Segurança da Informação Contra Crimes Cibernéticos nas Empresas: Estudo de Caso

Joseane Santos de Assis[1], Sergio Cleger Tamayo [2]

Resumo. *Este estudo teve como objetivo analisar como a Segurança da Informação atua nas empresas para mitigar os riscos provenientes de ataques cibernéticos, visando a preservações de seus dados e informações. A partir da metodologia, este estudo foi compreendido como uma pesquisa Exploratória, sendo constituído a partir da aplicação de um questionário semiestruturado nas empresas localizadas na cidade de Manaus. A partir da realização deste estudo, pode-se afirmar que a segurança da informação nas empresas são métodos indispensáveis para manter a ordem e boa performance e confiabilidade do produto, e quando se adotam um conjunto de ferramentas apropriadas.*

Abstract. *This study aimed to analyze how Information Security acts in companies to mitigate the risks from cyber-attacks, aiming at the preservation of their data and information. From the methodology, this study was understood as an Exploratory research, being constituted from the application of a semi-structured questionnaire in companies located in the city of Manaus. From this study, it can be stated that information security in companies are indispensable methods to maintain order and good product performance and reliability, and when adopting an appropriate set of tools.*

1. Introdução

O contexto atual da sociedade, em que a dominância das práticas virtuais se mostra cada vez mais presente em diversos aspectos, como a convivência social, comunicação e trabalho, tem sido conduzido cada vez salutar a necessidade de identificação de técnicas que busquem a segurança de dados, seja no cenário particular ou coletivo.

De acordo com Barbosa e Silva (2010), a imposição de salvaguardar as informações que tramitam no meio virtual é uma realidade que necessita do desenvolvimento constante de estudos considerando questões como a privacidade e a proteção de dados e tecnologias, sendo estes últimos os maiores alvos dos ataques cibernéticos no ambiente organizacional, o que se apresenta como uma questão cada vez mais eminente aos profissionais de sistemas de informação.

A realidade dos cybers ataques tem se mostrado cada vez mais recorrente no mundo organizacional, uma vez que, as inovações tecnológicas, as informações privilegiadas e o capital virtual de uma determinada empresa, são teoricamente salvaguardadas por sistemas de segurança, o que remete invariavelmente a necessidade de acesso através de investidas nestes sistemas.

De acordo com o Relatório de Ameaças Cibernéticas (2018), vem aumentando em níveis elevados desde 2017 em todo o mundo, ataques de *Ransomware, Malwares* e

demais ameaças existentes, e em 2018, foram registrados 5,99 bilhões de ataques de *Malware*, e de *Ransomware* alcançou o equivalente a 181,5 milhões de ataques.

Deste modo, surge a seguinte pergunta problema que norteará essa pesquisa: Quais são os principais tipos de ataques cibernéticos nas empresas?

O presente estudo justifica-se pela necessidade de compreender se um Sistema de Segurança de Informação de uma empresa realiza ou não a prevenção de ataques cibernéticos, quais as normas aplicadas, como eles desenvolvem as proteções das redes e da navegação da internet, como é executam suas manutenções e atualizações de sistemas, e se efetuam orientações junto a seus funcionários para prevenir ataques e identificar riscos.

Assim, este trabalho tem como objetivo geral analisar como a Segurança da Informação atua nas empresas para mitigar os riscos provenientes de ataques cibernéticos, visando a preservações de seus dados e informações.

Esta pesquisa divide-se em quatro sessões: a contextualização teórica, apresentando alguns conceitos de autores sobre a Segurança da Informação e Ataques Cibernéticos, a metodologia, destacando o tipo de pesquisa utilizada, resultados, abordando os principais eixos da coleta de dados, e por fim, as considerações finais.

2. Fundamentação Teórica

Anterior a apresentação das formas de prevenção à possíveis ataques cibernéticos é de suma importância a contextualização da Segurança da Informação, apresentando os conceitos que a permeia bem como as possibilidades que se apresentam como aplicação no contexto organizacional.

