Universidade Federal de Pernambuco

Centro de Informática

Departamento de Informática

Sistemas de Informação

Antônio Correia de Azevedo Júnior

Os Riscos das Plataformas Sociais na Segurança Corporativa

Trabalho de Graduação

Recife

2017

Antônio Correia de Azevedo Júnior

Os Riscos das Plataformas Sociais na Segurança Corporativa

Trabalho de Graduação apresentado à graduação em Sistemas de Informação do Centro de Informática da Universidade Federal de Pernambuco como requisito para obtenção do grau de Bacharel em Sistemas de Informação.

Orientador: Hermano Perrelli de Moura
Coorientador: Gliner Dias Alencar

Recife
2017

À Drielly Kelly, pessoa com quem amo partilhar a vida. Com você tenho me sentido mais vivo de verdade. Obrigado pelo carinho, a paciência e por sua capacidade de me trazer paz na correria de cada semestre.

AGRADECIMENTOS

Aos meus pais, pelo amor, incentivo e apoio incondicional.

À minha irmã, que por mais difícil que fossem as circunstâncias, sempre teve paciência e confiança.

À minha namorada que independente do estresse cotidiano, sempre esteve disposta a me ajudar uma vez mais.

Ao professor Hermano, pela orientação e apoio.

Ao Gliner por suas dicas sempre certeiras, oferecendo um novo olhar para a pesquisa.

“Acho que vírus de computador deve contar como vida. Creio que dizem algo sobre a natureza humana que a única forma de vida que criamos até agora é puramente destrutiva. Nós criamos vida à nossa própria imagem.”
- Stephen Hawking

RESUMO

No ramo da segurança, as redes sociais sempre trouxeram grandes riscos e duvidas para as empresas, seja por sua utilização em si ou pelas consequências de seu uso. Seus riscos vão muito além da perda de produtividade dos funcionários ou vazamento de dados. Assim, há a necessidade de uma análise sob um espectro mais amplo. Este trabalho destina-se a produção de um mapeamento sistemático da literatura dos riscos das plataformas sociais na segurança corporativa. O mesmo elenca pesquisas relevantes relacionadas aos riscos das redes sociais, analisa as evidencias encontradas, além de listar os principais riscos e impactos enfrentados pelas organizações neste âmbito, e o que as mesmas normalmente fazem para se proteger. Além disso, provê uma base para novas pesquisas relacionadas aos riscos das redes sociais no ambiente corporativo.

Palavras-chave: redes sociais, riscos, segurança corporativa, empresas.

ABSTRACT

Regarding the security field, social media have always brought great risks and uncertainties for companies, either by its own use or by the consequences of its use. Their risks go beyond the loss of employee productivity or data leakage. Therefore, there is a need for an analysis from a broader spectrum. This project aims to produce a systematic mapping of the literature regarding the risks of social media in the corporate security. Moreover, the present study lists relevant research related to the risks of social media and analyses the evidence found throughout the research. Besides that, this project names the main risks and impacts faced by organisations and which actions they normally take in order to protect themselves. In addition, it provides a basis for further research related to the risks of social media in the corporate environment.

Keywords: Social media, risks, corporate security, organisations.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS E SIGLAS

CE	Criterio de Exclusão
CI	Critério de inclusão
IEEE	Instituto de Engenheiros Eletricistas e Eletrônicos
TI	Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO

Neste capitulo é realizada a contextualização do tema principal bem como as motivações para sua escolha, logo após é exposto o problema de pesquisa e os objetivos na realização deste trabalho, finalizando com a estrutura completa do trabalho.

1.1 Contextualização

No mundo moderno ao qual fazemos parte, as Plataformas Sociais (ou Redes Sociais[1]) fazem parte da vida da maioria das pessoas, segundo pesquisa realizada pelo centro de pesquisa (PEW RESEARCH CENTER, 2016) em cada 10 pessoas, 8 fazem uso de redes sociais; de forma generalista, isso se traduz em uma empresa possuir 80% de sua equipe (no mínimo) acessando as redes sociais. Dada a normalidade do acesso as redes sociais na atualidade, esses são números considerados normais, entretanto, os riscos que todo esse acesso pode causar é algo alarmante.

Segundo dados do (PONEMON INSTITUTE, 2012) para 63% dos profissionais de segurança em TI, o uso das mídias sociais traz sérios riscos para as organizações, cerca de 52% dizem haver aumentos consideráveis nos ataques de malwares transmitida pela rede, quando permitido o uso das redes sociais; se isso já não bastasse, apenas 29% desses profissionais possuem ferramentas de controle e mitigação desses riscos.

De acordo com o (CERT.BR, 2017) os riscos envolvendo as redes sociais e sua utilização são os mais variados, iniciando pelo simples vazamento de dados de forma ingênua, passando por tentativas de engenharia social através das plataformas sociais e podendo chegar a invasões e ataques de vírus, fazendo destes casos, questões importantes para qualquer pessoa e empresa.

Ao identificar e analisar os riscos do fator humano, abstraindo itens como servidores, fluxo de redes e outros itens técnicos, podemos facilmente elaborar formas de conter o surgimento destes riscos, diretamente nas pessoas envolvidas, criando procedimentos internos para mitigar problemas simples como vazamentos acidentais de dados, além de no processo, garantir a segurança individual dos funcionários dentro e fora da empresa.

A produção científica tem como objetivo a captura da realidade para análise e, posteriormente a produção de informações, a discussão sobre os riscos das redes sociais na segurança corporativa, possui um aspecto pratico muito relevante, como

[1] Neste trabalho, o termo “Redes Sociais” tem o mesmo valor que “Plataformas Sociais”, sendo utilizado para simplificar o texto e dar ênfase neste tipo de plataforma.

já mencionado, além de sua importância no meio acadêmico (RODRIGUES.A.DE.J, 2006). Neste contexto, a produção de novos estudos neste tema, podem iniciar um processo de transformação sócio cultural nas empresas e nas pessoas, tornando este tipo de pesquisa de segurança das redes sociais nas empresas, cada vez mais necessário e pertinente.

1.2 Problema de pesquisa

Sabendo-se que as redes sociais estão em constante expansão no mundo e nas empresas (JUE *et al.*, 2011), observa-se que seus riscos no meio corporativo têm acompanhado seu crescimento acelerado, coloca-se como principal problema de pesquisa a seguinte questão: Quais os riscos que as plataformas sociais podem trazer para a segurança corporativa?

1.3 Objetivos

1.3.1 Objetivo geral

Este trabalho tem como objetivo geral mapear estudos que abordam os riscos das plataformas sociais na segurança corporativa.

O objetivo do trabalho é atingido através da condução de um Mapeamento Sistemático da Literatura de segurança da informação com ênfase nas redes sociais e seu impacto nas corporações.

1.3.2 Objetivos específicos

Para ser possível atingir o objetivo geral do trabalho, é necessária a definição de objetivos específicos que irão ajudar na consecução da pesquisa, são eles:

1) Identificar os riscos que mais ocorrem nas empresas em decorrência do uso das redes sociais;
2) Identificar os impactos causados pelas plataformas sociais na segurança da corporação;
3) Identificar as medidas tomadas para evitar e mitigar eventuais riscos na utilização das plataformas sociais.

1.4 Estrutura do trabalho

Este trabalho apresenta seus resultados ao longo de mais 4 capítulos, logo no capítulo 2 são abordados conceitos básicos relacionados a redes sociais, engenharia

social, malwares e outros temas abordados durante a pesquisa. No capítulo 3 é detalhada a metodologia de pesquisa utilizada, as definições e os métodos que foram adotados ao longo deste Mapeamento Sistemática da Literatura. O 4º capítulo relata a condução da pesquisa em si, a forma que foi realizada e seus resultados. Por fim, o 5º capítulo trata da conclusão do estudo e os trabalhos futuros que podem ser desenvolvidos.

2 REFERENCIAL TEÓRICO

Este capítulo apresenta os principais tópicos relacionados à redes sociais e os riscos de seu uso no cotidiano das empresas, como engenharia social, malwares e perdas de dados.

2.1 Redes sociais

As redes sociais segundo (NOGUEIRA, 2010) são: “o meio onde as pessoas se reúnem por afinidades e com objetivos em comum, sem barreiras geográficas e fazendo conexões com dezenas, centenas e milhares de pessoas conhecidas ou não.”

De forma mais abrangente, de acordo com (CASTRO, 2013):

> “As Redes Sociais representam um conjunto de participantes autônomos, unindo ideias e recursos em torno de valores e interesses compartilhados. A questão central das redes é a valorização dos elos informais e das relações, em detrimento das estruturas hierárquicas. As redes sociais são exatamente as relações entre os indivíduos na comunicação mediada por computador. Esses sistemas funcionam através da interação social, buscando conectar pessoas e proporcionar sua comunicação.”

De formas diferentes, essas citações expressam bastante o que podemos esperar do significado de uma rede social, algo que sirva para o meio de comunicação, propaganda e entretenimento, para que pessoas e empresas se conectem e se apresentem; para que sirva de ambiente de compartilhamento de experiências e vivencias no geral.

No geral, para participar da maioria das redes sociais, primeiramente deve-se fazer um cadastro no site com alguns dados pessoais (verdadeiros ou não, raramente há confirmações), estes dados servirão como seu perfil, que nada mais é, do que seu “cartão de visita” nesta rede social.

A partir deste momento, o usuário torna-se mais um da rede, podendo criar mensagens, postar fotos, itens de sua vida e até seu próprio currículo (em algumas redes voltadas para o mercado de trabalho); onde mediante seus gostos, vai poder entrar em contato com outros usuários ou grupos de usuários que tenham “assuntos” em comuns.

