DOI: 10.53660/CONJ-1177-T09

As principais ameaças digitais e suas formas de mitigação no contexto da segurança da propriedade intelectual

The main digital threats and their ways of mitigating them in the context of intellectual property security

José dos Santos Machado[1]*, Francisco Sandro Rodrigues Holanda[2], Arilmara Abade Bandeira[1], Adauto Cavalcante Menezes[3], Toniclay Andrade Nogueira[1], Jane Barbosa Santos[3], Jaziel Souza Lobo[1]

RESUMO

Considerando que a violação de dados digitais pode comprometer seriamente a propriedade intelectual organizacional, recursos, tempo e valor do produto, o presente estudo teve por objetivo identificar e analisar quais as principais ameaças digitais e suas formas de mitigação que se apresentam no sentido de garantir Segurança à Propriedade Intelectual (SPI) para os dados armazenados por meio digital. Foi realizada uma revisão *Scoping Review*, usando critérios do *Cochrane Systematic Reviews* associados ao PRISMA, na base Scopus e foram identificados 247 registros, usando os descritores d*igital threats e intellectual property*. Por meio dos métodos de seleção e classificação foram analisados 28 artigos, que sinalizam que as principais ameaças para a SPI foram os ataques: *Trojan*, *Brute Force*, Engenharia social e *Ransomware.* As medidas como implementação de certificado e assinatura digital, criptografia de dados, autenticação forte, treinamento de equipe, uso de *firewall* modernos e bem configurados, uso de antivírus, política de *backup* e uma política de cibersegurança se mostram eficientes na mitigação dessas ameaças. Segurança digital é necessária e deve ser trabalhada para sua constante atualização.

Palavras-chave: Ataque cibernético; Crime cibernético; Proteção de dados; Segurança digital.

ABSTRACT

Considering that digital data violation can seriously compromise organizational intellectual property, resources, time and value of the product, the objective of this study was to identify and analyze the main digital threats and their mitigation forms that are emerging to ensure intellectual property security (IPS) for data stored by digital. A scoping review was performed using Cochrane Systematic Reviews Criteria associated with Prisma at the Scopus base, and 247 records were identified, using the descriptors: digital threats and intellectual property. Through the selection and classification methods 28 articles were analyzed, showing that the main threats to IPS were the attacks: Trojan, Brute Force, Social Engineering and Ransomware. Measures such as digital certificate and signature implementation, data encryption, strong authentication, team training, modern and well configured firewall, antivirus use, backup policy, and a safety cyber policy show efficient in mitigating these threats. Digital security is necessary and must be constantly updated.

Keywords: Cyber Attack; Cybercrime; Data protection; Digital security.

[1] Instituto Federal de Sergipe - IFS
* E-mail: jsmac18@hotmail.com
[2] Universidade Federal de Sergipe - UFS
[3] Instituto Federal do Amapá - IFAP

INTRODUÇÃO

A Propriedade Intelectual (PI) é o bem mais valioso de um país, empresa ou indivíduo (MALIK, 2014). À medida que a tecnologia se torna cada vez mais sofisticada, aumentam as ameaças a esse bem inestimável (SENGUPTA, 2016), e as ameaças são crescentes devido ao fato de que há um aumento fenomenal no nível de dados armazenados em servidores, discos rígidos, pen drives, etc, (MACHADO, 2022). Uma violação de dados pode afetar seriamente a propriedade intelectual organizacional, recursos, tempo e valor do produto (GOMES, 2020). Esta situação é exacerbada no contexto do aumento da criminalidade através do uso indevido de tecnologias modernas de TIC para *cybercrime* (STJEPANDIĆ; LIESE; TRAPPEY, 2015).

Nas últimas duas décadas, a indústria vem implantando a retórica da "ameaça digital" para exigir medidas mais duras contra a pirataria (FROSIO, 2016). No cenário de ameaças da lógica digital moderna, a engenharia reversa e a clonagem ilegal representam dois riscos para aplicativos baseados em *hardware* com Propriedade Intelectual (PI) incorporada (MCDONALD, 2016). As proteções contra engenharia reversa maliciosa, clonagem e inserção de *trojan* são variadas (SENGUPTA, 2017). Em tempo, os *trojans* são s*oftwares* maliciosos que camuflam os programas originais assumindo a forma dos mesmos (SANABRIA-BORBÓN, 2021).

As indústrias de TI investem bilhões de dólares anualmente para prevenir ataques de segurança, como adulteração e engenharia reversa maliciosa (BEHERA; BHASKARI, 2015). Cada organização tem sua própria propriedade intelectual e é um grande desafio para eles proteger seus dados, ou seja, pirataria de *software* ou injeção de código malicioso etc (SENGUPTA, 2020). Os ataques de ambiguidade visam lançar dúvidas sobre a verificação da propriedade intelectual, e representam sérias ameaças aos métodos de defesa existentes (FAN, 2021).

Devido às crescentes ameaças de clonagem e falsificação de *hardware core* PI, a segurança continua sendo um importante assunto de pesquisa para esses aceleradores de *hardware* (RATHOR, 2020). Na ameaça de clonagem um *hacker* copia os arquivos de propriedade intelectual de um genuíno proprietário e os vende no mercado com uma marca diferente (BRANDMAN, 2020).