2.1 Segurança da Informação Aspectos Históricos e Conceituais

Segundo Fontes (2017), é possível definir a Segurança da Informação como um conjunto de estratégias em uma determinada organização que se destina em proteger dados, independentemente de sua natureza.

É observada através da definição apresentada de Segurança da Informação que esta área do conhecimento tem uma larga abrangência o que tange a proteção de dados importantes, sendo possível compreender sua aplicação nos mais diversos tipos de ambiente.

Aoki e Carvalho (2011), afirmam que a conceituação de Segurança da Informação pode ser melhor compreendida através da análise dos pilares que sustentam a prática da mesma, sendo estes a confidencialidade, integridade, disponibilidade e autenticidade.

A confidencialidade se caracteriza pelo princípio básico de que o acesso à dados e informações de uma determinada organização deve ser restrito a pessoas devidamente autorizadas. Já a integridade se define através de dois vieses, primeiro pela importância de manutenção da consistência e confiabilidade dos dados, seguida pela necessidade de backups, o que garante cópias em casos, por exemplo, de dados corrompidos (SÊMOLA, 2014).

O pilar da disponibilidade condiz com a possibilidade de acesso à informação pelas pessoas efetivamente autorizadas bem como quando necessitam, sempre com o intuito de agilizar os processos garantindo sua confidencialidade. E por fim a autenticidade, que se caracteriza pela manutenção da fidedignidade das informações, ou seja, é papel da Segurança da Informação traçar estratégias que mantenham a veracidade inicial dos dados (LEARDINI; SCHIMIGUEL, 2017).

2.2 Conceitos e Características dos Ataques Cibernéticos

Através da disseminação da internet ocorreu a oportunidade de se conectar com tudo, existe uma situação sem critérios nos acessos as informações sensíveis das empresas e do governo em todo o mundo e esses acessos passaram de um comum jogo de hackers que visava atingir um servidor para uma atividade organizada por empresas com o intuito de realizar a espionagem industrial (CARVALHO, 2011).

O espaço cibernético é uma área que é atingida no mundo todo, mesmo que compreenda a necessidade de segurança, não existem métodos implementados de forma articulada e sistemática que assegurem a preservação e confiabilidade dos sistemas utilizados (HOSANG, 2011).

No ambiente da Internet os ladrões cibernéticos classificam-se de várias formas, as mais identificadas são os denominados de hackers. Para Souza (2015), os Hackers são indivíduos que possuem conhecimento em Tecnologia da comunicação (TC) e Tecnologia da informação (TI) baseiam-se em seus conhecimentos e habilidades para aperfeiçoar explorar vulnerabilidades de sistemas. E os crackers são os que possuem bastante habilidades e conhecimento, assim, visam alcançar vantagem financeira sobre as informações obtidas.

No entanto, para Jesus *et al*. (2016), os Hackers visam melhorar os sistemas de redes, software de forma legalizadas, enquanto, os Crackers, visam somente o proveito pessoal praticando atos ilícitos. Deste modo, as empresas contratam os Hackers para combater e proteger seus sistemas dos Crackers.

A *Association of Information Technology Professionals* (AITP) adotou o termo o crime em informática para retratar uma ameaça constante para a sociedade, motivada pela irresponsabilidade de indivíduos e por ações criminosas, que tiram vantagem da internet, vulnerabilidade de computadores de forma abrangente (MOREIRA, 2016).

Os ataques são realizados por todos os veículos, como dispositivos móveis, *email*, tráfego da Web, e através de *exploits* automatizados, não levam em consideração o porte da empresa, uma vez que, utilizam ferramentas automatizadas para enviar e-mails ou *exploits*. Eles podem ocorrer de forma física, no qual os dispositivos possuem informações de fácil acesso, além de cabos, modens e mídias de armazenamento (BATISTA *et al*., 2018).

Mesmo como existam esforços da Administração Pública ainda permanecem lacunas na legislação brasileira, posto que, em outros países existem alguns tipos de ações que são consideradas crimes, e no Brasil, ainda não existem leis direcionadas para esses comportamentos (CARVALHO, 2011).