De acordo com (VEERACHT, 2015),

> O valor da rede social de cada usuário está exponencialmente ligado ao número de pessoas que se encontram nesta rede. Como se pode

> verificar, a designação de “amigo” nas redes sociais é usada de forma bastante alargada, pois basta que um usuário aceite um pedido de amizade (“friendrequest”) de outro indivíduo para que este figure na sua “lista de amigos”. A lista de amigos de uma pessoa é considerada, por muitos, um espelho da sua popularidade online. Há quem se considere mais popular de acordo com a quantidade de “amigos” que tiver nessa lista. Uma das atividades mais praticadas pelos internautas nas redes sociais é navegar pelos perfis à procura de pessoas com um determinado perfil para lhes enviar pedidos de amizade e, assim, estabelecer algum tipo de contato com elas.

Como já dito anteriormente, algumas pessoas não colocam seus dados verdadeiros nas informações de seu perfil, devido à alta exposição na rede social; entretanto, outras “pessoas não colocam seus dados verdadeiros por motivos obscuros, como roubar dados de outros usuários, fazer engenharia social e etc.” (BUCCO, 2016).

2.2 Engenharia social

A engenharia social, popularmente conhecida como a arte e a ciência de hackear seres humanos (SANTIAGO PONTIROLI, 2013), recebeu um aumento exponencial em sua aplicação, devido ao aumento do uso das redes sociais bem como a vida mais “on-line” das pessoas.

De acordo com (SANTIAGO PONTIROLI, 2013):

> “No campo da segurança da informação, este termo [engenharia social] é amplamente usado para fazer referência a um conjunto de técnicas usadas por cibercriminosos para manipular as suas vítimas com o objetivo de obter informações confidenciais ou convencê-las a executar ações que comprometam seu sistema.”

A engenharia social opera a partir da premissa: “O ser humano é o elo mais fraco na segurança da informação” (FIGUEIRÓ, 2010), onde os hackers passam a estudar suas vítimas e conseguem que elas passem dados que serão usados para o cometimento de crimes e ou até ajudar a invasão de suas contas; pois é muito mais fácil conseguir uma senha através de um usuário que “fala demais” do que invadir um complexo sistema de segurança.

A engenharia social tem duas modalidades de ataque:

- Ataques diretos: O atacante entra diretamente em contato com a vítima por e-mail, telefone, ou pessoalmente, os ataques diretos têm alvo fixo, ou seja, o engenheiro social sabe exatamente quem atacar, como e porquê.
- Ataques indiretos: São aqueles que não tem um alvo específico, um ótimo exemplo é um trecho retirado do livro “A arte de enganar” (SIMON, 2001): “Você

> está em um elevador quando, de repente, um disquete cai no chão, você olha tem um logotipo de uma grande empresa e a frase ”histórico salarial“, movido pela curiosidade você abre o disquete em sua casa e talvez haja um ícone para o Word então ao clicar aparece a frase ‘ocorreu um erro ao tentar abrir o arquivo’, você não sabe mas um backdoor foi instalado em sua máquina. Você imediatamente leva o disquete até o setor responsável em devolvê-lo ou guardá-lo, o setor por sua vez também abrirá o disquete, agora o hacker tem acesso a dois computadores. . . ” esse é um exemplo de ataque indireto, ou seja, não teve uma vítima definida desde o início.

Podemos traçar um paralelo com o livro, Prenda-me se For Capaz (SPIELBERG, 2003), onde é retratado um engenheiro social, Frank Abagnale, um engenheiro social muito famoso na década de 60, que conseguiu enganar a “todos” apenas com conversas; diante disso, fica claro que mesmo numa epoca em que não haviam tantos computadores, já era possível roubar dados ou “enganar as pessoas” apenas aproveitando-se da falta de atenção da vítima.

2.3 Malware

Malwares são pequenos programas maliciosos, sendo esta palavra (malware) uma forma de generalização de todos os programas maliciosos que podem causar danos a sistemas de indivíduos e empresas, seja, um sistema de computador, servidor, celular e outros.

Segundo a (BITDEFENDER, 2017) Malware é um termo proveniente do inglês: **malicious software**; é um software destinado a se infiltrar em um sistema de computador (no termo mais geral da palavra) de forma ilícita, com o objetivo de causar algum dano ou roubo de informações, os vírus de computador, worms, trojan horses (cavalos de troia) e spywares são exemplo de malwares.

Atualmente o malware que está em ascensão é chamado de ramsomware (CARDOSO, 2016), especializado em rapto de dados de computadores e seus sistemas operacionais utilizando criptografia para este fim; normalmente exige que o usuario infectado pague uma soma de dinheiro virtual (ex: bitcoin) para que tenha acesso novamente a seu computador e os dados que ele continha.

De acordo com a (LAB, 2017)tentativas de infecção por malware que visam roubar dinheiro via acesso on-line a contas bancárias foram registradas em 288 mil computadores usuários, cerca de 479.528.279 ataques maliciosos foram registrados e repelidos a partir de recursos online localizados em 190 países em todo o mundo; esta é a realidade dos códigos maliciosos, trojans sempre tentando invadir a segurança

do usuário e roubar seus dados e vírus procurando brechas para invasões em larga escala.

Atualmente a maioria dos malwares são desenvolvidos para gerar lucro para o criador ou simplesmente capturar dados, sejam eles bancários, empresariais ou apenas qualquer dado que seu "código" ache importante, por exemplo, o ransonware que exige o pagamento de um resgate para a liberação (CENTER, 2016).

2.4 Vazamento de dados

O vazamento de dados de acordo com (ROHR, 2015) ocorre quando informações que não deveriam ser públicas são disponibilizadas na web por um usuário desatento, ou por um invasor que obteve acesso aos dados. Essas duas formas de perdas de dados não são as únicas, mas para este tema, são as mais pertinentes.

Quando os dados são perdidos por um usuário mais desatento, pode-se expor um dado sigiloso da empresa, um possível segredo de marketing ou algo que possa ser utilizado contra a mesma; normalmente este tipo de "engano" ocorre em redes sociais ou grupos de conversas na web, como fóruns.

Segundo (CARRARETTO, 2017) os vazamentos de dados tem muitas formas de acontecer, tanto os não intencionais quanto os intencionais, algumas delas são:

I) **Vazamento não intencional:**

- Comentários e mensagens de erros em scripts, programas e similares
- Metadados "escondidos" em arquivos
- Informações disponíveis na rede (br, Who.is e informações indexadas por ferramentas de busca e outras)
- Perda de mídias removíveis (Pen Drive, HD, CD/DVD e Cartões de Memória)
- Conversas em locais públicos
- Postagens em Mídias Sociais
- Envio de informações conídenciais por e-mail
- Material esquecido em impressoras no escritório
- Material deixado em cima de mesas e em salas de reunião
- Falta de cuidado no descarte de informações
- Envio de informações para contas pessoais

II) **Vazamento intencional**

- Roubo de informações através de malwares
- Furto de dispositivos móveis e/ou mídias de armazenamento
- Cópias e/ou ílmagens
- Hacking
- Acesso autorizado sem monitoramento e através de cópias em mídias removíveis
- Engenharia Social

3 METODOLOGIA DE PESQUISA

Este capítulo trata da metodologia utilizada nesta pesquisa. A mesma se caracteriza como uma pesquisa descritiva, bibliográfica e quantitativa. Além de abordar o mapeamento sistemático e suas etapas.

3.1 Natureza da pesquisa

3.1.1 Quanto aos objetivos

Este trabalho tem como objetivo a produção de um Mapeamento Sistemático da Literatura nos riscos das redes sociais na segurança corporativa, apontando as principais pesquisas neste tema.

Na pesquisa descritiva realiza-se o estudo, a análise, o registro e a interpretação dos fatos do mundo físico sem a interferência do pesquisador (BARROS; LEHFELD, 2007); com a finalidade de realizar a observação, registro e analise dos fenômenos ou sistemas técnicos, sem entrar no mérito dos conteúdos.

Desta forma, através dos fatores apresentados e o objetivo tratado anteriormente, pode-se concluir que esta pesquisa é caracterizada como descritiva.

3.1.2 Quanto aos procedimentos

Foi realizada uma pesquisa de caráter bibliográfico com a função de mapear os conceitos fundamentais nos riscos provenientes do uso de redes sociais no ambiente corporativo, para a realização deste trabalho de mapeamento sistemático.

De acordo com (FONSECA, 2002, p. 32):

> A pesquisa bibliográfica é feita a partir do levantamento de referências teóricas já analisadas, e publicadas por meios escritos e eletrônicos, como livros, artigos científicos, páginas de web sites. Qualquer trabalho científico inicia-se com uma pesquisa bibliográfica, que permite ao pesquisador conhecer o que já se estudou sobre o assunto. Existem, porém pesquisas científicas que se baseiam unicamente na pesquisa bibliográfica, procurando referências teóricas publicadas com o objetivo de recolher informações ou conhecimentos prévios sobre o problema a respeito do qual se procura a resposta.

Com isso, conclui-se que esta pesquisa é quesito importante e inviável de remoção de qualquer estudo cientifico, para que seu embasamento teórico seja consistente.

3.1.3 Quanto a forma de abordagem

Segundo (FONSECA, 2002, P. 20) a respeito das pesquisas quantitativas: “Diferentemente da pesquisa qualitativa, os resultados da pesquisa quantitativa podem ser quantificados. Como as amostras geralmente são grandes e consideradas representativas da população, os resultados são tomados como se constituíssem um retrato real de toda a população alvo da pesquisa.”

Onde (HAYATI; KARAMI; SLEE, 2006, p. 361-394) relata que a aplicação de métodos quantitativos de investigação, permitem chegar a verdades universais. Sob esta ótica os resultados da pesquisa são reprodutíveis e generalizáveis.

Desta forma, esta pesquisa tem perfil quantitativo, em vista que um mapeamento sistemático tem como resultado a extração de uma visão global da área foco de pesquisa, assim identificando a quantidade de pesquisas realizadas na área.

