SIMPROFI Simpósio dos Programas de Mestrado Profissional 24 e 25 de novembro de 2021
Produção de Conhecimento em Programas de Mestrado e Doutorado Profissionais: Experiências e Desafios
Centro Paula Souza
GOVERNO DO ESTADO DE SÃO PAULO

Princípios Ágeis na Resposta a Incidentes de Segurança nos Sistemas Produtivos: uma Revisão Sistemática

Rodrigo Sotolani[1], Napoleão Galegale[2];

Resumo: Os sistemas produtivos têm se integrado ao cenário digital onde tudo está conectado impulsionados pela *Indústria 4.0*. Neste ambiente complexo, heterogêneo e interconectado, é necessária a observação dos pilares da segurança da informação: a integridade, a confidencialidade e a disponibilidade. Para responder aos incidentes de segurança da informação, governos e organizações mantém os CSIRTs, acrônimo de *Computer Security Incident Response Teams,* que gerenciam os incidentes por meio de processos para detectar, analisar, responder e aprender com incidentes. Entretanto, estas equipes de resposta a incidentes geralmente seguem uma estrutura rígida e hierárquica, indicando problemas em seus processos. A abordagem ágil vem sendo considerada uma boa opção para a solução desses problemas uma vez que os princípios ágeis vem sendo utilizados em áreas fora do desenvolvimento de software e também por atender nas soluções que não são muito claras no início, por focar nas pessoas, em constantes feedbacks e na aceitação de constantes mudanças O presente trabalho se objetivo a realizar uma revisão sistemática da literatura situada no domínio da resposta a incidentes de segurança nos sistemas produtivos agregados aos princípios e valores ágeis. Desse modo, a questão de pesquisa deste artigo “Quais resultados são encontrados na literatura sobre a utilização dos princípios ágeis nos processos de resposta a incidentes de segurança da informação dos sistemas produtivos?”, resultou em seis artigos que de abordam a utilização de princípios ágeis na resposta a incidentes de segurança da informação. Assim, a pesquisa demonstrou uma lacuna sobre a utilização de princípios ágeis na resposta a incidentes de segurança da informação. O resultado contribui demonstrando a necessidade de realização de novas pesquisas sobre a utilização dos princípios ágeis em segurança da informação. Vislumbra-se que esta área pode ter maiores contribuições ao longo da realização de futuras pesquisas.

Palavras-chave: Princípio Ágil, Resposta a Incidente, Segurança da Informação, Cyber Segurança, Sistemas Produtivos.

Abstract: Production systems have been integrated into the digital scenario where everything is connected, driven by Industry 4.0. In this complex, heterogeneous and interconnected environment, it is necessary to observe the pillars of information security: integrity, confidentiality and availability. To answer to information security incidents, governments and organizations maintain CSIRTs, acronym for Computer Security Incident Response Teams, which manage incidents through processes to detect, analyze, respond and learn from incidents. However, these incident response teams generally follow a rigid and

[1] Centro Estadual de Educação Tecnológica Paula Souza – CEETPS, rodrigo.sotolani@cpspos.sp.gov.br
[2] Centro Estadual de Educação Tecnológica Paula Souza – CEETPS, nvg@galegale.com.br

hierarchical structure, indicating problems in their processes. The agile approach has been considered a good option for solving these problems since agile principles have been used in areas outside of software development and also for addressing solutions that are not very clear at the beginning, for focusing on people, on constant feedback and acceptance of constant changes The present paper aims to carry out a systematic review of the literature located in the field of response to security incidents in production systems, in addition to agile principles and values. Thus, the research question of this article "What results are found in the literature on the use of agile principles in information security incident response processes in production systems?", resulted in six articles that address the use of agile principles in responding to information security incidents. Thus, the survey demonstrated a gap in the use of agile principles in responding to information security incidents. The result contributes demonstrating the need for further research on the use of agile principles in information security. It is envisioned that this area may have greater contributions during future research.

Keywords: Agile Principle, Incident Response, Information Security, Cyber Security, Productive Systems.

1. Introdução

Alavancados pela Indústria 4.0, os sistemas produtivos têm se integrado ao cenário digital onde tudo é interconectado. Por meio de uma representação virtual em um nível mais alto de automação, muitos sistemas e softwares podem se comunicar da fábrica com as últimas tendências de tecnologias da informação e comunicação, alcançando todos os elementos da cadeia produtiva de valor em um engajamento em tempo real (ALCÁCER; CRUZ-MACHADO, 2019).

