ARTIGO ORIGINAL

SILVA, Ricardo Leopoldo da ^[1], VIEIRA, Anderson ^[2]

SILVA, Ricardo Leopoldo da. VIEIRA, Anderson. Segurança Cibernética: O Cenário Dos Crimes Virtuais No Brasil. Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano 06, Ed. 04, Vol. 07, pp. 134-149. Abril de 2021. ISSN: 2448-0959, Link de acesso: <https://www.nucleodoconhecimento.com.br/ciencia-da-computacao/crimes-virtuais>, DOI: 10.32749/nucleodoconhecimento.com.br/ciencia-da-computacao/crimes-virtuais

Contents

- RESUMO
- 1. INTRODUÇÃO
- 2. ESTABELECENDO CONCEITOS
- 3. O IMPACTO DOS CRIMES ONLINE
- 4. ASPECTO JURÍDICO
- 5. ATAQUES CIBERNÉTICOS NO BRASIL
- 5.1 PHISHING
- 5.2 RANSOMWARE
- 5.2.1 TIPOS DE RANSOMWARE
- 5.2.2 FORMAS DE INFECÇÃO
- 6. CRIMES PRATICADOS NAS REDES SOCIAIS
- 7. CONCLUSÃO
- REFERÊNCIAS

RESUMO

O presente artigo tem por finalidade introduzir o tema da segurança cibernética direcionado aos crimes virtuais de maior ocorrência no cenário brasileiro em decorrência da evolução e do aumento significativo da utilização de tecnologias da informação e comunicação – as chamadas TICs. No momento atual, são marcantes a presença e a utilização de tais tecnologias, onde é possível observar do acesso à conta de e-mail à realização de transações

financeiras, além de múltiplas aplicações, serviços e negócios. Em consequência desse total envolvimento e, por conseguinte, da dependência das TICs, pessoas mal-intencionadas motivam-se ao desenvolvimento de ferramentas para exploração de vulnerabilidades, como também se beneficiam da imperícia, desatenção e inocência dos usuários, a fim de atingirem seus objetivos – seja a disseminação de infecções em dispositivos informáticos ou a obtenção de informações alheias nos âmbitos pessoal e financeiro. Por intermédio de uma comparação global, a pesquisa destaca os principais crimes virtuais de maior ocorrência no Brasil. Igualmente, mediante análise realizada em relatórios e *security reports* – disponibilizados na internet –, foi possível identificar as tecnologias de maior exploração, o comportamento e o modo como os ataques foram realizados. Ademais, este artigo expõe alguns conceitos referentes à segurança cibernética, apresentando diferentes definições, como a da Associação de Controle e Auditoria de Sistemas de Informação – organização global de profissionais de governança de TI, controle, segurança e auditoria – e, também, de empresas voltadas à segurança da informação, tais como a *Norton by Symantec* e a *Kaspersky Lab*. Da mesma forma, esclarece o aspecto jurídico em relação aos crimes virtuais, salientando a evolução da legislação brasileira para se adequar ao cenário atual, e, assim, aplicar de maneira correta as penalidades aos crimes informáticos. De modo final, explicita que somente investimentos em tecnologia e infraestrutura não são suficientes para a redução dos crimes virtuais; ressalta, conseqüentemente, que são necessários investimentos em educação e conscientização dos usuários para o melhor aproveitamento dos recursos tecnológicos disponíveis.

Palavras-chave: Cibercrime, Cibersegurança, *Phishing*.

1. INTRODUÇÃO

A evolução das tecnologias da informação e comunicação, que alcançou a sociedade moderna, é sem dúvida perceptível em diversas áreas, como: o comércio eletrônico, a educação à distância, a telemedicina, as redes sociais, o desenvolvimento científico-tecnológico, o desenvolvimento econômico, dentre outros.

Em consequência do massivo envolvimento e da forte dependência das ditas TICs, pessoas mal-intencionadas motivam-se ao desenvolvimento de ferramentas para exploração de

vulnerabilidades, como: *malware*, *ransomware*, *spyware*, entre outros. De mesmo modo, tais pessoas se beneficiam da imperícia, desatenção e inocência dos usuários, a fim de atingirem seus objetivos – seja a disseminação de infecções em dispositivos informáticos ou a obtenção de informações alheias nos âmbitos pessoal e financeiro.

O desenvolvimento da tecnologia da informação é muito ágil, e a problemática referente à privacidade e à proteção dos dados na internet permanece viva.

