**OS CRIMES CIBERNÉTICOS NO BRASIL**

**Frank William Miranda de Carvalho[[1]](#footnote-1)**

**Resumo**

Os crimes cibernéticos no Brasil tiveram um aumento exponencial da mesma magnitude que a internet avança no mundo globalizado, os crimes digitais causam grande preocupação, pois são inúmeras pessoas que sofrem com suas conseqüências. Os crimes digitais podem ser praticados através de um computador ou até mesmo uma rede interligada a uma corporação e graças os novos meios de comunicação expõem ainda mais a fragilidade que os usuários possuem em relação à segurança na internet. Sabendo que os danos causados pelos crimes digitais somam enorme prejuízo psicológico, psicossocial ou financeiramente, temos como missão a de analisar, alertar e divulgar as pessoas sobre os perigos que infestam as mídias sociais, nos diversos meios de comunicação que existem no mercado atual. Destacaremos como as boas práticas de navegação e as seguranças em atos simples podem auxiliar nesta corrente contra os cybers criminoso. Citaremos os pontos vulneráveis e conseqüentemente como transformar em ações corretivas e preventivas para não se tornar mais uma vítima dos crimes digitais como também abordará a legislação que trata especificamente dos crimes digitais.

**Palavras-Chaves:** Crimes Digitais. Segurança na Internet. Comunicação.

**CYBER CRIMES IN BRAZIL**

**Abstract**

Cybercrime in Brazil had an exponential increase of the same magnitude as the internet advances in the globalized world; cybercrime causes great concern because there are numerous cases of people suffering from its consequences. A computer can commit digital crime or even a corporation to an interconnected network and through new media expose further weaknesses that users have regarding Internet safety. Knowing that the damage caused by cybercrime add huge psychological, psychosocial or financial loss we have the mission to analyze, and disseminate warn people about the dangers that plague social media in various media that exist in the current market. We will highlight how good browsing practices and security guards in simple acts can help this current against the criminal cyber. We will quote the vulnerable points and consequently how to turn on corrective and preventive actions to avoid becoming a victim of cybercrime as well as discuss the legislation that deals specifically with digital crimes.

**Keywords:** Digital Crimes. Internet Safety. Communication.

**INTRODUÇÃO**

O trabalho procurou abordar um assunto muito importante nos tempos atuais, os perigos dos crimes digitais e as conseqüências que eles trazem para toda a sociedade trouxeram a tona para amplo debate para, os internautas, com intuito de ampliar a discussão de como o assunto é tratado, discutido, mas principalmente como devemos agir quando acessamos as mídias sociais e internet.

A fragilidade que é depositada nas redes sociais, em páginas de relacionamento, faz com que a engenharia social predomine no mundo digital. Tornando essas informações sugestivas a captura, não autorizada do proprietário. Ou mais simples ainda, os comentários ofensivos que muitos relatam sofrerem publicamente nas suas referidas páginas de contato pessoal.

O mal cuidado de como essas informações é disponibilizada para todos que acessam a mesma mídia social, torna vulnerável as informações para terceiros, com intuito de cometer crimes das mais diferenças esferas.

Seu processo de informação deve ser acentuado e de maneira cautelosa e ordenada. Desta maneira tornasse quase nula as brechas que podem ser usadas contra você pelos crimes digitais, são claramente pequenas atitudes que devemos tornar hábito e que nos trás uma segurança. O resultado das medidas de segurança, é que você não se torna mais uma vítima dos crimes digitais.

Devido ao aumento de relatos e denúncias de pessoas que tem sofrido com ataques de crimes digitais tem preocupado e muito a sociedade e as autoridades. A velocidade que as pessoas tem tido o acesso a informação e aos meios de telecomunicações, e a mesma velocidade que usuários vêm sofrendo com os cyber criminosos e com seus ataques.

Através da metodologia de estudo de caso e também de pesquisas bibliográficas sobre especialistas na área de segurança digital e autores da área do direito, abordaremos como devemos reagir a essa prática que tem atormentado a vida de empresas e usuários domésticos.

