Problemas e Questões nos Processos Tradicionais de Resposta a Incidentes de Segurança da Informação

Rodrigo Silva Sotolani
rodrigo.sotolani@cpspos.sp.gov.br
CPS

Napoleão Verardi Galegale
nvg@galegale.com.br
CPS

Resumo: Os CSIRTs (Computer Security Incident Response Teams) e seus processos apresentam problemas e necessidades de melhorias face aos avanços constantes das ameaças cibernéticas. A rigidez dos processos para responder a um incidente se contrasta com o dinamismo dos ataques. O objetivo do artigo é realizar pesquisa bibliométrica para identificar os principais problemas ou questões nos processos ou modelos tradicionais de resposta a incidentes de segurança da informação, tendo como objetivos específicos a pesquisa bibliométrica sobre os problemas nos processos ou modelos tradicionais de resposta a incidentes de segurança da informação e a análise quantitativa e qualitativa da pesquisa bibliométrica. Através da pesquisa na literatura pela base de dados acadêmica Google Scholar, encontraram-se os seguintes temas relevantes: Desempenho do processo de resposta a incidentes de segurança, Comunicação e Compartilhamento de Informação, Automatização dos Processos e Inteligência, Aprendizado com os Incidentes, Tratamento de Incidentes na Manufatura e Indústria, Incidentes em Infraestrutura de Informação Crítica, e Proteção de Dados.

Palavras Chave: Segurança - Informação - Resposta - Incidente - Sistema Produtivo

1. INTRODUÇÃO

Os processos tradicionais de resposta a incidentes de segurança da informação utilizam uma estrutura de abordagem linear de plano de ação, como ilustrado na Figura 1. Nesses tipos de abordagens, a preparação leva à detecção, que é seguida pela contenção, permitindo a erradicação e feedback para o próximo estágio de preparação. Embora grande parte da literatura tenha se concentrado nas práticas técnicas para implementar recursos de resposta a incidentes de segurança dentro das organizações, pesquisadores também identificaram e discutiram vários problemas com esses processos atuais. Essas críticas se concentraram em abordagens muito lineares, não refletindo o ciclo de vida simultâneo de tratamento de incidentes do mundo real, não fornecendo informações suficientes sobre as causas do incidente e não maximizando os benefícios dos recursos forenses digitais (GRISPOS; GLISSON; STORER, 2014).

Nos últimos anos, segundo (PAPASTERGIOU; MOURATIDIS; KALOGERAKI, 2019), uma série de abordagens e estruturas de resposta a incidentes de segurança foram introduzidas pelas comunidades de pesquisa e industriais, bem como por vários organismos de padronização. Embora muitas dessas abordagens forneçam orientações técnicas específicas, com o objetivo de aprimorar as capacidades de resposta a incidentes de segurança das organizações, elas apresentam limitações significativas.

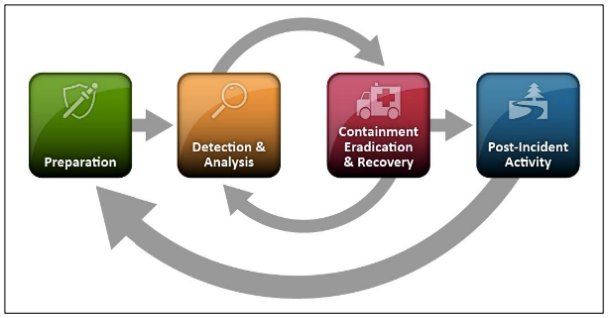

Figura 1 Ciclo de vida de resposta a incidente do NIST.
Fonte: (CICHONSKI, MILLAR, et al., 2012)

Desse modo, a questão da pesquisa é: Quais os problemas identificados na literatura em relação aos processos ou modelos tradicionais de resposta a incidentes de segurança da informação?

Os problemas identificados nos processos tradicionais de resposta a incidentes de segurança da informação são identificados na literatura através de uma pesquisa bibliométrica.

Entre a fundamentação para justificar a pesquisa, pode-se constar:

- Ajudar as equipes de resposta a incidentes a se desenvolverem;
- Encontrar os problemas do processo de resposta a incidentes de segurança e gerar melhorias;
- Identificar quais os pontos fracos dos processos de resposta a incidentes de segurança;

Além disso, de acordo com (IOANNOU; STAVROU; BADA, 2019), as principais limitações das abordagens existentes são as seguintes:

a) os tradicionais modelos lineares de resposta a incidentes são muito lentos, ineficazes e não atendem a capacidade altamente eficiente necessária para lidar e gerenciar incidentes atuais;

b) foco principalmente no elemento proativo (ou seja, fornecer assistência e informações para ajudar a preparar e proteger) da gestão de incidentes;
c) as abordagens atuais não fornecem uma visão suficiente clara sobre as causas subjacentes do incidente;
d) disposições insuficientes para o planejamento de incidentes;
e) subutilização do valor da evidência forense necessária para possível ação legal subsequente;
f) não levam em consideração os resultados relacionados ao risco produzidos pelas metodologias de avaliação de risco existentes.

Para (NYRE-YU; GUTZWILLER; CALDWELL, 2019), a resposta a incidentes de segurança é um domínio cada vez mais importante no fornecimento de suporte defensivo e ofensivo a empresas em todo o mundo. À medida que o campo avança tecnologicamente, é imperativo que os esforços dos fatores humanos acompanhem o ritmo de representação da metade humana do sistema homem-máquina.

O objetivo geral dessa pesquisa pode ser definido como: Realizar pesquisa bibliométrica com o objetivo de identificar os principais problemas ou questões nos processos ou modelos tradicionais de resposta a incidentes de segurança da informação.

Os objetivos específicos são: Pesquisa bibliométrica sobre os problemas nos processos ou modelos tradicionais de resposta a incidentes de segurança da informação; e Análise quantitativa e qualitativa da pesquisa bibliométrica;

2. BIBLIOMETRIA E REFERENCIAL TEÓRICO

A análise bibliométrica deste trabalho utilizou a base de pesquisa do Google Scholar e foram escolhidas palavras-chaves relacionadas ao problema da pesquisa. Entre as palavras chaves estão incluídas "*security incident response*", "*issue*", "*problem*", "*traditional method*".