Segundo Canongia e Júnior (2009):

E marcante a presença da alta tecnologia atrelada a constantes inovações com o domínio das empresas de países desenvolvidos. Esta convergência tecnológica vem nos bombardeando com novidades inimagináveis, como, por exemplo, o acesso à internet pelo celular, permitindo o envio de e-mails, a realização de transações financeiras, além de múltiplas aplicações, serviços e negócios que as TICs vêm proporcionando, e que são crescentes mundialmente.

Nesse ponto, convém considerar o aspecto negativo desse crescimento tecnológico, uma vez que tais avanços permitem que ataques cibernéticos se caracterizem como um grande desafio a ser superado. Dessa forma, é essencial assegurar a confidencialidade, integridade, disponibilidade e autenticidade da informação para a elaboração de estratégias e, de mesmo modo, para o processo decisório.

O grande desafio é equilibrar as duas dimensões: a primeira diz respeito à cultura do compartilhamento, da socialização e da criação de conteúdo; já a segunda refere-se às questões de proteção, segurança, confidencialidade e privacidade.

2. ESTABELECENDO CONCEITOS

Os conceitos de segurança cibernética vêm sendo construídos com a presença de diferentes e importantes agentes. Entende-se que o escopo de atuação da segurança cibernética compreende aspectos e atitudes tanto de prevenção quanto de repressão.

Para a Associação de Controle e Auditoria de Sistemas de Informação (ISACA, 2013), o termo

cibernético no contexto da segurança da informação necessita de uma explicação, pois é comumente confundido e utilizado de forma muito abrangente. A instituição define que segurança cibernética engloba tudo o que protege organizações e indivíduos de ataques intencionais, falhas e incidentes, assim como suas consequências. A maior parte dos ataques oportunistas e crimes geralmente podem ser evitados utilizando ferramentas e estratégias simples, mas eficazes.

Segundo Wamala (2011), também é importante contrastar os termos segurança da informação e segurança cibernética, uma vez que os entendimentos dos mesmos podem levar a um falso sentimento de segurança ou a uma confusão no que tange os riscos cibernéticos. Para ele,

Os dois conceitos visam a atender e manter as propriedades de segurança de confidencialidade, integridade e disponibilidade. Porém, o alcance global da internet dá à segurança cibernética um caráter especial. Enquanto o conceito de segurança da informação iniciou-se quando a maioria dos sistemas atuava de maneira isolada e raramente em jurisdições transversas, a segurança cibernética trabalha com ameaças globais sob a incerteza legal.

E, citando Sinks (2012), adiciona: a segurança cibernética tem de rivalizar com uma arquitetura de internet que torna virtualmente impossível de atribuir um ataque a um ator.

Em uma visão similar, Somls e Niekerk (2013) propõem que as fronteiras da segurança cibernética como um conceito são mais amplas do que aquelas da segurança da informação no que tange a sua definição formal. Segundo eles:

A segurança da informação é a proteção da informação, que é um ativo, contra possíveis danos resultantes de diversas ameaças e vulnerabilidades. Segurança cibernética, por outro lado, não é necessariamente apenas a proteção do ciberespaço por si só, mas também a proteção daqueles que trabalham no ciberespaço e qualquer um de seus ativos que podem ser alcançados através do ciberespaço.

Para Brookson et al (2015):

A segurança cibernética deve referir-se à segurança do ciberespaço, em que ciberespaço se refere ao conjunto de conexões e relacionamentos entre objetos que são passíveis de acesso através de uma rede de telecomunicações generalizada; e, ao conjunto de objetos por si só onde os mesmos apresentem interfaces permitindo seu controle remoto, acesso remoto a dados ou suas participações em ações de controle dentro deste ciberespaço.

O tratado do conselho europeu sobre crime cibernético usa o termo “*cibercrime*” para definir delitos que vão desde atividades criminosas contra dados até infrações de conteúdo e de copyright (KRONE, 2005). No entanto, outros autores sugerem que a definição é mais ampla e que inclui atividades como: a fraude, o acesso não autorizado, a pornografia infantil e o *cyberstalking* (ZEVIAR-GEESE, 1997, p. 98). O manual de prevenção e controle de crimes informáticos da Organização das Nações Unidas inclui: a fraude, a falsificação e o acesso não autorizado em sua definição de cibercrime (ONU, 1995).

