

CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA
UNIDADE DE PÓS-GRADUAÇÃO, EXTENSÃO E PESQUISA
MESTRADO PROFISSIONAL EM GESTÃO E TECNOLOGIA EM
SISTEMAS PRODUTIVOS

RODRIGO SILVA SOTOLANI

PRINCÍPIOS ÁGEIS NA RESPOSTA A INCIDENTES DE SEGURANÇA DA
INFORMAÇÃO

São Paulo
Junho/2022

RODRIGO SILVA SOTOLANI

PRINCÍPIOS ÁGEIS NA RESPOSTA A INCIDENTES DE SEGURANÇA DA
INFORMAÇÃO

Dissertação apresentado como exigência parcial para a obtenção do título de Mestre em Gestão e Tecnologia em Sistemas Produtivos do Centro Estadual de Educação Tecnológica Paula Souza, no Programa de Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos, sob a orientação do Prof. Dr. Napoleão Verardi Galegale.

São Paulo

Junho/2022

S718p

Sotolani, Rodrigo Silva

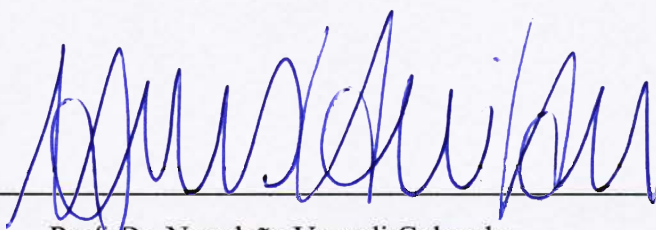
Princípios ágeis na resposta a incidentes de segurança da informação / Rodrigo Silva Sotolani. – São Paulo: CPS, 2022.
160 f. : il.

Orientador: Prof. Dr. Napoleão Verardi Galegale
Dissertação (Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos) – Centro Estadual de Educação Tecnológica Paula Souza, 2022.

1. Segurança da informação. 2. Princípios ágeis. 3. Resposta a incidente. 4. Poder judiciário. 5. CSIRT. I. Galegale, Napoleão Verardi. II. Centro Estadual de Educação Tecnológica Paula Souza. III. Título.

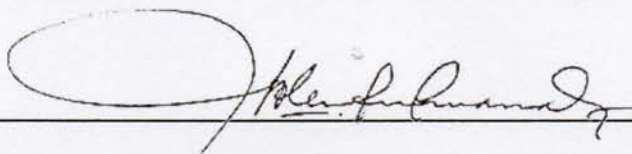
RODRIGO SILVA SOTOLANI

PRINCÍPIOS ÁGEIS NA RESPOSTA A INCIDENTES DE SEGURANÇA DA
INFORMAÇÃO



Prof. Dr. Napoleão Verardi Galeale

Orientador – CEETEPS



Prof. Dr. Joshua Onome Imoniana

Examinador Externo – USP



Prof. Dr. Carlos Hideo Arima

Examinador Interno - CEETEPS

São Paulo, 24 de junho de 2022

Dedico esta dissertação de mestrado a meu
marido Paulo, pelo enorme e fundamental
apoio dado no presente; a meus pais, Cristina e
Milton, pelo suporte dado no passado; e a
meus sobrinhos Emanuella, Alice e Frederico,
para se inspirarem a irem ainda mais longe no
futuro.

AGRADECIMENTOS

Quando se termina um trabalho de mais de dois anos e meio, após tantas fases, desafios, e ainda uma pandemia que obrigou o mundo todo a ficar em casa, tem-se muito a agradecer.

Sou grato à minha base, minha família, começando com os mais próximos, meu marido e meu filho canino que estiveram no dia a dia comigo durante toda essa jornada. Paulinho e Benji, sem vocês eu não teria conseguido, obrigado por tanto! E continuando com os que me permitiram estudar e me apoiaram no passado, meus pais Cristina e Milton, minhas irmãs, Dany e Paula que compartilharam comigo o início dessa jornada de educação. E minha tia Suzete que no passado sempre viu em mim um grande potencial e me incentivou.

Agradeço ao meu orientador, prof. Dr. Napoleão, por ter escolhido meu projeto e por realizar um trabalho orientação de forma leve, direta e cuidadosa, sempre apoiando, orientando e fazendo evoluir o trabalho durante todo o curso do mestrado.

Sou grato aos professores desse programa, que ao lado do meu orientador transformaram um estudante em um pesquisador, dando base e conhecimento para a realização desta pesquisa: doutores Arima, Duduchi, Marília, Galhardi, Formigone, Fabrício, Eliane, Okano e Rosinei.

Agradeço a todos os meus colegas das disciplinas que compartilharam essa caminhada comigo, em especial: Pedro Vitor, William Johnny, Isabella, Denis, Emerson e Mayara. E aos colegas já formados, das turmas anteriores, que me inspiraram: Diogo, Klauren e Antonio Celso.

Agradeço a toda equipe do Centro Paula Souza e da Secretaria especialmente à Débora e à Vilma que mantiveram constante apoio e contato. Um agradecimento à equipe técnica por ter viabilizado os acessos tecnológicos fazendo o mestrado acontecer mesmo à distância.

Aos meus colegas de trabalho no TRF3 e SJMS, e aos membros da CLRI, em especial: Eduardo, Laercio e Cristiano, que apoiaram diretamente nesta pesquisa. E à d. Níve e Leonardo, da JF de Dourados pelo enorme suporte nos últimos meses do curso.

Você não é uma gota no oceano. Você é um
oceano inteiro numa gota.
(*Rumi*)

RESUMO

SOTOLANI, R. S. **PRINCÍPIOS ÁGEIS NA RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO**. nn [160] f. Dissertação (Mestrado Profissional em Gestão e Tecnologia nos Sistemas Produtivos). Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2022.

O objetivo deste trabalho é adaptar e avaliar um processo baseado na aplicação dos princípios ágeis para tratamento e resposta de incidentes de segurança da informação em uma instituição do Poder Judiciário. A pesquisa identificou na literatura, problemas nos processos tradicionais de resposta a incidentes. Foi identificada a existência de lacuna de pesquisa da aplicação de princípios ágeis nestes processos. A metodologia utilizada para conduzir o estudo foi a *Design Science Research Methodology* – DSRM que incorpora princípios, práticas e procedimentos necessários para o *design*, desenvolvimento, demonstração e avaliação do processo em questão. O processo de resposta a incidentes de segurança da informação foi adaptado para utilizar princípios ágeis e implementado com um experimento prático com um time de resposta a incidentes (CSIRT) do TRF3 e nomeado de AIR-Jud. Avaliações interna e externa foram obtidas por meio de entrevistas semiestruturadas com profissionais da área de segurança da informação. Como resultado, o processo AIR-Jud foi avaliado como relevante e considerado contendo melhorias em relação aos processos tradicionais de resposta a incidentes. Como implicação prática, o AIR-Jud pode ser utilizado por CSIRTs do Poder Judiciário que visem a melhoria de seus processos. Como implicações teóricas, o presente trabalho contribui para a literatura preenchendo parte da lacuna sobre este tema.

Palavras-chave: Segurança da Informação. Princípios Ágeis. Resposta a Incidente. Poder Judiciário. CSIRT. DSRM.

ABSTRACT

SOTOLANI, R. S. **Agile principles in security incident handling**. nn [160] f. Dissertação (Mestrado Profissional em Gestão e Tecnologia nos Sistemas Produtivos). Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2022.

The objective of this work is to adapt and evaluate a process based on the use of agile principles for security incident handling in an institution of the Judiciary. The research identified problems in traditional incident response processes in the literature. The existence of a research gap in the application of agile principles in these processes was identified. The methodology used to conduct the study was the Design Science Research Methodology - DSRM, which incorporates principles, practices, and procedures necessary for the design, development, demonstration, and evaluation of the process in question. The information security incident response process was adapted to use agile principles and implemented with a practical experiment with a TRF3 incident response team (CSIRT) named AIR-Jud. Internal and external evaluations were obtained through semi-structured interviews with information security professionals. As a result, the AIR-Jud process was assessed as relevant and considered to contain improvements over traditional incident response processes. As a practical implication, AIR-Jud can be used by CSIRTs of the Judiciary that aim to improve their processes. As theoretical implications, the present work contributes to the literature filling part of the gap on this topic.

Keywords: Computer Security Information. Agile Principles. Incident Response. Judicial Power. CSIRT. DSRM.

LISTA DE QUADROS

Quadro 1 Critérios de inclusão do protocolo de revisão.....	25
Quadro 2 Critérios de exclusão do protocolo de revisão	25
Quadro 3 Títulos resultantes selecionados.....	28
Quadro 4 Resumo dos principais achados nas publicações selecionadas.....	30
Quadro 5 Resumo das etapas do processo de <i>Design Science</i>	53
Quadro 6 Tipos de Artefatos da DSRM.....	56
Quadro 7 Métodos para avaliação dos artefatos	59
Quadro 8 Papéis de uma equipe ágil de resposta a incidentes.....	67
Quadro 9 Os eventos do método <i>Scrum</i> adaptados para uma equipe de resposta a incidentes ágeis.....	69
Quadro 10 Artefatos do <i>Scrum</i> e <i>Kanban</i> adaptados ao contexto da resposta a incidentes de segurança cibernética	71
Quadro 11 Perfil dos avaliadores internos.....	84
Quadro 12 Perfil dos avaliadores externos	86

LISTA DE TABELAS

Tabela 1	Artigos localizados e seus termos de busca por base de pesquisa.....	26
Tabela 2	Autores dos trabalhos selecionados e índices de relevância do <i>Google Scholar</i>	29
Tabela 3	Resultado das médias das avaliações INTERNAS dos papéis.....	85
Tabela 4	Resultado das médias das avaliações INTERNAS dos artefatos.	85
Tabela 5	Resultado das médias das avaliações INTERNAS dos eventos.....	86
Tabela 6	Resultado das médias das avaliações EXTERNAS dos papéis.....	87
Tabela 7	Resultado das médias das avaliações EXTERNAS dos artefatos.	88
Tabela 8	Resultado das médias das avaliações EXTERNAS dos eventos.....	88