Usaremos como instrumento de coleta de dados, a forma estrutural e análise de conteúdo documental. Desta maneira iremos enriquecer o conteúdo abordado e proporcionaremos uma melhor orientação sobre a pesquisa proposta.

**CENÁRIO ATUAL**

Os crimes digitais têm recebido uma atenção redobrada nos últimos tempos, devido ao aumento constante dos números de vítimas. As pessoas nunca tiveram tão conectadas como estão nos dias de hoje, segundo o Ibope Nielsen[[2]](#footnote-2), o acesso à internet no Brasil em 2012, chegou a incríveis 83,4 Milhões de pessoas.

Segundo os dados do Facebook[[3]](#footnote-3), os números de usuários que acessam a rede social por dia, chegam a 1,19 bilhões.

Netview do Ibope Media[[4]](#footnote-4), nos relata que em Janeiro de 2013 o número de usuários ativos em ao menos uma rede social no Brasil, era mais de 46 Milhões.

O aumento do fluxo de informação disponível, transmitido e partilhado entre usuários, na rede mundial de computadores comprova essa realidade. Consequentemente nos mostra a importância e necessidade de termos cuidado com nossa vida pessoal no meio eletrônico. Por isso devemos nos atender a boas práticas que possam nos garantir uma segurança real na navegação pela internet. Essa fragilidade não é somente dos usuários domésticos. O portal da Ig, brasil econômico[[5]](#footnote-5), nos mostra um dado bastante alarmante, somente no Brasil em 2012 8% das empresas sofreram percas superiores a US$ 5 Milhões, e 5% registraram prejuízo entre 100 milhões à US$ 1 Bilhão de dólares com crimes digitais.

Através destes dados podemos entender que todos os usuários, independentemente de serem domésticos ou empresas, sofre com os crimes digitais em nosso país.

Segundo, AVRUCH. Márcia; um terço das empresas Brasileira foram vítimas de crime digital no último ano, os dados da PWC[[6]](#footnote-6) nos mostram que com exceção dos roubo ativo, os crimes digitais foram responsáveis por 32% de percas em 2011 e é a segunda maior perca entre os empresários.

Devemos nos preocupar em desenvolver uma boa prática de navegação em ambientes digitais, somente com nossa segurança reborada, podemos evitar que os crimes cibernéticos ocorram, e que nos tornemos índice de pesquisa.

Cada vez maior é a preocupação das organizações em disponibilizar na sua estrutura organizacional uma boa gestão de segurança, assegurando a seus clientes e colaboradores uma segurança confiável, quando utilizarem sua rede corporativa ou acesso ao portal na internet.

Devemos investir nas mesmas proporções de ataques, a busca de uma segurança realmente eficaz que proporcione uma tranquilidade aos clientes e usuários domésticos.

O conceito de crimes digitais podem ser descritos, como a prática de crimes que são produzidos ou intermediados pelo auxílio do computador ou conjuntos de computadores. Mas esse conceito não se restringe somente a computadores. Agora com a inserção no mercado de mídias portátil expande esse universo aos smartphones e aos tabletes.

Segundo dados da Mcaffe[[7]](#footnote-7), o Brasil está entre os 5 países que mais sofrem com ataques cibernético no mundo, através deste dado devemos explorar as boas práticas e aumentar a prevenção, para que dificulte a execução dessas ilicitudes.

Os crimes digitais ocorrem quando qualquer mídia digital, cause danos materiais, psicológicos ou afere a moral, reputação, ou que traga prejuízos financeiros, através da internet, por intermédio de ataques digitais.

Nos últimos anos estamos sofrendo com o aumento descontrolado dos crimes que usam as novas mídias de comunicação. Em maio de 2013, a Norton Security [[8]](#footnote-8)divulgou os dados das mídias que mais sofreram com os crimes digitais, ou seja:

Gráfico 1 Ataques Digitais e os tipos de mídias

Fonte (Norton Security – 2013)

Através destes dados podemos destacar a importância real do presente artigo, para alertar e também orientar os usuários para as boas práticas e os cuidados necessários ao acessar contas bancárias, redes sociais, e-mails; devemos tornar real a navegação consciente e segura.