Os avanços tecnológicos dos sistemas produtivos criam e tratam informações valiosas que precisam ser protegidas para o sucesso industrial e segurança de todo o sistema. Em um ambiente complexo, heterogêneo e interconectado, é necessária a observação das premissas da integridade, da confidencialidade e da disponibilidade, pilares da segurança da informação.

O crescimento exponencial das interconexões da Internet levou a um crescimento significativo de incidentes de ataque cibernético, muitas vezes com consequências desastrosas e graves. Segundo Liu et al. (2019) e Modarresi e Symons (2020), com a ampla adoção das tecnologias da Internet das Coisas (IoT), a superfície de cyber-ataques aumentou drástica e profundamente, dando novos mecanismos para a intrusão e potencializando para danos catastróficos à privacidade, à segurança e à proteção de indivíduos e corporações.

Em um ataque cibernético bem-sucedido, as vítimas não seriam apenas organizações comerciais com perdas financeiras, mas também a população de todo o país. A falha de sistemas integrados com indústrias críticas pode levar a catástrofes ambientais e acidentes fatais (PAVLENKO, 2019).

A maioria dos dispositivos conectados aos Sistemas Cyber-Físicos (CPS) tem vida útil longa e muitos deles não recebem atualizações de segurança suficientes ou nunca são atualizados, resultando em ataques que podem ter consequências graves em vidas humanas, produtividade empresarial e segurança nacional (WALKER-ROBERTS et al., 2020).

A gestão da segurança da informação nas organizações e a agilidade na resposta aos incidentes de segurança da informação internos e externos

poderiam proporcionar uma maior competitividade, redução de riscos, ampliação do desempenho nas empresas.

Para responder aos incidentes de segurança da informação e motivados inicialmente pela *US Defense Advanced Research Projects Agency* (DARPA), governos e organizações mantém os CSIRTs, acrônimo de *Computer Security Incident Response Teams,* isto é, grupo de resposta de incidentes de segurança da informação (RUEFLE et al., 2014). Os CSIRTs gerenciam incidentes de segurança através de processos para detectar, analisar, responder e aprender com incidentes que ameaçam a confidencialidade, a disponibilidade e a integridade de dados e de sistemas críticos. (RUEFLE et al., 2014).

Um incidente de segurança da informação, segundo (CICHONSKI et al., 2012), se define como uma violação ou iminente ameaça de violação das políticas de segurança, políticas de uso ou práticas padrões de segurança. Conforme Galegale, Fontes e Galegale (2017), a informação tem importância estratégica, é impulsionada com a utilização de Tecnologia da Informação (TI) nos processos organizacionais e deve ter proteção adequada.

Os CSIRTs atuais usam políticas definidas, procedimento e guias para ajudar criar processos consistentes, orientados à qualidade e repetíveis (RUEFLE et al., 2014). Entretanto, Grispos et al. (2014) destacam que esta abordagem de plano de ação linear apresenta alguns pontos problemáticos, tais como: (1) Falta de eficiência para tratar e gerenciar incidentes; (2) Interrupção da investigação ao não completar uma fase do processo; (3) Foco excessivo na contenção, erradicação e recuperação; (4) Falta de clareza às causas raízes do incidente; (5) Planejamento fraco; (6) Não maximizar benefícios da forense digital; (7) Enfraquecimento do valor da evidência forense. Para Ahmad et al. (2012) ainda existe negligência no uso das lições aprendidas dos incidentes e das funções pós-incidente.

Estes processos de resposta a incidentes rígidos e procedimentais estão aumentando a previsibilidade dos esforços de defesa e tornam mais difícil proteger a infraestrutura restante e as funções de negócios no contexto de ataques cibernéticos rápidos e multifacetados (SMITH et al., 2021).

A abordagem ágil vem sendo considerada uma opção para a solução dos problemas de resposta a incidentes tradicionais uma vez que os princípios ágeis vem sendo utilizados em áreas fora do desenvolvimento de software tais como consultoria, manufatura, *coaching* e também por atender nas soluções não são muito claras no início, por focar nas pessoas, em constantes feedbacks e na aceitação de constantes mudanças (AMORIM et al., 2018). De acordo com Stefani e Feitosa (2019), a colaboração em equipes apresentou-se maior quando adotado métodos ágeis.