LISTA DE FIGURAS

Figura 1 Fluxograma do Protocolo PRISMA-P	27
Figura 2 Panorama de Tecnologia da Informação do Poder Judiciário	32
Figura 3 Serviços na Nuvem por quantidade de órgãos judiciários	34
Figura 4 Contexto do tratamento de incidentes na gestão de risco de segurança da informação	38
Figura 5 Lista de serviços comuns do CSIRTs	42
Figura 6 Ciclo de vida de resposta a incidente do NIST	42
Figura 7 Gerenciamento de Incidente e Tratamento de Incidente da ENISA	43
Figura 8 Fluxo de Processo de Tratamento de Incidente da ENISA	44
Figura 9 <i>Workflow</i> de Tratamento de Incidentes da ENISA	45
Figura 10 Ciclos da <i>Design Science Research</i>	52
Figura 11 Modelo do processo da <i>Design Science Research Methodology</i> (DSRM)	54
Figura 12 Relação entre constructos, modelos, métodos e instanciação conforme o DSRM	62
Figura 13 Constructos da pesquisa	62
Figura 14 Modelo dos processos de tratamento de incidentes com métodos ágeis	63
Figura 15 O modelo de resposta a incidentes adaptado com o método <i>Scrum</i>	64
Figura 16 O método <i>Scrum</i> adaptado para o modelo de resposta a incidentes	66
Figura 17 Estados e Regiões da Justiça Federal brasileira	73
Figura 18 Mapeamento das práticas ágeis no processo de resposta a incidentes	77
Figura 19 Quadro <i>Kanban</i> inicial com os incidentes a serem analisados	79
Figura 20 Exemplo de atividades constantes em cada item de <i>Incident Backlog</i>	80
Figura 21 Quadro <i>Kanban</i> após autoajuste definido pelo time <i>Scrum</i>	81
Figura 22 Resultado do quadro <i>Kanban</i> após o ciclo da <i>Sprint</i>	81
Figura 23 Classificação do time de resposta a incidentes	83

LISTA DE SIGLAS

AIR	<i>Agile Incident Response</i>
BCP	<i>Business Continuity Plan</i>
CERT	<i>Computer Emergency Response Team</i>
CJF	Conselho da Justiça Federal
CLRI	Comissão Local de Resposta a Incidente
CNJ	Conselho Nacional de Justiça
CSIRT	<i>Computer Security Incident Response Team</i>
DARPA	<i>US Defense Advanced Research Projects Agency</i>
DRP	<i>Disaster Recovery Plan</i>
DS	<i>Design Science</i>
DSRM	<i>Design Science Research Methodology</i>
ENISA	<i>European Network and Information Security Agency</i>
ENSEC-PJ	Estratégia Nacional de Segurança Cibernética e da Informação do Poder Judiciário
ETIR	Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética
IA	Inteligência Artificial
ICS	<i>Industry Control System</i>
IoT	<i>Internet of Things</i>
ISO	<i>International Organization for Standardization</i>
ITIL	<i>Information Technology Infrastructure Library</i>
NIST	<i>National Institute of Standards and Technology</i>
PJ	Poder Judiciário
RI	Resposta a Incidente
SI	Sistema de Informação
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
TI	Tecnologia da informação
TRF3	Tribunal Regional Federal d Terceira Região
VUCA	Acrônimo de volátil, incerto, complexo e ambíguo

SUMÁRIO

INTRODUÇÃO	16
1 FUNDAMENTAÇÃO TEÓRICA.....	21
1.1 Revisão da literatura.....	23
1.2 A informatização do Poder Judiciário brasileiro	32
1.3 Continuidade do negócio e recuperação de desastres.....	38
1.4 Resposta a incidentes de segurança da informação	41
1.5 Princípios ágeis.....	45
1.5.1 Práticas ágeis além do desenvolvimento de software	46
1.5.2 Princípios ágeis na resposta a incidentes de segurança da informação.....	47
2 METODOLOGIA.....	50
2.1 Etapa de identificação do problema e motivações	54
2.2 Etapa de objetivos para a solução	55
2.3 Etapa de <i>design</i> e desenvolvimento.....	55
2.4 Etapa de demonstração	58
2.5 Etapa de avaliação	58
2.6 Etapa de comunicação	60
3 PESQUISA EMPÍRICA	61
3.1 <i>Design</i> e desenvolvimento	61
3.1.1 As relações entre os artefatos constructo, modelo, método e instanciação	61
3.1.2 Processos adaptados do método Scrum	65
3.1.3 Papéis	67
3.1.4 Eventos.....	68
3.1.5 Artefatos do Scrum	71
3.2 Demonstração	72
3.2.1 O Tribunal Regional Federal da 3 ^a . Região.....	72
3.2.2 A Comissão Local de Resposta a Incidentes de Segurança da Informação.....	74
3.2.3 Detalhamento dos incidentes analisados no experimento.....	75
3.2.4 Demonstração do novo processo.....	78
3.3 Etapa de avaliação	82
3.3.1 Avaliação interna.....	83
3.3.2 Avaliação externa	86

3.4 Comunicação	89
4 CONSIDERAÇÕES FINAIS.....	90
REFERÊNCIAS	92
APÊNDICE A – roteiro de avaliação interna e externa do processo	98
APÊNDICE B – Guia para utilização do processo	101
APÊNDICE C – Respostas individualizadas do questionário de avaliação interna	105
APÊNDICE D – Respostas individualizadas do questionário de avaliação externa.....	107
APÊNDICE E – Relatório técnico conclusivo.....	109

INTRODUÇÃO

Os avanços tecnológicos criam, transformam e tratam informações valiosas que precisam ser protegidas para o sucesso da organização e segurança de todo o sistema. Neste ambiente complexo, heterogêneo e interconectado, é necessária a observação das premissas da integridade, da confidencialidade e da disponibilidade, pilares da segurança da informação (SAMONAS; COSS, 2014).

No setor privado, os sistemas produtivos caminham para a era da digitalização alavancados pela "Indústria 4.0", um dos temas com maior crescimento de pesquisa nos últimos anos. Nesta nova indústria, tudo está interconectado em um cenário digital com a respectiva representação virtual, permitindo que, em um nível mais alto de automação, muitos sistemas e *softwares* se comuniquem da fábrica utilizando as últimas tendências de tecnologias de informação e comunicação, alcançando todos os elementos da cadeia de valor em um engajamento em tempo real (ALCÁCER; CRUZ-MACHADO, 2019).

Segundo Liu et al. (2019), com a ampla adoção das tecnologias da Internet das Coisas (IoT), a superfície de ataques cibernéticos aumentou drástica e profundidade, fornecendo novos mecanismos para a intrusão e aumentando o potencial 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).

O funcionamento e a resiliência das sociedades modernas tornaram-se cada vez mais dependentes de infraestruturas críticas, ao ponto que perturbações provavelmente revelarão condições operacionais caóticas, nas quais os provedores de serviços de infraestrutura, serviços de emergência, polícia, municípios e outras partes interessadas importantes devam agir de forma eficaz para minimizar os danos e restaurar as operações normais (HEINO et al., 2019).

No setor público, o poder judiciário brasileiro tem avançado na informatização de seus sistemas. Nos últimos anos, o Judiciário brasileiro inovou e criou soluções para atender a população em meio à crise sanitária causada pela pandemia da Covid-19. Tendo a tecnologia como aliada, essas iniciativas garantiram a continuidade da prestação jurisdicional de forma célere e eficiente. Entre essas iniciativas, designadas como Justiça 4.0 pelo Conselho da Justiça

Federal, estão o Juízo 100% Digital, a Plataforma Digital do Poder Judiciário, a Plataforma Sinapes e Codex e o Balcão Virtual (CNJ, 2021a).

Os tribunais têm investido em modernização e tecnologia para manter os sistemas processuais em alta performance e garantir a segurança dos dados com a finalidade de viabilizar um atendimento ágil e seguro pelas unidades judiciais. Entretanto, diversas ações de *hackers* têm atingido o Poder Judiciário em seus vários níveis e especialidades (AGÊNCIA BRASIL, 2020a, 2020b, 2020c; BAGUETE, 2021; CONJUR, 2021a, 2021b; FOLHA, 2020; G1, 2021; STJ, 2020; TERRA, 2020; UOL, 2022).

Entre os ataques cibernéticos mais notáveis está o realizado no Superior Tribunal de Justiça (STJ) em novembro de 2020 que causou a interrupção de julgamentos que ocorriam nas suas seis turmas. Os sistemas do tribunal e o site oficial ficaram fora do ar e todos os prazos processuais foram suspensos por dez dias. Todos os funcionários se encontravam em regime de teletrabalho e tiveram seus acessos suspensos (AGÊNCIA BRASIL, 2020c).

Este ataque *hacker* foi tratado por peritos como 'o mais grave ataque' cibernético já verificado não apenas ao judiciário, mas em todos os órgãos públicos da capital federal. Mais de 255 mil processos tramitam na Corte e teriam sido capturados pelo *hacker* que adicionou chaves de criptografia a mais de 1,2 mil máquinas virtuais, além de destruir seus backups com um *ransomware* chamado RansomEXX (BAGUETE, 2021; TERRA, 2020). Os prejuízos à sociedade e a extensão dos danos causados pelo ataque e das informações a que os *hackers* tiveram acesso são difíceis de aferir, mas advogados temem que os dados dos clientes, que estavam na base do STJ, sejam usados para chantagem pelos criminosos (FOLHA, 2020).