As etapas que foram seguidas para a elaboração do mesmo foi de pesquisa e contextualização das informações adquiridas através de autores que tratam do referido tema, também foram efetuadas pesquisa de campo com os usuários que tiveram suas vidas expostas e prejudicadas pelos crimes; também foi analisado o contexto histórico, e informações fornecidas por especialistas da área de segurança digital. A pesquisa foi fundamentada com referências bibliográfica, mas principalmente com os estudos de casos e relatos de usuários, que tiveram prejuízos devido aos crimes digitais. Como a análise na legislação que trata do referido assunto.

**CRIMES DIGITAIS NO BRASIL**

A abrangência dos crimes digitais é mais complexa e ampla do que podemos imaginar. Esse tema não abrange apenas as: fraudes bancárias; criação e propagação de vírus; spam ou pedofilia. Atitudes aparentemente ‘inocentes’ são classificadas como crime digital, Podemos destacar tais comportamentos como:

1. - Comentários maldosos em redes sociais;
2. - Envios de e-mails com informação fictícias sobre pessoas física ou jurídicas que ofendam a imagem;
3. - Inverdades de correntes, reunir maior números de pessoas para ajudar financeiramente supostas vítimas de tragédia naturais ou por enfermidades;
4. - Espalhar boatos ou colocar pessoas em situações vexatórias;

Segundo dados do IPDI (instituto de Peritos em Tecnologias Digitais e telecomunicação)[[9]](#footnote-9) destacaremos os principais tipos de ataques de crimes digitais que ocorrem em nosso país.

1. Roubo de identidade: Os criminosos enganam suas vítimas e se apropriam indevidamente de seus dados pessoais e informações bancárias para realizar compras online, transferências financeiras.
2. Pedofilia: Propagação de abuso sexual infantil.
3. Calúnia e Difamação: Divulgar espalhar informações irreais que prejudicam a reputação das vítimas, crimes frequentes em redes sociais.
4. Ameaça: Afirmar que a pessoa será vítima de alguma mal.
5. Discriminação: Divulgação de atos que sinalizam preconceitos de raça, cor, gênero, etnia, sexo, religião. Tornou comum com a popularização de redes sociais.
6. Espionagem Industrial: Transferência de arquivos sigilosos sem a devida autorização do responsável para fins desconhecidos.

PRINCIPAIS DELITOS COMETIDOS ATRAVÉS DA INTERNET.

Crimes digitais:

TABELA 1 – Os crimes mais comuns e suas

|  |
| --- |
| Delitos mais comuns |
|  |  | **Artigo** | **Pena** |
| Falar em um chat que alguém cometeu um crime (ex. - ele é um ladrão...) | Calúnia | 138 do C.P. | Detenção de 6 meses a 2 anos e multa |
| Encaminhar um e-mail para várias pessoas de um boato eletrônico | Difamação | 139 do C.P. | Detenção de 3 meses a 1 ano e multa |
| Enviar e-mail para a pessoa dizendo sobre características dela (ex. - gorda, feia, vaca...) | Injúria | 140 do C.P. | Detenção de 1 ano a 6 meses ou multa |
| Enviar um e-mail dizendo que "vai pegar" a pessoa | Ameaça | 147 do C.P. | Detenção de 1 ano a 6 meses ou multa |
| Enviar um e-mail para terceiros com informação considerada confidencial | Divulgação de segredo | 153 do C.P. | Detenção de 1 a 6 meses ou multa |
| Enviar um vírus que destrua equipamento ou conteúdos | Dano | 163 do C.P. | Detenção de 1 a 6 meses ou multa |