A pesquisa bibliométrica utilizou como referencial inicial o trabalho realizado por (GRISPOS; GLISSON; STORER, 2014). Os autores publicaram em 2014 alguns dos problemas relacionados à resposta de incidentes de segurança da informação, conforme resumido na Figura 2.

Security Incident Response Issue	Citation(s)
The traditional linear incident response model does not support the highly efficient capability that is required to handle and manage today's incidents.	(Gonzalez 2005; Grimes 2007; Werlinger et al. 2010)
There is a progression flaw in linear processes, if one phase in the linear process is not completed, the entire process cycle may stop midstream.	(Grimes 2007)
Important steps, are often skipped because the incident response process is too focused on containment, eradication, and recovery.	(Ahmad et al. 2012; Grimes 2007; Tan et al. 2003)
Current approaches do not provide enough insight into the underlying causes of the incident.	(Ahmad et al. 2012; Jaatun et al. 2009; Shedden et al. 2010; Shedden et al. 2011)
Poor provisions for incident planning.	(Tan et al. 2003)
Do not maximize the benefits of digital forensic capabilities.	(Casey 2005; Casey 2006)
Undermine the value of forensic evidence possibly required for subsequent legal action.	(Casey 2005; Tan et al. 2003)

Figura 2 Questões sobre resposta a incidentes de segurança
Fonte: (GRISPOS; GLISSON; STORER, 2014).

Os documentos resultados encontrados foram analisados quantitativamente e qualitativamente com a utilização do protocolo de pesquisa PRISMA-P (*Preferred Reporting Items for Systematic Review and Meta-Analysis Protocols*) com o objetivo fornecer a justificativa para a revisão sistemática e uma abordagem metodológica e analítica pré-planejada, antes do início de uma revisão.

O protocolo PRISMA-P foi desenvolvido como um guia para ajudar os autores a planejarem revisões sistemáticas e meta-análises que retornem um conjunto mínimo de itens importantes a serem incluídos no protocolo de pesquisa (MOHER et al., 2015) e vem sendo amplamente utilizado em pesquisas associadas às ciências humanas.

3. METODOLOGIA

A metodologia deste estudo, de acordo com PRODANOV & DE FREITAS (2013), pode ser classificada quanto à natureza como *pesquisa básica*. Quanto ao objetivo, como *pesquisa exploratória e descritiva*. E quanto ao procedimento científico, *pesquisa bibliométrica*.

Esta pesquisa contará com abordagem quantitativa e qualitativa para análise e tratamento dos dados que serão obtidos por meio de análise bibliométrica e revisão sistemática.

Para a realização da bibliometria foram escolhidos os termos de pesquisa em inglês: *Security Incident Response*, *Traditional Method*, *Issue* e *Problem*. Foram pesquisados artigos científicos em idioma inglês, publicados nos últimos seis anos e de acesso público.

A ferramenta de pesquisa utilizada foi o *Publish or Perish* para consulta à base científica Google Scholar. Foram configurados os artigos que possuíssem os termos escolhidos no título e corpo do texto. O período de pesquisa e coleta dos artigos deu-se no mês de outubro de 2020.

Para revisão sistemática utilizou-se o protocolo PRISMA-P (MOHER et al., 2015), que conta com quatro etapas: identificação, triagem, elegibilidade e documentos incluídos para análise crítica.

3.1. FORMA DE EXECUÇÃO DA PESQUISA

A pesquisa foi realizada utilizando a ferramenta *Publish or Perish* e escolhendo a base de dados Google Scholar foi selecionada.

Após aplicação dos termos de pesquisa, foram coletados os metadados dos documentos localizados extraídos do *Publish or Perish*. Este agrupamento de metadados foi realizado com auxílio do Microsoft Excel, na qual se procurou eliminar os documentos duplicados e extrair dados bibliométricos para compor parte dos dados para análise quantitativa deste trabalho.

Buscou-se em seguida o acesso aos artigos publicados para realização da análise qualitativa, leitura integral e crítica dos documentos selecionados.

Para análise qualitativa e revisão sistemática, foi elaborada uma tabela de registro de avaliação, com critérios definidos como importantes e pertinentes para seleção dos documentos.

3.2. PROCEDIMENTOS DA PESQUISA

A Tabela 1 ilustra a quantidade de artigos encontrados com os termos de busca indicados na respectiva coluna. As demais colunas tratam-se das métricas dos artigos de cada busca, as quais são o total de citações que o grupo de artigos tiveram e as citações por ano e por artigo. Uma vez que os resultados não foram analisados, existem artigos repetidos que aparecem em cada busca.

Tabela 1 Artigos localizados e seus termos de busca.

Termos de busca	Quantidade de artigos	Total de citações	Citações por ano	Citações por artigo
“security incident response” AND “problem” AND "traditional method" from 2014	14	38	9,50	2,71
“security incident response” AND "traditional model" AND "problem" from 2014	22	143	23,83	6,50
“security incident response" [title], "process" AND "issue" from 2014	45	312	52,00	6,93
“security incident response" [title], "incident response process" AND "issue" from 2014	19	76	2,67	4,00
Total	**100**			

Fonte: elaborado pelo autor

Após a eliminação dos artigos duplicados, o resultado da pesquisa inicial produziu uma quantidade de 72 itens, os quais foram submetidos a tentativas de *download* e verificação se realmente são artigos científicos. Entretanto, a partir desse resultado foi possível analisar a quantidade de artigos por ano e a distribuição dos artigos por país.

A Figura 3 mostra a quantidade total dos artigos localizados agrupados por ano, indicando uma tendência de aumento de artigos publicados com os termos utilizados na busca a partir do ano de 2017.