As principais ações de proteção aos ativos do judiciário visam assegurar o princípio constitucional da segurança jurídica, preservar a continuidade da Justiça e proteção das informações dos processos e sistemas judiciais. Os impactos de ordem financeira, operacional e de reputação, demandam do Poder Judiciário uma resposta que minimize os danos dos eventuais ataques e reduza o tempo de não-funcionamento dos sistemas (CNJ, 2021b).

A pesquisa aqui realizada vai ao encontro da estratégia do judiciário em elevar o nível de segurança das infraestruturas críticas por meio das equipes de resposta a incidentes de segurança cibernética, conforme Estratégia Nacional de Segurança Cibernética e da Informação do Poder Judiciário aprovada pelo Conselho Nacional de Justiça.

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 e ampliação do desempenho nas organizações.

Os CSIRTs atuais, acrônimo de *Computer Security Incident Response Team*, isto é, grupo de resposta de incidentes de segurança da informação, usam políticas definidas, procedimento e guias para ajudar criar processos consistentes, orientados à qualidade e repetíveis (RUEFLE et al., 2014). Os processos utilizados são estilo modelo cascata, em que uma fase é seguida de outra, isto é, um plano de ação linear.

Estes processos 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).

Grispos et al. (2014) destacam que esta abordagem de plano de ação linear apresenta alguns pontos de atenção e problemas, tais como: (1) pouca 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) redução dos benefícios da forense digital; (7) enfraquecimento do valor da evidência forense. Para Ahmad et al. (2012) ainda existe a negligência no uso das lições aprendidas e das funções pós-incidente.

Em face a esses problemas, o paradigma ágil, em especial os princípios do *Scrum*, poderia ser considerado uma opção de solução devido à sua consagrada utilização em áreas fora do desenvolvimento de *software*. De acordo com Stefani & Feitosa (2019), a colaboração em equipes apresentou-se maior quando adotado métodos ágeis. Assim, poderia também atender quando as soluções não são muito claras no início, por focar nas pessoas, em constantes *feedbacks* e na aceitação de constantes mudanças (AMORIM et al., 2018).

Questão da pesquisa:

A questão de pesquisa é “Como os princípios ágeis podem ser aplicados nos processos de tratamento e resposta a incidentes de segurança da informação no Poder Judiciário?”

Objetivo geral:

O objetivo deste trabalho é examinar como adaptar e avaliar um processo baseado na aplicação dos princípios ágeis nos processos de tratamento e resposta de incidentes de segurança da informação no Poder Judiciário.

Os **objetivos específicos** deste trabalho são:

- i. Identificar o problema e motivação por meio do levantamento bibliométrico e revisão da literatura recente e da identificação dos problemas e questões em processos de resposta a incidentes;
- ii. Definir os objetivos da solução para melhoria nos processos de um CSIRT do Poder Judiciário;
- iii. Projetar e desenvolver a adaptação dos processos de um CSIRT do Poder Judiciário por meio da identificação dos princípios e práticas do método ágil;
- iv. Demonstrar a utilização de práticas ágeis nos processos de resposta a incidentes de segurança de informação em uma instituição do Poder Judiciário;
- v. Avaliar o processo com os atores envolvidos;
- vi. Comunicar os resultados da pesquisa;

Linha de pesquisa:

Este trabalho desenvolvido no Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos do pertence à Linha de Pesquisa de *Sistemas de Informação e Tecnologias Digitais* e ao Projeto de Pesquisa *Gestão Estratégica da Tecnologia da Informação* e explorou os temas da tecnologia da informação e segurança da informação.

Os sistemas produtivos e a engenharia de produção tratam de projetos, aperfeiçoamento e implantação de sistemas integrados de pessoas, materiais, informações, equipamentos e energia, para a produção de bens e serviços. Dentro dessa abordagem cabem não apenas os setores produtivos tradicionais, mas também outras atividades como ONGs, redes de empresas, interfaces colaborativas, e as entidades governamentais (DE JESUS; COSTA, 2014).

Os movimentos da Nova Gestão Pública e da Governança Digital, apesar de algumas diferenças, convergem para um sistema de pensamento caracterizado pela importação de ideias geradas em áreas do setor privado para dentro das organizações do setor público, visando atender às demandas da sociedade por melhores serviços (DE JESUS; COSTA, 2014).

O Poder Judiciário, como os demais órgãos públicos, presta serviços à sociedade, e atualmente são orientados ao cumprimento de metas, melhorias de processos, governança estratégica, orientação a resultados entre outros. Desse modo, se observa uma interface e associação aos preceitos dos sistemas produtivos aos serviços do Poder Judiciário.

Contribuições:

Do ponto de vista da gestão e da tecnologia em sistemas produtivos, a pesquisa contribui para a melhoria dos processos de resposta a incidentes de segurança da informação e dos seus CSIRTs, em especial aos órgãos do Poder Judiciário e aos gestores de segurança da informação.

Pretende-se com este trabalho, contribuir para que as organizações e os membros de CSIRTs possam agregar práticas ágeis em seus processos e com isso trazer outros subsídios para o aprofundamento desta temática.

Sob a perspectiva acadêmica, esta pesquisa colabora com a discussão a respeito da utilização de práticas ágeis em processos da segurança de informação dentro do escopo do Poder Judiciário, possibilitando a abertura de novas oportunidades de pesquisas envolvendo contextos específicos descritos neste trabalho. Por meio de um experimento prático, este estudo contribui para a literatura de resposta a incidentes, mostrando como a integração de princípios ágeis em processos lineares pode melhorar a resposta a incidentes.

1 FUNDAMENTAÇÃO TEÓRICA

Desde que o manifesto ágil foi criado em 2001, a comunidade de pesquisa dedicou muita atenção ao desenvolvimento ágil de *software*, trazendo mudanças sem precedentes no campo da engenharia de *software* (DINGSØYR et al., 2012). Por meio dos princípios e fundamentos contidos no manifesto ágil, o método auxiliou na solução para o problema da elaboração de requisitos, adaptação a mudanças, implementação de melhorias e aproximação de desenvolvedores com os donos dos produtos e de quem define os seus requisitos. A partir da filosofia ágil, foi possível realizar a implementação de *softwares* de maneira iterativa e incremental, agregando valor ao processo produtivo de maneira que melhorias contínuas são entregues ao produto (BECK et al., 2001; COHEN; LINDVALL; COSTA, 2004; CONBOY; FITZGERALD, 2004; DINGSØYR et al., 2012).

Em termos gerais, muitas áreas fora do desenvolvimento de *software* foram inspiradas a adotar os princípios ágeis. Entre os princípios, primeiro pode-se citar o desenvolvimento colaborativo, dando mais privilégios às pessoas do que aos processos. Em segundo lugar, a mentalidade predominantemente “enxuta” que visa minimizar o trabalho desnecessário, no lugar de criar extensa documentação. Terceiro, a participação ativa dos clientes ou partes interessadas na evolução do produto ou serviço e não mais ficarem à margem do desenvolvimento de *software*. Quarto, utilizar a incerteza como parte integrante do desenvolvimento de *software* (DINGSØYR et al., 2012).

Ao mesmo tempo em que, como proposto Viega & Mcgraw (2008), foram adicionadas camadas de segurança da informação na área de desenvolvimento de *software* envolvendo o ciclo de vida de projetos ágeis, os princípios ágeis passaram a ser considerados para área de resposta a incidentes, que é o foco desta pesquisa.

Fica demonstrado em alguns trabalhos (GRISPOS; GLISSON; STORER, 2014, 2017, 2015b; HE et al., 2022; HE; JANICKE, 2015; NASEER et al., 2021; SMITH et al., 2021), que existe uma lacuna de pesquisa na utilização do método ágil na área de resposta a incidentes de segurança da informação.

A área da segurança da informação lida com o aumento crescente de incidentes cibernéticos, muitas vezes por vulnerabilidades introduzidas no desenvolvimento de *software* que podem comprometer as garantias fundamentais da segurança da informação - a confidencialidade, a disponibilidade e a integridade (SAMONAS; COSS, 2014).

Conforme apresentado nas estatísticas do CERT.BR (2022), os ataques a servidores Web totalizaram 26.567 em 2020, um aumento de 19% em relação a 2019. Neste mesmo ano, o número de notificações de máquinas comprometidas teve um aumento 130%. No primeiro semestre de 2020, o número de notificações de servidores DNS maliciosos, utilizados como parte da infraestrutura para realização de fraudes financeiras, cresceu 66%.

Conforme relatório da Symantec (SYMANTEC, 2019), os ataques *web* aumentaram 56%, e os de *ransomware* contra empresas 12%. Os ataques à cadeia de suprimentos, assumindo formas como o sequestro de atualizações de *software* e a injeção de códigos maliciosos em softwares legítimos, aumentaram 78% em relação a 2018. Os desenvolvedores continuaram a ser explorados como origem de ataques, seja por meio de grupos de ataque que roubavam credenciais para ferramentas de controle de versão, ou por invasores que comprometiam bibliotecas de terceiros integradas em projetos de *software* maiores (SYMANTEC, 2019).

A resposta a incidentes de segurança da informação, como os relatados nos parágrafos anteriores, reflete como funciona a política de segurança da informação da organização. A implementação destas políticas, num ambiente de TI, é condição *sine qua non* para o processo de gerenciamento estratégico de qualquer organização (IMONIANA, 2004).

Imoniana (2004) cita que vários estudos apresentam evidências de que a responsabilidade pela manutenção de uma política de segurança recai principalmente sobre o Chefe de Segurança (*Chief Security Officer* - CSO). Este, ao fazê-la, busca aprimorar a atualização de tecnologias, a fim de atender às políticas de planejamento de continuidade de negócios abrangentes. Portanto, para que tal política seja efetiva, ela tem que ser totalmente adotada pelo Chefe do Executivo (*Chief Executive Officer* - CEO) (IMONIANA, 2004).

Para Souza et al. (2016), a melhoria e continuidade das operações dos governos e organizações é auxiliada com investimentos na segurança de seus ativos de informação visando a prevenção da perda, dano, destruição ou acesso não autorizado à informação.