A *Symantec* – empresa fundada em 1982, por *Gary Hendrix*, com atividades em segurança da internet e em redes para usuários domésticos e corporações – define cibercrime como qualquer delito em que tenha sido utilizado algum dispositivo informático. O computador ou dispositivo podem ser os agentes, os facilitadores ou as vítimas do crime. Para melhor compreensão de sua definição, os crimes estão agrupados em duas categorias.

Categoria 1:

Do ponto de vista da vítima, trata-se de um evento que acontece normalmente apenas uma vez. Por exemplo: a vítima realiza o download – sem o seu conhecimento – de um “Cavalo de Troia”, e este instala um programa de registro de digitação (*keylogger*) no computador. Também é possível que a vítima receba um e-mail contendo um link para acesso à página de uma entidade conhecida, mas, na realidade, este link pertence a um site malicioso.

Em muitos casos, falhas ou vulnerabilidades no software fornecem um ponto de apoio ao criminoso. Por exemplo: ao obter o controle de um web site, é possível utilizar a vulnerabilidade do navegador de internet (*browser*) para introduzir um programa com código malicioso (*malware*) no computador da vítima.

Exemplos de crimes cibernéticos da categoria 1 incluem: o *phishing*, o roubo ou a manipulação de dados, o roubo de identidade e a fraude no setor bancário ou de comércio eletrônico.

Categoria 2:

Os crimes cibernéticos desta categoria também incluem – mas não se limitam a elas – atividades como: o assédio, a violência contra crianças, a extorsão, a chantagem, a manipulação do mercado de valores, a espionagem empresarial ou a execução de atividades terroristas na internet.

Trata-se, normalmente, de uma série contínua de eventos envolvendo interações repetidas com a vítima. Por exemplo: o criminoso entra em contato com a vítima por meio de um site de relacionamentos, para estabelecer uma relação ao longo do tempo, com o objetivo de conquistar a confiança da vítima e, assim, aproveita desta relação para praticar o crime. Outro exemplo: membros de uma célula terrorista ou organização criminosa utilizam mensagens ocultas para se comunicarem em fóruns públicos com intuito de planejar suas atividades ou discutirem sobre localizações para a realização de suas atividades terroristas.

Geralmente, são utilizados programas que não estão incluídos na classificação de atividades ilegais. Por exemplo: as comunicações são realizadas por meio de serviços, sites e aplicativos de mensagens instantâneas ou transferências de arquivos por meio de conexão FTP (*File Transfer Protocol*).

A partir dessas definições, é possível observar que o cibercrime engloba uma série de ataques, e é importante compreender essa ampla variedade de crimes cibernéticos para saber o procedimento correto a ser tomado, com o objetivo de melhorar a segurança.

3. O IMPACTO DOS CRIMES ONLINE

Foi publicada, em outubro de 2016, a *Norton Cyber Security Insights Report* – pesquisa encomendada pela empresa Norton by Symantec Corporation, com a finalidade de obter o resultado do impacto dos crimes virtuais.

A imagem abaixo apresenta alguns dos principais resultados obtidos por meio dessa pesquisa, realizando uma comparação do Brasil como outros 21 países:

Figura 1: Impacto dos crimes virtuais

PRINCIPAIS RESULTADOS	BRASIL	GLOBAL (21 países)
Usuários afetados pelo cibercrime em 2016	42.4 milhões (39%)	689.4 milhões (31%)
Prejuízo financeiro gerado pelo cibercrime em 2016	US\$10.3 bilhões	US\$125.9 bilhões
Tempo gasto lidando com consequências cibercrime em 2016	16.9 horas	19,7 horas
Cibercrime mais comum	Roubo de dispositivo móvel: 25%	Senha comprometida: 18%
Entrevistados capazes de detectar corretamente os e-mails de phishing	68%	72%
Entrevistados capazes de avaliar se a rede Wi-Fi é segura	59%	48%

Fonte: Cyber Security Insights Report Brasil, 2016.

4. ASPECTO JURÍDICO

No sentido de adequar o direito às mudanças tecnológicas que transformam continuamente a sociedade, foi editada a Lei nº 12.737/2012 – também conhecida como “Lei Carolina Dieckman” -, responsável pela tipificação criminal de delitos informáticos.

Art. 154-A

Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante 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 vantagem ilícita.

Ação penal – detenção, de 3 (três) meses a 1 (um) ano, e multa.