Várias técnicas foram publicadas para proteger a PI de circuitos analógicos e de sinal misto, essas técnicas são baseadas em travar o circuito analógico com uma chave de entrada (SANABRIA-BORBÓN, 2021).

Muitas organizações correm o risco de violação de dados e ataques cibernéticos em um determinado ponto, e uma estrutura de resposta a incidentes repetível e bem desenvolvida é fundamental para protegê-las (IMRAN, 2019). A tecnologia facilita o processamento de informações, mas apresenta vários riscos, incluindo *hackers* e problemas de confidencialidade (SYED, 2022). Sistemas que operam na *web* enfrentam muitas ameaças cibernéticas e ataques de partes mal-intencionadas (BICKFORD, 2015). Ataques de negação de serviço (DDoS) têm sido o tipo mais frequente de ataque de segurança visado por cibercriminosos, reduzindo assim o desempenho da rede (MISHRA; SHARMA; ALOWAIDI, 2021).

Apesar de *hackers* externos serem um perigo constante e repetidamente destacados pela mídia, ameaças mais silenciosas e potencialmente mais perigosas geralmente vêm de dentro das próprias empresas (PALMER, 2016). Os ataques à segurança da informação (SI) por meio de dados obtidos da internet ou na própria instituição estão ficando cada vez mais avançados e complexos (TORTEN; REAICHE; BOYLE, 2018). Sendo a engenharia social (ES) uma preocupação cada dia mais forte (SOUZA, 2016), atualmente, os ataques persistentes e avançados estão combinando diversos vetores de ataque para chegar aos seus objetivos (HITAJ, 2019).

De acordo com Beebe, Liu e Ye, (2017), pessoas internas por vontade própria e não maliciosas incluem usuários que conscientemente subvertem medidas de segurança para atingir metas de trabalho e pessoas internas que violam políticas de uso aceitável para ganho ou satisfação pessoal. Incidente de espionagem, roubo de propriedade intelectual, fraude ou abuso de computador organizacional pode ajudar a detectar ameaças internas (MITCHELL; ZUNNURHAIN, 2019).

Conforme evidenciado na literatura atual as Ameaças Digitais (AD), no contexto da segurança da propriedade intelectual no mundo conectado é um fator de grande preocupação para economia e crescimento de um país (MACHADO, 2022), sendo as formas de mitigação dessas ameaças um campo de pesquisa de enorme relevância para pesquisadores do mundo inteiro. O objetivo desse trabalho foi identificar e analisar quais as principais ameaças digitais e suas formas de mitigação que se apresentam no sentido de garantir SPI para os dados armazenados por meio digital.

MATERIAIS E MÉTODOS

A revisão de escopo (RE) em documentos acadêmicos buscou atingir o objetivo, uma vez que é projetada para coletar evidências que atendam aos critérios de elegibilidade

pré-especificados, buscando a compreensão de lacunas existentes na temática proposta (MUNN et al., 2018). Para identificar, avaliar e interpretar os resultados relevantes das revisões sistemáticas em trabalhos acadêmicos publicados, conforme os princípios das regras empíricas relacionadas aos levantamentos bibliométricos na literatura, atualmente são amplamente adotados e aceitos os procedimentos de classificação, descrição e qualificação de documentos que adotam princípios metodológicos, tais como as revisões do Cochrane (CHANDLER et al., 2021).

Neste artigo foram adaptadas as recomendações do *Cochrane Handbook for Systematic Reviews of Interventions* (HIGGINS et al., 2020), adotando como procedimentos deste estudo: formulação da pergunta e rodadas: (i) localização dos estudos (artigos), (ii) elegibilidade dos estudos, (iii) qualificação dos artigos e extração dos dados e (iv) síntese da revisão interpretação dos dados.

Os Dados foram dispostos no repositório de dados abertos OSF sob o DOI: 10.17605/OSF.IO/Y8H25

Para este estudo foi atribuído o seguinte questionamento: Quais as principais ameaças digitais e suas formas de mitigação apresentadas para prover segurança à propriedade intelectual para os dados armazenados.

Rodada 1: Extração dos estudos

Inicialmente foi realizada uma busca com descritores primários nas bases de dados Scopus. Os descritores foram trabalhados na língua inglesa vinculados por operadores booleanos, seguindo as regras descritas por Slamet et al., (2016), por meio de artigos publicados entre os anos de 2013 a 2022. O critério de inclusão e exclusão para esta rodada das recomendações aceitou apenas artigos completos, escritos na língua inglesa apresentando os descritores primários nos seguintes campos: título (*title*), resumo (*abstract*) e palavras-chave (*keywords*). Para a base Scopus foi utilizado a seguinte string de busca: (TITLE-ABS-KEY (*digital* AND *threat*) AND ALL (*intellectual* AND *property*)) PUBYEAR > 2012