Desse modo, a questão de pesquisa deste artigo é “Quais resultados são encontrados na literatura sobre a utilização dos princípios ágeis nos processos de resposta a incidentes de segurança da informação dos sistemas produtivos?”.

O objetivo deste artigo é realizar um estudo de revisão sistemática em bases de artigos científico para identificar os trabalhos que tratam da abordagem ágil nos processos de resposta a incidentes de segurança da informação.

A sequência do presente artigo apresenta o referencial teórico na Seção 2; o método utilizado para o desenvolvimento do estudo na Seção 3; na Seção 4 são apresentados os resultados e discussões relativos aos documentos coletados; e por fim na Seção 5, as considerações finais.

2. Referencial Teórico

Nesta seção serão abordados em um breve referencial teórico na literatura pesquisada sobre as práticas ágeis aplicadas fora da área de desenvolvimento de *software* e a utilização dos princípios ágeis na resposta a incidentes de segurança da informação.

2.1 Práticas ágeis além do desenvolvimento de *software*

Os processos e práticas ágeis são caracterizados por seus valores e princípios subjacentes (BECK et al., 2001; FOWLER; HIGHSMITH, 2001). Seu uso trouxe solução para a crise do *software*, resolvendo o problema da elaboração de requisitos, mudanças e melhorias de *software*, aproximando desenvolvedores e donos dos produtos. Foi possível realizar a implementação de maneira iterativa e incremental, agregando valor ao produto através de melhorias contínuas.

Após um período de aumento nas taxas de sucesso no desenvolvimento de *software*, melhoria da qualidade e da velocidade e incentivo à motivação e produtividade de times de TI, os métodos ágeis estão se espalhando através de uma ampla faixa de indústrias e funções e até mesmo na alta gestão (RIGBY; SUTHERLAND; TAKEUCHI, 2016). Por exemplo, citam-se: produção de máquinas agrícolas, produção de novos jatos de caça, marketing, recursos humanos e até produção de vinho.

O uso híbrido dos métodos ágeis com métodos tradicionais foi sugerido por COOPER & SOMMER (2016) ao integrar a abordagem ágil ao método *Stage-Gate* visando alcançar benefícios potenciais para fabricantes de produtos físicos B2B. Também foi utilizado por Amorim et al. (2018) para gerenciar a implementação governança de TI com COBIT 5, chamada de *Water-Scrum-Fall*, que visava superar desafios como a falta de apoio da alta gestão e o desalinhamento de escopos e soluções.

2.2 Princípios ágeis na resposta a incidentes de segurança da informação

As práticas e princípios ágeis poderiam ajudar na solução dos desafios dos processos tradicionais de um CSIRT, como expostos por Grispos, Glisson e Storer (2014), os processos não refletem o dinamismo do mundo atual, são lentos e não são apropriados à natureza altamente colaborativa desses times.

Um *framework* para melhorar processos de resposta a incidentes em Sistemas de Controle Industrial (ICS) aplicando os benefícios dos valores e práticas ágeis foi proposto por He e Janicke (2015). Sob a perspectiva gerencial, os autores relacionam as características únicas dos ICS com os valores ágeis, mencionando a disponibilidade como principal preocupação.

Para Shedden et al. (2010) os atuais acompanhamentos de incidentes e atividades *post-mortem* representam uma fase crítica no processo. Os autores apontam a aplicação de aprendizado de *loop* duplo para questionar processos e princípios fundamentais, uma forma semelhante à retrospectiva do *SCRUM*.

O relatório técnico de Pfleeger (2017), dá perspectiva às habilidades sociais de um CSIRT, o que vai ao encontro do tema investigado nesta pesquisa. O ambiente de trabalho dos CSIRTs envolve atividades coletivas entre diferentes perfis de profissionais e se assemelham ao tipo VUCA, acrônimo para *volátil*,

incerto, *complexo* e *ambíguo*, um modo muito próximo aos princípios ágeis. O autor identificou diversos processos e dinâmicas sociais que contribuem para uma resposta de incidentes mais efetiva.

Tratando do tema sobre o processo de resposta a incidentes, os autores Grispos, Glisson e Storer (2017) destacam a sua fase final: o *feedback*/*follow-up*. Trazem que organizações encontram dificuldades em aprender com os incidentes e investigam a integração de retrospectivas leves ágeis e meta-retrospectivas ao processo de resposta a incidentes de segurança para aprimorar os esforços de *feedback* e *follow-up*.