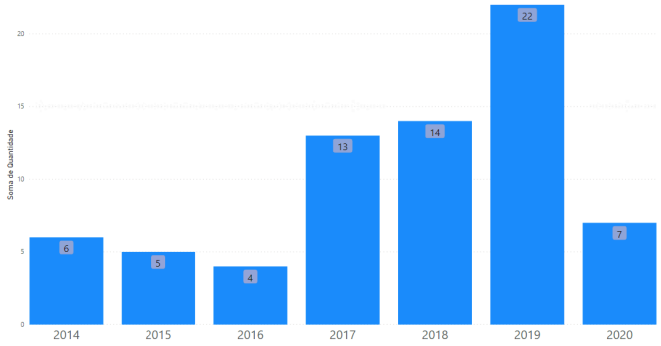

Figura 3 Quantidade total de artigos localizados agrupados por ano
Fonte: elaborado pelo Autor

A Figura 4 é a representação da distribuição dos artigos no mapa *mundi* com a quantidade de publicações por país. Percebe-se a existência de concentração de publicações nos Estados Unidos (24) e também a distribuição dos demais artigos em 22 países.

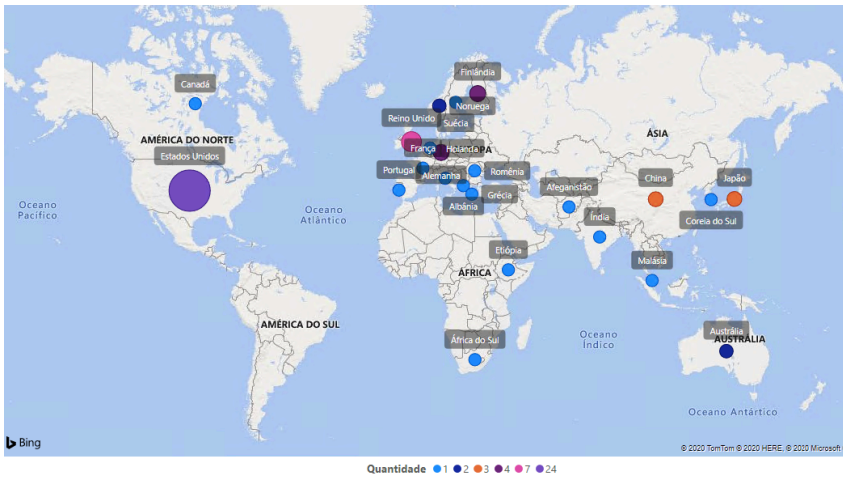

Figura 4 Distribuição dos artigos por países de acordo com as quantidades de documentos
Fonte: elaborado pelo Autor

A ilustra o fluxograma do protocolo PRISMA-P contendo passo a passo o processo de triagem em que, a partir 100 documentos, obteve-se o resultado de 20 documentos selecionados.

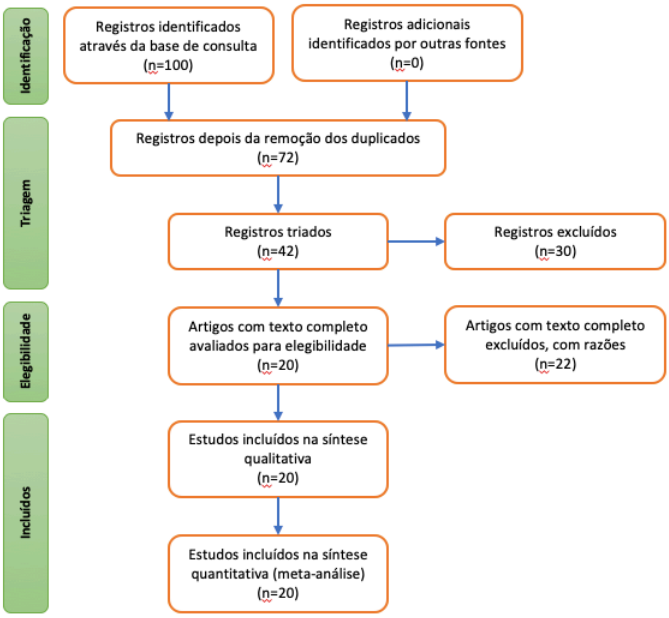

Figura 5 Fluxograma PRISMA-P
Fonte: elaborado pelo autor.

A Tabela 2 apresenta o resultado da pesquisa após a aplicação do protocolo PRISMA-P Desse modo, dos 71 itens resultaram listados um total de 20 artigos científicos, os quais serão submetidos a uma análise qualitativa. Os documentos da tabela estão ordenados primeiro pelo número decrescente de citações; segundo pelo número decrescente do ano da publicação; e terceiro pela ordem crescente do seu título.

Tabela 2 Quantidade de artigos localizados no *Publish or Perish* após triagem inicial.

Cita-ções	*Autores*	*Título*	*Ano*	*País*
184	R Baskerville, P Spagnoletti, J Kim	Incident-centered information security: Managing a strategic balance between prevention and response	2014	Estados Unidos
123	N Tuptuk, S Hailes	Security of smart manufacturing systems	2018	Reino Unido
18	G Grispos, WB Glisson, T Storer	Rethinking security incident response: The integration of agile principles	2014	Reino Unido
16	G Grispos, WB Glisson, T Storer	Security incident response criteria: A practitioner's perspective	2015	Estados Unidos
9	G Grispos, WB Glisson, T Storer	Enhancing security incident response follow-up efforts with lightweight agile retrospectives	2017	Estados Unidos
5	G Grispos, WB Glisson, T Storer	How good is your data? Investigating the quality of data generated during security incident response investigations	2019	Estados Unidos
3	Z Dsouza	Are Cyber Security Incident Response Teams (CSIRTs) Redundant or Can They Be Relevant to International Cyber Security	2017	Estados Unidos
3	WZA Zakaria	Application of case based reasoning in IT security incident response	2015	Malásia
2	A Ahmad, KC Desouza, SB Maynard	How integration of cyber security management and incident response enables organizational learning	2019	Austrália
2	S Souissi, A Serhrouchni, L Sliman	Security incident response: Towards a novel decision-making system	2017	França