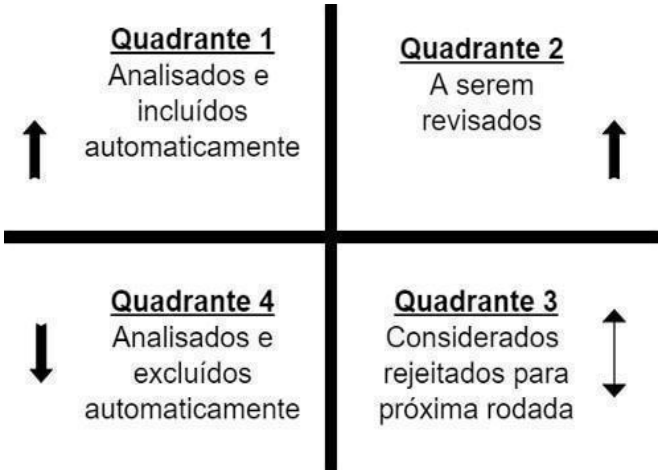
Rodada 2: Elegibilidade dos dados

Seleção automática

Pela possibilidade de se trabalhar com bancos de dados, a seleção inicial dos estudos foi realizada na sua primeira fase utilizando a busca por trabalhos duplicados a partir da seleção dos artigos únicos com o emprego do sistema StArt (LAPES, 2005). O

método SCAS do sistema StArt foi adotado como classificador automático por pontuação, organizando os artigos em duas fases. A primeira fase foi dividida em dois recursos, ou seja, por pontuação e por citação, e a segunda fase classificou nos seguintes quadrantes Q1 (3 pontos), Q2 (2 pontos), Q3 (1 ponto) e Q4 (0 pontos) (OCTAVIANO et al., 2015; OCTAVIANO et al., 2016). A Figura 1 apresenta os quadrantes adotados pelo Sistema. Para completar a extração dos artigos classificados no Q2, foram lidos títulos, resumos e palavras-chave para verificação efetiva da inclusão ou exclusão.

Figura 1 – Quadrantes e categorias adotados no posicionamento hierárquico de pontos



Fonte: Machado et al., (2022)

Seleção manual dos artigos

Buscando mitigar possíveis artigos não relacionados ao tema proposto, foram selecionados os artigos que apresentaram valores maiores nos índices de inclusão e para os índices de exclusão (Tabela 1), podendo ainda ser elegível na próxima rodada.

Tabela 1 – Critérios de Inclusão/Exclusão dos artigos observados

Critérios adotados	Grupo de Índices
Apresenta os dois descritores no título	Inclusão (I)
Periódico com fator de impacto internacional	Inclusão (I)
Correlação entre as duas áreas temáticas	Inclusão (I)
Não é trabalho sobre temas relacionados	Exclusão (E)
Não é trabalho sobre métodos inovadores	Exclusão (E)
Não apresenta solução inovadora	Exclusão (E)
Não apresenta possibilidade de replicação do experimento	Exclusão (E)
É uma revisão bibliográfica	Exclusão (E)
Pouca aderência aos descritores primários	Exclusão (E)

Fonte: Elaborado pelos autores

Os demais trabalhos foram considerados automaticamente inelegíveis para a próxima rodada. Todas as seleções nesta rodada foram realizadas por dois pesquisadores, independentemente, assim como restrita, de modo a evitar influência pessoal nos resultados. As discrepâncias observadas durante esta rodada foram resolvidas por consenso.

Rodada 3: Qualificação dos artigos e extração dos dados

Índice de qualidade dos artigos

Para classificação de qualidade dos artigos selecionados, foram adotados indicadores presentes na Tabela 2:

Tabela 2 — Indicadores adotados para descrição de qualidade dos artigos.

Siglas	Indicador	Índice de inclusão
DMA	Descreve o método/meios da ameaça digital	Índices de qualidade
MMA	Apresenta o método/meios para a mitigação da ameaça	Índices de qualidade
ACR	Apresenta capacidade de reprodução	Índices de qualidade
INV	Aparenta ser uma inovação	Índices de qualidade
TPI	Aplicação de uma tecnologia direcionada à proteção da PI	Índices de qualidade
DES	Apresenta descrição do procedimento metodológico	Índices de qualidade
TSD	Envolve tecnologia direcionada a área da segurança digital	Índices de qualidade

Fonte: Elaborado pelos autores

Foram atribuídos para cada indicador os valores: 0 para “não atende o indicador”, 0,5 “atende parcialmente o indicador” e 1 para “atende o indicador”, assim como os valores alcançados na classificação de prioridade (3 Muito alto, 2 Alto e 1 Baixo). Nesta fase foram excluídos os manuscritos que apresentavam grandes similaridades com os demais, e os que foram pontuados como prioridade baixa, mantendo o que apresentou maior pontuação dentre estes, assim como trabalhos que mantinham caráter de continuidade de uma pesquisa macro, pelos mesmos autores ou grupo de pesquisa.