As equipes de segurança da informação devem constantemente atuar, seja de forma proativa, por meio da avaliação de possíveis vulnerabilidades dos sistemas, seja de forma reativa, investigando as causas dos incidentes que venham a acontecer. Os times de resposta de incidentes das organizações, conhecidos como CSIRTs (*Computer Security Incident Response Team*) ou CERT (*Computer Emergency Response Team*), são responsáveis por receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores (CERT.BR, 2022a).

Um CSIRT normalmente presta serviços para uma comunidade bem definida, que pode ser a entidade que o mantém, como uma empresa, um órgão governamental ou uma organização acadêmica, podendo ser um grupo formal ou um grupo "*ad hoc*"(CERT.BR, 2022a).

O processo de resposta a incidentes geralmente é composto por cinco fases: preparação; detecção e análise; contenção; erradicação e recuperação (que podem constituir fases distintas); e revisão pós-incidente. No entanto, as abordagens lineares de resposta a incidentes, ou seja, um modelo cascata, geralmente consomem tempo, são ineficazes na resposta a ataques de grande escala, são muito complexas ao lidar com incidentes sofisticados e não têm oportunidades de aprendizado (GRISPOS; GLISSON; STORER, 2014; HE; JANICKE, 2015).

Desse modo, se propõe estudar a aplicação dos valores ágeis no atendimento dos serviços dos times de resposta de incidentes de maneira que estes valores possam ser incorporados nos processos de tratamento de incidentes. Com isso, pretende-se agregar valor ao plano continuidade de negócio das organizações.

A pesquisa realizada neste trabalho pode contribuir para a solução de alguns dos problemas enfrentados pelos times de tratamento de incidente em face aos desafios atuais. Entre eles, a diferença da constante evolução e aprimoramento da tecnologia, desenvolvimento de *software*, ameaças e riscos cibernéticos ao passo que os processos de tratamento de incidentes continuam os mesmos. Os princípios ágeis poderiam contribuir para aproximar as pessoas, os processos e as ferramentas dentro do escopo da resposta a incidentes de segurança cibernética no Poder Judiciário.

1.1 Revisão da literatura

A realização da pesquisa bibliométrica e da revisão da literatura foi uma das atividades iniciais desse trabalho para apresentar uma análise sistemática e síntese de pesquisa sobre a utilização de práticas ágeis nos processos de resposta a incidentes de segurança da informação. A revisão integrativa da literatura é uma forma de pesquisa que revisa, critica e sintetiza a literatura representativa sobre um tema de forma integrada, de modo que novos referenciais e perspectivas sobre o tema sejam gerados (TORRACO, 2005).

O foco da pesquisa é identificar a utilização dos princípios do manifesto ágil nos processos de resposta e tratamento de incidentes de segurança da informação. O método usa a redução e exibição dos dados de forma agrupada, comparando-os com base na verificação análoga.

Inicialmente, antes da pesquisa, ao pesquisar em bases de dados abertas como *Google Scholar* por “*princípios ágeis no tratamento e resposta a incidentes de segurança da informação*” de maneira completa ou com as principais palavras nos títulos das publicações, não houve retorno significativo de respostas indicando lacuna de pesquisa nesse tema.

A metodologia utilizada para esta revisão da literatura, 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 e revisão sistemática.

A revisão bibliográfica utilizou as bases de dados SCOPUS, *Web of Science*, *Scielo* e *Google Scholar*, por suas abrangências 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*) (MOHER D et al., 2015), 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 atingir a confiabilidade e validade dos resultados por meio da avaliação qualitativa dos artigos científicos selecionados. A escolha mostrou-se adequada para operacionalizar a pesquisa e ajudar para solução do problema, podendo ser reutilizado para chegar aos resultados.

Os dados foram coletados em abril de 2021 e depois atualizados em setembro de 2021. Os termos de pesquisa utilizados foram as palavras chaves “*agile principles*”, “*security incident response*” e as variações “*agile method*”, “*security incident handling*”. Foram aplicados os filtros de seleção de documentos publicados entre 2014 e 2021. O **Quadro 1** apresenta uma visão geral do protocolo de revisão da literatura e os motivos para sua inclusão.

Quadro 1 Critérios de inclusão do protocolo de revisão

Critério	Motivo de inclusão
Palavra-chave	"Agile principles" AND "security incident response", "Agile method" AND "security incident handling" e suas combinações.
Foco da pesquisa	Identificação de trabalhos que indiquem a utilização de práticas ou princípios ágeis na área de resposta a incidentes de segurança da informação.
Ferramentas da pesquisa	Sistema de busca do <i>Google Scholar</i> (https://scholar.google.com), do <i>Scopus</i> (https://www.scopus.com), do <i>Scielo</i> (https://search.scielo.org) e da <i>Web of Science</i> (https://www.webofscience.com).
Base de dados	SCOPUS, Web of Science, Scielo e Google Scholar
Período da pesquisa	2014 a 2021, considerando abranger publicação recentes, excluindo o ano corrente devido atributo do critério de exclusão.
Estudo quantitativo	Estudos que contenham a indicação de uso de algum princípio ou prática ágil na área de resposta a incidentes de segurança da informação

Fonte: Resultado da pesquisa

Como critérios de exclusão, apresentados no **Quadro 2**, foram considerados o tipo de publicação (livros, relatórios, *data sets*, somente citações a artigos e matérias jornalísticas), os artigos publicados em idioma que não sejam o inglês ou português, os com acesso não abertos e realizada análise para os que contenham terminologias não pertinentes ao tema do presente estudo, os artigos repetidos nos motores de pesquisa das bases de dados, e resumos dos artigos que não sejam condizentes e avaliação dos resumos dos artigos com o objeto de estudo.

Quadro 2 Critérios de exclusão do protocolo de revisão

Critério	Motivo de exclusão
Tipo de publicação	Somente artigos científicos, excluindo-se livros, relatórios, somente citação, compêndios e <i>datasets</i>
Análise	Artigos com terminologias não pertinentes ao tema, artigos repetidos nos motores de busca e resumos não condizentes com o objetivo da pesquisa
Idioma	Artigos escritos em idioma diferente do inglês ou português
Atributo	Artigo com acesso restrito ou não aberto

Fonte: Resultado da pesquisa

A Tabela 1 ilustra a quantidade de artigos encontrados com os termos de busca indicados na respectiva coluna. No total foram identificados 82 trabalhos publicados que compõem o corpus deste levantamento bibliométrico, exportados do *Publish or Perish*, *Web of Science*, *Scielo.gov* e *SCOPUS* para o *Microsoft Excel*.

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

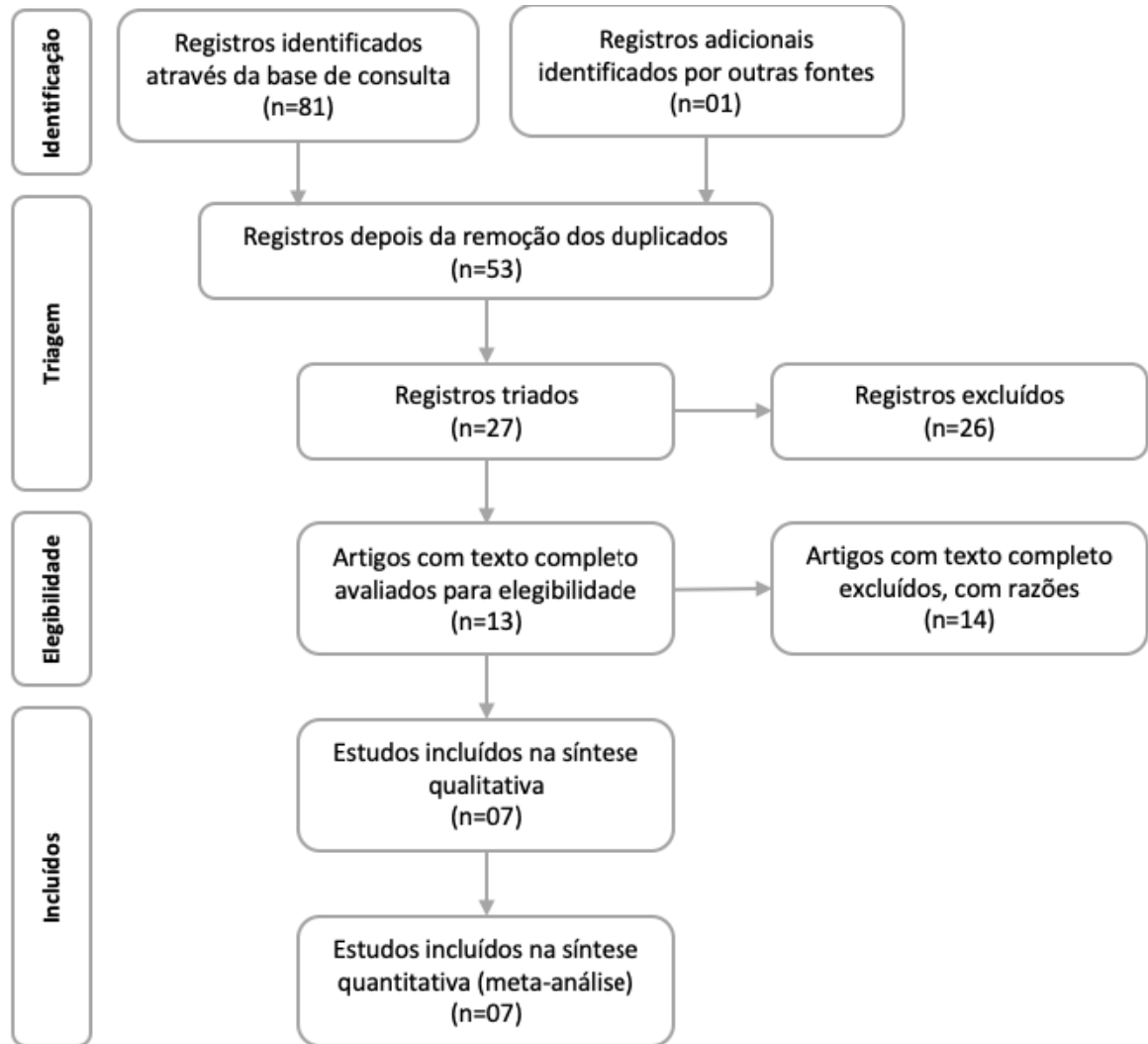
Base de Pesquisa	Termos de busca	Artigos
SCOPUS	<i>(TITLE-ABS-KEY ("agile" OR "agile method" OR "agile principle*")) AND ((ALL ("cybersecurity" OR "computer security")) AND (incident AND response))</i>	24
Web of Science	<i>(TS= ("agile method*" OR "agile principle*" OR agile)) AND (ALL= ("security incident" OR "cybersecurity incident") AND (response OR handling) OR CSIRT)) AND IDIOMA: (English) AND TIPOS DE DOCUMENTO: (Article) / Índices=SCI-EXPANDED, SSCI, A&HCI, CPCI-S, CPCI-SSH, ESCI Tempo estipulado=2014-2021</i>	00
Scielo	<i>(método ágil) AND (segurança da informação) AND (incidente)</i>	00
Google Scholar	<i>"Agile principles" AND "security incident response" from 2014</i>	31
Google Scholar	<i>"Agile principles" AND "security incident handling" from 2014</i>	23
Google Scholar	<i>"Agile method" AND "security incident handling" from 2014</i>	03
Google Scholar	<i>"princípios ágeis" and "segurança da informação" and "resposta a incidentes"</i>	00
Outras fontes	<i>Registros adicionais identificados por outras fontes</i>	01
Total		82