Cita-ções	*Autores*	*Título*	*Ano*	*País*
1	S Papastergiou, H Mouratidis	Cyber Security Incident Handling, Warning and Response System for the European Critical Information Infrastructures (CyberSANE)	2019	Grécia
1	T Yohannes, L Lessa, S Negash	Information Security Incident Response Management in an Ethiopian Bank: A Gap Analysis	2019	Etiópia
1	S von Maltzan	No Contradiction Between Cyber-Security and Data Protection? Designing a Data Protecton Compliant Incident Response System	2019	Alemanha
0	M Ioannou, E Stavrou, M Bada	Cybersecurity Culture in Computer Security Incident Response Teams: Investigating difficulties in communication and coordination	2019	Reino Unido
0	M Nyre-Yu, KA Sprehn, BS Caldwell	Informing Hybrid System Design in Cyber Security Incident Response	2019	Estados Unidos
0	M Nyre-Yu, RS Gutzwiller	Observing Cyber Security Incident Response: Qualitative Themes From Field Research	2019	Estados Unidos
0	M Ohmori	On Automation and Orchestration of an Initial Computer Security Incident Response by Introducing Centralized Incident Tracking System	2019	Japão
0	YN Imamverdiyev	A Model For Optimal Planning Of Information Security Incident Response Operations	2018	Arzebaijão
0	M BONFANTI	Another–Int On The Horizon? Cyber-Intelligence Is The New Black	2017	Romênia
0	G Harde, J Großmann	Car Security Incident Response	2017	Alemanha

Fonte: elaborado pelo autor.

A análise qualitativa dos documentos selecionados utiliza a avaliação de cinco critérios no formato de perguntas assertivas que podem ser pontuados com os valores de 1 (um), quando o critério for plenamente atendido, 0,5 (meio), quando o critério for parcialmente atendido, ou 0 (zero), quando o critério não for atendido.

Após a atribuição das notas de cada critério para cada documento e a sua somatória, houve a reclassificação dos documentos refletindo as suas qualidades de modo que os documentos com pontuação próxima a zero têm menor qualidade, enquanto os próximos a cinco têm maior qualidade. Assim, a tabela está ordenada de forma decrescente na coluna *Pontos*. O resultado da classificação pode ser observado na

Tabela 3.

Tabela 3 Avaliação qualitativa dos documentos selecionados

Cita-ções	***Título***	***Ano***	***Critérios****					***Pontos***
			A	***B***	***C***	***D***	***E***	
16	Security incident response criteria: A practitioner's perspective	2015	1,0	1,0	1,0	1,0	1,0	5,0
9	Enhancing security incident response follow-up efforts with lightweight agile retrospectives	2017	1,0	1,0	1,0	1,0	1,0	5,0
2	How integration of cyber security management and incident response enables organizational learning	2019	1,0	1,0	1,0	1,0	1,0	5,0
1	Information Security Incident Response Management in an Ethiopian Bank: A Gap Analysis	2019	1,0	1,0	1,0	1,0	1,0	5,0
0	Cybersecurity Culture in Computer Security Incident Response Teams: Investigating difficulties in communication and coordination	2019	1,0	1,0	1,0	1,0	1,0	5,0
0	Observing Cyber Security Incident Response: Qualitative Themes From Field Research	2019	1,0	1,0	1,0	1,0	1,0	5,0
184	Incident-centered information security: Managing a strategic balance between prevention and response	2014	1,0	1,0	0,5	1,0	1,0	4,5

Cita-ções	*Título*	*Ano*	*Critérios**					*Pontos*
			A	*B*	*C*	*D*	*E*	
3	Application of case based reasoning in IT security incident response	2015	1,0	1,0	0,5	1,0	1,0	4,0
2	Security incident response: Towards a novel decision-making system	2017	1,0	1,0	0,5	1,0	1,0	4,5
1	Cyber Security Incident Handling, Warning and Response System for the European Critical Information Infrastructures (CyberSANE)	2019	0,5	1,0	1,0	1,0	1,0	4,5
0	On Automation and Orchestration of an Initial Computer Security Incident Response by Introducing Centralized Incident Tracking System	2019	1,0	1,0	0,5	1,0	1,0	4,5
18	Rethinking security incident response: The integration of agile principles	2014	0,5	1,0	1,0	1,0	0,5	4,0
5	How good is your data? Investigating the quality of data generated during security incident response investigations	2019	1,0	1,0	0,5	1,0	0,5	4,0
0	Informing Hybrid System Design in Cyber Security Incident Response	2019	1,0	0,5	1,0	1,0	0,5	4,0
0	A model for optimal planning of information security incident response operations	2018	1,0	0,5	1,0	1,0	0,5	4,0
0	Car Security Incident Response	2017	0,5	0,5	1,0	1,0	1,0	4,0
3	Are Cyber Security Incident Response Teams (CSIRTs) Redundant or Can They Be Relevant to International Cyber Security	2017	0,0	0,5	0,5	1,0	0,5	2,5
1	No Contradiction Between Cyber-Security and Data Protection? Designing a Data Protecton Compliant Incident Response System	2019	0,5	1,0	0,0	0,5	0,5	2,5
0	Another–int on the horizon? Cyber-intelligence is the new black	2017	0,5	0,5	0,5	0,5	0,5	2,5
123	Security of smart manufacturing systems	2018	0,5	0,5	0,0	0,5	0,5	2,0

Legenda: * Critérios usados: A. O documento é um artigo de pesquisa? B. Os objetivos da pesquisa são claramente descritos? C. O documento aborda exatamente o tema pesquisado nesta pesquisa? D. Os resultados estão descritos no documento? E. O estudo possui valor para a academia ou para a indústria?

4. RESULTADOS E DISCUSSÃO

Após a filtragem e classificação qualitativa dos documentos, foram encontradas indicações de algumas questões aos processos tradicionais de resposta de incidente de segurança da informação, as quais serão tratados nesta seção. Relembrando, estes processos seguem uma abordagem linear de plano de ação, na qual a preparação leva à detecção que é seguida pela contenção que permite a erradicação e feedback para o próximo estágio de preparação. A Tabela 4 resume as questões encontradas nos artigos selecionados.