Extração e síntese dos dados

A última rodada foi responsável pela classificação da qualidade dos trabalhos selecionados. Para identificar os artigos mais relevantes considerando as pontuações e classificações de toda a revisão, foi estabelecido um valor de corte correspondente a 85% do somatório dos critérios de classificação de escore por valor, obtidos na seleção dos estudos. O limite de 85% do somatório foi baseado no postulado de Pareto, que afirma, a maioria do efeito se origina de um pequeno número de causas (PARETO, 1964). No

contexto desta pesquisa, este postulado afirma que os artigos com maior pontuação representarão a maior parte do reconhecimento científico no conjunto bibliográfico atual (AZEVEDO; ENSSLIN; JUNGLES, 2014).

Os dados a serem extraídos seguiram as seguintes classificações: classificação da atividade da ameaça digital para a Propriedade Intelectual (dados armazenados na computação em nuvem, dados governamentais, da indústria e pessoais) e a área de estudo/pesquisa (segurança digital, inovações na segurança de dados, proteção da propriedade intelectual).

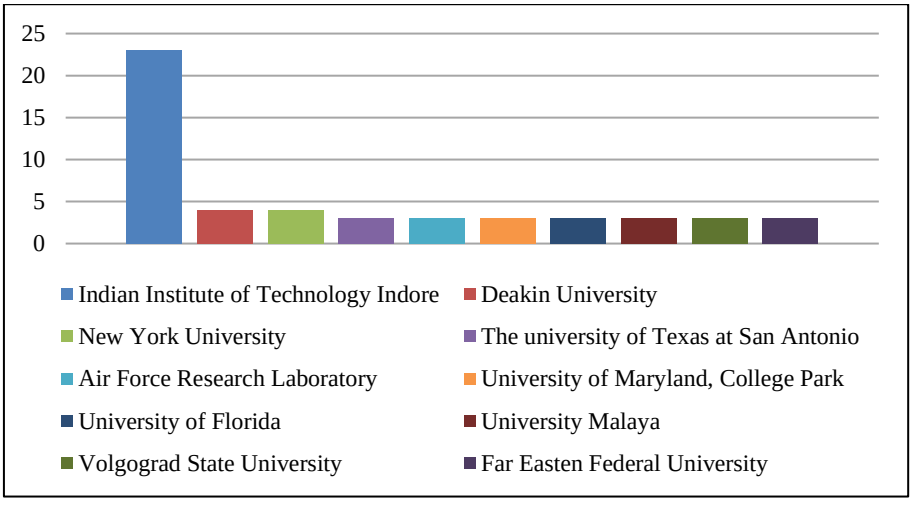
RESULTADOS E DISCUSSÃO

Bibliometria dos artigos selecionados

A busca na base de dados Scopus resultou em 247 artigos, e todos os artigos não duplicados minerados no banco de dados, que emergiram utilizando os descritores de busca, foram inicialmente considerados elegíveis para avançar para a rodada 3, sendo esta a seleção inicial dos estudos.

Observando as publicações identificadas no universo desta pesquisa a maioria dos artigos foi publicada em periódicos internacionais, sendo eles do tipo *Journal* (53,44%), *Conference Proceeding* (21,45%), *Book* (11,33%) e *Book Series* (11,33%). As principais fontes dos títulos foram; *IEEE Consumer Eletronics Magazine* (2,42%), *ACM International Conference Proceedings Series* (2,02%) e *Lecture Notes In Computer Science* (2,02%). Na Figura 2 percebemos que a maioria das publicações foram produzidas pelo *Indian Institute of Technology Indore* (9,31%).

Figura 2 – Publicações por instituição



Fonte: Elaborado pelos autores

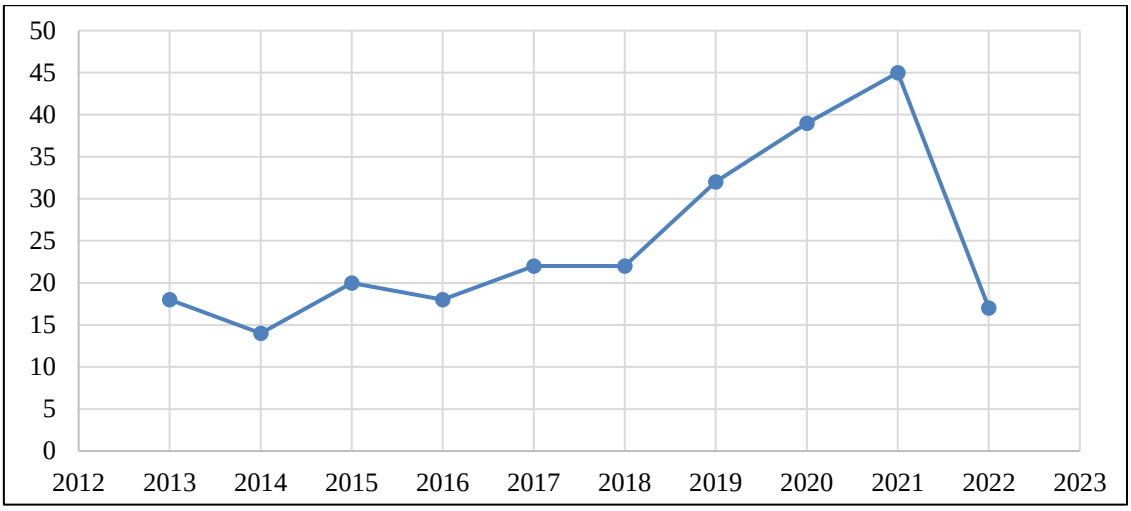
Evidenciamos que todas as publicações foram produzidas pelo grupo de pesquisa coordenado por Sengupta, A. que faz parte do quadro de pesquisadores da instituição.