Fonte: Resultado da pesquisa

A **Figura 1** ilustra o fluxograma do protocolo PRISMA-P contendo passo a passo em que, a partir 82 documentos reunidos de todas as fontes de busca, obtiveram-se o resultado de 27 documentos selecionados na fase de triagem, excluídos os artigos duplicados e que se enquadravam nos critérios de exclusão. Avançando para a fase de elegibilidade, 13 artigos continham texto completo avaliados para elegibilidade, excluindo-se os artigos que não

atendiam o objetivo da pesquisa. Finalmente, na última fase do PRISMA-P, chegou-se ao número de sete artigos incluídos na síntese qualitativa e quantitativa (meta-análise).

Figura 1 Fluxograma do Protocolo PRISMA-P



Fonte: Resultado da pesquisa

O **Quadro 3** apresenta o resultado da pesquisa após a aplicação elegibilidade do protocolo PRISMA-P. São mostrados sete estudos incluídos na síntese qualitativa, realizada com a sua leitura e 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 3 Títulos resultantes selecionados

Título	Referência
<i>Rethinking security incident response: The integration of agile principles</i>	(GRISPOS; GLISSON; STORER, 2014)
<i>Security incident response criteria: A practitioner's perspective</i>	(GRISPOS; GLISSON; STORER, 2015a)
<i>Enhancing security incident response follow-up efforts with lightweight agile retrospectives</i>	(GRISPOS; GLISSON; STORER, 2017)
<i>Towards agile industrial control systems incident response</i>	(HE; JANICKE, 2015)
<i>Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis</i>	(NASEER et al., 2021)
<i>The Agile Incident Response for Industrial Control Systems (AIR4ICS) framework</i>	(SMITH et al., 2021)
<i>Agile incident response (AIR)- Improving the incident response process in healthcare</i>	(HE et al., 2022)

Fonte: Resultado da pesquisa

Os artigos foram publicados em seis periódicos indexados e escritos por cinco autores e coautores distintos. As publicações são: *Computers & Security 109*; *20th e 21st Americas Conference on Information Systems*; *Elsevier Digital Investigation*; *3rd International Symposium for ICS & SCADA*; e *International Journal of Information Management*.

Considerando o número reduzido de publicações selecionadas, todos os autores podem ter seus índices de relevância de publicações e de citações, conforme descrito na **Tabela 2**, obtida de dados consultados no *Google Scholar* nos perfis de autores cadastrados. A tabela está ordenada pelo número de artigos selecionados, seguido pelo índice *h* e número de citações totais, todos de forma decrescente.

Tabela 2 Autores dos trabalhos selecionados e índices de relevância do *Google Scholar*

Autor	Artigos selecionados	Índice h	Índice i10	Citações totais
Glisson, William Bradley	3	23	42	1687
Storer, Tim	3	17	31	1208
He, Ying	3	15	20	847
Grispos, George	3	15	19	804
Janicke, Helge	2	29	72	469
Ahmad, Atif	1	28	52	2757
Maynard, Sean B.	1	23	40	2286
Smith, Richard	1	21	93	2803
Zamani, Efpraxia D.	1	14	18	1053
Luo, Cunjin	1	8	7	225
Naseer, Humza	1	7	5	123
Naseer, Ayesha	1	2	1	14
Albakri, Adham; Ferra, Fenia; Lloyd, Stefan; Masood Siddiqui, Adil	1	Sem informação para esses autores		

Fonte: Resultado da pesquisa

Com o objetivo de identificar os termos e as palavras-chaves que indiquem oportunidades de refinamento para futuras pesquisas, foi realizado o levantamento das palavras-chaves mais utilizadas pelos autores e das palavras que mais se repetiram nos títulos. Quanto às palavras-chaves, são: *incident response* (5), *security incident response* (2), *agile* (3), *agile incident response* (1), *agile manifesto* (1), *agile methodologies* (1); *agile principles* (1), *incident learning* (1), *information security* (2), *security incident* (2), *security investigations* (1), *real-time analytics* (1), *resource-based view* (1), *enterprise cybersecurity performance* (1), *healthcare* (1), *industrial control systems* (1), *SCADA* (1). Quanto aos títulos, as palavras citadas mais de uma vez são: *incident* (7), *response* (7), *agile* (6) e *security* (3).

O **Quadro 4** resume os achados das sete publicações selecionadas, agrupadas por seus autores. Este quadro não é exaustivo, apresenta de maneira resumida os principais achados.

Quadro 4 Resumo dos principais achados nas publicações selecionadas

Autores	Resumo dos achados
Grispos, WB Glisson, T Storer	<p>Os autores propõem (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. Sugerem mais estudos para trabalhos futuros chamando de <i>Agile Incident Response</i>.</p> <p>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.</p> <p>Em (GRISPOS; GLISSON; STORER, 2017) investigam a integração de retrospectivas e meta-retrospectivas ágeis leves no processo de resposta a incidentes de segurança, para melhorar o feedback e/ou esforços follow-up.</p>
Y He, H Janicke	Os autores examinam em (HE; JANICKE, 2015) o procedimento de resposta a incidentes de um <i>Industrial Control System</i> (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 <i>framework</i> 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 <i>framework</i> fornece uma abordagem dinâmica para melhorar a consciência

Autores	Resumo dos achados
	<p>situacional, compartilhamento de informações, tomada de decisão coletiva e flexibilidade de resposta dentro do contexto único do ICS.</p> <p>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 <i>design</i> modular do <i>framework</i> 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 <i>framework</i> 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.</p>
He et al.	<p>Neste estudo, inspirado no Manifesto Ágil, foi proposto o <i>framework Agile Incident Response</i> para refinar, ajustar e melhorar o atual processo linear de resposta a incidentes do <i>National Health Service</i> (NHS) do Reino Unido, usado como um caso ilustrativo. A atual estrutura linear de resposta a incidentes foi analisada criticamente e demonstrado como ela pode ser transformada em uma estrutura de resposta a incidentes híbrida. Usando um estudo de caso ilustrativo do domínio da saúde, este estudo contribui para a literatura de resposta a incidentes, mostrando como a integração de princípios ágeis em processos lineares pode melhorar a resposta a incidentes.</p>

Fonte: Resultado da pesquisa

Ao realizar a construção da síntese dos artigos selecionados neste estudo, identificou-se como lacunas de pesquisa sobre o uso dos princípios ágeis na resposta a incidentes de segurança da informação em sistemas produtivos.

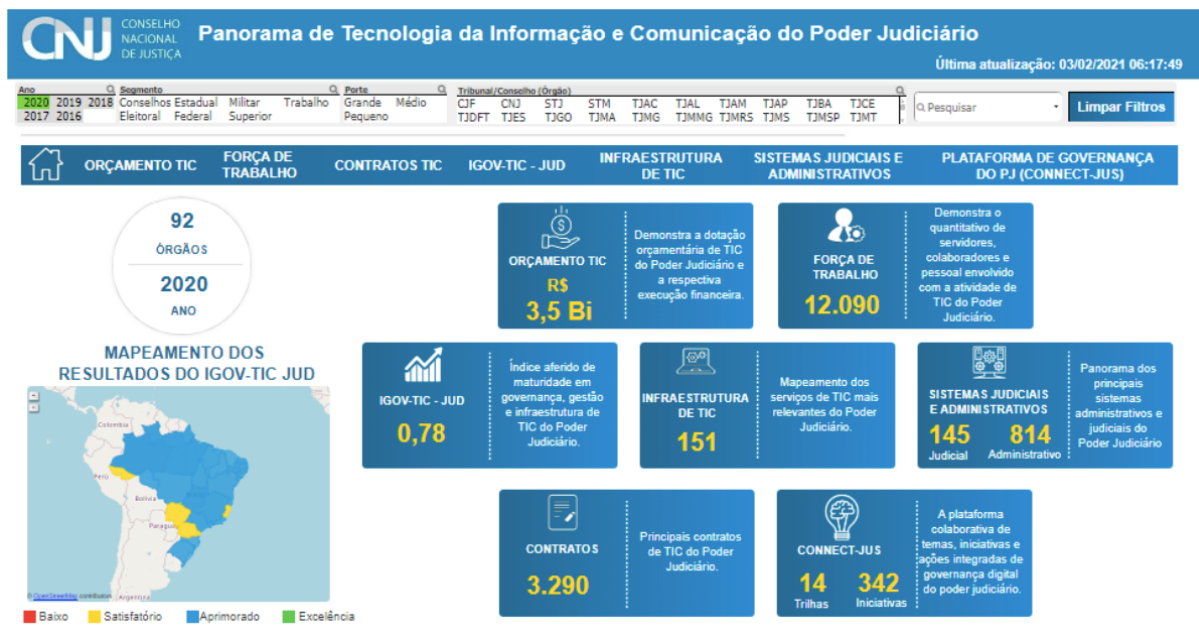
1.2 A informatização do Poder Judiciário brasileiro

O Poder Judiciário brasileiro tem avançado na informatização de seus sistemas. Um exemplo disso é indicado pelos números de processos eletrônicos que em 2009 eram de apenas 11,2% dos processos a julgar enquanto em 2020, o índice saltou para 96,9%, de acordo com o anuário estatístico do CNJ (CNJ, 2022a). Desde março de 2022 já não é mais possível receber nenhum novo processo judicial em papel, todos devem ser eletrônicos.

