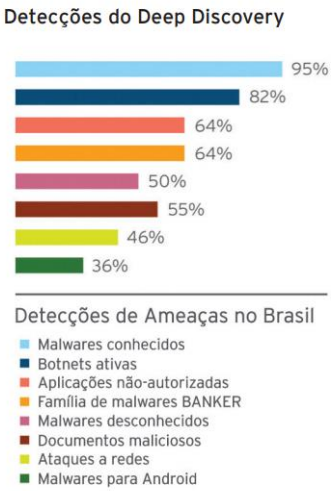
Fatores econômicos também devem ser destacados, pois a grande maioria dos softwares são desenvolvidos fora do Brasil e devido à alta carga tributária dos impostos vinculadas a esse tipo de produto o valor final cotado em dólar, torna-se inacessível para pessoas e organizações, à aquisição e uso de forma licenciada.

[3] ABES – Associação Brasileira das Empresas de Software

3 OS REFLEXOS NEGATIVOS DO BRASIL FRENTE AOS DEMAIS PAÍSES DA AMÉRICA LATINA, NAS RELAÇÕES POLÍTICAS DE SEGURANÇA DIGITAL.

Nos últimos anos o Brasil tem liderado o ranking referente a todas as pesquisas relacionadas à problemas segurança cibernética, de acordo com Trend Micro (2013 pag. 10, 11) “o Brasil envia a maior quantidade de spam da América Latina. Quase dois de cada cinco e-mails maliciosos vêm do Brasil”. Cerca de 36,30% são spam, já 58% são de URLs maliciosas todas hospedadas em provedores e servidores no Brasil seguido por México, Argentina e Colômbia que possuem todas juntas a metade desses números. Segundo Lopes (2016, pag. 109) “o panorama brasileiro aponta para uma ênfase maior nas chamadas novas ameaças à segurança internacional, envoltas em áreas não correlatas a RI. Uma delas é a segurança cibernética”.

Com o objetivo de conscientizar mostrando através de gráficos e dados estatísticos significativos, por exemplo através do *Deep Discovery* essa ferramenta de detecção de ameaças em tempo real, nos mostra que os riscos existem e são uma ameaça presente no cotidiano de pessoas e organizações, mas contundo eles podem ser evitados através de medidas de segurança classificadas como simples ou em alguns casos intermediária com a ajuda de empresas especializadas ou com apoio de profissionais qualificados ou ainda sim, através de pesquisas na internet, em fóruns que tratam o assunto de forma séria e relevante, os usuários facilmente podem obter informações valiosas que ajudaram fazer uso dessas novas ferramentas existentes nesse modelo de negócio chamado de economia moderna na era digital.



Fonte: http://www.trendmicro.com.br/cloud-content/br/pdfs/home/wp-brasil-final.pdf

[4] RI – Relações Internacionais

3.1 AS LEIS BRANDAS E OS IMPACTOS POLÍTICOS ECONÔMICOS NO BRASIL

A falta de comprometimento com relação a política de segurança cibernética no Brasil, compromete todo o sistema sócio econômico com impactos relevantes não apenas na américa latina, mas em todo o mundo. Mesmo sendo um assunto amplamente discutido em todas agendas internacionais, órgãos e entidades do governo não se mobilizam a esta causa com o intuito de garantir reformas nas leis existentes ou mesmo a criação de novas para qualificar e tipificar os incidentes que ocorrem diariamente no país, isso resulta em infratores que se quer, são punidos em consequência do país possuir leis brandas e ineficientes, onde as organizações criminosas contam com o apoio de pessoas que conhecem essas vulnerabilidades e brechas na lei e utilizam esses caminhos para se beneficiar na prática de crimes de segurança cibernética.

Segundo (Gomes, pag. 90) “a formação das organizações internacionais é reflexo da sociedade moderna. Os estados ao perceberem as dificuldades em resolver grandes problemas da humanidade, criaram entidades para que auxiliassem em questões relevantes”. No Brasil isso não ocorre, pois, as entidades citadas anteriormente como a NIC e CERT.br tem um apoio mínimo ou na maioria das vezes nenhum com as preocupações de segurança cibernéticas, essas entidades têm visibilidade no cenário nacional, no entanto outras menores as lideranças políticas e os demais órgãos nem se quer conhecem a existência delas e de seu trabalho.