Analisando mais detalhadamente os autores que mais publicaram na base de dados da pesquisa realizada, foram destacados: Sengupta, A. com surpreendente (9,31%), Rathor, M. (3,64%) e Roy, D. (1,21%).

Outro fator importante a se observar são as publicações por ano, onde pode ser verificado um crescimento significativo de publicações relevantes ao tema (Figura 3), com destaque para o ano de 2013 com 18 publicações. Em 2021 foram registradas 45 publicações, apresentando um crescimento de 250%, demonstrando um significativo interesse por pesquisadores sobre o tema "ameaças digitais na SPI".

A Figura 3 demonstra o crescimento das publicações no período pesquisado do ano de 2013 até o mês de abril do ano de 2022.

Figura 3 – Evolução das publicações por ano



Fonte: Elaborado pelos autores

Elegibilidade dos artigos

Seleção Automática de Citação e Pontuação

O sistema SCAS categorizou automaticamente 10 artigos no quadrante Q1, os quais foram aceitos automaticamente para a próxima rodada, que abordam majoritariamente métodos estratégicos ou inovações tecnológicas para mitigação dos ataques digitais, com ênfase na Segurança da Propriedade Intelectual (SPI) voltada ao Governo ou instituição na área de inovação.

Dos trabalhos categorizados no Q1, foi identificado que o principal artigo que atingiu 48 pontos pelo SCAS foi Malik, (2014). Este trabalho apresenta informações

sobre proteção da propriedade intelectual com uma nova abordagem de *watermarking* baseada em contador, sendo possível provar o roubo de propriedade intelectual em um tribunal de justiça, por meio da comprovação da titularidade e retendo os *royalties* provenientes do uso dessas invenções. Igualmente contidos neste quadrante estão pesquisas que apresentaram a afirmação que, as condições de mercado podem incentivar a pirataria. Além disso, levantam-se dúvidas sobre o argumento de que a pirataria é uma ameaça à criatividade, especialmente no ambiente digital (FROSIO, 2016). No trabalho de Fan et al., (2021), os autores apresentam novos esquemas de verificação da propriedade intelectual baseados em passaporte que são robustos para modificações de rede e resistentes a ataques de ambiguidade.

No Q3 e Q4 foram classificados 202 artigos e no quadrante Q4 186 artigos para classificação, sendo estes rejeitados para a próxima fase. Os artigos classificados no Q2 (35 artigos) que contavam com o escore de frequência de termos acima de 12 pontos foram conduzidos para seleção manual, buscando uma leitura mais aprofundada destes para posterior pontuação, sendo aceitos 28 artigos do total. A Tabela 3 descreve mais detalhadamente a quantidade de artigos incluídos por critérios de maior relevância.

Evidenciamos nessa fase que muitos artigos se referenciavam a ameaças digitais genéricas e não especificas para a segurança da propriedade intelectual.

Tabela 3 – Quantidade de artigos incluídos por critérios de seleção

Critérios adotados	Grupo de Índices	Q. de artigos
Apresenta os dois descritores no título	Inclusão (I)	8
Periódico com Fator de impacto Internacional	Inclusão (I)	4
Correlação entre as áreas temáticas	Inclusão (I)	6
Selecionado automaticamente pelo método SCAS	Inclusão (I)	10

Fonte: Elaborado pelos autores

Vários artigos foram excluídos, restando 28 artigos para as demais fases metodológicas deste estudo, visto que apresentavam pontuação relevante sobre a ótica de ocorrência dos descritores secundários no corpo textual e atenderam aos critérios propostos na fase de seleção. A Tabela 4 apresenta a quantidade de artigos excluídos por critérios de maior relevância.

Tabela 4 – Quantidade de artigos excluídos por critérios de seleção

Critérios adotados	Grupo de Índices	Q. de artigos
Não é trabalho sobre temas relacionados	Exclusão (E)	6
Não apresenta os dois descritores no título	Exclusão (E)	3
Não apresenta solução inovadora	Exclusão (E)	4
Não apresenta possibilidade de replicação do experimento	Exclusão (E)	1
É uma revisão bibliográfica	Exclusão (E)	1
Pouca aderência aos descritores primários	Exclusão (E)	2
Selecionado pelo método SCAS	Exclusão (E)	202

Fonte: Elaborado pelos autores

Extração e síntese dos dados dos trabalhos selecionados

A partir das análises apresentadas anteriormente, partiu-se para uma síntese qualitativa mais minuciosa do material selecionado, sendo possível a classificação dos artigos por meio do somatório dos valores obtidos em todas as rodadas. A partir desse ponto foi realizado um corte correspondente a 85% do somatório de todos os critérios, sendo possível chegar a somente dez artigos, mas que expressam bem o perfil dos trabalhos que abordam as principais ameaças digitais e suas formas de mitigação na Segurança da Propriedade Intelectual (SPI).