Mais avanços são vistos no relatório anual Justiça em Números, um importante instrumento de transparência e governança do Poder Judiciário. Nele, o Conselho Nacional de Justiça (CNJ), reúne dados orçamentários, de pessoal e de diagnóstico do desempenho da atividade judicial dos 90 órgãos do Poder Judiciário previstos na Constituição Federal.

As informações também se originam da Base Nacional de Dados do Poder Judiciário (DataJud), responsável pelo armazenamento centralizado dos dados e metadados processuais relativos a todos os processos físicos ou eletrônicos, públicos ou sigilosos dos tribunais, que atualmente representa o armazenamento de mais de 11 bilhões de movimentações processuais de ações em andamento e já baixadas (CNJ, 2021c).

Figura 2 Panorama de Tecnologia da Informação do Poder Judiciário



Fonte: Dados Coletados entre 2016 e 2020 no Levantamento em Maturidade de Governança, Gestão e Infraestrutura de TIC do Poder Judiciário (IGovTIC-JUD) (CNJ, 2022b).

A **Figura 2** mostra um panorama da Tecnologia da Informação e Comunicação do Poder Judiciário (CNJ, 2022b). O orçamento de TIC em 2020 foi de R\$ 3,5 bilhões enquanto a força de trabalho de pessoal da TI soma mais de 12.000 funcionários. O painel ainda mostra a utilização de 145 sistemas judiciais, de 814 sistemas administrativos, e de 151 serviços relevantes de TIC. O índice aferido de maturidade em governança, gestão e infraestrutura de TIC do Poder Judiciário é de 0,78.

A importância destacada pelo relatório (CNJ, 2021c) mostra a tendência de reinvenção das formas de trabalho e o emprego maciço da tecnologia no Poder Judiciário, os quais auxiliaram a atividade finalística jurisdicional. O desenvolvimento humano sustentável, o progresso social e a estabilidade econômica são parâmetros afetados também pela atividade judicial, sendo esta indispensável para o desenvolvimento nacional em todos os aspectos.

Nos últimos anos, o Judiciário brasileiro inovou e criou soluções para atender a população em meio à crise sanitária causada pela pandemia da Covid-19. Por meio da tecnologia, iniciativas buscaram garantir a continuidade da prestação jurisdicional de forma célere e eficiente. Entre essas iniciativas, designadas como Justiça 4.0 pelo CNJ, estão o Juízo 100% Digital, a Plataforma Digital do Poder Judiciário, a Plataforma Sinapes e Codex e o Balcão Virtual (CNJ, 2021a).

A Plataforma Digital do Poder Judiciário Brasileiro - PDPJ-Br visa incentivar o desenvolvimento colaborativo entre os tribunais, preservando os sistemas públicos em produção, mas consolidando pragmaticamente a política para a gestão e expansão do Processo Judicial Eletrônico – PJe. O principal objetivo é modernizar a plataforma do PJe e transformá-la em um sistema multisserviço que permita aos tribunais fazer adequações conforme suas necessidades e que garanta, ao mesmo tempo, a unificação do trâmite processual no país.

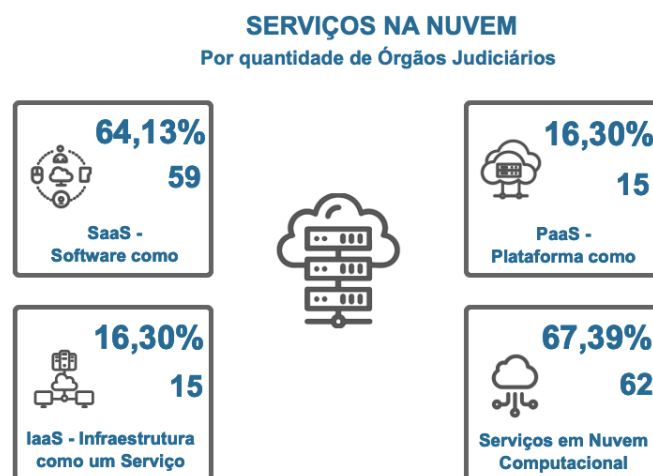
O Juízo 100% Digital, regulamentado pela Resolução CNJ n. 345/2020, é uma modalidade de tramitação de processos que visa transformar a Justiça em um serviço. Neste ambiente, juízes e as partes do processo atuam remotamente, realizando todos os atos processuais pelo meio digital utilizando os sistemas judiciais, aplicativos de mensagem instantânea e plataformas de videoconferência. A comunicação dos atos, como citação, notificação e intimação, é admitida por meio eletrônico, e as audiências e sessões de julgamento ocorrem exclusivamente por videoconferência.

O Sinapses é uma plataforma nacional de armazenamento, treinamento supervisionado, controle de versionamento, distribuição e auditoria dos modelos de Inteligência Artificial. A gestão e responsabilidade pelos modelos e *datasets* cabe a cada um dos órgãos do Poder Judiciário, por meio de seu corpo técnico e usuários colaboradores da plataforma. Já o Codex, desenvolvido pelo Tribunal de Justiça de Rondônia (TJRO) com o CNJ, consolida as bases de dados processuais e, assim, provê o conteúdo textual de documentos e dados estruturados. Ele funciona como um *data lake* de informações processuais, que pode ser consumido pelas mais diversas aplicações: a produção de painéis e relatórios de inteligência de negócios (*business intelligence*); a implementação de pesquisas inteligentes e unificadas; a alimentação automatizada de dados estatísticos; e até mesmo o fornecimento de dados para a criação de modelos de Inteligência Artificial.

Por fim, o “Balcão Virtual” visa desburocratizar e tornar mais ágil o atendimento do Judiciário aos cidadãos, tornando permanente o acesso remoto direto e imediato dos usuários dos serviços da Justiça às secretarias das Varas em todo o país por intermédio de ferramenta de videoconferência que permita imediato contato durante o horário de atendimento ao público.

A infraestrutura dos órgãos judiciários tem utilizado cada vez mais os serviços na nuvem, que fica ilustrado na **Figura 3** a utilização dos serviços na nuvem pela maioria dos tribunais.

Figura 3 Serviços na Nuvem por quantidade de órgãos judiciários



Fonte: (CNJ, 2022b)

Os tribunais têm investido em modernização e tecnologia para manter os sistemas processuais em alta performance e garantir a segurança dos dados com a finalidade de viabilizar um atendimento ágil e seguro pelas unidades judiciais (CNJ, 2021a). Se antes as unidades do poder judiciário se preocupavam em cuidar da segurança física do seu acervo de processos em papel, como incêndios, alagamento, pragas e insetos, desaparecimento, perda e roubo de processos, hoje as preocupações são outras.

Nos últimos anos, diversas ações de *hackers* têm atingido o Poder Judiciário em seus vários níveis e especialidades (AGÊNCIA BRASIL, 2020a, 2020b, 2020c; BAGUETE, 2021; CONJUR, 2021a, 2021b; FOLHA, 2020; G1, 2021; STJ, 2020; TERRA, 2020; UOL, 2022).

Entre os ataques mais notáveis e importantes está o realizado no Superior Tribunal de Justiça (STJ) em novembro de 2020 que causou a interrupção de diversos julgamentos que ocorriam simultaneamente, por videoconferência, nas seis turmas do STJ. Os sistemas do tribunal, incluindo o site oficial, ficaram fora do ar e todos os prazos processuais foram suspensos por dez dias. Nesta ocasião todos os funcionários se encontravam em regime de teletrabalho e tiveram seus acessos suspensos (AGÊNCIA BRASIL, 2020c).

Este ataque *hacker* foi tratado por peritos como 'o mais grave ataque' cibernético já verificado não apenas ao judiciário, mas em todos os órgãos públicos da capital federal. Mais de 255 mil processos tramitam na Corte e teriam sido capturados pelo *hacker* que adicionou chaves de criptografia a mais de 1,2 mil máquinas virtuais, além de destruir seus backups com um ransomware chamado RansomEXX (BAGUETE, 2021; TERRA, 2020).

Os prejuízos e danos à sociedade causados pelo ataque e das informações a que os *hackers* tiveram acesso são difíceis de aferir, e apesar de ser apurado pela Polícia Federal, advogados temem que os dados dos clientes, que estavam na base do STJ e foram recuperados por um sistema de *backup*, sejam usados para chantagem pelos criminosos (FOLHA, 2020).

As funcionalidades começaram a retornar somente após nove dias do ataque, entre elas a restauração de sistemas, as sessões de julgamento, os serviços de consulta processual e de jurisprudência, os portais eletrônicos, o peticionamento eletrônico, o recebimento de guias de custas processuais, a autuação de processos e até mesmo os serviços de saúde dos funcionários. Cerca de dez mil processos ficaram represados para publicação de decisões, acórdãos e despachos (STJ, 2020).