|  |  |  |  |
| --- | --- | --- | --- |
| Copiar conteúdo e não mencionar a fonte, baixar MP3 | Violação ao direito autoral | 184 do C.P. | Detenção de 3 meses a 1 ano ou multa |
| Criar comunidade online que fale sobre pessoas e religiões | Escárnio | 208 do C.P. | Detenção de 1 mês a 1 ano ou multa |
| Acessar sites pornográficos | Favorecimento da prostituição | 228 do C.P. | Reclusão de 2 a 5 anos |
| Criar uma comunidade para ensinar como fazer "um gato" | Apologia ao crime ou criminoso | 287 do C.P. | Detenção de 3 a 6 meses ou multa |
| Enviar e-mail com remetente falso (caso comum de spam) | Falsa identidade | 307 do C.P. | Detenção de 3 meses a 1 ano, ou multa, se o fato não constitui elemento de crime mais grave |
| Inserir dados falsos em sistema da administração pública | Adulterar dados em sistema | 313-A do C.P. | Reclusão de 2 a 12 anos e multa |
| Entrar na rede administração pública e mudar informações (mesmo que com uso de um software) | Adulterar dados em sistema de informações | 313-B do C.P. | Detenção de 3 meses a 2 anos e multa |
| Receber spam e devolver com vírus ou com mais spam | Exercício arbitrário das próprias razões | 345 do C.P. | Detenção de 15 dias a 1 mês ou multa, além da pena correspondente à violência |
| Participar de cassino online | Jogo de azar | 50 da L.C.P. | Prisão simples, de 3 meses a 1 ano e multa, estendendo-se os efeitos da condenação à perda dos móveis e objetos de decoração do local |
| Falar mal de alguém em um chat por sua cor | Preconceito ou Discriminação Raça-Cor-Etnia | 20 da Lei 7.716/89 | Reclusão de 1 a 3 anos e multa |
| Ver ou enviar fotos de crianças nuas online | Pedofilia | 247 da Lei 8.069/90 | Multa de 3 a 20 salários de referência, aplicando-se o dobro em caso de reincidência |
| Usar logomarca de empresa em um link na página da internet, em uma comunidade, em um material, sem autorização do titular, no todo ou em parte | Crime contra a propriedade industrial | 195 da Lei 9.279/96 | Detenção de 3 meses a 1 ano ou multa |
| Empregar meio fraudulento para desviar clientela de outrem (Exemplo: uso da marca do concorrente como palavra-chave ou link patrocinado em buscador) | Crime de concorrência desleal | 95 da Lei 9.279/96 | Detenção de 3 meses a 1 ano ou multa |
| Usar cópia de software sem ter a licença para tanto | Crimes contra software, "pirataria" | 12 da Lei 9.609/98 | Detenção de 6 meses a 2 anos ou multa |

Fonte: <http://ww1.tavarespericias.com/index.php?option=com_content&view=article&id=52&Itemid=75>[[10]](#footnote-10).)

**AÇÕES CONTRA OS CRIMES DIGITAIS**

Para penalizar ainda mais e transformar os crimes digitais, em 2012 foi criada a Lei Brasileira 12.737/12[[11]](#footnote-11), que trata especificamente dos crimes digitais[[12]](#footnote-12)\* crimes informáticos[[13]](#footnote-13)\*, cyber crimes[[14]](#footnote-14)\*.

Esta lei especificamente acrescentou no código Penal Brasileiro, Decreto-Lei Nº2.848/1940[[15]](#footnote-15), os Artigos 154A – 154B.

Artigo 154A – Invadir, dispositivo Informático Alheio, conectado ou não à rede de computadores diante a violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagens ilícitas: (Lei 12.737/2012. Artigo 154ª).