2.3 Principais Tipos de Ataques Cibernéticos

Segundo Batista *et al*. (2018), a engenharia social é responsável pelo ataque humano, e pelo meio lógico, são utilizadas técnicas de invasão para prejudicar os serviços (DDoS) pelo qual o atacante atua para ampliar o sistema de foco. Métodos que utilizam a instabilidade de portas de acesso, a disparada de *malwares* e vírus, e decodificadores de senhas que se baseia em um script que pode decodificar senhas.

Para Geraldo e Takeda (2019), existe uma enorme série de técnicas de invasão embasadas em engenharia social, entre elas podem ser citadas: o contato telefônico, a internet e redes sociais, a abordagem pessoal, o *Phishing* e as falhas humanas. como apresentado no Quadro- 1 a seguir.

Técnicas	Características
Contato Telefônico	Para iniciar o processo de coleta de informações da empresa, o hacker geralmente se passa por um terceiro funcionário ou fornecedor, e utiliza o contato telefônico para recolher informações.
Internet e Redes Sociais	Neste método, o engenheiro social pode subtrair informações que estavam abertas, assim, analisa a vítima através de informações e sites da empresa em que trabalha, objetivando buscar o máximo de informações.
Abordagem Pessoal	Esta técnica é realizada, quando o próprio Hacker visita a própria empresa, e começa a se passar por um funcionário, fornecer ou conhecido de um colaborador que possui importante função para extrair informações valiosas da organização que pretende atingir.
Phishing	É identificado como os e-mails falsos que são conduzidos e encaminhados para os indivíduos ou empresas, com o intuito que ele desenvolva as operações enviadas.
Falhas Humanas	Uma das técnicas mais fracas na segurança da informação relacionasse as pessoas, que geralmente são exploradas as suas vulnerabilidades, como curiosidade, confiança, medo, ingenuidade entre outros pelos invasores.

Quadro 1: Técnicas de invasão utilizadas na engenharia social
Fonte: Geraldo e Takeda (2019).

Compreende-se que também existem diversos tipos de crimes cibernéticos, entre os quais podem ser citados, segundo Jesus *et al*. (2016, p. 2-3):

> 1.Mobile malware: Vírus desenvolvidos para roubar informações e causar dan os;
> 2.Espionagem industrial: Roubar informações sigilosas de empresas, e fornecê-las a seus concorrentes;
> 3.Worm: Atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede;
> 4.Dos:Ataques de negação de serviço, nele o atacante utiliza um computador;
> 5.Scan: Varreduras em redes de computadores, visando identificar quais serviços e ativos estão sendo disponibilizados por eles.

Para O’Brien e Marakas (2013), os principais métodos de ataques dos crackers são:

- Scans: baseia-se em analisar profundamente a internet, para especificar os tipos de serviços, computadores e conexões em utilização, assim, pode se aproveitar de determinada fraqueza de software ou recurso do computador;
- Negação de Serviços: uma técnica comum que se direciona em atingir o equipamento de um site da web através de várias solicitações de informações;
- Spoofing: falsificar a página da internet e endereço para defraudar os usuários para que repassem informações importantes;
- Password Crackers: Software que tem a capacidade de descobrir senhas;
- SQL Injection: é um tipo de ataque cibernético que se beneficia de falhas em sistemas que utiliza a comunicação voltados para a base de dados de comandos SQL, assim, pode ser identificado como um tipo de ataque bastante simples.

No Brasil, existem algumas leis direcionadas a crimes cibernéticos, são normas jurídicas já existentes que são aplicadas para subsidiar a legislação ausente, são normas do código penal utilizadas para não deixar o invasor impune, entre elas cita-se a:

- Lei de Software nº 9.609/98: Refere-se à proteção da propriedade intelectual de sua comercialização no país, de programa de computador e de outras providências.
- Lei Carolina Dieckmann nº 12.737/2012: Determine e pune os crimes informático de roubos de dados.
- Lei nº12.735/12: Modifica o código penal para cuidar de crimes cibernéticos, e tipifica condutas desenvolvidas frente a utilização de sistema digital, eletrônico ou similar (JESUS *et al*., 2016).