Além do STJ, outros tribunais sofreram ataques como o Tribunal de Justiça do Rio Grande do Sul que teve o site do sistema de consulta e peticionamento aos processos

adulterados por *hackers* (TERRA, 2020). Em fevereiro de 2021, *hackers* promoveram ataques cibernéticos ao sistema de processo eletrônicos da Justiça Federal da 3ª Região, com o propósito de alterar documentos eletrônicos com assinatura de agentes públicos, indicando transferências de R\$ 225 mil e de R\$ 600 mil para uma conta de titularidade de um homem incluído como beneficiário, mesmo não sendo ele a parte exequente do processo (CONJUR, 2021a).

Continuando os exemplos de ataques direcionados ao judiciário, em maio de 2021, o sistema eletrônico do Supremo Tribunal Federal (STF) sofreu um ataque que tirou do ar seu o site para usuários externos, além de ter tido aumento expressivo na quantidade de acessos no portal por meio de robôs (G1, 2021). Em 2021, novamente o Tribunal de Justiça do Rio Grande do Sul foi alvo de um ataque *hacker* que deixou a corte sem acesso aos sistemas por mais de 24 horas a rede interna foi infectada, sendo aconselhado que os funcionários não usassem computadores conectados a ela (CONJUR, 2021b). Em outubro de 2021, o Tribunal Regional do Trabalho da 4ª Região detectou “registros suspeitos de atividades maliciosas” e sofreu uma invasão da sua infraestrutura tecnológica (BAGUETE, 2021).

Os recentes ciberataques repercutiram preocupação na Justiça Eleitoral, e coloca em teste o processo eleitoral de 2022, observando relatórios internacionais que mostram que 58% dos ataques têm origem na Rússia, cuja legislação não é adequada ao controle da divulgação e propagação de *fake news*, apologia ao nazismo, terrorismo e venda de armas (UOL, 2022).

Enquanto esta dissertação era escrita, o TRF3 sofreu um ataque de *ransomware* em 30 de março de 2022. Como parte da estratégia para proteção dos sistemas judiciais eletrônicos e dados pessoais dos jurisdicionados, foi determinado o desligamento de todos os sistemas a fim de não ocorrer contaminação. Além de suspender o acesso aos sistemas aos magistrados, funcionários, advogados e partes por mais de 12 dias, houve o adiamento do envio dos precatórios, acatado pelo presidente do CNJ, Luiz Fux (CONJUR, 2022; TRF3, 2022).

Todos esses exemplos ilustram a importância na preservação de todo o ecossistema digital do Poder Judiciário, principalmente na pronta resposta aos incidentes cibernéticos que venham a sofrer. Os danos causados por uma resposta a incidentes insatisfatória podem ocasionar enormes prejuízos à vida das pessoas, às organizações, aos operadores do direito, e ao Poder Judiciário como um todo.

O Poder Judiciário julga cerca de 18 milhões de processos por ano, cerca de 77 milhões de processos estão em tramitação (CNJ, 2021c). Uma vez que a maioria desses processos tem tramitação eletrônica, a infraestrutura dos tribunais pode sofrer ataques cibernéticos e ameaças

que poderão afetar as premissas da segurança da informação: a integridade, a disponibilidade e a confidencialidade (SAMONAS; COSS, 2014).

Os avanços tecnológicos, como a tecnologia 5G em redes móveis e de banda larga, também são fontes de preocupação pois o Judiciário estará em um ambiente ainda mais virtualizado, levando-o a uma nova fronteira com ganhos em termos de velocidade de conexão, possibilidades maiores de exploração da IoT, de comunicação entre máquinas e no uso de IA e de robótica com inúmeras implicações para os serviços da Justiça (CNJ, 2021d).

Motivado por todos esses acontecimentos recentes, o CNJ aprovou a criação da Estratégia Nacional de Segurança Cibernética e da Informação do Poder Judiciário (ENSEC-PJ), um instrumento para orientar a resposta dos órgãos da Justiça à crescente ameaça de ataques de *hackers* à infraestrutura virtual dos tribunais brasileiros (CNJ, 2021b).

A ENSEC-PJ tem quatro objetivos principais: tornar a Justiça mais segura e inclusiva no ambiente digital; aumentar a resiliência às ameaças cibernéticas; estabelecer governança de segurança cibernética e fortalecer a gestão e coordenação integrada de ações de segurança cibernética nos órgãos do Judiciário; e permitir a manutenção e a continuidade dos serviços, ou o seu restabelecimento em menor tempo possível (CNJ, 2021b).

As principais ações de proteção aos ativos do judiciário visam assegurar o princípio constitucional da segurança jurídica, preservar a continuidade do funcionamento da Justiça e proteger as informações constantes nos processos e sistemas judiciais. Os impactos podem ser de ordem financeira, operacional, reputação, e demandam uma resposta que minimize os danos dos eventuais ataques e reduza o tempo de não-funcionamento dos sistemas (CNJ, 2021b).

A pesquisa aqui realizada vai ao encontro da estratégia do judiciário em elevar o nível de segurança das infraestruturas críticas por meio das ETIRs, que são responsáveis por responder e tratar os incidentes de segurança cibernética, podendo recorrer a tecnologias e técnicas de inteligência na análise dos ataques.

Além disso, o presente trabalho pode contribuir para o objetivo da ENSEC-PJ de estimular uma relação colaborativa entre as cortes no tratamento de incidentes e vulnerabilidades cibernéticas verificadas, e de realizar exercícios em conjunto com as equipes responsáveis por gerenciar crises causadas por ataques *hackers*.

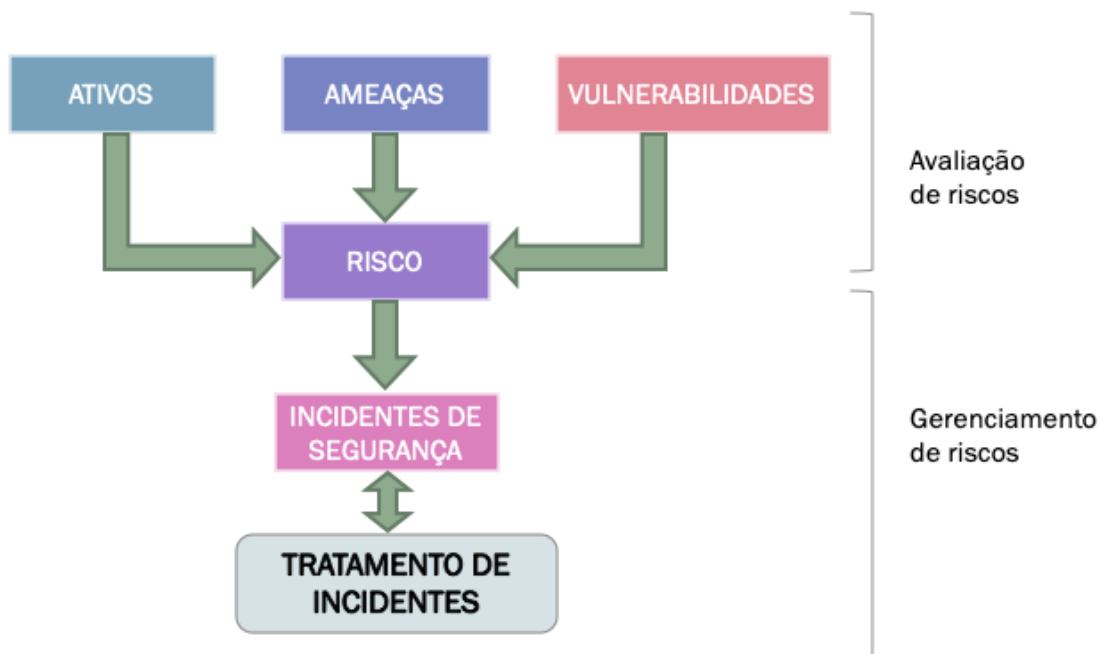
1.3 Continuidade do negócio e recuperação de desastres

É importante contextualizar os riscos e ameaças da seção anterior no contexto da continuidade do negócio e da recuperação de desastres.

O gerenciamento de riscos de segurança da informação geralmente engloba um processo sistemático criado pela gestão da organização e visa determinar a aplicação equilibrada de controles de segurança diante do seu perfil de riscos.

A ISO/IEC 27005 (ABNT, 2019) é uma das normas base usadas para a criação de um modelo de gestão de riscos. Suas finalidades incluem (i) uma descrição de um processo genérico para a gestão do risco de segurança da informação; (ii) um guia para gestão do risco que pode ser usado em empresas, projetos, ciclos de melhoria contínua etc; (iii) um guia para desenvolvimento de métodos e metodologias que atendam às necessidades de gestão de riscos apontadas na norma ABNT NBR ISO/IEC 27001; e (iv) uma norma de consenso entre diversas outras normas e metodologias de gestão de riscos em nível mundial.

Figura 4 Contexto do tratamento de incidentes na gestão de risco de segurança da informação



Fonte: Adaptado de ITIL, ISO/IEC 27005 e CERT.br (ABNT, 2019; AXELOS, 2019; CERT.BR, 2002)

Desse modo, descreve-se brevemente os itens constantes na **Figura 4** com base nos conceitos apresentados em ISO/IEC 27005 e FAQ CERT.br (ABNT, 2019; CERT.BR, 2002).