Tabela 4 Resumo das questões e respectivos artigos

Grupo de questões	*Publicações*
Desempenho do processo de resposta a incidentes de segurança	(GRISPOS; GLISSON; STORER, 2014); (GRISPOS; GLISSON; STORER, 2015); (PAPASTERGIOU; MOURATIDIS; KALOGERAKI, 2019); (OHMORI, 2019)
Comunicação e Compartilhamento de Informação	(GRISPOS; GLISSON; STORER, 2015); (ZAKARIA, 2015); DSOUZA (2017); (IOANNOU; STAVROU; BADA, 2019); (NYRE-YU; GUTZWILLER; CALDWELL, 2019);
Automatização dos Processos e Inteligência	SOUISSI et al. (2017); BONFANTI (2017); (IMAMVERDIYEV, 2018); (OHMORI, 2019); (NYRE-YU; SPREHN; CALDWELL, 2019);
Aprendizado com os Incidentes	(AHMAD et al., 2020); (GRISPOS; GLISSON; STORER, 2017); (GRISPOS; GLISSON; STORER, 2019);

Tratamento de Incidentes na Manufatura e Indústria	(TUPTUK; HAILES, 2018); (GUNNARHARDE, 2018);
Incidentes em Infraestrutura de Informação Crítica	(PAPASTERGIOU; MOURATIDIS; KALOGERAKI, 2019); (YOHANNES; LESSA; NEGASH, 2019);
Proteção de Dados	(VON MALTZAN, 2019)

Fonte: elaborado pelo autor

4.1 DESEMPENHO DO PROCESSO DE RESPOSTA A INCIDENTES DE SEGURANÇA

GRISPOS et al. (2014) foram uns dos primeiros autores a reunir e apresentar crítica aos problemas com os processos de resposta a incidentes de segurança. Entre as críticas estão: os processos tradicionais possuem abordagens muito lineares, não refletindo o ciclo de vida simultâneo de tratamento de incidentes do mundo real, não fornecendo informações suficientes sobre as causas do incidente e não maximizando os benefícios dos recursos forenses digitais.

GRISPOS et al. (2014) propuseram como uma possível solução para esses problemas a integração de princípios e práticas ágeis disciplinadas no processo de resposta a incidentes de segurança. O tratamento iterativo e incremental de incidentes, a redução da incerteza e a atenção contínua à excelência técnica para melhorar a eficiência e eficácia da resposta a incidentes de segurança do mundo real.

Do ponto de vista da estratégia organizacional da segurança da informação, as estruturas de segurança são centradas em medidas de prevenção a incidentes. Entretanto, em um ambiente de segurança cada vez mais dinâmico, é necessário maior estrutura de segurança orientada para a resposta aos incidentes (GRISPOS; GLISSON; STORER, 2015).

PAPASTERGIOU et al. (2019) também abordam a existência de uma falha de progressão nos processos tradicionais, pois se uma fase do processo linear não for concluída, todo o ciclo do processo pode parar no meio do caminho e observa que os processos atuais de resposta a incidentes estão muito focados na contenção, erradicação do tratamento de incidentes de segurança cibernética e atividades relacionadas à recuperação e geralmente ignoram, pulam ou não enfatizam outras etapas importantes, como ações de investigação.

Entre os desafios identificados estão a falta de conscientização dos funcionários, a lacuna de informações entre os departamentos, a falta de responsáveis por incidentes experientes e qualificados e o aprimoramento de novas ameaças (OHMORI, 2019).

4.2 COMUNICAÇÃO E COMPARTILHAMENTO DE INFORMAÇÃO

GRISPOS et al. (2015) identificaram em sua pesquisa que conflitos entre a equipe de resposta a incidentes de segurança e as unidades de negócio sustentam a ideia de equipes multidisciplinares. A ideia é encorajar o aumento da comunicação entre todas as partes interessadas em resolver um incidente. Uma equipe multidisciplinar de resposta a incidentes de segurança pode exigir a integração de profissionais técnicos de segurança e especialistas em tecnologia da informação, com as partes interessadas de ativos relevantes (GRISPOS; GLISSON; STORER, 2015)

O compartilhamento de habilidades e informações entre as equipes de resposta a incidentes é uma outra questão da comunicação trazido por Zakaria (2015). A enorme quantidade de notificações de incidentes recebidos representa um grande desafio para os responsáveis pelo tratamento dos incidentes responderem da forma mais eficaz possível.

Enquanto no submundo do crime, os criminosos cibernéticos cooperam compartilhando informações sobre *exploits* e *zero-days* e até mantendo uma espécie de mercado negro que vende registros confidenciais roubados, *exploit kits* e *templates* de *malware*, do outro lado os

responsáveis por incidentes, em sua maioria, têm outras funções a cumprir dentro de sua organização e têm recursos limitados para lidar com quaisquer incidentes no menor tempo possível. Por isso, os responsáveis pelo tratamento dos incidentes são aconselhados a compartilhar suas experiências, melhores práticas, habilidades e truques com outros responsáveis por incidentes (ZAKARIA, 2015).

Se os CSIRTs não forem capazes de se adaptar para responder a incidentes cada vez mais sofisticados em uma escala maior, a segurança cibernética global se tornará menos estável. Devem adaptar seu comportamento funcional e operacional através das lições de outros esforços de resposta a emergências para poder ajudar as vítimas e contribuir com a comunidade auxiliando no desenvolvimento de outros CSIRTs (DSOUZA, 2017).

Uma dificuldade apontada por Dsouza (2017) é que as leis nacionais impedem a capacidade dos CSIRTs de compartilhar dados e as informações coletadas e compartilhadas podem ser imprecisas devido a subnotificação e inconsistências.

Ioannou et al. (2019) argumentam que para melhorar a eficácia dos CSIRTs, as informações relevantes como confiança, compartilhamento de dados, melhor comunicação e cooperação devem ser exploradas, e são importantes para atingir altos níveis de desempenho.

A pesquisa de Ioannou et al. (2019) revelou que, apesar da gestão tentar melhorar a comunicação e coordenação entre as diferentes equipes dentro da organização, são muitos os obstáculos que os funcionários encontram durante a análise de um evento. O principal aspecto para criar uma cultura de segurança cibernética em um CSIRTs é o gerenciamento de equipe. Os gerentes precisam ter a capacidade de treinar suas equipes, definir metas, fornecer orientações e coordenar cada grupo de indivíduos para completar uma tarefa com sucesso, mantendo um alto nível de espírito de equipe.

Nyre-Yu et al. (2019) conduziu um estudo de campo qualitativo em três equipes de resposta a incidentes de segurança de computadores (CSIRTs) e incluiu as perspectivas de equipes do governo, da academia e do setor privado. Foram fornecidas percepções sobre vários aspectos da resposta a incidentes, incluindo compartilhamento de informações, organização, aprendizado e automação e se apresentou a necessidade de se concentrar na integração vertical de problemas em diferentes níveis do sistema de resposta a incidentes também é discutida.