A finalidade do objetivo proposto foi alcançada na análise dos artigos apresentados na Tabela 5.

Tabela 5 - Artigos com maior pontuação após somatório da síntese de qualidade

Pontos	Autor/Título	Área de pesquisa	Proteção ameaça
48	Malik, (2014) - *Counter based approach to intellectual property protection in sequential circuits and comparison with existing approach.*	*Digital Circuits*	Clonagem
45	Mcdonald, (2016) - *Functional polymorphism for intellectual property protection.*	Circuito Eletrônico	Engenharia reversa
40	Behera, (2015) - *Different Obfuscation Techniques for Code Protection.*	Código *Software*	Pirataria
37	Sengupta, (2018) - *Protecting DSP kernels using robust hologram-based obfuscation.*	*Digital Signal Processing*	*Trojan*
31	Brandman, (2020) - *A physical hash for preventing and detecting cyber-physical attacks in additive manufacturing systems.*	*Analog/RF circuits*	*Brute-Force Attacks*
26	Palmer, (2016) - *Cracking the code: Identifying criminals using communication patterns.*	Segurança PI	Engenharia social
22	Beebe, (2017) - *Insider threat detection using time-series-based raw disk forensic analysis.*	*Forensic Analysis*	Espionagem
19	Mishra, (2021) - *Multilayer self-defense system to protect enterprise cloud.*	*Cloud Computing*	*Denial of service attacks*
14	Bickford, (2015) - *Safe Internet Browsing Using a Transparent Virtual Browser.*	*Virtual Browser*	*Malware*
13	Syed, (2022) - *Traceability in supply chains: A Cyber security analysis.*	Cyber Threats	*Ransomware*

Fonte: Elaborado pelos autores

Conforme apresentado na Tabela 5 as principais ameças para a segurança dos dados digitais na Segurnça da Propriedade Intelectual (SPI) nas instituições identificados foram:

- ***Trojan* ou cavalo de tróia**: É um *malware* muito utilizado para invasões e roubos de dados, as formas mais avançadas de trojan agem abrindo canais de comunicação entre a máquina hackeada e o cibercriminoso, as chamadas backdoors.
- ***Brute Force***: É o tipo de ataque que com uso de *software* específico baseia-se em múltiplas tentativas de combinações de login, nesse sentido, implementar o recurso que limita essas tentativas é uma maneira eficiente de impedir a execução do ataque.
- **Engenharia social**: É uma técnica empregada por criminosos virtuais para induzir usuários desavisados a enviar dados confidenciais, infectar seus computadores com *malware* ou abrir links para sites infectados.
- ***Ransomware***: É um *malware* que criptografa arquivos importantes no armazenamento local e de rede e exige um resgate para descriptografar os arquivos, os atacantes desenvolvem esse *malware* para ganhar dinheiro com extorsão digital.

Evidenciamos que não são os ataques digitais populares os mais bem-sucedidos, e sim, aqueles direcionados, limitados e principalmente sofisticados.

A Tabela 6 apresenta algumas medidas de mitigação dessas ameaças para aumentar a segurança dos dados digitais na Segurança da Propriedade Intelectual (SPI).

Tabela 6 – Medidas de mitigação

Tipo	**Ameaça**	**Mitigação**
Trojan	Clonagem e pirataria.	Uso de métodos anti-cópia e anti-clonagem, funções físicas não clonáveis.
Malware	Adulteração física e de dados sigilosos	Implementar detecção de adulteração para códigos, integrando a assinatura digital.
Brute Force	Clonagem de dispositivos IoT	Uso de mecanismo de autenticação forte, autenticação mútua e autenticação multifator.
Trojan	Engenharia reversa para extrair certificados digitais	Criptografar dados, uso de operações criptográficas resistentes à análise de canal lateral, codificar chaves de criptografia no *firmware*.
Brute Force	Uso de certificados digitais roubados para forçar autenticação	Manter os certificados digitais em locais seguros, como em um dispositivo criptográfico e módulo de segurança de *hardware.*
Cavalo de tróia	Engenharia social	Evitar compartilhamento de informações confidenciais não autorizadas, ter uma política de *cyber* segurança.
Engenharia social	Roubo de informações confidenciais	Evitar erros do usuário, falta de conhecimento ou descuido ao usar a TI, uso de política de *backup*.
DDoS	*Spam* ou ataques DDoS	Incorporar uma solução confiável de detecção e mitigação de DDoS como *firewall* moderno.
Ransomware	Ações maliciosas para exclusão de logs	Uso configurações de log corretas e auditoria regular de módulos de log para evitar erros, opções de registro externo seguro para evitar adulteração.
Ransomware / Trojan	Explorar as vulnerabilidades em o *software*	Treinar a equipe sobre *ransomware* e como eles afetam o sistema, verificar os sistemas regularmente com um bom antivírus.

Fonte: Elaborado pelos autores

Nesta revisão de escopo ficou evidenciado que existem muitas publicações direcionadas para a segurança de dados digitais, porém, poucas apresentam ênfase exclusivamente para a Segurança da Propriedade Intelectual (SPI), demonstrando haver necessidade de mais pesquisas nesta área.