Hoje no Brasil existem apenas 4 leis que qualificam os crimes cibernéticos no país sendo, Estratégia de Defesa Nacional de 2008, especificamente o decreto 6703. Lei Azeredo (PL 84/99) “Projeto de lei de Crimes Digitais” de 2008. Lei Carolina Dieckmnann (PL 2793/11) e o Marco Civil da Internet de (PL 12.965/14).

Todos os cyber crimes precisam ser qualificados e tipificados dentro das leis citadas acima uma vez que isso não é possível o infrator cracker ou a organização criminosa não responderá por nenhum crime, uma vez que suas ações não puderam ser relacionadas as leis, isso explica o crescimento exponencial dos ataques nos últimos anos o número de novas vítimas cresce mais a cada dia e as entidades políticas e governamentais não se mobilizam afim de se posicionar com ações e atitudes para combater a criminalidade digital e surgimento de novos casos e o crescimento descontrolado dessas ameaças no país e no mundo.

É interessante analisar que todas as leis citadas só foram criadas e ajustadas através de emendas constitucionais sempre de forma corretiva e nunca de forma preventiva, o que reforça ainda mais a ideia que no Brasil sempre precisa ocorrer algum evento de impacto sócio econômico, ou que empresas e organizações sofram consequências severas para que, as lideranças políticas e demais entidades responsáveis comecem a se mexer, por esse motivo temos um estatuto e leis ultrapassadas, que ao longo dos anos sofreram algumas alterações através das emendas constitucionais, afim de minimizar os crimes cibernéticos no país.

3.1.1 Estratégia de Defesa Nacional, especificamente o decreto 6703, com o objetivo de pacificar as relações comerciais e institucionais com os países vizinhos logo no inicio dos primeiros casos de crimes cibernéticos no Brasil, em 18 de dezembro de 2008, o governo aprova a lei com um único objetivo de fortalecer a infraestrutura da rede militar no Brasil, nessa ocasião várias entidades criminosas estavam invadido órgãos e entidades do governo com o objetivo de interceptar informações sigilosas do governo apenas para causar desordem e desequilíbrio nas relações entre os países; esses acontecimentos levou o governo a criar um centro de defesa cibernética para a proteção das redes públicas para proteger as informações administrativas do país.

3.1.2 Lei Azeredo lei 12.735 “Projeto de lei de Crimes Digitais” de 30 de novembro 2012, contava inicialmente com apenas 6 artigos com o objetivo de combater a falsificação e clonagem de documentos, atos de racismo e crimes de menor potencial na internet, uma lei mal elaborada, vaga e contraditória foi vetada em virtude da amplitude do conceito crimes eletrônicos ser extremamente abrangente inviabilizou o uso, e não conseguiu estabelecer normas de proibição e o cumprimento da lei.

3.1.3 Lei Carolina Dieckmnann lei 12.737 de 30 de novembro de 2012, essa lei foi estabelecida com objetivo de criminalizar o usuário que expor de forma não autorizada conteúdo pessoal, intimo de pessoas ou organizações isso ocorreu depois que uma atriz deve suas fotos interceptadas e divulgadas da internet por esse motivo a lei recebeu o nome da atriz.

3.1.4 Marco Civil da Internet lei 12.965 de abril de 2014, essa lei foi estabelecida com o intuito de garantir a disciplina do uso de internet no Brasil, respeitando a liberdade de expressão, direitos humanos, defesa do consumidor, privacidade e demais aspectos preservando a cidadania através dos meios digitais.

4 CONSIDERAÇÕES FINAIS

Ao concluir essa pesquisa tornou-se evidente que enquanto não houver uma reforma criteriosa nas leis de nosso país, relacionado aos crimes cibernéticos cada vez mais, teremos índices mais elevados e em constante crescimento onde o Brasil não deixará de ser o líder do ranking entre todos os países da américa latina, com o maior número de casos registrados de cyber crimes e passando a ser em um futuro não muito distante uma ameaça mundial.