O trabalho de Nyre-Yu et al. (2019) revela percepções valiosas baseadas no contexto de três CSIRTs diferentes, e os resultados indicam que examinar a integração vertical de questões revela conexões entre fatores em uma variedade de perspectivas e disciplinas. Os resultados deste estudo indicam que há uma infinidade de áreas nas quais a pesquisa pode se expandir para ajudar a construir uma compreensão mais completa dos ambientes.

4.3 AUTOMATIZAÇÃO DOS PROCESSOS E INTELIGÊNCIA

Souissi et al. (2017) destaca que a criação de uma ferramenta de tomada de decisão que simplifique o tratamento de alertas e ajude os analistas de segurança é uma prioridade. O autor propõe um novo sistema de tomada de decisão baseado em aprendizado de máquina em um ambiente heterogêneo, enfrentando diferentes ataques e fornecendo respostas adequadas.

O desafio é como garantir uma boa e rápida resposta de um ataque ou mesmo uma decisão de resposta automática, enquanto fornece uma descrição de ataque precisa e simplicidade e flexibilidade de integração. Isso permite fazer interface com outras ferramentas de segurança e responder até mesmo a novos ataques de acordo com uma política de segurança definida pelo usuário (SOUISSI et al., 2017).

Bonfanti (2017) propõe a adoção de conceitos, ferramentas e práticas para a elaboração e compartilhamento de uma inteligência mais abrangente sobre ameaças cibernéticas. Essa inteligência, que ele rotula como "ciber-inteligência" (cyber-INT ou CYBINT), deve permitir que seus consumidores compreendam os contextos operacionais, táticos e estratégicos das ameaças, prevendo seus desenvolvimentos no curto, médio e longo prazos, e tomar decisões informadas sobre as ações preventivas a serem tomadas.

O modelo tradicional tem uma aplicabilidade limitada ao ciberespaço e não pode explicar com precisão o processo de elaboração da ciber-inteligência. Entendida como um ciclo linear e reiterativo, não enfatiza a natureza inter-relacionada das atividades (planejamento, coleta, processamento etc.) em que consiste o processo de ciber-inteligência e sua relevância mútua (BONFANTI, 2017).

Imamverdiyev (2018) propõe uma abordagem para modelagem dos processos de tratamento de incidentes de segurança da informação através do algoritmo de Evolução Diferencial (ED) para solucionar a questão urgente da distribuição operacional de incidentes de segurança da informação em tempo real entre os grupos.

É difícil automatizar os processos de resposta a incidentes de segurança da informação, que é principalmente executado pelo ser humano. Além disso, atualmente a resposta a incidentes é composta por uma série de novas dificuldades: a perda de controle sobre o ambiente de computação em nuvem e serviços *auto sourcing*, o aumento da complexidade dos ataques e os custos insuficientes de segurança das organizações. (IMAMVERDIYEV, 2018)

Abordagens sistemáticas para atividades de gerenciamento de incidentes contribuem para responder com sucesso a um incidente. Conforme descrito em muitos padrões internacionais e boas práticas, a política, o plano e os procedimentos de gerenciamento de incidentes de segurança da informação fazem parte da capacidade de gerenciamento de incidentes da organização. Não se pode negar que, por não ter um plano e procedimentos tão importantes, pode-se pausar questionando se uma organização realmente possui forma efetiva e eficiente de resposta a incidentes. (OHMORI, 2019)

Ohmori (2019) analisa que uma resposta inicial eficaz pode evitar a operação incorreta e, portanto, manter essa disponibilidade. No entanto, pode ser difícil fazer uma resposta inicial mais rápida e adequada. Para isso, ele propõe automatizar e orquestrar uma resposta inicial a incidentes usando o Sistema de Rastreamento de Incidentes (ITS)

Nyre-Yu et al. (2019) relatam que além da pressão de escassez de mão de obra, sistemas e ataques estão se tornando mais avançados, e as estratégias de defesa do analista de resposta de incidentes devem se adaptar para fornecer segurança consistente para organizações. Uma abordagem emergente é buscar soluções híbridas que combinem a criatividade e adaptabilidade dos humanos com a velocidade e o poder de computação da inteligência artificial (IA).

As descobertas do trabalho de Nyre-Yu et al. (2019) revelam outros aspectos das organizações que surgem ao investigar os processos de resposta a incidentes de segurança básicos, incluindo fatores como política, vários níveis de gerenciamento e práticas de comunicação e compartilhamento de informações.

4.4 APRENDIZADO COM OS INCIDENTES

Uma das principiais críticas ao processo tradicional de resposta a incidentes é a pouca ênfase na utilização da fase de acompanhamento pós-incidente. Esta fase permite a reflexão sobre a experiência do tratamento de incidentes, em que as "lições aprendidas" são identificadas para incorporação nos procedimentos operacionais padrão (AHMAD et al., 2020). Se espera que uma organização use as informações coletadas durante uma investigação para aprender

com um incidente, melhorar seu processo de resposta a incidentes e impactar positivamente o ambiente de segurança mais amplo (GRISPOS; GLISSON; STORER, 2017).

Muitas vezes o aprendizado normalmente é feito por meio de uma série de relatórios formais, reuniões e apresentações para a gerência após o encerramento de uma investigação de incidente. As lições aprendidas de uma investigação podem incluir informações sobre melhorias nos controles de segurança existentes, juntamente com a análise da necessidade de mudanças nos processos e procedimentos de resposta a incidentes de segurança existentes (GRISPOS; GLISSON; STORER, 2019).

Um fator que contribui para a deficiência de aprendizado, conforme GRISPOS et al. (2017) é que as abordagens de resposta a incidentes de segurança com foco na indústria, normalmente, fornecem poucas informações práticas sobre ferramentas ou técnicas que podem ser usadas para extrair lições aprendidas de uma investigação. Assim, se concentram em melhorar os controles técnicos de segurança e não em reexaminar a eficácia ou eficiência das políticas e procedimentos internos.