Naseer et al. (2021) argumentam que (1) as organizações devem desenvolver agilidade em seus processo de resposta a incidentes para agirem com rapidez e eficiência às sofisticadas e potentes ameaças cibernéticas e que (2) a análise em tempo real dá às organizações uma oportunidade única de conduzir seu processo de resposta a incidentes de maneira ágil, detectando incidentes de segurança cibernética rapidamente e respondendo a eles de maneira proativa.

As equipes tradicionais de resposta a incidentes geralmente seguem uma estrutura rígida e hierárquica. Os indivíduos são alocados para uma função especializada, como *firewalls*, caça a ameaças, entre outros. Essa segregação de tarefas geralmente leva à criação de silos de informações e conhecimento, onde as tentativas de passar informações e habilidades para outras unidades relevantes podem ser abaixo do ideal (SMITH et al., 2021).

Há evidências empíricas de que os *playbooks*, ou seja, os procedimentos padrões estáticos de resposta a incidentes geralmente adotados, não oferecem flexibilidade suficiente para dar suporte a situações fora de seu escopo inicial e que foram ignorados quando os incidentes ocorreram. Uma análise temática de entrevistas semiestruturadas com profissionais de resposta a incidentes da ICS identificou três áreas principais de preocupação: comunicação, compartilhamento de informações entre áreas de conhecimento e obtenção de adesão externa (SMITH et al., 2021).

Smith et al. (2021) propõem que os princípios ágeis visam quebrar os silos de informações e conhecimento criando equipes mais integradas e para tanto, listam apenas três funções distintas dentro de uma equipe: proprietário do incidente, *SCRUM master* e membro da equipe, criando para isso um framework chamado de AIR4ICS, acrônimo de *Agile Incident Response For Industrial Control Systems*, dando novo significado às práticas ágeis aplicadas em segurança da informação.

3. Método

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, revisão sistemática.

A revisão bibliográfica utilizou a base de dados SCOPUS por sua abrangência de cobertura de áreas do conhecimento científico e se integrarem a ferramentas computacionais que auxiliam na recuperação dos metadados.

Os achados foram analisados quantitativa e qualitativamente com o protocolo de pesquisa PRISMA-P (*Preferred Reporting Items for Systematic*

Review and Meta-Analysis Protocols), visando uma revisão sistemática e uma abordagem metodológica e analítica pré-planejada. O uso deste protocolo motivou-se para assegurar a qualidade da pesquisa e também atingir a confiabilidade e validade dos resultados por meio da avaliação qualitativa dos artigos científicos selecionados.

Os dados foram coletados em setembro de 2021, com as palavras chaves utilizadas: "*agile principles", "security incident response"* e as variações "*agile method", "security incident handling"*. Não foram aplicadas limitações de data.

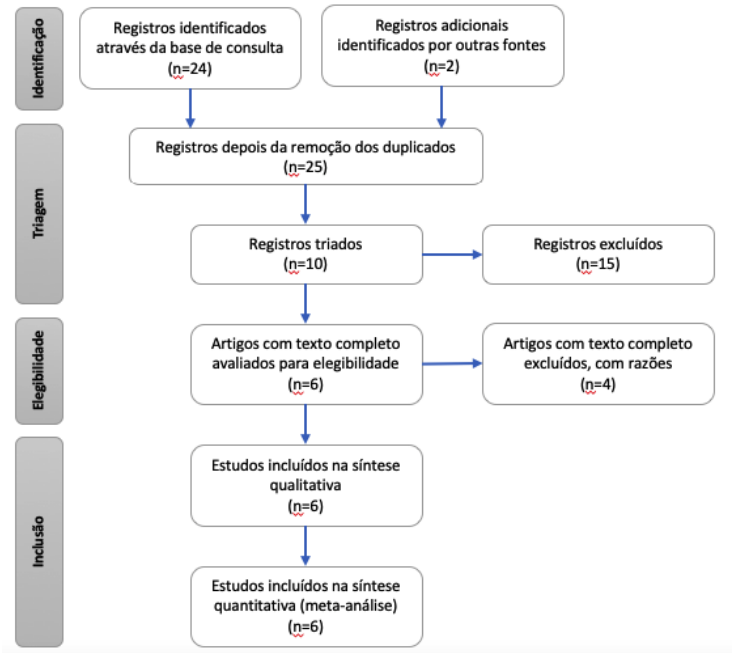
A Tabela 1 ilustra a quantidade de artigos encontrados com os termos de busca indicados na respectiva coluna. No total foram identificados 24 trabalhos publicados que compõem o corpus deste levantamento bibliométrico, exportados do SCOPUS para o Microsoft Excel.