3.2 Definição da amostra

Conforme (LUCIO; COLLADO; LUCIO, 2013), na amostra probabilística a escolha dos elementos ocorre independentemente da sua probabilidade, estando relacionada às características da pesquisa ou da forma de pesquisa.

Enquanto (MATTAR, 1996) explica que: “A Amostragem não probabilística é aquela em que a seleção dos elementos da população para compor a amostra depende ao menos em parte do julgamento do pesquisador ou do entrevistador no campo”. A partir de (Loyola, 1992) ressaltamos que a amostragem não probabilística de julgamento é utilizada em pesquisas quando o pesquisador se sente familiarizado com as características relevantes à população.

Por conseguinte, nesta pesquisa, optou-se por realizar a pesquisa em forma de amostragem de julgamento, devido a familiarização do pesquisador para julgar quais trabalhos serão relevantes.

3.3 Mapeamento Sistemático da Literatura

Mapeamentos sistemáticos são estudos capazes de prover uma informação geral a cerca de uma determinada área, como seu principal objetivo.

(KITCHENHAM *et al.*, 2007) diz que o mapeamento sistemático é uma revisão abrangente de estudos em uma área especifica, buscando identificar as evidencias que estão disponíveis na área. Em uma das principais obras encontradas sobre o assunto, (PETERSEN *et al.*, 2008) afirmam que “um mapa sistemático é um método definido de construir um esquema de classificação e estrutura em um campo de interesse”.

Este tipo de metodologia foi utilizada anteriormente no trabalho de graduação de (MOREIRA, 2016) tratando sobre desenvolvimento ágil de software, bem como no Trabalho de pesquisa do grupo de pesquisa do amazonas, (VALENTIM; SILVA; CONTE, 2017) a respeito de desenvolvimento de software.

3.3.1 Etapas do Mapeamento Sistemático da Literatura

Normalmente o Mapeamento Sistemático da Literatura segue uma espécie de modelo, com etapas para realizar a pesquisa corretamente, este modelo ganha o nome de protocolo, que irá possuir o conjunto de regras que irá reger toda a pesquisa e ajudará a definir como será a pesquisa e sob quais critérios ela será baseada (KITCHENHAM; CHARTERS, 2007).

Segundo (PETERSEN *et al.*, 2008) o mapeamento deve ser dividido em 2 etapas, onde a partir destas etapas podemos dividir em 6 fases mais simples; a primeira etapa consiste no planejamento do mapeamento, que de antemão é dividido em duas fases, a primeira responsável pela análise da necessidade e ou viabilidade do mapeamento, enquanto, a 2º fase estipula uma proposta do mapeamento, ao mesmo tempo em que delimita o escopo da literatura a ser analisada.

A 2º etapa é dividida em 4 fases, e é responsável pela condução da revisão; a divisão ocorre da seguinte forma, 3º etapa identifica as pesquisas similares que podem participar do mapeamento, logo em seguida a quarta etapa analisa estes estudos selecionados e promove uma espécie de filtro através de indicadores já definidos no protocolo.

A quinta fase realiza a avaliação da qualidade dos estudos que sobraram depois da fase anterior, normalmente analisando se as questões podem ser respondidas através dos estudos selecionados até o momento; por fim é possível reportar os dados coletados durante a pesquisa.

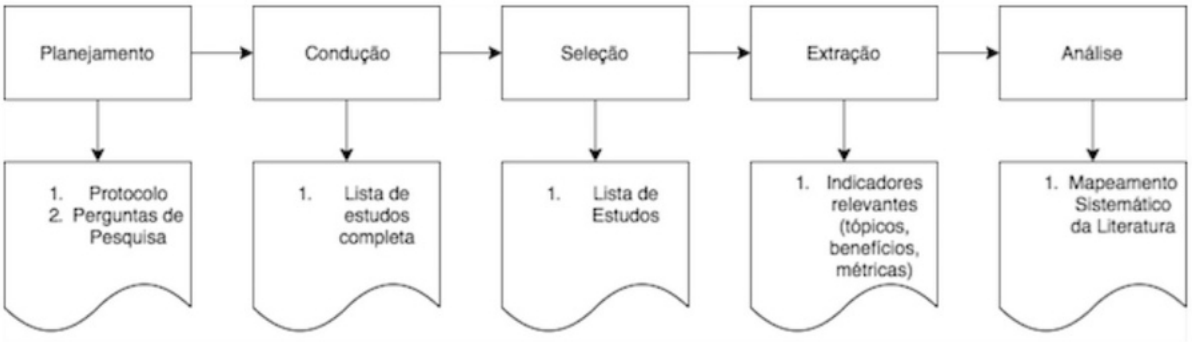
4 CONDUÇÃO DO MAPEAMENTO SISTEMÁTICO DA LITERATURA

Este capítulo trata sobre como a pesquisa foi realizada, desde o planejamento até sua conclusão; primeiramente o processo de planejamento, logo em seguida o protocolo que geriu a pesquisa e por fim os resultados.

4.1 Processo de planejamento

O processo descrito na imagem 1 foi baseado no processo de planejamento de (Silva R. et. al, 2011), iniciando-se pela fase de planejamento, responsável pela definição dos itens do protocolo e das perguntas de pesquisa, logo em seguida a etapa de condução que elabora a lista de estudos sem filtragem. A etapa de seleção é responsável por gerir a filtragem de conteúdo (lista de estudos), aplicando os filtros que serão detalhados posteriormente. A extração dos dados se deu a partir dos artigos selecionados na 3º etapa. Após, ocorre a análise e síntese dos dados, encerrando o mapeamento.

Figura 1 – Processo de Planejamento do Mapeamento Sistemático, baseado no de (Silva R.et. al, 2011).



4.2 Protocolo

(KITCHENHAM *et al.*, 2007) diz que o protocolo de mapeamento especifica os métodos que serão usados para realizar um mapeamento sistemático específico, fazendo que este diminua a possibilidade de viés do pesquisador.

O processo de planejamento deste mapeamento foi projetado com base no proposto por (KITCHENHAM; CHARTERS, 2007) e foi dividido em seis etapas: Especificação da pergunta de pesquisa, especificação da estratégia de busca, buscas experimentais e estratégia de seleção, estratégia de extração e resultados; visando a redução da complexidade e melhor adequação ao objetivo da pesquisa.

4.2.1 Perguntas de pesquisa

Este trabalho apresenta o resultado de um Mapeamento Sistemático da Literatura orientado pela pergunta de pesquisa: *"Quais riscos as plataformas sociais podem trazer para a segurança corporativa?",* a partir da mesma torna-se possível elencar os pontos mais relevantes e mais investigados no tema da pesquisa.

Dessa forma, este trabalho pode auxiliar no desenvolvimento de pesquisas no tema, de forma mais focada em algum dos pontos levantados, sem que o tempo seja gasto em uma investigação primaria já realizada previamente.

Entretanto alcançar a resposta da questão principal é algo complexo, para suavizar este processo, foram desenvolvidas 3 questões especificas de pesquisa, com o objetivo de responder à questão de pesquisa principal, são elas:

1) PP1: Quais os riscos que mais ocorrem nas empresas em decorrência do uso das redes sociais?
2) PP2: Quais são os impactos das plataformas sociais na segurança das corporações?
3) PP3: Quais medidas vêm sendo tomadas para mitigar ou reduzir incidentes deste tipo?

4.2.2 Estratégia de busca

Conforme (KITCHENHAM; CHARTERS, 2007), o mapeamento sistemático tem como função encontrar estudos primários que tem relação com a pergunta de pesquisa. Para que isso seja realizado da melhor forma possível é necessário que a estratégia de busca seja rigorosa, fazendo com que a busca seja imparcial, pois a mesma é um dos fatores que diferenciam um mapeamento sistemático de uma mapeamento tradicional.

Em resumo, a estratégia de busca é a etapa onde cria-se a string de pesquisa, seguindo os seguintes passos:

1) Divide-se a questão principal de pesquisa em termos objetivos;
2) A partir destes termos, lista-se uma serie de sinônimos e termos associados;
3) Realiza-se a tradução de todos os termos para a língua inglesa;
4) Por fim, é realizado o agrupamento dos termos, utilizando operadores lógicos AND e OR além de adicionar aspas duplas nos termos com mais de uma palavra. Ex: "Social Networking".

Definida qual será a estratégia, começamos as fases para a criação da string, primeiramente são separados os termos da questão principal, em seguida são definidos os sinônimos necessários a pesquisa.

Quadro 1 – Sinônimos (à direita) dos principais termos

Sinônimos dos principais termos	
plataformas sociais	"redes sociais"
	"midias sociais"
corporações	compania
	empresa
	corporação
segurança	"segurança da informação"
	riscos
	segurança

Produzido pelo Autor

A terceira e quarta etapas tiveram como objetivo a tradução dos termos para a língua inglesa bem como o agrupamento com os operadores lógicos, além da escolha dos melhores termos para serem adicionados a string de busca.

Quadro 2 – Tradução (à direita) dos termos da pesquisa

Tradução dos termos da pesquisa	
social platforms	"social networks"
	"social media"
corporations	company
	enterprise
	corporation
security	"Information security"
	risks
	safety

Produzido pelo Autor

Por fim, o resultado é a string de busca na forma abaixo.

Quadro 3 – String final genérica

"Information security" AND ("social networks" OR "social media") AND (company OR corporation OR enterprise) AND safety AND risks

Produzido pelo Autor

4.2.2.1 Buscas experimentais

Buscas experimentais foram realizadas para analisar os estudos retornados para a pesquisa, realizada no período de abril de 2017, o objetivo principal das buscas experimentais consiste em otimizar a quantidade e qualidade de retorno da string, neste processo ocorre a calibração da string para atender melhor os critérios das buscas nas bases utilizadas nestes estudos.