GRISPOS et al. (2017) propuseram que a implementação de retrospectivas ágeis leves, em um processo de resposta a incidentes de segurança, pode melhorar o *feedback* e/ou esforços de acompanhamento e indicam que retrospectivas podem ser usadas para aprimorar os dados coletados durante futuras investigações de segurança.

AHMAD et al. (2020) destacam o aprendizado de ciclo duplo (*double-loop learning*), que envolve em ciclos de experimentação e *feedback* por meio da reestruturação de estratégias, normas e processos. Para organizações que operam em ambientes turbulentos, o *double-loop learning* oferece a oportunidade única de comparar as normas estabelecidas com o ambiente em mudança e institucionalizar as mudanças necessárias nas rotinas organizacionais.

A pesquisa de Ahmad et al. (2020), expõe a necessidade de maiores pesquisas nas interações dentro de cada equipe e entre a organização e atores da ameaça, no compartilhamento eficaz informações de segurança, *know-how* e no desenvolvimento colaborativo de habilidades e conhecimentos entre os indivíduos nas equipes de gestão de segurança da informação e resposta a incidentes. Outro ponto importante trazido por Grispos et al. (2019) é que quaisquer dados coletados durante o curso de uma investigação sejam traduzidos em informações acionáveis terão um impacto direto na viabilidade da inteligência derivada.

4.5 TRATAMENTO DE INCIDENTES NA MANUFATURA E INDÚSTRIA

Com o avanço tecnológico, o processo de resposta a incidentes é cada vez mais necessário na manufatura e na indústria. Entretanto, de acordo com Tuptuk e Hailes (2018), embora existam esforços para padrões internacionais e nacionais para automação industrial e sistemas de controle, atualmente não há padrões de segurança cibernética específicos para a manufatura, muito menos manufatura inteligente.

Na prática, segundo Tuptuk e Hailes (2018), pouco se sabe sobre as capacidades de resposta e recuperação a incidentes de segurança dos operadores de sistemas de manufatura, e menos ainda sobre as operações de manufatura inteligentes. Portanto, é difícil determinar o quão bem as organizações estão preparadas e respondendo aos incidentes de segurança. Um dos poucos estudos realizados nesta área mostra que medidas comuns de gerenciamento de incidentes, como documentação, conscientização e treinamento, e resposta, são limitadas e mal estabelecidas na indústria. Eles também relatam que, apesar das normas e diretrizes, existem diferenças fundamentais entre os operadores sobre o que constitui um incidente de segurança.

As ameaças que os sistemas de manufatura enfrentam são críticas e os incidentes, sejam eles maliciosos ou acidentais, ocorrerão pelo menos ocasionalmente. No entanto, não seria um

eufemismo dizer que a abordagem existente das organizações de sistemas de manufatura para o gerenciamento de incidentes é assistemática e manual; os incidentes são gerenciados quando são notados, usando quaisquer meios que estejam disponíveis (TUPTUK; HAILES, 2018).

Gunnarhard (2018) apresenta um processo de resposta a incidentes de segurança específico para automóveis. Os clientes, o público e os reguladores esperam que os fabricantes e fornecedores tomem medidas técnicas e organizacionais para garantir que os incidentes de segurança de automóveis desencadeados por ataques cibernéticos e outras atividades indesejáveis sejam identificados, e tenham suas causas eliminadas e consequências mitigadas.

O modelo de referência de processo proposto por Gunnarhard (2018) é genérico o suficiente para que, em princípio, qualquer empresa da indústria automotiva possa utilizá-lo para derivar um processo adequado para si; ao mesmo tempo, o modelo leva em consideração os processos já existentes na indústria automotiva. O autor destaca três desafios especiais a serem superados pelo processo de resposta de incidentes de segurança de automóveis:

Detectar e resolver incidentes de segurança de automóveis requer um alto grau de experiência em segurança. Na análise de um incidente de segurança de veículos e na criação de um plano de ação, as dependências funcionais e não funcionais dos componentes de TI devem ser compreendidas e levadas em consideração. É crucial ter visão sistêmica, e não tanto visão de componente (GUNNARHARD, 2018)

4.6 INCIDENTES EM INFRAESTRUTURA DE INFORMAÇÃO CRÍTICA

Conforme Papastergiou et al. (2019), as informações de segurança disponíveis e as soluções de gerenciamento de eventos carecem de recursos reativos e pós-incidentes significativos para gerenciar incidentes e eventos no escopo das CIIs (*Critical Information Infrastructures*) baseada em TI, fornecendo orientação técnica inadequada para os profissionais de resposta a incidentes sobre como detectar, investigar e reproduzir ataques.

Apesar da importância socioeconômica das ferramentas e técnicas para lidar com incidentes, ainda não existe uma maneira fácil, estruturada, padronizada e confiável de gerenciar e prever incidentes de segurança cibernética que leve em consideração a heterogeneidade e complexidade das CIIs. Portanto, há uma necessidade premente de desenvolver novos sistemas para tratamento eficiente de incidentes e ataques cada vez mais sofisticados (PAPASTERGIOU; MOURATIDIS; KALOGERAKI, 2019).

Papastergiou et al. (2019) propõem uma solução chamada de sistema CyberSANE, que visa melhorar a detecção e análise de ciberataques e ameaças em CIIs e aumentar o conhecimento do cenário atual de ciberameaças. Em particular, o sistema CyberSANE ajuda as organizações a aumentar sua preparação, melhorar sua cooperação entre si e adotar as medidas adequadas para gerenciar riscos de segurança, relatar e lidar com incidentes de segurança.

Outra área de informações críticas, o setor bancário, para Yohannes et al. (2019) os analistas de ciberataque que participaram da pesquisa apontaram que a lacuna de informações entre departamentos e o atraso na resposta são desafios notáveis que afetam a prática de gerenciamento de incidentes no banco. A experiência de um analista de incidentes pode ser obtida de duas maneiras: por meio de ensaio e atividades de aprendizagem pós-incidente. Não é uma boa prática esperar pela ocorrência de um incidente para aprender com ela; em vez disso, é recomendável conduzir um ensaio baseado em cenário para melhorar a experiência do respondente ao incidente e identificar lacunas a serem gerenciadas de antemão.