Tabela 1 - Artigos localizados e seus termos de busca por base de pesquisa

Base	Termos de busca	Artigos
SCOPUS	(TITLE-ABS-KEY ("agile" OR "agile method" OR "agile principle*")) AND ((ALL (("cybersecurity" OR "computer security"))) AND (incident AND response))	24
	Total	24

Fonte: elaborado pelos autores

Figura 1 - Fluxograma do Protocolo PRISMA-P



Fonte: elaborado pelos autores

A Figura 1 ilustra o fluxograma do protocolo PRISMA-P contendo passo a passo em que, a partir 26 documentos, após triagem obtiveram-se o resultado de 10 documentos. Avançando para a fase de elegibilidade, resultaram 6 artigos, número que persistiu até a última fase.

A **Erro! Fonte de referência não encontrada.** apresenta o resultado da pesquisa após a aplicação elegibilidade do protocolo PRISMA-P. São mostrados seis estudos incluídos na síntese qualitativa, realizada com a sua leitura.

4. Resultados e discussão

Após o levantamento e tratamento dos dados, foram identificados seis artigos, exibidos no **Quadro 1** que atendiam o escopo do estudo, restrito aos artigos que tratam da utilização de princípios ágeis na resposta a incidentes de segurança da informação.

Quadro 1 Títulos resultantes selecionados

Título	Referência
Rethinking security incident response: The integration of agile principles	(GRISPOS; GLISSON; STORER, 2014)
Security incident response criteria: A practitioner's perspective	(GRISPOS; GLISSON; STORER, 2015)
Enhancing security incident response follow-up efforts with lightweight agile retrospectives	(GRISPOS; GLISSON; STORER, 2017)
Towards agile industrial control systems incident response	(HE; JANICKE, 2015)
Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis	(NASEER et al., 2021)
The Agile Incident Response for Industrial Control Systems (AIR4ICS) framework	(SMITH et al., 2021)

Fonte: elaborado pelos autores

Além do que foi mencionado na Seção 2, de referencial teórico, apresentamos na sequência o **Quadro 2** que resume os principais achados das publicações selecionadas, agrupado-os por seus autores.

Quadro 2 Resumo dos principais achados nas publicações selecionadas

Autores	Resumo dos achados na literatura pesquisada
G Grispos, WB Glisson, T Storer	Os autores propõem em (GRISPOS; GLISSON; STORER, 2014) uma integração ágil aos processos de resposta a incidentes de segurança da informação com (1) resposta a incidentes iterativo e incremental; (2) redução das incertezas; e (3) atenção contínua para excelência técnica. Os autores indicam que poucas pesquisas investigam a integração de princípios e práticas ágeis dentro dos processos de resposta de incidente de segurança da informação. Sugerem mais estudos para trabalhos futuros chamando de *Agile Incident Response*. Em (GRISPOS; GLISSON; STORER, 2015) propuseram que as organizações podem se beneficiar de uma abordagem alternativa para lidar e gerenciar incidentes de segurança, identificado como Critérios de Resposta a Incidentes de Segurança (SIRC) e que poderiam se integrar aos princípios e práticas ágeis. Em (GRISPOS; GLISSON; STORER, 2017) investigam a integração de retrospectivas e meta-retrospectivas ágeis leves em um processo de resposta a incidentes de segurança, para melhorar o feedback e/ou esforços follow-up.