2.4 A Segurança da Informação na Prevenção de Ataques Cibernéticos

A Segurança da Informação é uma área do conhecimento que se dedica a estudar e traçar metodologias que visem assegurar a integridade das informações de uma determinada organização, considerando a possibilidade de ataques cibernéticos, principalmente como medidas preventivas a tais acessos, garantindo a confidencialidade dos dados (GALEGALE; FONTES; GALEGALE, 2017).

Um dos sistemas de informação instalado nas organizações para proteger o seu sistema é a rede interna que atua externamente chamada firewall, necessária para deter os ataques de hacker, realizam os bloqueios nos servidores, que como ameaça solicitam resgate em bitcoins, no entanto, é possível modificando a situação, ao formatar o sistema, reimplantando a parte da segurança (SANCHEZ, 2018).

Desse modo, é importante que as empresas trabalhem com os servidores criptografados, virtualizados e com sistema de firewall para ataque externo. O Update de soluções, que é o administrador de desenvolvedor do sistema, disponibiliza um suporte imediato do sistema de firewall até o sigilo interno (SANCHEZ, 2018).

Ferramenta / Formas	Objetivo
Antivírus	Programas que visam proteger o computador de vírus, realiza o monitoramento das atividades on-line e bloqueia as atividades maliciosas, por isso, é importante utilizar com frequência.
S.O e softwares atualizado	Atualiza continuamente o computador, bloqueando possiblidades de se aproveitarem de falhas do software dificultando o acesso.
Senhas	Utilizar palavras que não são facilmente identificadas, utilizando no mínimo 8 caracteres como combinação de números, letras e símbolos, trocando a senha a cada 90 dias.

Quadro-2 Sugestões de prevenção a ataques cibernéticos
Fonte: Adaptado de (NORTON, 2016).

3.Metodologia

De forma geral, este estudo pode ser compreendido como uma pesquisa Exploratória e Descritiva, com abordagem Qualitativa, sendo desenvolvido a partir aplicação de um Questionário Semiestruturado em 10 empresas localizadas na cidade de Manaus-AM.

A pesquisa Exploratória tem como objetivo buscar se aprofundar fatos, explorar ideias relacionadas ao tema. A pesquisa descritiva visa apresentar características bem claras do fenômeno estudado, sem influenciar nos resultados (VERGARA, 2013).

Em relação a coleta de dados, utilizou-se como técnica, o questionário estruturado, realizada in loco, contendo 11 questões semiestruturadas que foram aplicadas apenas ao setor de Segurança da Informação de 10 empresas, sendo 7 de médio porte e 3 de pequeno porte, com o objetivo de analisar a importância da Segurança da Informação nas empresas na prevenção de ataques cibernéticos. E sobre o sigilo e confidencialidade sobre as informações, os dados serão utilizados exclusivamente para fins didáticos, sendo garantido o anonimato e sigilo deles.

Quanto à definição da amostragem, ressalta-se que os colaboradores do Setor de Sistema da Informação contemplaram o universo, ou seja, os 10 funcionários, 1 de cada empresa, participaram da pesquisa não necessitando de cálculo de amostragem.

Critérios de Inclusão: Ser funcionário (ativo) contratado ou prestador de Serviço da que atua no setor de Segurança da Informação e ser voluntário para participar da pesquisa.

Critérios de Exclusão: Funcionários de outros setores da empresa, não ser voluntário para participar da pesquisa e funcionários não presentes.

4 Resultados

Para o alcance dos resultados foram consideradas apenas as perguntas mais relacionadas aos objetivos, o mesmo questionário foi aplicado em 10 empresas, diretamente com 10 funcionários que atuam na área do Sistema da Informações, todos

contribuíram de forma expressiva, o período de pesquisa ocorreu durante o mês de setembro de 2019.