As buscas foram realizadas de forma automática nas bases de dados descritas nos quadros 4 e 5, seguindo estes critérios:

1) Deverá ser possível consultar os artigos por meio da fonte eletrônica da base de dados;
2) As fontes para buscas automáticas deverão ter mecanismos de busca por string, ou recursos que facilitem este processo, com mesma eficácia;
3) Será realizada a Identificação das principais fontes de busca relacionadas ao tema deste mapeamento;
4) As bases deverão ser exploradas com pesquisas datadas nos últimos 10 anos.

Quadro 4 – Bases de dados automáticas

Bases Automáticas	Link
IEEE Xplore	http://ieeexplore.ieee.org/Xplore/home.jsp
ScienceDirect	http://www.sciencedirect.com/
SCOPUS	https://www.scopus.com/

Produzido pelo Autor

4.2.2.1.1 Aprimoramento das buscas

O aprimoramento da pesquisa foi realizado a partir de buscas em duas novas bases, onde segundo a (CAMBRIDGE, 2016) estas bases (em conjunto com as mencionadas anteriormente) contém os periódicos mais reconhecidos na área de segurança da informação.

As buscas seguiram os mesmos critérios ja definidos anteriormente, as bases utilizadas neste aprimoramento estão listadas no quadro 5, e foram adicionados subsequentemente as listas de estudos, que serão analisadas pelos filtros de busca.

Quadro 5 – Bases de dados para aprimoramento da pesquisa

Bases Automáticas	Link
Elsevier	https://www.elsevier.com
ACM	http://dl.acm.org/

Produzido pelo Autor

4.2.3 Estratégia de seleção

A estratégia de seleção deve ser feita a partir de critérios de inclusão e exclusão (KITCHENHAM; CHARTERS, 2007). Através desses critérios aplicados ao processo de seleção dos estudos, é possível descobrir quais estão aptos a serem selecionados. Os critérios de inclusão (CI) e os critérios de exclusão (CE) que foram definidos para orientar esta pesquisa seguem abaixo:

- **Critérios de Inclusão (CI):**

1) CI-1 - Pesquisas que identificam os riscos das redes sociais nas empresas;
2) CI-2 - Pesquisas que argumentam sobre os efeitos das redes sociais nas empresas;
3) CI-3 - Pesquisas que identificam técnicas que levam a supressão dos riscos das redes sociais nas empresas.

- **Critérios de Exclusão (CE):**

1) CE-1 - Pesquisas não relacionadas com o tema principal de redes sociais e riscos corporativos;
2) CE-2 - Documentos incompletos, indisponíveis, rascunhos, limitados ou em slides;

3) CE-3 - Não acessíveis pela internet e/ou pagos;

4) CE-4 - Pesquisas escritas em línguas diferentes do inglês;

5) CE-5 - Pesquisas duplicadas nas diferentes bases de dados;

6) CE-6 - Documentos publicados fora da data alvo da pesquisa, entre 2007 e 2017.

A estratégia de seleção foi dividida em 3 passos, são eles: Buscas Automáticas, Filtros (1 e 2) e Seleção Final. Para a geração das listas uma série de planilhas foram criadas na ferramenta online Google Sheets, dividindo as, por base de dados. O quadro 6 ilustra uma destas planilhas, a de busca automática na planilha da base de dados SCOPUS.

Quadro 6 – Exemplo de planilha com documentos selecionados.

Busca Automática Inicial Scopus				
Título do documento	Link da base de dados	Primeiro Filtro	Segundo filtro	Critérios
Security & safety (S&S) and the logistics business	https://www.scopus.com/recc	não		CE-1
Information security awareness through the use of social media	https://www.scopus.com/recc	sim		
Information security and privacy in social media: The threat landscape	https://www.scopus.com/recc	sim		
Risk assessment quantification of social-media utilization in enterprise	https://www.scopus.com/recc	sim		
Behavior of Brazilian Banks Employees on Facebook and the Cybersecurity Governance	https://www.scopus.com/recc	sim		
The dark side of social networking sites:Understanding phishing risks	https://www.scopus.com/recc	sim		
Unryderstanding the relationship between human behavior and susceptibility to cyber attacks: A data-driven approach	https://www.scopus.com/recc	talvez	nao*	CE-2
A risk management process for consumers: The next step in information security	https://www.scopus.com/recc	talvez	nao*	CE-2

Produzido pelo Autor

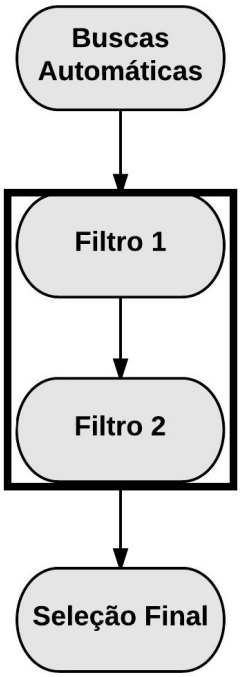
Buscas Automáticas: Neste primeiro passo, foram realizadas as buscas em bases automáticas, utilizando a string genérica adaptada a cada base. Cada base de dados retornou uma lista de documentos contendo informações sobre o título, autor, resumo, ano de publicação e link para acesso online. Estas listas foram agrupadas cada uma em sua própria tabela, intitulada “Busca Automática Inicial (base)”, como pode ser vista no quadro 6. Os critérios de inclusão e exclusão foram utilizados para a análise, que foi dividida em 2 fases, a primeira do filtro 1 e a segunda do filtro 2.

Filtro 1 e 2: No filtro 1 foram analisados os critérios de exclusão, os documentos duplicados começaram a ser mapeados (CE-5) e foram removidos ao finalizar o filtro. A partir deste filtro, realizou-se a análise do título e palavras chaves de todos os documentos retornados, após a execução dos CE.

O filtro 2 foi executado em seguida, como parte do mesmo passo, analisando os critérios de Inclusão nos documentos, a partir da leitura do resumo (abstract) dos documentos.

Seleção Final: Durante o último passo, a lista resultante foi analisada por meio da leitura da introdução dos documentos, como medida, para garantir a qualidade dos documentos a serem selecionados para a composição do presente Mapeamento.

Figura 2 – Processo de Busca



Produzido pelo Autor

4.2.4 Estratégia de extração

Para (RICHARDSON, 1989) uma pesquisa quantitativa é caracterizada pela aplicação da quantificação, bem como pela coleta das informações e seu tratamento. Sabendo disso, a estratégia de extração tem como objetivo analisar, classificar e selecionar os estudos primários a fim de responder à pergunta de pesquisa principal e as perguntas de pesquisa específicas (KITCHENHAM; CHARTERS, 2007).

A partir do supracitado, o esquema de classificação levou em consideração os seguintes aspectos:

1) Identificação do estudo;
2) Objetivo do estudo;
3) Fatores que levam aos riscos das empresas;
4) Fatores que indicam riscos envolvendo as redes sociais;

5) Avaliação dos riscos das redes sociais nas empresas;

6) Técnicas que levam à mitigação e ou redução destes riscos;

4.3 Resultados da seleção

A seleção inicial de estudos através das bases automáticas, ocorreu em duas fases, a primeira, foi realizada nas bases: IEEE Explorer, ScienceDirect e Scopus, logo após, uma segunda busca realizada nós mesmo parâmetros da primeira, utilizando duas novas bases: Elsevier e ACM.

1) **Passo**

Primeira Busca automática

Esta busca automática consistiu em obter estudos primários das bases selecionadas inicialmente por meio da string de busca genérica. A string de busca retornou um total de 969 estudos primários. O quadro 7 detalha o retorno desta primeira busca.

Quadro 7 – Retorno de busca automática

Base eletrônica	Estudos Retornados
IEEE Xplore	665
ScienceDirect	198
SCOPUS	106
Total:	**969**

Produzido pelo Autor

Segunda Busca Automática

Uma segunda busca foi realizada com o objetivo de aprimorar a pesquisa, expandindo as bases de dados utilizadas e agregando novos estudos para a análise. Esta busca retornou 263 estudos primários, conforme mostra o quadro 8.

Quadro 8 – Retorno de busca automática

Base eletrônica	Estudos Retornados
Elsevier	244
ACM	19
Total:	**263**

Produzido pelo Autor

2) **Passo (Filtro 1 e 2)**

Nesta etapa, foi executado o primeiro filtro (que foi detalhado anteriormente), onde foram lidos o título e as palavras chave dos 1232 estudos, e aquelas que não cumprissem os critérios CE-1, CE-2, CE-3, CE-4 e CE-6 foram excluídos.

Os estudos resultantes passaram pelo 2° filtro, onde foi analisado se no mínimo 1 dos critérios de inclusão eram atendidos, a partir da leitura do abstract.

Os estudos selecionados nesta etapa foram para a lista denominada “Lista de estudos possíveis”. A partir desta lista, foi executado uma ferramenta auxiliar baseada no google sheets, que analisava os títulos e comparava se eram repetidos.

O quadro abaixo mostra o resultado desta etapa, com os estudos que foram selecionados de cada base e a porcentagem em relação ao total de estudos.

Quadro 9 – Tabela de estudos selecionados por base X porcentagem em relação ao total de cada base

Base eletrônica	Estudos Retornados	Estudos Selecionados	Porcentagem (%)
IEEE Xplore	665	10	1,5
ScienceDirect	198	3	1,51
SCOPUS	106	2	1,88
Elsevier	244	2	0,81
ACM	19	1	5,26

Produzido pelo Autor

3) **Passo**

Neste último passo, foi realizada a análise dos estudos, onde todos tiveram a introdução lida, para verificar se era condizente com o padrão de CE e CI pretendido. Neste passo, não houveram exclusões de estudos.