TABELA 2 Penalidades infringentes do Artigo 154 A – Lei Brasileira Nº 12.737/12

|  |  |  |
| --- | --- | --- |
| **Ação** | **Pena** | **Artigo 154-A** |
|  Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no **caput** | Detenção 3 Meses à 1 ano e Multa | § 1o |
|  Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.  | Detenção 3 Meses à 1 ano e Multa | § 2o |
| Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido. | Reclusão, de 6 meses a 2 anos, e multa, se a conduta não constitui crime mais grave. | § 3.o |
|  Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos. | Reclusão, de 6 meses a 2 anos, e multa, se a conduta não constitui crime mais grave. | § 4o |
| Aumenta-se a pena de um terço à metade se o crime for praticado contra:  I - Presidente da República, governadores e prefeitos;  II - Presidente do Supremo Tribunal Federal;  III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou  IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal | Reclusão, de 6 meses a 2 anos, e multa, se a conduta não constitui crime mais grave. | § 5o |

Fonte: Lei Nº 12.737/2012

Artigo 154B – Nos crimes definidos no artigo 154-A, somente se proceder mediante representação salvo se o crime é cometido contra administração pública direta ou indireta de qualquer dos poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos. (Lei 12.737/2012. Artigo 154B).

Artigo 3o, os artigos 266 e 298 do Decreto-Lei no 2.848[[16]](#footnote-16), de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação:

**“Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública**

[Artigo. 266.](http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm#art266)

[§ 1º](http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm#art266§1) Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

§ 2o Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.” (NR)

**“Falsificação de documento particular**

[Artigo. 298.](http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm#art298)

**Falsificação de cartão**

Parágrafo único.  Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.” (NR)

Podemos observar que as penalidades a quem afere algum destes crimes é exemplar. Essa modificação na estrutura na execução das penas foi importantíssima para assegurar a todos cidadãos a certeza de que, quem comete algum crime cibernético não ficará impune, pois seu causador sofrerá as punições legais.

**EVITANDO SER VÍTIMA DOS CRIMES DIGITAIS**

Todo usuário deseja navegar tranquilamente e ter seus arquivos longe do alcance de terceiros, principalmente assegurado que seu perfil em rede social não seja atacado por algum meliante.

O aumento dos ataques de crimes digitais é assustador, devemos orientar os usuários, que o bom senso e a prevenção são as melhores armas contra os crimes de informática. Vamos aqui destacar algumas das técnicas que devemos tomar para dessa maneira evitarmos ser mais uma vítima na estatística Brasileira.

Sabendo que os crimes digitais não estão mais presos apenas a ataques de cyber- criminosos[[17]](#footnote-17) aos computadores e as redes domesticas, os crimes digitais ganharam novas versões, como ataques a smartphones e aos tabletes, além de clonagem de cartões magnéticos.

1. Senhas Pessoas: Evite usar nome de familiares, datas comemorativas, placas de carro, endereços ou algo que está próximo de vocês, preferencialmente use uma junção de caracteres especiais, letras maiúsculas e minúsculas alfa numéricos.
2. Nunca acesse contas bancárias ou faça transação eletrônica como compra on-line em redes abertas e principalmente em computadores desconhecidos, geralmente redes abertas como cidade digital e cyber café, pois as informações trafegam indefinidamente, muitas vezes sem criptografia, deixando os seus dados expostos a quem conseguir capturar e utilizar sem o seu conhecimento ou autorização.
3. Realize com frequência a manutenção de senhas de acesso pessoal á contas bancárias, e-mails, e nunca use a mesma senha para mais de uma conta.
4. Realize compras eletrônicas em sites de confiança e que tenha a credibilidade comprovada, evite realizar compras em sites desconhecidos e nunca, identifique seus dados bancários.
5. Jamais abra arquivos de anexos via e-mails de desconhecidos.
6. Cuidado com a utilização de e-mails corporativos, muitas vezes o e-mail é monitorado pelo empregado ou especificamente pelo administrador da conta.
7. Empregador, você é responsável pelos danos causados a terceiros por seu empregado no exercício da sua função, inclusive via web.
8. Utilize softwares originais, seja gratuito ou pago, evite utilizar softwares pirata, muitas vezes dentro do programa instalado contém arquivos de captura de imagem, de digitação e registro infiltrados de maneira oculta.
9. Mantenha seu programa de Antiviris e AntiSpam sempre atualizados.
10. Não seja um “clicador” compulsivo, navegue na internet de maneira consciente e com cuidado redobrado.
11. Pense muito bem antes de clicar em links contidos em e-mails, redes sociais, e fóruns na internet. Evite sempre!
12. Nunca forneça suas senhas de acesso a redes sociais, bancárias, e-mails etc.
13. Fique Atento aos endereços de web que você navegue.
14. Nunca participe de sorteios fáceis dando a você a chance de sua vida, acredite nada cai do céu, isso é um golpe, que espera algum usuário descuidado acessar essas informações.
15. Resista a ofertas tentadoras, não há milagres, duvide de compras coletivas ou em sites, dando um produto ou serviço muito em conta.
16. Siga sempre as sugestões do internet banking ao realizar transações eletrônicas.
17. Proteja sua rede sem fio, utilize e mescle sempre sua senha usando caracteres alfa numéricos e periodicamente altere sua senha.
18. Evite pastas compartilhadas com arquivos muito sigilosos.
19. Realize backup com frequência, armazenando seus dados em discos ópticos.
20. Preferencialmente tenha um técnico de informática quando precisar de sua extrema confiança.
21. Evite empresas terceirizadas para realizar manutenção em seu equipamento de informática.
22. Preferencialmente tenha uma pasta contendo arquivos pessoais com chave e criptografia.
23. Guarde para si as informações pessoais.
24. Evite utilizar caixas eletrônicos em locais desconhecidos ou suspeitos, pois a grande chance de haver alguma ameaça que possa clonar seus dados é maior.
25. Mantenha software de Localização Global em seu aparelho de dispositivo móvel, como também senhas de acesso ao seu smartphone ou tablete.
26. Evite acessar redes abertas via dispositivos móveis e realizar transações eletrônicas.
27. Preferencialmente utilize sua Rede 3G.
28. Acesse a redes apenas de sua confiança, mas evite sempre trafegar informações de alto sigilo.