Os resultados da coleta, estão estruturados de acordo com a ordem do questionário aplicado e consequentemente uma análise baseada na literatura utilizada. As questões utilizadas serão apresentadas a seguir.

Entre os respondentes, 6 eram do sexo feminino e 4 do sexo masculino, entre as faixas etárias de 20 a 40 anos, todos com Ensino Superior Completo e atuantes na área do Sistema de Informação.

Com a finalidade de compreender as funções desempenhas pelos profissionais de Segurança da Informação, através da questão 1: Quais as principais funções relacionadas à área de segurança da informação que os profissionais desempenham?

Constatou-se que 40% dos funcionários realizam principalmente a atividade de identificar e definir objetivos de proteção e informação, 30% desenvolvem as atribuições de detecção de ameaças e vulnerabilidades em serviços de TI que comprometam as atividades da empresa, 20 % definem as políticas de segurança da informação e 10% realizam a manutenção e implementação de sistemas.

Segundo os resultados e informações fornecidas, 5 empresas estão se direcionando mais suas práticas para a Segurança da Informação, visando assegurar a integridade de sistemas e dados. Outras 5, ainda possuem dificuldades em investir nesse profissional, por conta do custo, no entanto, mesmo de forma tímida estão buscando sua implantação.

Através da questão 2: Quem são os responsáveis por manter a segurança das informações dentro da empresa?

Pode-se observar que 50% dos respondentes afirmaram a instituição regulamentadora do segmento é responsável por manter a segurança das informações dentro da empresa, 40% toda organização e qualquer funcionário, e apenas 10% informaram que são os clientes e fornecedores.

Com intuito de compreender quais os principais ataques cibernéticos que ocasionam mais danos a empresa, foi desenvolvida a questão 3: Qua**is** os tipos de ataques cibernéticos que mais causam danos a empresa?

E teve como resultados, 30% afirmaram que são os ataques DoS, 30% ataques DMA, 20% a corrupção de rede, 10% os *Malwares* e 10% Backdoor, como mostra o Gráfico-1.

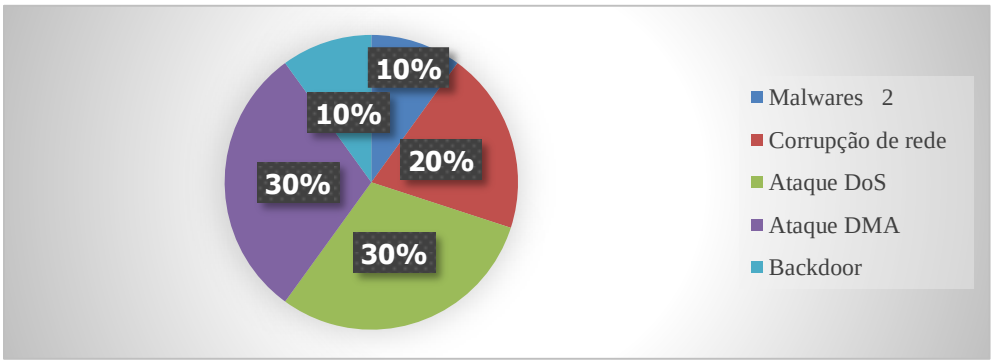

Gráfico 1- Tipos de ataques cibernéticos que ocasionam mais danos a empresa.
Fonte: Resultados da pesquisa em campo (2019).

A partir desses resultados, afirma-se que 7 colaboradores têm conhecimento mais profundo dos tipos de ataques cibernéticos que mais afetam as empresas, 2 foram mais cautelosos sobre as informações fornecidas. E os tipos de ataques que mais ocorrem são os DoS e DMA, informaram que as empresas apresentaram instabilidade e ficaram fora do ar devido os ataques que sobrecarregaram o serviço do portal, desabilitações dos computadores, entre os casos mais recorrentes são nas organizações que não possuem políticas definidas sobre o Sistema de Segurança da Informação.