CONCLUSÕES

Surgem inúmeras ameaças digitais em um curto espaço de tempo e as medidas de segurança para mitigação dos danos causados para a segurança da propriedade intelectual devem ser atualizadas e inovadas constantemente.

As ameaças estão cada vez mais modernas e são combinadas com vários tipos de ataques, o perigo pode estar dentro da instituição, sendo por um colaborador mal-intencionado ou não, que pode vazar informações confidenciais através da Engenharia social colocando em risco anos de pesquisas e comprometendo a segurança da propriedade intelectual.

Medidas como implementação de certificado e assinatura digital, criptografia de dados, autenticação forte, treinamento de equipe, uso de *firewall* modernos e bem configurados, uso de antivírus, política de *backup* e uma política de cibersegurança se mostram eficientes na mitigação dessas ameaças.

Segurança digital será sempre necessário, e as instituições devem cada vez mais investir em ciência, tecnologia e inovação para manter segura e protegida a propriedade intelectual institucional.

REFERÊNCIAS

AZEVEDO, Rogério Cabral De; ENSSLIN, Leonardo; JUNGLES, Antônio Edésio. A Review of Risk Management in Construction: Opportunities for Improvement. **Modern Economy**, v. 05, n. 04, p. 367–383, 2014. DOI: 10.4236/me.2014.54036.

BEEBE, Nicole; LIU, Lishu; YE, Zi. Insider Threat Detection Using Time-Series-Based Raw Disk Forensic Analysis. In: **IFIP International Conference on Digital Forensics**. Springer, Cham, 2017. p. 149-167.

BEHERA, Chandan Kumar; BHASKARI, D. Lalitha. Different obfuscation techniques for code protection. **Procedia Computer Science**, v. 70, p. 757-763, 2015.

BICKFORD, Jeffrey; GIURA, Paul. Safe internet browsing using a transparent virtual browser. In: **2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing**. IEEE, 2015. p. 423-432.

BRANDMAN, Josh et al. A physical hash for preventing and detecting cyber-physical attacks in additive manufacturing systems. Journal of Manufacturing Systems, v. 56, p. 202-212, 2020.

CHANDLER, Jacqueline; CUMPSTON, Miranda; THOMAS, James; HIGGINS, Julian PT; DEEKS, Jonathan J.; CLARKE, Mike J. **Cochrane Capítulo I: Introdução | Treinamento**. 2021. Disponível em: https://training.cochrane.org/handbook/current/chapter-i.

FAN, Lixin et al. Deepip: Deep neural network intellectual property protection with passports. **IEEE Transactions on Pattern Analysis and Machine Intelligence**, 2021.

FROSIO, Giancarlo. Digital piracy debunked: A short note on digital threats and intermediary liability. **Internet Policy Review**, v. 5, n. 1, 2016.

GOMES, Rita de Cássia Medeiros. O direito e a propriedade intelectual: constitucionalização, campo de atuação e responsabilidade a violação do direito. **PIDCC–Revista de Propriedade Intelectual–Direito Contemporâneo e Constituição, Aracaju, ano IX**, v. 1, n. 01, p. 60-82, 2020.

HIGGINS, Julian; THOMAS, James; CHANDLER, Jacqueline; CUMPSTON, Miranda; LI, Tianjing; PAGE, Matthew J.; WELCH, Vivian A. **Manual de Cochrane para Revisões Sistemáticas de Intervenções 6.1**. 2. ed. Oxford UK: Wiley-Blackwell, 2020. v. 1

HITAJ, Dorjan; HITAJ, Briland; MANCINI, Luigi V. Evasion attacks against watermarking techniques found in MLaaS systems. In: **2019 Sixth International Conference on Software Defined Systems (SDS)**. IEEE, 2019. p. 55-63.

IMRAN, Muhammad; FAISAL, Muhammad; ISLAM, Noman. Problems and Vulnerabilities of Ethical Hacking in Pakistan. In: **2019 Second International Conference on Latest trends in Electrical Engineering and Computing Technologies (INTELLECT)**. IEEE, 2019. p. 1-6.

LAPES, Laboratório de Pesquisa em Engenharia de Software. **StArt — LaPES - Laboratório de Pesquisa em Engenharia de SoftwareLaPES-Laboratório de Pesquisa em Engenharia de Software**, 2005. Disponível em: http://lapes.dc.ufscar.br/tools/start_tool.

MACHADO, J. dos S.; HOLANDA, F. S. R.; SANTOS, L. D. V. .; BANDEIRA, A. A. .; MENEZES, A. C. .; NOGUEIRA, T. A. . Proteção da Propriedade Intelectual: uma revisão da segurança dos dados digitais e seus desafios. **Conjecturas**, [S. l.], v. 22, n. 5, p. 76–92, 2022. DOI: 10.53660/CONJ-908-I14. Disponível em: http://www.conjecturas.org/index.php/edicoes/article/view/908. Acesso em: 9 maio. 2022.

MALIK, Siddhant. Counter based approach to intellectual property protection in sequential circuits and comparison with existing approach. In: **2014 International Conference on Circuits, Systems, Communication and Information Technology Applications (CSCITA)**. IEEE, 2014. p. 48-53.