4.3.1 Considerações finais da seleção de estudos

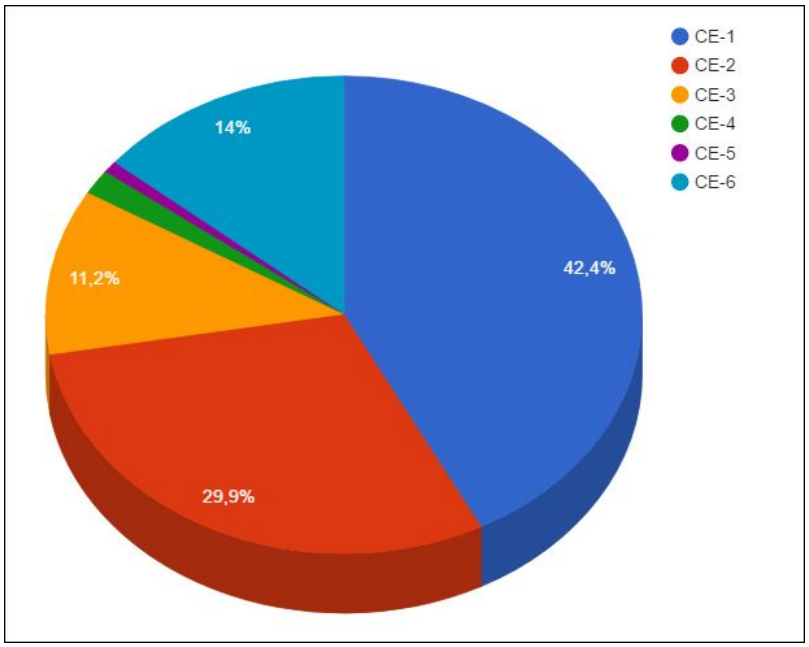
A maioria dos estudos foi excluída a partir dos critérios de exclusão:

1) CE-1 que afirma que pesquisas não relacionadas aos riscos das redes sociais na segurança corporativa não devem ser incluídas neste mapeamento;
2) CE-2 que afirma que documentos incompletos, indisponíveis, rascunhos, limitados ou em slides não poderão ser incluídos nesta pesquisa;

3) CE-6 que afirma que pesquisas duplicadas em 1 ou mais bases, terão apenas sua primeira entrada como valida e as demais excluídas.

Abaixo um gráfico mostrando a porcentagem de estudos excluídos em relação ao critério de exclusão utilizado.

Gráfico 1 – Gráfico de critérios de exclusão



Produzido pelo Autor

O CE-3 afirma que pesquisas indisponíveis para acesso através da internet (normalmente por serem pagos) não poderão ser adicionados ao estudo, uma lista com estes estudos estará no Apêndice C. No CE-4 referente as pesquisas com língua diferente do inglês, foram removidos mediante observação manual dos artigos (durante o filtro 1), em vista que a maioria utiliza títulos e resumo em inglês e o restante do texto no idioma de origem, o total de artigos removidos neste CE foi de 21 artigos ou 1,7%.

Como dito anteriormente o CE-5 foi executado de forma automática, trazendo 9 artigos repetidos (0,8%), as repetições ocorreram em todas as 4 bases, alguns artigos chegaram a estar repetidos em 4 das 5 bases.

4.4 Resultados da extração e análise das evidências

Nesta etapa será realizada a demonstração e analise dos resultados, que foram encontrados durante a etapa de extração dos estudos. Com o objetivo de quantificar e qualificar: os objetivos dos estudos, métodos utilizados, técnicas de coleta de dados e as respostas as perguntas de pesquisa.

Durante este processo, os 18 estudos selecionados foram lidos em sua totalidade, entretanto, 11% dos estudos tiveram de ser excluídos por se enquadrarem nos critérios de Exclusão CE-2 que excluem artigos incompletos, indisponíveis ou limitados.

Desta forma, 16 estudos passaram pela leitura completa. Destes, 6% não responderam a nenhuma pergunta de pesquisa, sendo então, removidos da lista de artigos. Por fim, 15 artigos responderam ao menos 1 pergunta de pesquisa, a lista completa com os artigos poderá ser encontrada no apêndice A.

Os estudos selecionados neste mapeamento estão associados a 32 autores diferentes, sendo apenas 5 autores em conjunto responsáveis por 2 estudos. A lista completa de autores se encontra no quadro 10:

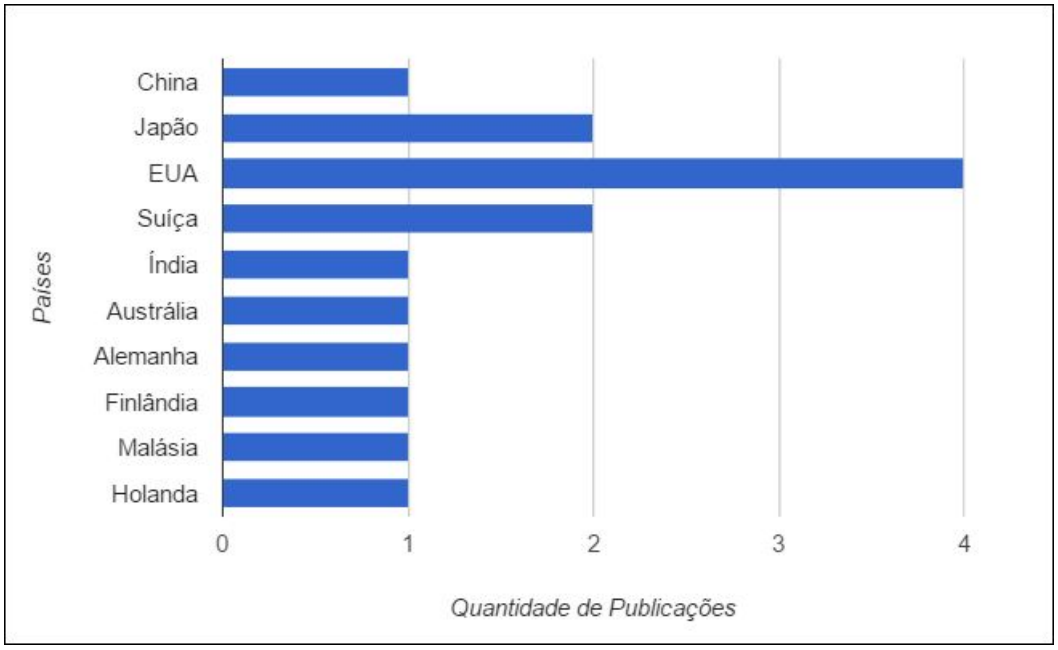
Quadro 10 – Lista de autores dos estudos

AUTORES		
Bo Gao	Jianming Zhu	Kenichi Ohata
Shigeaki Tanimoto	Hiroyuki Sato	Shoichi Yoneda
EDDIE RABINOVITCH	Yoshiaki Seki	Atsushi Kanai
Caroline Oehri	Stephanie Teufel	Motoi Iwashita
Brian M. Gaff	McDermott Will	Werner Esswein
Dr. Priyanka Sharma	Maumita Bhattacharya	Jari Jussila
Rakesh Singh Kunwar	Hannu Kärkkäinen	Tero Päivärinta
Heidi Wilcox	Andrea Back	Asma Md. Ali
Richard Braun	Shuhaili Talib	Mumi Mahmud
Ilona Ilvonen	André van Cleeff	Kevvie Fowler
Mario Silic	Nurul Nuha Abdul Molok	

Produzido pelo Autor

Os autores estão associados a 10 países diferentes. Dentre os países com maior frequência de publicação estão: Estados Unidos, Japão e Suíça, como mostra o gráfico 2.

Gráfico 2 – Representação de quantidade de publicações em relação aos países



Produzido pelo Autor

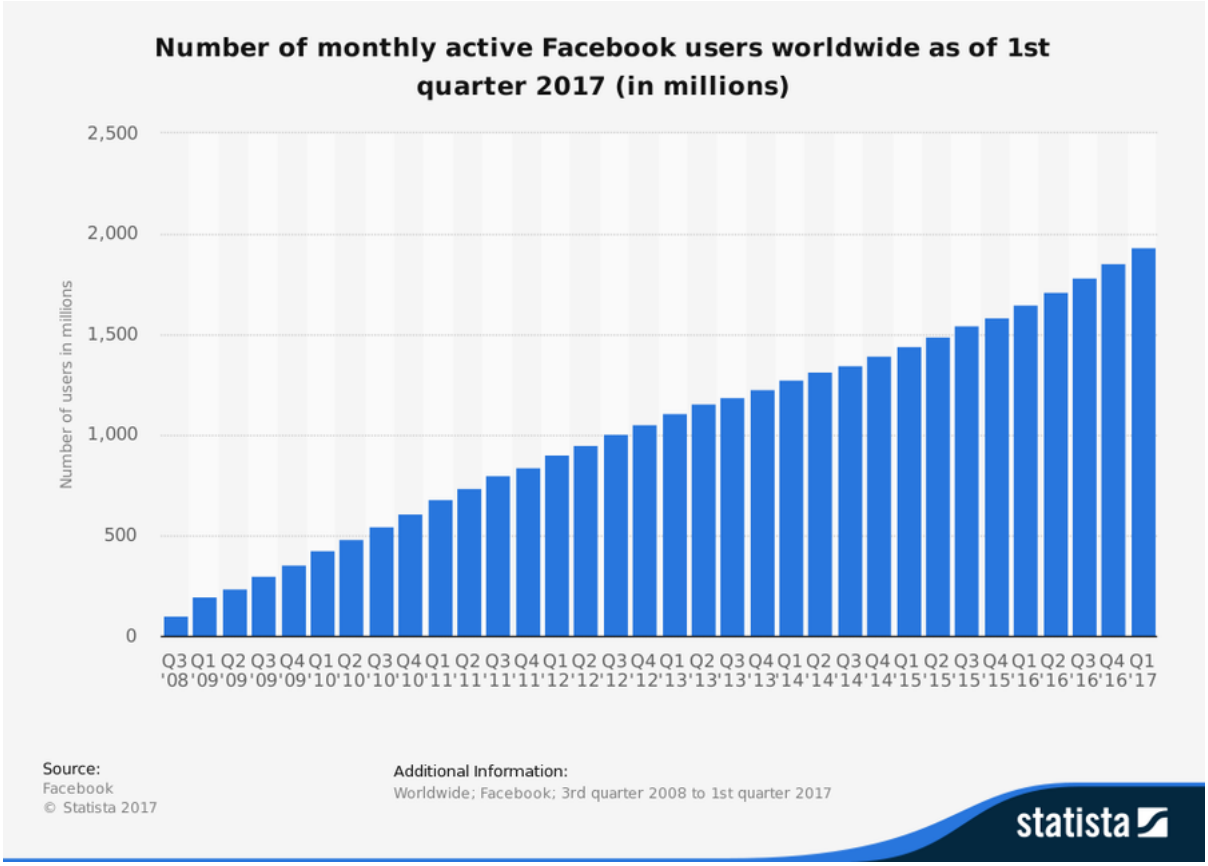
Nos resultados é possível perceber que existem publicações desde 2007 até 2016, onde a partir de 2014, formou-se uma curva de crescimento na quantidade de estudos neste tema, evidenciando que o mesmo vem se tornando uma tendência, a cada ano, mais evidente no meio acadêmico e na área de segurança.