Autores	Resumo dos achados na literatura pesquisada
Y He, H Janicke	Os autores examinam em (HE; JANICKE, 2015) o procedimento de resposta a incidentes de um *Industrial Control System* (ICS) sob perspectiva gerencial, identificando as características exclusivas de resposta a incidentes de sistemas de controles industriais e propõe uma estrutura para melhorar as capacidades da resposta a incidentes. Em particular, avalia o benefício dos valores ágeis para abordar características específicas da resposta a incidentes de sistemas de controle industrial.
A Naseer et al.	Os autores propõem em (NASEER et al., 2021) que as organizações podem obter agilidade na resposta a incidentes de segurança: (1) permitindo flexibilidade na resposta a incidentes (2) permitindo rapidez na resposta a incidente; e (3) permitindo inovação na resposta a incidentes.
R Smith et al.	O *framework* de Resposta Ágil a Incidentes para Sistemas de Controle Industrial (AIR4ICS) foi desenvolvido pelos autores para integrar técnicas ágeis no domínio da Segurança Cibernética de resposta a incidentes. O *framework* fornece uma abordagem dinâmica para melhorar a consciência situacional, compartilhamento de informações, tomada de decisão coletiva e flexibilidade de resposta dentro do contexto único do ICS. A AIR4ICS garante que as informações relevantes estejam disponíveis de forma clara e concisa, fornecendo recursos e técnicas para atribuir e apresentar as informações a todo o grupo. Ao garantir que todos os membros da equipe tenham um maior entendimento da estratégia de resposta geral, eles estarão mais aptos a tomar decisões informadas em seu próprio trabalho. O *design* modular do *framework* significa que pode ser adaptado para se adequar a outras práticas de trabalho, conjuntos de habilidades e prioridades de organizações. Os autores ressaltam que o *framework* melhora a comunicação, promove o compartilhamento de informações entre áreas de conhecimento e aumenta a adesão externa. Em última análise, o AIR4ICS fornece uma estrutura de decisão dinâmica que permite que as equipes de resposta a incidentes gerenciem a incerteza e imprevisibilidade para reduzir o tempo necessário para restaurar operações normais.

Fonte: elaborado pelos autores

Ao realizar a construção da síntese dos artigos selecionados neste estudo, identifica-se como lacunas de pesquisa o uso dos princípios ágeis na resposta a incidentes de segurança da informação em sistemas produtivos mas que começam a ser preenchidas nas pesquisas mais recentes como o trabalho de Smith et al. (2021).

5. Considerações finais

O presente trabalho de revisão sistemática da literatura situa-se no domínio da segurança da informação enfatizando a resposta aos incidentes de segurança nos sistemas produtivos. Foram agregados uma visão relacionada à

abordagem dos princípios e valores ágeis, os quais vem sendo utilizados fora da área de desenvolvimento de *software*.

O objetivo da pesquisa foi atendido ao realizar uma revisão sistemática em bases de artigos científico para identificar os trabalhos que tratam da abordagem ágil nos processos de resposta a incidentes de segurança da informação.

Em resposta a questão de pesquisa “Quais resultados são encontrados na literatura sobre a utilização dos princípios ágeis nos processos de resposta a incidentes de segurança da informação dos sistemas produtivos?”, a revisão sistemática realizada encontrou seis artigos que de abordam a utilização de princípios ágeis na resposta a incidentes de segurança da informação.

Assim, a pesquisa demonstrou uma lacuna sobre a utilização de princípios ágeis na resposta a incidentes de segurança da informação. Apesar de ter haver diversas pesquisas sobre o método ágil e sobre segurança da informação, ao aplicar filtros para princípios ágeis e resposta a incidentes de segurança da informação, ficou exemplificado o diminuto número de trabalhos.

O *framework* AIR4ICS demonstrou ser o mais próximo de uma proposta prática de aplicação dos princípios ágeis na resposta a incidentes.

O resultado contribui para o preenchimento da lacuna indicada demonstrando a necessidade de realização de novas pesquisas sobre este tema. Vislumbra-se que esta área poderia ter maiores contribuições ao longo da realização de futuras pesquisas. Além disso, o *framework* AIR4ICS pode ser incrementado com a sua aplicação e adaptação a outras áreas além dos sistemas de controle industrial.

Referências

AHMAD, A.; HADGKISS, J.; RUIGHAVER, A. B. Incident response teams - Challenges in supporting the organisational security function. **Computers and Security**, v. 31, n. 5, p. 643–652, 2012.

ALCÁCER, V.; CRUZ-MACHADO, V. **Scanning the Industry 4.0: A Literature Review on Technologies for Manufacturing SystemsEngineering Science and Technology, an International Journal**Elsevier B.V., , 1 jun. 2019.

AMORIM, A. C.; MIRA DA SILVA, M.; PEREIRA, R.; GONÇALVES, M. **Using scrum for implementing IT governance with COBIT 5**. Proceedings - 2018 IEEE 22nd International Enterprise Distributed Object Computing Conference, EDOC 2018. **Anais**...Institute of Electrical and Electronics Engineers Inc., 14 nov. 2018.