**CONSIDERAÇÕES FINAIS**

Por se tratar de um tema ainda pouco explorado, utilizamos pesquisa bibliográficas e também estudos de especialistas na área de segurança digital, mas principalmente experiências de quem já foi alvo dos crimes digitais. Ao transcorrer da pesquisa analisamos passo a passo o que são crimes digitais, as esferas onde ocorrem suas ações. Podemos observar que durante muitos anos não havia uma legislação específica para se tratar do assunto em nosso país, e apenas no ano passado houve uma alteração no código Penal Brasileiro. Fica claro que a melhor arma contra os crimes digitais é a prudência e a precaução, pois se o usuário tiver em sua rotina algumas boas políticas e cuidados, certamente o risco de se tornar vítima dos cyber criminosos é reduzida.

O resultado das pesquisas é extremamente válido, pois trouxemos a público, algumas boas ações que devemos implementar em nossa rotina, nas situações mais adversas possíveis, a navegação consciente e responsável, deve ser repassada de pai para filho, de colega para colega. Devemos refletir nos resultados expostos até aqui, o dever dos usuários é ter a sabedoria que a boa segurança parte de todos que trocam informações eletrônicas. Lembrar que sempre a cautela é a melhor ação contra as falhas e armadilhas que a internet tem, só desta maneira iremos combater efetivamente o mal pela raiz e definitivamente tornar nula as ações de crimes digitais.

**REFERÊNCIAS**

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 6022. **Informação e documentação – Artigo em publicação periódica científica impressa -apresentação**. Rio de Janeiro: ABNT, 2003. 5p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 6023. **Informação e documentação - referências - elaboração**. Rio de Janeiro: ABNT, 2002. 24p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 10520. **Informação e documentação - citações em documentos - apresentação**. Rio de Janeiro: ABNT, 2002. 7p.

CANONGIA, Cláudia; MANDARINO, J. Raphael: **Livro Verde Segurança Digital no Brasil**. Brasília, 2010.

CRIMES DIGITAIS. **Ataques de crimes digitais mais comuns.** Disponível em<http://www1.folha.uol.com.br/folha/informatica/ult124u19455.shtml>. Acesso em 26 de novembro de 2013.