Gráfico 3 – Quantidade de estudos vs. Ano

Produzido pelo Autor

Podemos traçar um paralelo interessante sobre o crescimento dos estudos sobre riscos das redes sociais, com o crescimento das próprias redes, por exemplo, o crescimento de usuários do Facebook (analisar gráfico abaixo), segue a mesma linha de tendência que o gráfico 3, logo acima; isto se traduz de forma simples, em mais uma evidencia de que os riscos envolvendo as redes sociais estão ligados diretamente a sua utilização, e quanto mais cresce esta utilização, maior o indicio de risco em uma empresa.

Gráfico 4 – Número de usuários ativos no Facebook, por mês, a partir de 2008



https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

Nos estudos selecionados, todos conseguiram responder no mínimo 1 das questões de pesquisa. Dos estudos analisados, 87% conseguiram responder a PP1, no que diz respeito aos riscos das redes sociais na segurança corporativa. Em relação a PP2, 40% dos estudos conseguiram obter sucesso nas respostas sobre impactos do uso das redes sociais. Por fim, na PP3 27% dos estudos conseguiram responder à questão de pesquisa proposta no que diz respeito a mitigação ou redução dos riscos das redes sociais no ambiente corporativo.

4.4.1 **PP1: Quais os riscos que mais ocorrem nas empresas em decorrência do uso das redes sociais?**

O resultado dessa pergunta forneceu um conjunto de riscos, que normalmente ocorrem em empresas, onde devido a utilização das redes sociais na corporação, acabam aumentando a chance de o risco ocorrer, como explicito no E07578896 "... it is unfortunate to note that social media sites can pose a variety of serious security risk and threats to users and organizations.".

Os estudos em sua maioria são compostos por metodologias, processos e surveys sobre os riscos das redes sociais. Cerca de 73% dos estudos analisados para esta pergunta, tratam os riscos das redes sociais, como um problema das pessoas e da tecnologia que elas utilizam, como e-mail, sites e etc.; segundo E06320436 "Employees can cause considerable harm to themselves and their business organizations through social media activity without due reflection."

Os outros 27% tratam os riscos como falhas da organização em instruir seus funcionários ou não terem condição de se protegerem habilmente, de sites de pishing, por exemplo; o estudo E06750454, corrobora com esta afirmação: "Risks can be minimized and opportunities maximized if all employees can Adequate online presence and conduct through Training and procedures provided by the company".

Ao todo, os estudos listaram 21 riscos, que podem ser organizados de forma simples, a partir das divisões entre pessoas, processos e tecnologia; os riscos encontrados, tiveram seus semelhantes agrupados em 9 tipos de riscos, como pode ser visto no Quadro 11.

Quadro 11 – Riscos mais comentados nos estudos analisados

Riscos		
Processos	Tecnologias	Pessoas
Perda de dados (intencional ou não)	Pishing	Engenharia Social
Perca de controle (DDoS e outros)	Malwares	Roubo de Identidade
Rapto de sistemas (Ransomware)	Spam	Problemas de comunicação

Produzido pelo Autor

4.4.2 **PP2: Quais são os impactos das plataformas sociais na segurança das corporações?**

Ao realizar a análise dos estudos primários, foram encontrados apenas cinco artigos que respondessem de forma satisfatória esta questão de pesquisa, os estudos tratam sobre quatro impactos do uso das redes sociais na segurança das corporações, entretanto perda de privacidade e exposição de dados foram unificados, por terem os mesmos "efeitos" na empresa.

1) Dano a reputação, segundo o estudo E06658287:

> "There are two reasons for loss of reputation through OSN: Own faults and customer activities. Own faults address all inadequate communication and advertising in OSN, inadequate management of complaints and active manipulations like buying positive customer feedback or using fake users. The publication of internal data as consequence of the mixture of private and professional statements can also lead to reputational damage. "

2) Espionagem industrial, a partir do estudo E06658287:

> "Businesses aim to protect all internal data carefully and want to avoid any kind of data leakage that can generated some value for third parties (e.g., trade secrets, proprietary information). The risk characterizes the leakage of internal data through OSN. [. . .] Data leakage can also enforce competitive analysis. If data is gained mischievously, industrial espionage is possible."

3) Perda de privacidade / exposição de dados, mediante estudo E06658287:

> "Businesses want their internal stakeholders aware of privacy in terms of the avoidance of internal data leakage. OSN can blur that awareness. There are two main reasons for privacy unawareness in OSN: the technology and the user. Often, users do not have a good understanding of the flow and reach of their personal data in OSN."

No geral, os estudos sempre colocam como os maiores impactos, aqueles que interferem na renda da empresa, diretamente ou não; como o dano a reputação que pode criar uma imagem ruim da empresa e como consequência a empresa pode vir até mesmo a fechar, devido à perda de clientes; as perdas de dados tem um efeito bastante similar, especialmente quando feita de maneira consciente.

4.4.3 **PP3: Quais medidas vêm sendo tomadas para mitigar ou reduzir incidentes deste tipo?**

A formas de mitigar ou reduzir os riscos das redes sociais foram mencionadas em 27% dos artigos selecionados, 38% deles tratam sobre frameworks, alguns deles abordam apenas a parte técnica da empresa, outros abordam a empresa como um todo, inclusive seus funcionários e seu uso das redes sociais, como o caso do SESM, como menciona o estudo E076603735:

> "the SESM policy framework aims to provide management the means to implement an effective policy development guideline that addresses technical, procedural, and human components. The framework provides a point of reference for the governance of social media to inculcate an cceptable level of information security in these technologies and within the security culture of the users."

A outra porção dos artigos tratam sobre a utilização de programas SETA (Security Education, Training, and Awareness), algo como um programa de educação em segurança, treinamento e conscientização dos funcionários na utilização das redes sociais, bem como o alinhamento da alta administração com as medidas de prevenção e controle destes riscos, como bem mencionado pelo E07020668:

> "In general, current information security studies suggest that SETA programs and preventive security systems as key deterrents to insider threats, In addition, and point out that the governance of information security is crucial for organizations to protect their critical information, suggesting the involvement of top management to spearhead security initiatives in organizations."

As formas de mitigação dos riscos referente as redes sociais, ainda se baseiam quase que inteiramente na conscientização do usuário, através de programas de educação e conscientização; poucas empresas chegam a considerar implantar frameworks (normalmente grandes e complexos) para gerenciamento desses riscos, provavelmente devido um custo-benefício deficiente a curto e médio prazo.

5 CONCLUSÕES

As redes sociais são definidas como um “”o meio onde as pessoas se reúnem por afinidades e com objetivos em comum. . . “. Todavia seu uso não atento, pode criar brechas para invasões, problemas internos nas organizações, perda nos lucros e muitos outros. Assim, há a necessidade de uma análise sob um espectro mais amplo, abrangendo todos estes riscos em relação a segurança corporativa.

Desta forma, este trabalho tem como principal objetivo elencar as pesquisas relevantes relacionadas aos riscos das plataformas sociais na segurança corporativa, identificar categorias e frequências de publicações neste âmbito além de prover uma base para novas pesquisas relacionadas a este tema. Para alcançar esta meta, foi realizado o planejamento e a condução de um Mapeamento Sistemático da Literatura.

Este mapeamento da literatura nos mostrou que poucos estudos primários tem seu foco voltado para as redes sociais e os riscos que as mesmas oferecem em um ambiente corporativo. Demonstrando certa carência na área de segurança, de estudos que explorassem todos os riscos, seus impactos e a posição adotada pelas empresas para solução deste caso, isso pode ser visto pela pequena quantia de resultados nas buscas.

Dentre os riscos, foi possível encontrar mais de 20 riscos, relacionados as redes sociais, que ao agrupar seus semelhantes podemos encontrar 9 tipos de riscos que ameaçam a segurança corporativa, atingindo as pessoas, a tecnologia que as rodeia e até mesmo o nome da empresa. Além disso seus maiores impactos foram relacionados, inclusive as atitudes utilizadas pelas corporações para mitigar estes problemas.

Podemos concluir que com base na análise quantitativa das respostas das perguntas de pesquisa, percebemos que os riscos encontrados nas redes sociais, vão muito além de como é visto e retratado em nosso dia a dia. Estes riscos podem gerar perdas gigantescas para empresas, levando até mesmo a seu fechamento, as estratégias de contensão empregadas ainda são simples, se comparado com a capacidade de evolução e destruição que estes riscos podem causar.