Entre as questões no tratamento de incidentes no setor bancário estão relacionados a conscientização dos funcionários, falta de analistas de incidentes qualificados, problemas na

comunicação e necessidade de aprimoramento para novas ameaças. (YOHANNES; LESSA; NEGASH, 2019)

4.7 PROTEÇÃO DE DADOS

Von Maltzan (2019) traz à discussão que os métodos de coleta, análise e compartilhamento de dados e o estabelecimento de políticas e procedimentos para priorizar o tratamento de incidentes levantam várias questões jurídicas.

Devido às crescentes e complexas ameaças de ataques externos e internos aos sistemas de TI é exigido um compartilhamento mais eficaz de informações entre empresas e autoridades. Von Maltzan (2019) propõe que organizar as técnicas práticas de detecção, notificação e compartilhamento de informações comumente usadas na Resposta a Incidentes de fato protegem, ao invés de ameaçar, a privacidade e os direitos de proteção de dados.

O processo de resposta a incidentes lida rotineiramente com informações pessoais. Desse modo, deve haver medidas apropriadas implementadas para garantir que o escopo dos dados fornecidos a organizações externas seja estritamente controlado, havendo a remoção de informações de identificação pessoal ou o uso de criptografia sempre que possível. (VON MALTZAN, 2019).

Von Maltzan (2019) sugere que uma política de compartilhamento bem definida para determinar quais tipos de informações podem ser fornecidos a diferentes organizações deve ser implementada.

5. CONCLUSÃO

Este trabalho descreveu a realização de uma pesquisa bibliométrica que procurou responder a questão de pesquisa “Quais os problemas identificados na literatura em relação aos processos ou modelos tradicionais de resposta a incidentes de segurança da informação?”. A pesquisa encontrou vinte artigos que descrevem problemas e desafios no processo de resposta a incidentes. Estes resultados foram agrupados em sete grupos e discutidos na seção 4.

Os temas relevantes encontrados foram: Desempenho do processo de resposta a incidentes de segurança, Comunicação e Compartilhamento de Informação, Automatização dos Processos e Inteligência, Aprendizado com os Incidentes, Tratamento de Incidentes na Manufatura e Indústria, Incidentes em Infraestrutura de Informação Crítica, e Proteção de Dados.

Como sugestão de trabalhos futuros pode se citar a necessidade de realização de *survey* com os profissionais das equipes de resposta a incidente de segurança da informação com o objetivo de mapear os problemas e questões que estes profissionais conseguem perceber ao executar suas atividades.

REFERÊNCIAS

AHMAD, A. et al. How integration of cyber security management and incident response enables organizational learning. **Journal of the Association for Information Science and Technology**, v. 71, n. 8, p. 939–953, 1 ago. 2020.

BONFANTI, M. E. **Another-Int on the horizon? Cyber-Intelligence is the new black**. [s.l: s.n.]. Disponível em: <http://stixproject.github.io/supporters/.>.

CICHONSKI, P. et al. Computer Security Incident Handling Guide - 800-61 V2. [S.l.]. 2012.

ENISA, EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY. **Good Practice Guide for Incident Management**. [S.l.]. 2010.

DSOUZA, Z. Are Cyber Security Incident Response Teams (CSIRTs) Redundant or Can They Be Relevant to International Cyber Security? **Federal Communications Law Journal**, p. 201, 2017.

ENISA, EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY. **Good Practice Guide for Incident Management**. [S.l.]. 2010.

GRISPOS, G.; GLISSON, W. B.; STORER, T. Rethinking Security Incident Response: The Integration of Agile Principles. 2014.

GRISPOS, G.; GLISSON, W. B.; STORER, T. How Good is Your Data? Investigating the Quality of Data Generated During Security Incident Response Investigations. 2019.

GRISPOS, G.; GLISSON, W.; STORER, T. Security Incident Response Criteria: A Practitioner's Perspective. **21st Americas Conference on Information Systems (AMCIS 2015)**, 2015.

GUNNARHARDE. Car Security Incident Response. [s.l: s.n.].

IMAMVERDIYEV, Y. A model for optimal planning of information security incident response operations. **Problems of Information Technology**, v. 09, n. 2, p. 69–80, 10 jul. 2018.

IOANNOU, M.; STAVROU, E.; BADA, M. Cybersecurity Culture in Computer Security Incident Response Teams Investigating difficulties in communication and coordination. 2019.

MOHER, David et al. Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement. Systematic Reviews, v. 4, n. 1, p. 1, 2015. Disponível em: <https://systematicreviewsjournal.biomedcentral.com/articles/10.1186/2046-4053-4-1>

NYRE-YU, M.; GUTZWILLER, R. S.; CALDWELL, B. S. Observing Cyber Security Incident Response: Qualitative Themes From Field Research. **Proceedings of the Human Factors and Ergonomics Society Annual Meeting**, v. 63, n. 1, p. 437–441, nov. 2019.

NYRE-YU, M.; SPREHN, K. A.; CALDWELL, B. S. **Informing Hybrid System Design in Cyber Security Incident Response**. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). **Anais**...Springer Verlag, 2019

OHMORI, M. On automation and orchestration of an initial computer security incident response by introducing centralized incident tracking system. **Journal of Information Processing**, v. 27, p. 564–573, 2019.

PAPASTERGIOU, S.; MOURATIDIS, H.; KALOGERAKI, E. M. Cyber security incident handling, warning and response system for the european critical information infrastructures (cyberSANE). Communications in Computer and Information Science. Anais...Springer Verlag, 2019

SOUISSI, S. et al. **Security incident response: Towards a novel decision-making system**. Advances in Intelligent Systems and Computing. **Anais**...Springer Verlag, 2017

VON MALTZAN, S. No contradicton between Cyber-Security and Data Protecton? Designing a Data Protecton compliant Incident Response System. **European Journal of Law and Technology**, v. 10, n. 1, 2019.

YOHANNES, T.; LESSA, L.; NEGASH, S. Information Security Incident Response Management in an Ethiopian Bank: A Gap Analysis. 2019.

ZAKARIA, W. Z. Application of Case Based Reasoning in IT Security Incident Response CBR for incident response View project intelligent low-interaction honeypot deployment View project. **3rd International Conference Recent treads in Engineering and Technology (ICRET'2015)**, 2015.