De acordo com Silveira (2015), antes do ano de 2012, a falta de uma legislação específica tornava muito difícil a apuração dos crimes cibernéticos, uma vez que a legislação até então vigente havia sido direcionada aos crimes de forma geral, independentemente do meio utilizado para a sua prática. Dessa forma, com a não especificidade da legislação, era muito difícil a identificação dos sujeitos e a obtenção de provas para a condenação criminal quanto aos crimes cibernéticos. Para ele:

É importante destacar o Art. 154-A do Código Penal, que trouxe para o ordenamento jurídico o crime de “Invasão de Dispositivo Informático”, consistente na conduta de “invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita”. A pena prevista para o crime simples é de detenção de três meses a um ano e multa, havendo, entretanto, a previsão das formas qualificada e causas de aumento de pena.

A legislação supracitada demonstrou uma evolução da mesma, na medida em que notamos uma preocupação da sociedade com a segurança e com a proteção do direito ao sigilo de seus dados no âmbito digital. A edição da Lei nº 12.737/2012 constituiu um importante avanço ao tipificar expressamente o crime de “invadir dispositivo informático”, criando um tipo penal que visou eminentemente proteger o sigilo dos dados e das informações pessoais e profissionais.

5. ATAQUES CIBERNÉTICOS NO BRASIL

Com o objetivo de elucidar o conteúdo proposto, serão elencados alguns dos principais ataques cibernéticos com maior ocorrência no Brasil – segundo o relatório de segurança digital, publicado pelo DFNDR Lab no terceiro trimestre de 2017, e baseado na coleta de dados sobre detecções e bloqueios de ciberataques a celulares Android dos mais de 21 milhões de usuários dos aplicativos de segurança DFNDR.

A análise, que foi realizada entre os dias 01 de Julho e 30 de Setembro de 2017, identificou

que houve um crescimento de 44% dos ciberataques. O mesmo relatório determinou o total de malwares detectados nos meses de: Julho, 1.633.043; Agosto, 2.106.341; e Setembro, 1.846.730. Ademais, determinou o total de links maliciosos detectados nos meses de: Julho, 14.092.026; Agosto, 24.306.873; e Setembro, 27.342.028.

Figura 2: Principais tipos de ataques por links maliciosos

Fonte: DFNDR Lab, 2017

Figura 3: Principais tipos de ataques por malwares

Fonte: DFNDR Lab, 2017

Com base nas informações acima, o relatório publicado pelo DFNDR Lab expõe que os links maliciosos são 12 vezes mais utilizados em ataques do que os malwares.

5.1 PHISHING

De acordo com CERT.BR (2012), *phishing* é um tipo de fraude onde o atacante tem por objetivo obter os dados pessoais e financeiros de um usuário por meio da união de recursos técnicos e de engenharia social.

O *phishing* ocorre por meio do envio de mensagens eletrônicas, onde o atacante:

- Tenta se passar por um comunicado oficial de uma instituição conhecida, como um banco, uma empresa ou um site popular;
- Procura atrair a atenção do usuário, seja por curiosidade, por caridade ou pela possibilidade de obter alguma vantagem financeira;
- Informa que a não realização dos procedimentos descritos pode acarretar sérias consequências, como a inscrição em serviços de proteção de crédito, como, também, o cancelamento de seu cadastro, de uma conta bancária ou de um cartão de crédito;
- Induz o usuário a fornecer seus dados pessoais e financeiros por meio do preenchimento de formulários contidos em páginas falsas, projetadas para coletar informações sensíveis; e
- Para atrair a atenção dos usuários, as mensagens apresentam diferentes tópicos e temas, normalmente explorando campanhas de publicidade e assuntos em destaque.

A Kaspersky Lab publicou o relatório *Spam e Phishing* no segundo trimestre de 2017; este apresenta o Brasil como sendo o país com o maior percentual (18,09%) de usuários afetados por ataques de *phishing*. Assim como no 1º trimestre, os principais alvos de ataques de *phishing* continuam os mesmos e foram, principalmente, do setor financeiro: bancos, serviços de pagamento e lojas virtuais.

A tabela abaixo apresenta os países com maior índice de usuários afetados por crimes virtuais:

Figura 4: Países por porcentagem de usuários atacados

Brasil	18,09%
China	12,85%
Austrália	12,69%
Nova Zelândia	12,06%
Azerbaijão	11,48%
Canadá	11,28%
Catar	10,68%
Venezuela	10,68%
África do Sul	9,38%
Argentina	9,35%
Reino Unido	9,29%

Fonte: Kaspersky Lab, 2017

5.2 RANSOMWARE

De acordo com CERT.BR (2012), “*ransomware* é um tipo de código malicioso – um malware – que tornam inacessíveis os dados armazenados em um equipamento, utilizando criptografia e exigindo pagamento para restabelecer o acesso a eles”. Além de infectar o equipamento, o *ransomware* também buscar por outros dispositivos conectados localmente ou à rede, e os criptografa. O pagamento solicitado para o resgate das informações, geralmente, é realizado via *bitcoins* (moeda digital do tipo criptomoeda, que permite transações financeiras sem intermediários e possui maior dificuldade do seu rastreamento).