O ataque DoS que é uma tipo de ataque que baseia-se em um computador central utilizando outros computadores para atingir um site, o DMA, é um ataque direto na memória, possibilitando que vários programas acessem o computador. Os furtos ocorrem na corrupção de rede.

O malware é um termo muito usado para descrever qualquer programa ou código malicioso que seja prejudicial aos sistemas. Ele invade danifica ou até mesmo desabilita computadores, redes, tablets e dispositivos móveis. Todos são prejudiciais, torna-se essencial um investimento inteligente em cibersegurança nas empresas.

A questão 4- Quais são as maiores ameaças no que se refere a segurança da informação? De acordo com os participantes, entre elas, 40% estão os programas instalados que visam a violação, outros 40%, os vazamentos de informações, e o correspondente a 20% o desfalque nos recursos tecnológicos, conforme destaca o Gráfico-2.

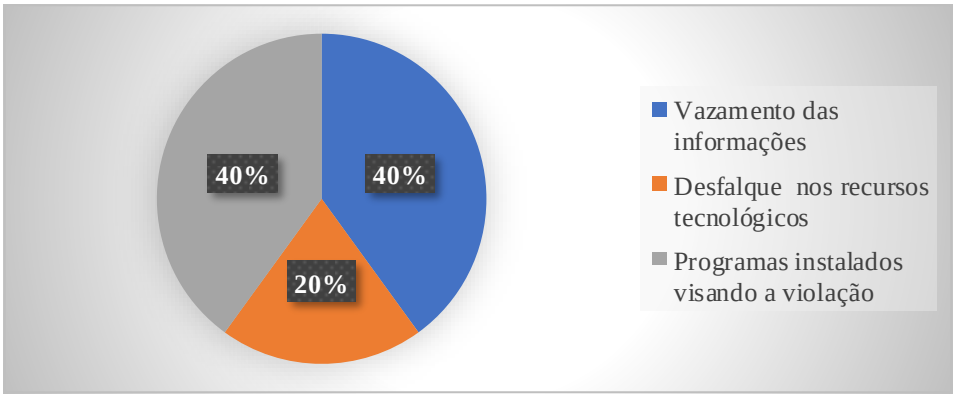

Gráfico 2- Maiores ameaças no que se refere a segurança da informação.
Fonte: Resultados da pesquisa em campo (2019).

Pode-se perceber que são várias ameaças que comprometem a Segurança da Informação das organizações. Entre os respondentes, 4 afirmaram que são vazamentos das informações, outros 4 desfalques nos recursos tecnológicos e 2 os programas instalados, faz-se fundamental não somente se direcionar para a proteção do setor de TI, mas, nos contratos de confidencialidade, restrição do acesso as informações e criações de senhas nas empresas.

Os principais fatores que contribuem para essa ocorrência nessas empresas é o nível de maturidade baixo e são pouco protegidas. É essencial se atentar, pois, os impactos

podem ser grandes, resultando em falência.

Na questão 5, Quais são as ferramentas de segurança da informação utilizadas por sua empresa para mitigar os riscos provenientes de ataques cibernéticos à rede corporativa?

O resultado apresentado mostra que as ferramentas da informação mais utilizadas pelas empresas, são em média 30% das Políticas de Senhas, 20% dos Detectores de Intrusão, 20% Filtros AntiSpam, 20% Antivírus e 10% *Firewall*, como apresenta o Gráfico-3.