5.1 Trabalhos futuros

É facilmente percebido que há uma variedade de tópicos a serem muito mais explorados em pesquisas futuras, como por exemplo, uma análise qualitativa dos dados apresentados neste mapeamento. Trazendo inúmeros benefícios à comunidade de segurança em informação que carece de novas informações e pesquisas desta

área, em alto crescimento. Novas pesquisas sobre os riscos das redes sociais mobile, que também é uma tendência mundial, pesquisas focadas na engenharia social e phishing e seus impactos nas empresas, em vista que são os riscos que mais impactam as empresas, ou até mesmo pesquisas concentradas em novos critérios, como impactos nos serviços de TI provocados pelo uso das redes sociais no ambiente corporativo, seu consumo de recursos vitais da empresa e muitos outros.

REFERÊNCIAS

BARROS, A. J. P.; LEHFELD, N. A. D. S. *FUNDAMENTOS DE METODOLOGIA CIENTIFICA*. [S.l.]: MAKRON, 2007. ISBN 8576051567. Acesso em: 06/05/2017. Citado na página 21.

BITDEFENDER. *Malware o que é, e quais os tipos existentes?* 2017. Disponível em: <https://www.oficinadanet.com.br/post/8550-malware-o-que-e-e-quais-os-tipos-existentes>. Acesso em: 25/04/2017. Citado na página 18.

BUCCO, R. B. *EXITEM MAIS DE 80 MILHÕES DE PERFIS FALSOS NAS REDES SOCIAIS*. 2016. Disponível em: <http://www.telesintese.com.br/exitem-mais-de-80-milhoes-de-perfis-falsos-nas-redes-sociais/>. Acesso em: 19/04/2017. Citado na página 17.

CAMBRIDGE, U. of. *Journals on computer security*. 2016. Disponível em: <http://www.cl.cam.ac.uk/research/security/journals.html>. Acesso em: 08/05/2017. Citado na página 28.

CARDOSO, P. *O que é Ransomware?* 2016. Disponível em: <http://www.techtudo.com.br/noticias/noticia/2016/06/o-que-e-ransomware.html>. Acesso em: 05/04/2017. Citado na página 18.

CARRARETTO, A. *A onda dos "mega" vazamentos de dados*. 2017. Disponível em: <https://canaltech.com.br/coluna/seguranca/A-onda-dos-mega-vazamentos-de-dados/>. Acesso em: 05/05/2017. Citado na página 19.

CASTRO, R. *Redes Sociais e a sua contínua evolução*. 2013. Disponível em: <http://petcomufam.com.br/2013/06/redes-redes-sociais-e-sua-continua-evolucao.html>. Acesso em: 21/04/2017. Citado na página 16.

CENTER, M. . M. P. *Ransomware*. 2016. Disponível em: <https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx>. Acesso em: 16/04/2017. Citado na página 19.

CERT.BR. *Segurança em Redes Sociais*. 2017. Disponível em: <https://cartilha.cert.br/fasciculos/redes-sociais/fasciculo-redes-sociais-slides.pdf>. Acesso em: 12/04/2017. Citado na página 13.

FIGUEIRÓ, T. *O ser humano é o elo mais fraco na segurança da informação*. 2010. Disponível em: <https://www.computerworld.com.pt/2010/03/16/o-ser-humano-e-o-elo-mais-fraco-na-seguranca-da-informacao/>. Acesso em: 03/04/2017. Citado na página 17.

FONSECA, J. J. S. *Metodologia da pesquisa científica*. Fortaleza: UEC, 2002. Disponível em: <http://www.ufrgs.br/cursopgdr/downloadsSerie/derad005.pdf>. Acesso em: 05/05/2017. Citado 2 vezes nas páginas 21 e 22.

HAYATI, D.; KARAMI, E.; SLEE, B. *Combining qualitative and quantitative methods in the measurement of rural poverty*. [S.l.]: Social Indicators Research - Springer, 2006. Acesso em: 06/05/2017. Citado na página 22.

JUE, A. L. *et al. Mídias sociais nas empresas*. [S.l.]: Editora Évora, 2011. ISBN 9788563993090. Citado na página 14.

KITCHENHAM, B. *et al.* Protocol for a Tertiary study of Systematic Literature Reviews and Evidence-based Guidelines in IT and Software Engineering. 2007. Disponível em: <https://community.dur.ac.uk/ebse/study.php?type=protocol&id=1>. Acesso em: 12/05/2017. Citado 2 vezes nas páginas 22 e 24.

KITCHENHAM, B.; CHARTERS, S. *Guidelines for performing systematic literature reviews in software engineering*. [S.l.]: Software Engineering Group Department of Computer Science Keele University, 2007. Acesso em: 20/04/2017. Citado 5 vezes nas páginas 23, 24, 25, 28 e 30.

LAB, K. *Kaspersky Lab*: ransomware móvel triplicou significamente no primeiro trimestre de 2017. 2017. Disponível em: <https://www.kaspersky.com.br/about/press-releases/2017_kaspersky-lab-ransomware-movel-triplicou-significamente-no-primeiro-trimestre-de-2017>. Acesso em: 10/06/2017. Citado na página 18.

LUCIO, R. H. S. M. del P. B.; COLLADO, C. F.; LUCIO, M. del P. B. *Metodologia de Pesquisa*. 5. ed. Porto Alegre: Penso, 2013. (Métodos de Pesquisa). Acesso em: 06/05/2017. Citado na página 22.

MATTAR, F. *Pesquisa de marketing*. [S.l.]: Ed. Atlas, 1996. Acesso em: 06/05/2017. Citado na página 22.

MOREIRA, B. de A. *SIMPLICIDADE NO CONTEXTO DE DESENVOLVIMENTO ÁGIL DE SOFTWARE*: Um mapeamento sistemático da literatura. 2016 — Universidade de Pernambuco, Caruaru. Acesso em: 10/04/2017. Citado na página 23.

NOGUEIRA, J. *O que são Redes Sociais?* . 2010. Disponível em: <http://www.administradores.com.br/artigos/tecnologia/o-que-sao-redes-sociais/45628/>. Acesso em: 21/04/2017. Citado na página 16.

PETERSEN, K. *et al.* Systematic Mapping Studies in Software Engineering. In: 12TH INTERNATIONAL CONFERENCE ON EVALUATION AND ASSESSMENT IN SOFTWARE ENGINEERING, 2008. [S.l.], 2008. Citado 2 vezes nas páginas 22 e 23.

PEW RESEARCH CENTER. *Social Media Update 2016*. 2016. Disponível em: <http://www.pewinternet.org/2016/11/11/social-media-update-2016/>. Acesso em: 18/04/2017. Citado na página 13.

PONEMON INSTITUTE. The Impact of Cybercrime on Business Studies of IT practitioners in the United States, United Kingdom, Germany, Hong Kong and Brazil. 2012. Disponível em: <http://www.ponemon.org/library/the-impact-ofcybercrime-on-business-studies-of-it-practitioners-in-the-united-states-unitedkingdom-germany-hong-kong-and-brazi?s=media>. Acesso em: 02/02/2017. Citado na página 13.

RICHARDSON, R. J. Metodologia em pesquisas sociais. 1989. Citado na página 30.

RODRIGUES.A.DE.J. *Metodologia Científica*: completo e essencial para a vida universitária. São Paulo: Avercamp, 2006. Citado na página 14.

ROHR, A. *Como acontecem os vazamentos de dados?* 2015. Disponível em: <https://www.linhadefensiva.org/2015/11/como-acontecem-os-vazamentos-de-dados/>. Acesso em: 11/04/2017. Citado na página 19.

SANTIAGO PONTIROLI. *A engenharia para enganar pessoas*. 2013. Kaspersky Lab. Disponível em: <https://blog.kaspersky.com.br/engenharia-social-hackeando-humanos/1845/>. Acesso em: 24/04/2017. Citado na página 17.

SIMON, K. D. M. W. L. *A Arte de Enganar*. [S.l.]: Pearson Universitario, 2001. ISBN 9798576050550. Acesso em: 05/05/2017. Citado na página 17.

SPIELBERG, S. *Prenda - me se For Capaz*. 2003. Filme. Citado na página 18.

VALENTIM, N. M. C.; SILVA, W.; CONTE, T. *Mapeamento Sistemático para a geração de um Framework que Projetam e/ou Avaliam a Usabilidade nos Estágios Iniciais do Processo de Desenvolvimento de Software*. 2017. Dissertação (Programa de Pós-Graduação em Informática) — Universidade Federal do Amazonas, Manaus. Acesso em: 12/04/2017. Citado na página 23.

VEERACHT, P. As redes sociais - SeguraNet. 2015. Disponível em: <http://www.seguranet.pt/art1589>. Acesso em: 19/04/2017. Citado na página 16.

Apêndices

APÊNDICE A – LISTA DE ESTUDOS SELECIONADOS

Neste apêndice segue a lista dos estudos selecionados, um total de 15 artefatos, resultantes do processo de condução do mapeamento sistemático da literatura realizado neste trabalho.