CRIMES DIGITAIS. **Aumenta o número de empresas que sofrem com ataques de crimes digitais no Brasil**. Disponível em < http://www.brasileconomico.ig.com.br/noticias/aumenta-numero-de-empresas-que-sofrem-ataques-virtuais\_113477.html>. Acesso em 25 de novembro de 2013.

CRIMES DIGITAIS. **Brasil vira centro de crimes digitais.** Disponível em <http://amaivos.uol.com.br/amaivos09/noticia/noticia.asp?cod\_noticia=3405&cod\_canal=37>. Acesso em 26 de novembro de 2013.

CRIMES DIGITAIS. **Crimes mais comuns de ataques digitais aplicação da legislação – jurisdição aplicável nos casos de crimes digitais**. Disponível em<http:// http://ww1.tavarespericias.com/index.php?option=com\_content&view=article&id=52&Itemid=75/>. Acesso em 26 de novembro 2013.

FACEBOOK. **Número de usuários que acessam a rede social.** Disponível em <http://br.noticias.yahoo.com/facebook-possui-1-19-bilh%C3%A3o-usu%C3%A1rios-ativos-ao-141422715.html>. Acesso em 25 de novembro de 2013.

IBOPE. **Número de usuários de redes sociais no brasil.** Disponível em <http://www.ibope.com.br/pt-br/noticias/Paginas/Numero-de-usuarios-de-redes-sociais-ultrapassa-46-milhoes-de-brasileiros.aspx >. Acesso em 25 de novembro de 2013.

1. Pós Graduando. Uniasselvi. frankmirandacarvalho@gmail.com [↑](#footnote-ref-1)
2. Ibope Nielsen. Pesquisa divulgada de acesso à internet em 2012. [↑](#footnote-ref-2)
3. Facebook. Acesso a rede social. [↑](#footnote-ref-3)
4. Netview do Ibope Brasil, revelou que 46 milhões de pessoas que navegam a internet tem alguma mídia ou participa de alguma rede social. [↑](#footnote-ref-4)
5. Brasil Econômico Ig. Portal de notícias relatam os prejuízos aferidos das empresas Brasileiras em 2012 que sofreram percas devidos aos crimes digitais. [↑](#footnote-ref-5)
6. PWC. Relatório sobre o número de empresas que tiveram percas em 2011. [↑](#footnote-ref-6)
7. McAffe. Dados representativos de crimes digitais no Brasil. [↑](#footnote-ref-7)
8. Norton Security. Dados sobre as mídias que sofreram com os crimes Cibernéticos em 2012. [↑](#footnote-ref-8)
9. IPDI. Instituto de Peritos em Tecnologias Digitais e Telecomunicações, principais ataques digitais que ocorrem no Brasil. [↑](#footnote-ref-9)
10. TRAVARES PERÍCIAS. Ações em 2011 que mais houve representação jurídica contra os crimes digitais no Brasil. [↑](#footnote-ref-10)
11. Lei Brasileira Nº 12.737/12. Lei de Alteração do Código Penal, acrescentando artigos específicos para punições dos crimes digitais. [↑](#footnote-ref-11)
12. CRIMES DIGITAIS. Nomenclatura para especificar os crimes efetuados pelos dispositivos que acessam a internet. [↑](#footnote-ref-12)
13. CRIMES INFORMÁTICOS. Nomenclatura para especificar os crimes efetuados pelos dispositivos que acessam a internet. [↑](#footnote-ref-13)
14. CYBER-CRIMES. Nomenclatura para especificar os crimes efetuados pelos dispositivos que acessam a internet. [↑](#footnote-ref-14)
15. LEI Nº 2.848/1940. Código Penal Brasileiro. Artigos Nº 154A e 154B [↑](#footnote-ref-15)
16. DECRETI-LEI Nº 2848/40. Código Penal Brasileiro, Artigos 266 e 268 [↑](#footnote-ref-16)
17. CYBER CRIMINOSO. Nome para identificar os criminosos que se utilizam de meios digitais para a prática de crimes contra o governo, população, empresa pública ou privada. [↑](#footnote-ref-17)