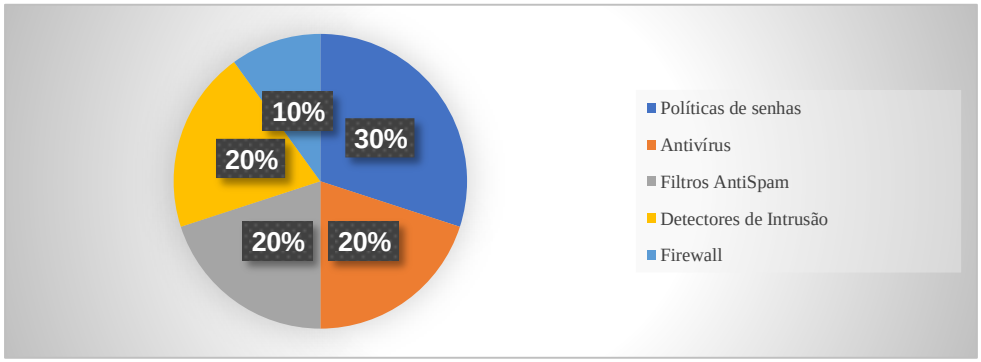

Gráfico 3- Ferramentas de segurança da informação utilizadas por sua empresa.
Fonte: Resultados da pesquisa em campo (2019).

Entre grande parte das empresas pesquisadas, o antivírus é a ferramenta mais utilizada para assegurar a segurança da informação, presente em 100% das empresas, seguido pelo firewall (82,9%) e Filtros Antispam (62%). Afirma-se que as ferramentas de segurança de informação têm função proativa e preventiva e melhoram a segurança virtual dos ambientes corporativos.
Os resultados mostraram que todos os profissionais estão buscando o aprimoramento no que se refere as Ferramentas de Segurança da Informação, mesmo com certas debilidades tentam relacionar a realidade da organização com a ferramenta mais apropriada, enfatizando que as mais apropriadas são os Antivírus, Detectores de Intrusão e Filtros Antispam, pela eficiência e baixo custo.

Na questão-6: Em casos de invasão cibernética ou roubo de dados, como você como profissional agiria?

40% dos respondentes informaram que é realizar uma varredura com um bom antivírus, como um *anti-spyware*, que remove ameaças de malware, 30% afirmaram que desenvolvem imediatamente um backup através da utilização de software e outros 20% confirmaram que coletam as evidências do crime cibernético, salvando os arquivos.

Pode-se constatar que, grande parte dos profissionais tem conhecimento sobre as melhores ferramentas de segurança e muitas estão disponibilizadas nas organizações, no entanto, é importante evidenciar que em casos de roubos de dados as decisões necessitam ser tomadas rapidamente, pois, existe a possibilidade dos custos crescerem exponencialmente a medida que passa o tempo para solucioná-los.

5 Considerações Finais

Com base nas pesquisas, é correto afirmar que grande parte das empresas pesquisadas tem investido na modernização de suas estruturas, e estão atentas as ameaças

cibernéticas, com disposição a melhorar na segurança de dados, investindo em profissionais capacitados, tecnologias e acessos mais restritos para proteger informações.

No entanto, em algumas organizações se estabelece a dificuldade no que diz respeito os conhecimentos dos ataques cibernéticos e das Ferramentas de Segurança da Informação, os principais fatores identificados no estudo são, a falta de investimento em profissionais capacitados, métodos de prevenção e treinamentos com os colaboradores. Mesmo sendo percebida como prioridade ainda existe a necessidade de ser mais difundida nas tomadas de decisão.

Na teoria foi identificada que a melhor estratégia para combater os ataques são os antivírus instalados e na prática isso foi realmente evidenciado, pois, grande parte das organizações utilizam com frequência essa ferramenta para realizar o monitoramento e bloqueio das atividades consideradas maliciosas.

Os cibercriminosos tem compreensão que possuem as informações sigilosas, assim seu maior objetivo é a invasão. Deste modo, as ferramentas de segurança da informação como Antivírus, Firewall, Políticas de Senhas, entre outras, são métodos fundamentais para garantir a segurança e o sucesso das empresas.

Sendo assim, é essencial que as empresas utilizem algumas estratégias para prevenir ou reduzir os riscos à segurança da informação entre eles podem ser citadas: manter os antivírus, drivers e softwares atualizados, controlar os acessos na empresa, criar políticas de segurança e treinar os colaboradores para as medidas de segurança, isso pode levar tempo e altos custos, no entanto, é importante analisar quais possíveis prejuízos que um ataque cibercriminoso traz para a empresa.