BECK, K.; BEEDLE, M.; VAN BENNEKUM, A.; COCKBURN, A.; CUNNINGHAM, W.; FOWLER, M.; GRENNING, J.; HIGHSMITH, J.; HUNT, A.; JEFFRIES, R. **Manifesto for Agile Software Development**. Disponível em: <http://agilemanifesto.org/>. Acesso em: 22 ago. 2020.

CICHONSKI, P.; MILLAR, T.; GRANCE, T.; SCARFONE, K. NIST Special Publication 800-61 Rev 2: Computer Security Incident Handling Guide. **National Institute of Standards and Technology (NIST)**, 2012.

FOWLER, M.; HIGHSMITH, J. **The Agile Manifesto**. [s.l: s.n.]. Disponível em: <www.martinfowler.com/articles/newMethodology.html>.

GALEGALE, N. V.; FONTES, E. L. G.; GALEGALE, B. P. Uma contribuição para a segurança da informação: Um estudo de casos múltiplos com

organizações brasileiras. **Perspectivas em Ciencia da Informacao**, v. 22, n. 3, p. 75–97, 1 jul. 2017.

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

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

GRISPOS, G.; GLISSON, W. B.; STORER, T. Enhancing security incident response follow-up efforts with lightweight agile retrospectives. **Digital Investigation**, v. 22, p. 62–73, 1 set. 2017.

HE, Y.; JANICKE, H. **Towards Agile Industrial Control Systems Incident Response**. BCS Learning & Development, 2015.

LIU, X.; QIAN, C.; HATCHER, W. G.; XU, H.; LIAO, W.; YU, W. Secure Internet of Things (IoT)-Based Smart-World Critical Infrastructures: Survey, Case Study and Research Opportunities. **IEEE Access**, v. 7, p. 79523–79544, 2019.

MODARRESI, A.; SYMONS, J. **Technological Heterogeneity and Path Diversity in Smart Home Resilience: A Simulation Approach**. Procedia Computer Science. **Anais**...Elsevier B.V., 2020.

NASEER, A.; NASEER, H.; AHMAD, A.; MAYNARD, S. B.; MASOOD SIDDIQUI, A. Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis. **International Journal of Information Management**, v. 59, 1 ago. 2021.

PAVLENKO, E. Y. Model of Cyberattacks on Digital Production Systems. **Automatic Control and Computer Sciences**, v. 53, n. 8, p. 1017–1019, 1 dez. 2019.

PFLEEGER, S. L. **IMPROVING CYBERSECURITY INCIDENT RESPONSE TEAM (CSIRT) SKILLS, DYNAMICS AND EFFECTIVENESS**. Rome, NY: [s.n.]. Disponível em: <http://www.dtic.mil>.

RIGBY, D. K.; SUTHERLAND, J.; TAKEUCHI, H. Embracing Agile. **Harvard Business Review**, v. 94, n. 5, p. 40–50, 2016.

RUEFLE, R.; DOROFEE, A.; MUNDIE, D.; HOUSEHOLDER, A. D.; MURRAY, M.; PERL, S. J. Computer Security Incident Response Team Development and Evolution. **IEEE Security & Privacy**, v. 12, n. 5, p. 16–26, 2014.

SHEDDEN, P.; AHMAD, A.; RUIGHAVER, A. B. Organisational Learning and Incident Response: Promoting Organisational Learning and Incident Response: Promoting Effective Learning Through The Incident Response Process Effective Learning Through The Incident Response Process. 2010.

SMITH, R.; JANICKE, H.; HE, Y.; FERRA, F.; ALBAKRI, A. The Agile Incident Response for Industrial Control Systems (AIR4ICS) framework. **Computers and Security**, v. 109, 1 out. 2021.

STEFANI, C. E.; FEITOSA, M. D. Colaboração no Desenvolvimento Ágil de Software: Um Estudo a Partir da Visão dos Participantes do Processo Produtivo. 2019.

WALKER-ROBERTS, S.; HAMMOUDEH, M.; ALDABBAS, O.; AYDIN, M.; DEHGHANTANHA, A. Threats on the horizon: understanding security threats in the era of cyber-physical systems. **Journal of Supercomputing**, v. 76, n. 4, p. 2643–2664, 1 abr. 2020.