5.2.1 TIPOS DE RANSOMWARE

Existem dois tipos de *ransomware*: o *Locker*, que impede o acesso ao equipamento infectado; e o *Crypto*, que impede o acesso aos dados armazenados no equipamento infectado – geralmente, por meio de criptografia.

5.2.2 FORMAS DE INFECÇÃO

O *ransomware* pode se propagar de diversas formas, embora as mais comuns sejam: através de e-mails contendo código malicioso em anexo ou por meio de links utilizados para realizar o download de um arquivo infectado. Em ambos os casos, a infecção ocorrerá com a execução do arquivo, como também por meio da exploração de vulnerabilidades em sistemas que não tenham recebido as devidas atualizações de segurança.

Segundo a empresa Kaspersky, o Brasil concentra 92,31% dos casos de ameaças do tipo *ransomware* da América Latina. Os ataques são mais direcionados a pequenas e médias empresas devido a maior probabilidade de seus equipamentos estarem mal configurados e/ou ainda utilizando as credenciais *default*, além de utilizarem senhas consideradas fracas. Desta forma, é possível explorar as vulnerabilidades das redes corporativas com o objetivo de inserir o malware.

Os principais vetores de infecção no Brasil são os trojans relacionados ao setor financeiro – internet banking – infectados com *ransomware*, além de alguns casos de instalação manual em desktops remotos com baixos níveis de segurança. Isso é possível devido ao grande número de equipamentos com versões falsificadas de sistema operacional – prática que facilita a distribuição desses malwares, porque as ferramentas como *keygens* e *cracks* (utilizadas para registrar a versão falsificada do sistema operacional), em sua grande maioria, estão contaminadas com algum tipo de malware.

6. CRIMES PRATICADOS NAS REDES SOCIAIS

As redes sociais tornaram-se o principal canal de comunicação, produção e

compartilhamento de conteúdo, e se agrupam de acordo com interesses em comum. Alguns exemplos: *Facebook, WhatsApp, YouTube, Instagram, LinkedIn, Pinterest, Twitter, TikTok*, entre outros.

Segundo CERT.BR (2012), as redes sociais possuem algumas características próprias que as diferenciam de outros meios de comunicação, como: a velocidade com que as informações se propagam, a grande quantidade de pessoas alcançadas e a riqueza de informações pessoais que estas disponibilizam. Essas características, somadas ao alto grau de confiança que os usuários costumam depositar entre si, fizeram com que as redes sociais chamassem a atenção, também, de pessoas mal-intencionadas: os cibercriminosos.

O CERTS (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), por meio de sua cartilha de segurança para internet, lista alguns dos principais riscos relacionados a utilização das redes sociais:

- Contato com pessoas mal-intencionadas: é possível criar um perfil falso e se passar por outra pessoa, e, sem que você saiba, pode haver em sua rede pessoas com as quais você jamais se relacionaria;
- Furto de identidade: assim como você pode ter um impostor em sua lista de contatos, também pode acontecer de alguém tentar se passar por você, criando um perfil falso. Quanto mais informações você divulgar, mais convincente o perfil falso se tornará;
- Uso indevido de informações: suas publicações, além de contribuírem para a criação de um perfil falso, também podem ser utilizadas em ataques de força bruta e engenharia social, com intuito, por exemplo, de responder a questões de segurança usadas no processo de recuperação de credenciais de acesso;
- Invasão de privacidade: quanto maior sua rede de contatos, maior é o número de usuários que possuem acesso ao conteúdo que você divulga, e, por conseguinte, menores são as garantias de que as suas publicações não serão compartilhadas;
- Vazamento de dados: há diversos casos de empresas e pessoas que tiveram conteúdos sensíveis divulgados na internet;
- Disponibilização de informações confidenciais: a partir de uma troca “amigável” de mensagens, você pode ser persuadido a fornecer seus dados pessoais e bancários. Isto pode gerar inúmeras consequências – do recebimento de mensagens indesejáveis, até a utilização dos seus dados por terceiros;
- Ofensas à imagem e à reputação: a calúnia e a difamação podem rapidamente se propagar e causarem grandes danos às pessoas envolvidas, prejudicando a vida profissional e trazendo problemas familiares e psicológicos. Também podem prejudicar a reputação de empresas, causando perda da credibilidade e prejuízos financeiros;
- Furto de bens: ao divulgar que estará ausente por um determinado período, esta informação pode ser usada por um criminoso. Desta forma, haverá tempo para ele se programar, a fim de realizar o furto de seus bens.