Para o desenvolvimento desse estudo ocorrem certas limitações no que se refere a pesquisa nas empresas, pela dificuldade na coleta das informações, pois, muitas se privam de passar informações por segurança. Porém, a partir de algumas tentativas em várias organizações, foi-se possível realizar a coleta das informações.

Recomenda-se que seja dada continuidade a estudos futuros para melhores compreensão, visando verificar a amplitude dessa temática, Segurança da Informação que se transforma de acordo com as necessidades do mercado e sociedade, poderia revelar mais informações e permitir a indicações de novos fatores inibidores.

6 Referências

Aoki. Eric Komiyama; Carvalho, Alan Henrique Pardo de. (2011). Prática de Segurança para o Desenvolvimento de Sistema Web. Fasci-Tech – Periódico Eletrônico da FATEC-São Caetano do Sul, São Caetano do Sul, v. 1, n. 5, Out/Dez.

Barbosa, Simone D. J.; Silva, Bruno S. (2010). Interação Humano-computador. Rio de Janeiro: Campus.

Batista, Lucas Oliveira. (2018). Utilização de Redes Neurais Nebulosas para criação de um Sistema Especialista em Invasões Cibernéticas. ICOFCS, São Paulo, Brazil October 29-30.

Carvalho, P. S. M. D. (2011). A defesa cibernética e as in-fraestruturas críticas nacionais. Coleção Meira Mattos-Revista das Ciências Militares.

Fontes, E.L.G. (2017). Segurança da Informação. Ed. Saraiva.

Galegale, N. V., Fontes, E. L. G., & Galegale, B. P. (2017). Uma contribuição para a segurança da informação: um estudo de casos múltiplos com organizações brasileiras. Perspectivas em Ciência da Informação, 22(3), 75-97.

Geraldo, Vinicius da Silva; Takeda, Fábio Bento. (2019). Engenharia Social: um perigo oculto em simples técnicas. Interface Tecnológica.

Hosang A. (2011). Política Nacional de Segurança Cibernética: uma necessidade para o Brasil. Escola Superior De Guerra, Rio De Janeiro.

Jesus, Luana Natielle Costa Leal de. (2016). Crimes cibernéticos: abordagem, práticas e considerações; *et al*. Anais do IX Simpósio de Informática, IFNMG, Câmpus Januária.

Leardini, Rafael Tafarello; Schimiguel, Juliano. (2017). Estudo sobre Segurança da Informação no Ambiente Corporativo. Revista Observatorio de la Economía Latinoamericana, Brasil, marzo.

Moreira, Robson Antônio. (2016). Principais Formas de Ataque e Prevenção a Informação no Ambiente da Internet. Revista FATEC Sebrae em debate: gestão, tecnologias e negócios, v. 3, n. 5.

Norton. L.(2016). "As melhores sugestões de prevenção.Disponível em:<" http://br.norton.com/preventiontips/article>. Acesso em: 10 set. 2019.

O'Brien, J. A; Marakas, G. M. (2013). Administração de Sistemas de Informação. Tradução Rodrigo Dubal; revisão técnica: Armando Dal Colleto. 15. ed. Porto Alegre: AM GH.

Sanchez, Steven Wagner. (2018). A Importância de um Sistema de Informação para as Organizações: Estudo de Caso na Pousada Raio de Sol. Anais do Seminário Nacional de Sociologia da UFS.

Sêmola, M. (2014). Gestão da Segurança da Informação - Uma Visão Executiva - 2 ed**.** São Paulo: Elsevier.

Souza, E. D. de. (2015). A Ciência da Informação: fundamentos epistêmico-discursivos do campo científico e do objeto de estudo. Alagoas: Edufal.

Sonic, Wall. (2018). Relatório de Ameaças Cibernéticas. Disponível em:< https://www.sonicwall.com/resources/white-papers/2018-sonicwall-cyber-threat-report-2/>. Acesso em: 27 ago. 2019.

Vergara, Sylvia. (2013). Projetos e Relatórios de Pesquisa em Administração. 14° ed. - São Paulo: Atlas, 2013.