Quadro 12 – Lista de estudos selecionados

Estudos Selecionados (ID)	Titulo	Autor	Respondeu a pergunta de pesquisa
E07369815	The Application of Game Theory in Mobile Social Media Security Analysis for Companies	Bo Gao, Jianming Zhu	PP1
E07176262	Risk Assessment of Social-media Utilization in an Enterprise	Shigeaki Tanimoto, Kenichi Ohata, Shoichi Yoneda, Motoi Iwashita, Hiroyuki Sato, Yoshiaki Seki, Atsushi Kanai	PP1, PP2, PP3
E04342845	STAYING PROTECTED FROM "SOCIAL ENGINEERING"	EDDIE RABINOVITCH	PP1, PP2
E06320436	Social Media Security Culture - The Human Dimension in Social Media Management	Caroline Oehri, Stephanie Teufel	PP1, PP3
E06750454	Corporate Risks from Social Media	Brian M. Gaff, McDermott Will & Emery	PP1
E07521417	Unryderstanding the relationship between human behavior and susceptibility to cyber attacks: A data-driven approach	Ovelgönne M., Dumitras T., Prakash B.A., Subrahmanian V.S., Wang B.	PP1
E07578896	Social Media: A New Vector for Cyber Attack	Rakesh Singh Kunwar, Dr. Priyanka Sharma	PP1
E07603735	A Framework to Mitigate Social Engineering through Social Media within the Enterprise	Heidi Wilcox, Maumita Bhattacharya	PP2, PP3
E06658287	Towards a Conceptualization of Corporate Risks in Online Social Networks	Richard Braun, Werner Esswein	PP1
E07070291	Knowledge security risk management in contemporary companies toward a proactive approach	Ilona Ilvonen, Jari Jussila, Hannu Kärkkäinen, Tero Päivärinta	PP1
E07475632	The dark side of social networking sites:Understanding phishing risks	Mario Silic, Andrea Back	PP1
E07020668	Information Security Awareness through the use of Social Media	Nurul Nuha Abdul Molok, Asma Md. Ali, Shuhaili Talib, Mumi Mahmud	PP2, PP3
E07550891	Risk Assessment Quantification of Social-media Utilization in Enterprise	Shigeaki Tanimoto, M otoi Iwashita, Yoshiaki Seki, Hiroyuki Sato, Atsushi Kanai	PP1, PP2
E09780128	Cybersecurity	Kevvie Fowler	PP1
E02598107	A Risk Management Process for Consumers: The Next Step in Information Security	André van Cleeff	PP1, PP2

Produzido pelo Autor

APÊNDICE B – PLANILHA DE ACOMPANHAMENTO DO MAPEAMENTO SISTEMÁTICO

Nesta seção seguem as versões resumidas das planilhas de acompanhamento, utilizadas para auxiliar o processo de escolha de artefatos e mapear o andamento da condução do mapeamento.

Quadro 13 – Planilha com documentos selecionados e eliminados da base Elsevier

Busca Automática Inicial (Elsevier)		
Titulo do artigo	Link Direto	CE
Corporate Security Management	https://www.elsevier.com/boo	CE-6
The Corporate Security Professional's Handbook on Terrorism	https://www.elsevier.com/boo	CE-1
Social Media Security	https://www.elsevier.com/boo	CE-5
Securing Social Media in the Enterprise	https://www.elsevier.com/boo	CE-5
Information Security Risk Assessment Toolkit	https://www.elsevier.com/boo	CE-2
The dark side of social networking sites:Understanding phishing risks	https://www.elsevier.com/boo	ok
Challenges for the security analysis of Next Generation Networks	https://www.elsevier.com/boo	ok

Produzido pelo Autor

Quadro 14 – Planilha com documentos selecionados e eliminados da base IEEE Xplorer

Busca Automática Inicial (IEEE Xplore)		
Titulo do artigo	Link Direto	CE
E-reputation: A case study of organic cosmetics in social media	http://ieeexplore.ieee.org/doc	CE-1
A Resource-Based View of Using Social Media for Material Disclosures	http://ieeexplore.ieee.org/doc	CE-3
Enterprise Security Governance; A practical guide to implement and control Information Se	http://ieeexplore.ieee.org/doc	CE-1
Corporate Risks from Social Media	http://ieeexplore.ieee.org/doc	ok
Risk assessment of social-media utilization in an enterprise	http://ieeexplore.ieee.org/doc	ok
A framework to mitigate social engineering through social media within the enterprise	http://ieeexplore.ieee.org/doc	ok
The application of game theory in mobile social media security analysis for companies	http://ieeexplore.ieee.org/doc	ok
Towards a Conceptualization of Corporate Risks in Online Social Networks: A Literature Ba	http://ieeexplore.ieee.org/doc	ok
Social media security culture	http://ieeexplore.ieee.org/doc	ok
Social media: A new vector for cyber attack	http://ieeexplore.ieee.org/doc	ok
Staying Protected from "Social Engineering"	http://ieeexplore.ieee.org/doc	ok
Using social networks: Impact on enterprise reputation	http://ieeexplore.ieee.org/doc	ok
Knowledge Security Risk Management in Contemporary Companies -- Toward a Proactive	http://ieeexplore.ieee.org/doc	ok
Security Risk Management in complex organization	http://ieeexplore.ieee.org/doc	CE-2
A Review of Social Media and Social Business	http://ieeexplore.ieee.org/doc	CE-3
Access Control in Social Enterprise Applications: An Empirical Evaluation	http://ieeexplore.ieee.org/doc	CE-1

Produzido pelo Autor

Quadro 15 – Planilha com documentos selecionados e eliminados da base Science Direct

Busca Automática Inicial (Science Direct)		
Titulo do artigo	Link Direto	CE
The Future of Online Security	http://www.sciencedirect.com	CE-1
The Business, Careers, and Challenges of Security and Loss Prevention	http://www.sciencedirect.com	CE-1
A Paradigm Shift in Cyberspace Security	http://www.sciencedirect.com	CE-3
Self-efficacy in information security: Its influence on end users' information security practic	http://www.sciencedirect.com	CE-2
Information security concerns in IT outsourcing: Identifying (in) congruence between clients	http://www.sciencedirect.com	CE-1
Analysis of personal information security behavior and awareness	http://www.sciencedirect.com	CE-1
Information security awareness training: Your most valuable countermeasure to employee	http://www.sciencedirect.com	CE-2
Risks of Social Media	http://www.sciencedirect.com	ok
Cybersecurity	http://www.sciencedirect.com	ok
Opportunities of Social Media	http://www.sciencedirect.com	ok
The prospects of easier security for small organisations and consumers	http://www.sciencedirect.com	CE-1
A situation awareness model for information security risk management	http://www.sciencedirect.com	CE-2
Reinforcing the security of corporate information resources: A critical review of the role of t	http://www.sciencedirect.com	CE-3
Monitoring information security risks within health care	http://www.sciencedirect.com	CE-6

Produzido pelo Autor

Quadro 16 – Planilha com documentos selecionados e eliminados da base ACM

Busca Automática Inicial (ACM)		
Titulo do artigo	Link Direto	CE
Securing the Clicks Network Security in the Age of Social Media	http://dl.acm.org/citation.cfm	CE-2
Knowledge Security Risk Management in Contemporary Companies -- Toward a Proactive	http://dl.acm.org/citation.cfm	CE-5
Managing Risk and Information Security: Protect to Enable	http://dl.acm.org/citation.cfm	CE-2
A risk management process for consumers: the next step in information security	http://dl.acm.org/citation.cfm	ok
Social networking and the risk to companies and institutions	http://dl.acm.org/citation.cfm	CE-3
Collaboration with Cloud Computing: Security, Social Media, and Unified Communications	http://dl.acm.org/citation.cfm	CE-1
Discovering Potential Victims Within Enterprise Network via Link Analysis Method	http://dl.acm.org/citation.cfm	CE-3
Managing Malicious Insider Risk through BANDIT	http://dl.acm.org/citation.cfm	CE-1
A methodology for estimating the tangible cost of data breaches	http://dl.acm.org/citation.cfm	CE-6
Advanced Persistent Security: A Cyberwarfare Approach to Implementing Adaptive Enterp	http://dl.acm.org/citation.cfm	CE-2

Produzido pelo Autor

Quadro 17 – Planilha com documentos selecionados e eliminados da base Scopus

Busca Automática Inicial (Scopus)		
Titulo do artigo	Link Direto	CE
Security & safety (S&S) and the logistics business	https://www.scopus.com/recc	CE-1
Information security awareness through the use of social media	https://www.scopus.com/recc	ok
Information security and privacy in social media: The threat landscape	https://www.scopus.com/recc	CE-3
Risk assessment quantification of social-media utilization in enterprise	https://www.scopus.com/recc	ok
Behavior of Brazilian Banks Employees on Facebook and the Cybersecurity Governance	https://www.scopus.com/recc	CE-1
Information Security Risk Assessment Toolkit	https://www.scopus.com/recc	CE-1
Unryderstanding the relationship between human behavior and susceptibility to cyber attac	https://www.scopus.com/recc	CE-2
A risk management process for consumers: The next step in information security	https://www.scopus.com/recc	CE-2

Produzido pelo Autor

APÊNDICE C – PLANILHA DE ARTEFATOS REMOVIDOS POR SEREM PAGOS

Nesta seção são apresentados os artefatos que não puderam fazer parte da pesquisa em vista de serem pagos.

Figura 3 – Planilha com artefatos pagos

Título	Autor
Social networking and the risk to companies and institutions	Marc Langheinrich, Günter Karjoth
Securing the Clicks Network Security in the Age of Social Media	Gary Bahadur, Jason Inasi, Alex de Carvalho
Collaboration with Cloud Computing: Security, Social Media, and Unified Communications	Ric Messier
Discovering Potential Victims Within Enterprise Network via Link Analysis Method	Kai-Fung Hong, Hsiu-Chuan Huang, Shun-Te Liu, Yu-Ting Chiu
Social Media Security	Michael Cross
Securing Social Media in the Enterprise	Henry Dalziel
Risk perceptions of cyber-security and precautionary behaviour	Paul van Schaika, , Debora Jeskeb, , Joseph Onibokunc, , Lynne Coventryd, , Jurjen Jansene, , Petko Kusevf
The Security Risks of Web-Based Applications in the Workplace	Amine, A., Mohamed, O.A., Benattallah, B.
Mobile Security: A Practitioner's Perspective	S. Tully*,Y. Mohanraj†
International Perspectives on Security in the Twenty-First Century	Paul A. Caron, K.C. Goswami, Ona Ekhomu, H.D.G.T. Oey, Bruce W. Dobbins, Erik D. Erikson
Analysis of personal information security behavior and awareness	Gizem Öğütçü, Özlem MügeTestikb

Produzido pelo Autor