7. CONCLUSÃO

A presente época – conhecida como a era da sociedade da informação –, na qual nos tornamos cada vez mais dependentes da tecnologia, a segurança cibernética é um assunto que precisa estar em pauta nas esferas pública e privada, bem como nos âmbitos pessoal e profissional.

É possível identificar através das informações explicitadas neste artigo que a maioria dos

crimes virtuais ocorre por meio do *phishing* e, de mesmo modo, a partir da utilização da engenharia social. Através dessas técnicas, os cibercriminosos exploram as vulnerabilidades tecnológicas e humanas.

O presente artigo não explorou todas as técnicas e crimes atualmente praticados no ambiente digital. Todavia, conclui que somente investimentos em infraestrutura não são suficientes para a redução dos crimes virtuais. Para isso, a conscientização dos usuários sobre os riscos do mundo digital e a orientação sobre a forma correta de utilização dos recursos tecnológicos são indispensáveis.

Não existe um ambiente totalmente seguro. Porém, a partir do equilíbrio entre o investimento em tecnologia e a educação dos usuários, será possível utilizar os recursos tecnológicos disponíveis com maior confiança e, por conseguinte, serão todos eles melhor aproveitados para fins benéficos à sociedade.

REFERÊNCIAS

(APDSI). Glossário da Sociedade da Informação. Portugal: APDSI. 2005.

ASSOCIAÇÃO PARA A PROMOÇÃO E DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO

CANONGIA, Claudia; JUNIOR, Raphael Mandarino. Segurança cibernética: o desafio da nova Sociedade da Informação. Disponível em: <http://seer.cgee.org.br/index.php/parcerias_estrategicas/article/viewFile/349/342>. Acesso em: 17 dez. 2017.

CERT.BR, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança No Brasil (Org.). Cartilha de Segurança para Internet. 2ª. ed. São Paulo: Comitê Gestor da Internet No Brasil, 2012. 140 p. Disponível em: <<https://cartilha.cert.br/livro/>>. Acesso em: 28 dez. 2017.

GUDKOVA, Darya et al. Spam and phishing in Q2 2017. Disponível em: <<https://securelist.com/spam-and-phishing-in-q2-2017/81537/>>. Acesso em: 20 dez. 2017.

LIMA, Davi Marques; LIMA, Álvaro Vieira. A IMPORTÂNCIA DA SEGURANÇA CIBERNÉTICA EM

SISTEMAS DE CONTROLE INDUSTRIAL. Disponível em: <http://www.convibra.com.br/upload/paper/2016/29/2016_29_13228.pdf>. Acesso em: 17 dez. 2017.

O QUE é crime cibernético? Disponível em: <<https://br.norton.com/cybercrime-definition>>. Acesso em: 21 dez. 2017.

RELATÓRIO da Segurança Digital no Brasil. Disponível em: <<https://lab.dfndrsecurity.com/pt-br/relatorio-da-seguranca-digital/>>. Acesso em: 30 jan. 2018.

SILVEIRA, Artur Barbosa. Os crimes cibernéticos e a Lei nº 12.737/2012 (“Lei Carolina Dieckmann”). Disponível em: <<https://jus.com.br/artigos/35796/os-crimes-ciberneticos-e-a-lei-n-12-737-2012-lei-carolina-dieckmann>>. Acesso em: 21 dez. 2017.

SOUZA, Taynah Lopes de; CANONGIA, Claudia. Technical infrastructure and its importance to national systems of innovation in BRICS. Projeto “Estudo Comparativo dos Sistemas de Inovação no Brasil, Rússia, Índia, China e África do Sul” – BRICS – Nota Técnica Final em Inglês. Brasília: CGEE. Disponível em: <www.cgee.org.br/atividades/redirect.php?idProduto=4111>. Acesso em: 17 dez. 2017.

^[1] Pós-graduação.

^[2] Orientador.

Enviado: Janeiro, 2021.

Aprovado: Abril, 2021.