Esse artigo foi elaborado com ênfase na divulgação de resultados de incidentes ocorridos através dos meios digitais com o avanço e a popularização da internet no país. O objetivo de sensibilizar pessoas e organizações que essas ameaças podem sim, ser evitadas desde que todos tenham uma nova postura com responsabilidade social de forma criteriosa, do que pode ser acessado, ter conhecimento sobre os riscos e porque eles existem e que muito pode ser evitado apenas com uma nova conduta sócio cultural, pois a mudança de comportamento é fundamental para que se possa alcançar novos resultados quanto no meio social quanto corporativo.

É de grande importância ressaltar que a aplicação dessas práticas não resolverá todos os problemas que surgirão ao longo do tempo, pois se tratando de tecnologia estamos tratando de algo que se encontra em constante processo de mudança e as práticas adotadas hoje podem não servir no futuro.

A contribuição adquirida através dessa pesquisa de forma geral é que da mesma forma que pessoas e organizações mudam, evoluem e se modificam os crimes eletrônicos também mudaram se modernizando e acompanhando as novas tendências do mundo moderno na era digital.

Olhando para o futuro com uma grande expectativa, espera-se que empresas e organizações cada vez mais continuem investido e melhorando ferramentas de segurança o governo tenha consciência dessas ações reduzindo os impostos e tornando esse produto acessível a todos, para que todos tenham acesso e façam parte do mundo moderno de forma tranquila e segura.

REFERÊNCIAS

ABES - Associação Brasileira de Empresas de Software. **Uso ilegal de software prejudica o Brasil.** Disponível em: http://denunciepirataria.org.br/ Acesso em 22 nov 2017.

BRASIL. **Decreto nº 6.703, de 18 de dezembro de 2008.** Aprova a Estratégia Nacional de Defesa, e dá outras providências. Brasília, 18 dez. 2008.

BRASIL. **Lei nº 12.735, de 30 de novembro de 2012.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências., Brasília, 30 nov. 2012.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012.** dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências. Brasília, 30 nov. 2012.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, Brasília, 23 Abr. 2014.

Cordeiro, Gisele do Rocio. **Orientações e dicas práticas para trabalhos acadêmicos.** Gisele do Rocio Cordeiro, Nilcemara Leal Molinna; Vanda Fattori Dias (org.). 2ª ed. rev. e atual. - Curitiba: InterSaberes, 2014.

Eleuterio, Marco Antônio Masoller. **Sistemas de informações gerenciais na atualidade.** 1ª edição, Curitiba: InterSaberes, 2015.

Gomes, Eduardo Biacchi. **Introdução aos estudos de direito internacional.** Eduardo Biacchi Gomes, Juliana Ferreira Montenegro. Curitiba: InterSaberes, 2016.

Kaspersky Lab. **Brasil é o país que mais sofre com ataques de ransomware na America Latina.** Disponível em: https://www.kaspersky.com.br/blog/brasil-e-pais-que-mais-sofre-com-ataques-de-ransomware-na-al/9626/ Acesso em 15 out. 2017.

Lopes, Gills Vilar. tese de doutorado em **Relações cibernéticas (CiberRI) : uma defesa acadêmica a partir dos estudos de segurança internacional.** / Gills Vilar Lopes. Recife: UFPE, 2016
.
NIC.br. **Revista .br - Marco civil modo de usar.** Disponível em: < http://www.nic.br/publicacao/revista-br-ano-06-2015-edicao-08/>. Acesso em: 28 nov. 2017.

Norton Symantec. **Segurança: quais serão os principais alvos do cyber crime em 2017?** Disponível: https://www.tecmundo.com.br/seguranca-de-dados/112139-seguranca-principais-alvos-cibercrime-ano-2017.htm. Acesso em 22 nov. 2017.

PwC Brasil. **Cyber e privacidade da informação em 10 minutos.** Disponível em: https://www.pwc.com.br/pt/10minutes/assets/2017/10min-cyber-privacidade-informacao-17.pdf. Acesso em 21 nov. 2017.

Trend Micro. **Brasil desafios da segurança cibernética enfrentados por uma economia em rápido crescimento.** Disponível em: http://www.trendmicro.com.br/cloud-content/br/pdfs/home/wp-brasil-final.pdf Acesso em 19 out. 2017.

UBER. **Visão geral.** Disponível em: https://www.uber.com/pt-BR Acesso em 24 nov. 2017.