MCDONALD, Jeffrey T. et al. Functional polymorphism for intellectual property protection. In**: 2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)**. IEEE, 2016. p. 61-66.

MISHRA, Shailendra; SHARMA, Sunil Kumar; ALOWAIDI, Majed A. Multilayer self-defense system to protect enterprise cloud. **Computers, Materials & Continua**, v. 66, n. 1, p. 71-85, 2021.

MITCHELL, Nicholas J.; ZUNNURHAIN, Kazi. Vulnerability scanning with Google cloud platform. In: **2019 International Conference on Computational Science and Computational Intelligence (CSCI)**. IEEE, 2019. p. 1441-1447.

MUNN, Zachary; PETERS, Micah D. J.; STERN, Cindy; TUFANARU, Catalin; MCARTHUR, Alexa; AROMATARIS, Edoardo. Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach. **BMC Medical Research Methodology**, v. 18, n. 1, p. 1–7, 2018. DOI: 10.1186/S12874-018-0611-X/TABLES/1. Disponível em: https://bmcmedresmethodol.biomedcentral.com/articles/10.1186/s12874-018-0611-x.

OCTAVIANO, Fábio R.; FELIZARDO, Katia R.; MALDONADO, José C.; FABBRI, Sandra C. P. F. Semi-automatic selection of primary studies in systematic literature reviews: is it reasonable? **Empirical Software Engineering**, v. 20, n. 6, p. 1898–1917, 2015. DOI: 10.1007/s10664-014-9342-8. Disponível em: http://link.springer.com/10.1007/s10664-014-9342-8.

OCTAVIANO, Fábio; SILVA, Cleiton; FABBRI, Sandra. Using the SCAS strategy to perform the initial selection of studies in systematic reviews: an experimental study. *In*: 2016, **Anais** [...]: Association for Computing Machinery, 2016. p. 1–10. DOI: 10.1145/2915970.2916000. Disponível em: https://doi.org/10.1145/2915970.2916000.

PALMER, Adrian. Cracking the code: identifying criminals using communication patterns. **Computer Fraud & Security**, v. 2016, n. 5, p. 5-7, 2016.

PARETO, Vilfredo. **Cours d'économie politique**. Librairie Droz, 1964. v. 1

RATHOR, Mahendra; SENGUPTA, Anirban. IP core steganography using switch based key-driven hash-chaining and encoding for securing DSP kernels used in CE systems. **IEEE Transactions on Consumer Electronics**, v. 66, n. 3, p. 251-260, 2020.

SANABRIA-BORBÓN, A. et al. Analog/RF IP protection: Attack models, defense techniques, and challenges. **IEEE Transactions on Circuits and Systems II: Express Briefs**, v. 68, n. 1, p. 36-41, 2020.

SENGUPTA, Anirban; RATHOR, Mahendra. Enhanced security of DSP circuits using multi-key based structural obfuscation and physical-level watermarking for consumer electronics systems. **IEEE Transactions on Consumer Electronics**, v. 66, n. 2, p. 163-172, 2020.

SENGUPTA, Anirban; RATHOR, Mahendra. Protecting DSP kernels using robust hologram-based obfuscation. **IEEE Transactions on Consumer Electronics**, v. 65, n. 1, p. 99-108, 2018.

SENGUPTA, Anirban. Hardware security of CE devices [hardware matters]. **IEEE Consumer Electronics Magazine**, v. 6, n. 1, p. 130-133, 2017.

SENGUPTA, Anirban. Intellectual property cores: Protection designs for CE products. **IEEE Consumer Electronics Magazine**, v. 5, n. 1, p. 83-88, 2016.

SLAMET, Cepy; RAHMAN, Ali; RAMDHANI, Muhammad Ali; DARMALAKSANA, Wahyudin. Clustering the verses of the Holy Qur'an using K-means algorithm. **Asian Journal of Information Technology**, v. 15, n. 24, p. 5159–5162, 2016. Disponível em: http://digilib.uinsgd.ac.id/5117/1/5159-5162 Clustering the Verses of the Holy Quran using K-Means Algorithm.pdf.

SOUZA, Raul Carvalho; FERNANDES, Jorge Henrique Cabral. Um estudo sobre a confiança em segurança da informação focado na prevenção a ataques de engenharia social nas comunicações digitais. **Brazilian Journal of Information Science: research trends**, v. 10, n. 1, 2016.

STJEPANDIĆ, Josip; LIESE, Harald; TRAPPEY, Amy JC. Intellectual property protection. In: **Concurrent Engineering in the 21st Century**. Springer, Cham, 2015. p. 521-551.

SYED, Naeem Firdous et al. Traceability in supply chains: A Cyber security analysis**. Computers & Security**, v. 112, p. 102536, 2022.

TORTEN, Ron; REAICHE, Carmen; BOYLE, Stephen. The impact of security awarness on information technology professionals' behavior. **Computers & Security**, v. 79, p. 68-79, 2018.

Recebido em: 20/05/2022

Aprovado em: 25/06/2022

Publicado em: 29/06/2022