- i. Ativo é qualquer coisa que tenha valor para a organização. Um ativo é uma parte da organização, podendo ser tangível como um equipamento, ou intangível como uma marca comercial ou segredo industrial;
- ii. *Ameaça* é a causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;
- iii. *Vulnerabilidade* é uma fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;
- iv. *Risco de Segurança da Informação* é o potencial que uma ameaça tem de explorar vulnerabilidades de um ativo e desta forma prejudique uma organização. Um risco é mensurado em termos de probabilidade de sua materialização e seus impactos;
- v. *Incidente de segurança*, é um evento de segurança ou um conjunto deles, confirmado ou sob suspeita de impactar a disponibilidade, integridade, confidencialidade ou a autenticidade de um ativo de informação, bem como qualquer violação da política de segurança da informação;
- vi. *Tratamento de incidentes* é composto por notificação do incidente, análise do incidente e resposta ao incidente;

O gerenciamento de riscos é fundamental no planejamento de contingências e gerenciamento de continuidade a fim de tratar as interrupções na operação do negócio. Recuperar rápida e eficientemente a atividade depois de um acidente, minimizando os seus efeitos, deverá ser uma preocupação vinculada e real dos decisores (REIS; AMARAL, 2016).

A continuidade de negócio bem como a recuperação de desastres são práticas mencionados nas normas (ABNT, 2013, 2019; AXELOS, 2019; BRITISH STANDARDS INSTITUTE, 2006; ISACA, 2019).

De acordo com Bras & Ribeiro (2016), construir resiliência e gerenciar mudanças imprevisíveis nos ecossistemas de TI e de negócios são fundamentais para garantir a segurança de uma empresa. Os objetivos-chaves precisam estar alinhados com a continuidade de seus processos-chaves no caso de um incidente disruptivo. Para isso, as organizações precisam ter planos de continuidade de negócios e de recuperação de desastres bem estruturados, que tenham uma visão ampla a fim de atingir o objetivo de manter e restaurar operações críticas.

Um plano de continuidade de negócios (*Business Continuity Plan* – BCP) é uma ferramenta essencial que visa garantir que a empresa esteja preparada para a recuperação imediata de suas atividades críticas e de seus sistemas e aplicativos de suporte, em caso de desastre (BRAS; RIBEIRO, 2016). Seu foco é no planejamento da recuperação de processos e funções de negócios, abrangendo resposta a emergências, continuidade de negócios, recuperação de desastres e gerenciamento de uma situação de crise (KLIEM; RICHIE, 2015; TASHI; GHERNAOUTI-HÉLIE, 2011).

O plano de recuperação de desastres (*Disaster Recovery Plan* - DRP), por sua vez, é o componente técnico do BCP e aborda a recuperação dos sistemas centrais, seus dados e tecnologias de comunicação que suportam o negócio. A recuperação de desastres é um subconjunto da continuidade de negócios (BRAS; RIBEIRO, 2016; SNEDAKER, 2014).

Ambos os planos (BCP/DRP) devem descrever as ações a serem implementadas, os recursos necessários e os procedimentos a serem seguidos antes, durante e após um desastre. Eles são desenhados para minimizar os impactos em termos de recursos humanos, impactos operacionais e financeiros inerentes a uma situação de desastre (BRAS; RIBEIRO, 2016).

Snedaker (2014) destaca que, além da recuperação de desastres que causam danos a estruturas físicas, a recuperação dos serviços de TI também envolve responder, interromper e reparar problemas causados por falhas de sistemas, violações de segurança, corrupção ou destruição intencional de dados. Dependendo da natureza ou gravidade do ataque ou incidente, pode ser necessário ativar uma equipe de resposta a incidentes de segurança da informação (*Computer Security Incident Response Team* - CSIRT), assunto que será tratado com mais detalhes na próxima seção.

A resposta a incidentes de segurança da informação é uma atividade que abrange recuperação de desastres, continuidade de negócios e operações normais. Os membros de um CSIRT devem ter responsabilidades integradas aos BCP e DRP e devem manter suas habilidades atualizadas para que estejam alertas para responderem às ameaças, vulnerabilidades e problemas na área de TI (SNEDAKER, 2014).

A próxima seção continua a explicação sobre os CSIRTs, seu funcionamento e apresenta alguns dos problemas em seus processos que motivaram a presente pesquisa.

1.4 Resposta a incidentes de segurança da informação

O código malicioso *Morris Worm*, criado em 1988 por um estudante de 23 anos, é considerado o motivo da criação do primeiro CSIRT (RUEFLE et al., 2014). Após esse fato, motivados pela *US Defense Advanced Research Projects Agency* (DARPA), governos e organizações criaram seus próprios CSIRTs para gerenciar incidentes de segurança da informação por meio de processos para detectar, analisar, responder e aprender de 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 et al. (2017), a informação tem importância estratégica, é impulsionada com a utilização de Tecnologia da Informação (TI) nos processos organizacionais e deve ter proteção adequada.

Assim, os CSIRTs se tornam essenciais para as organizações, em especial as dos sistemas produtivos, reduzirem o impacto de um incidente, retomarem a disponibilidade e os valores da segurança da informação, conforme discutido na seção sobre continuidade do negócio e recuperação de desastres.

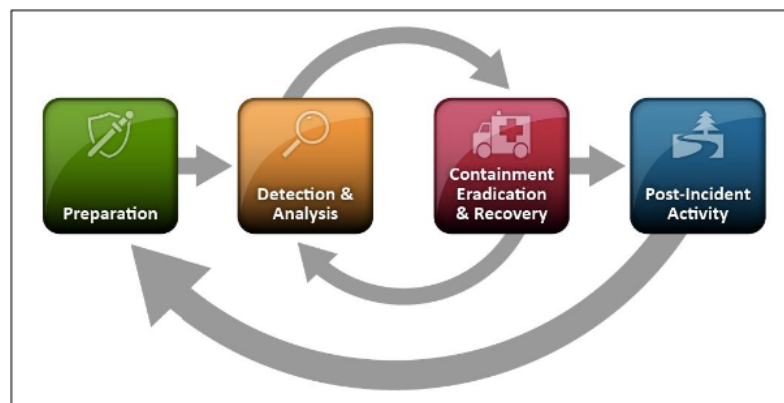
Para que uma equipe seja considerada um CSIRT, ela deve fornecer um ou mais dos serviços de tratamento de incidentes: análise de incidentes, resposta a incidentes no local, suporte à resposta a incidentes ou coordenação da resposta a incidentes. O serviço de tratamento de incidentes inclui análise de incidentes com pelo menos um dos outros serviços de tratamento de incidentes: resolução de resposta a incidentes, suporte de resposta a incidentes ou coordenação de resposta a incidentes. A lista de serviços comuns de um CSIRT é representada na **Figura 5** (WEST-BROWN et al., 2003).

Figura 5 Lista de serviços comuns do CSIRTs

Fonte: (WEST-BROWN et al., 2003)

O problema a ser analisado e proposto para este trabalho está inserido na área de resposta a incidentes da segurança da informação no Poder Judiciário, os quais são limitados a computadores, dispositivos de redes, redes e informações contidas e transmitidas por eles.

Guias com técnicas, melhores práticas e processos foram publicados pela ENISA (MAJ; REIJERS; STIKVOORT, 2010), NIST (CICHONSKI et al., 2012) e ISO. Em 2015, (STIKVOORT, 2015) propôs um modelo de maturidade de gerenciamento de incidentes de segurança chamado SIM3 e em 2018, a CMU/SEI (DOROFEE et al., 2018) publicou o relatório técnico sobre maturidade *Incident Management Capability Assessment*.

Figura 6 Ciclo de vida de resposta a incidente do NIST

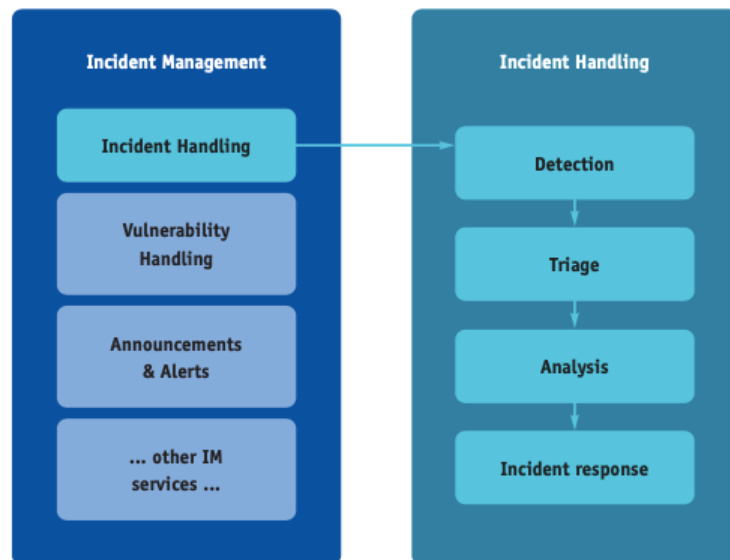
Fonte: (CICHONSKI, MILLAR, GRANCE, & SCARFONE, 2012)

Em geral, o processo de resposta a incidentes de segurança é um plano de ação linear como mostra a **Figura 6**.

Esta abordagem de plano de ação linear e tradicional apresentou alguns importantes pontos de atenção e problemas, conforme relatados em (GRISPOS; GLISSON; STORER, 2014). Os autores identificam alguns problemas a serem superados, como por exemplo: como melhorar os processos tradicionais para que reflitam as necessidades do mundo atual, como a mudança constante? Como tratar os ataques cibernéticos automatizados? Como melhorar as lições aprendidas a cada incidente? Como aplicar de maneira efetiva um modelo de maturidade em gerenciamento de incidentes de segurança em um CSIRT? Ainda existe uma negligência nos aspectos das lições aprendidas de respostas a incidentes e funções pós-incidente? (AHMAD; HADGKISS; RUIGHAVER, 2012b)

O guia da ENISA (MAJ; REIJERS; STIKVOORT, 2010) apresenta a importância do tratamento de incidentes como principal serviço oferecidos pelos CSIRTs, conforme ilustrado na **Figura 7**. Se observa a característica de processo de ação linear, semelhante um modelo cascata de desenvolvimento de *software*, onde um processo é seguido de outro.

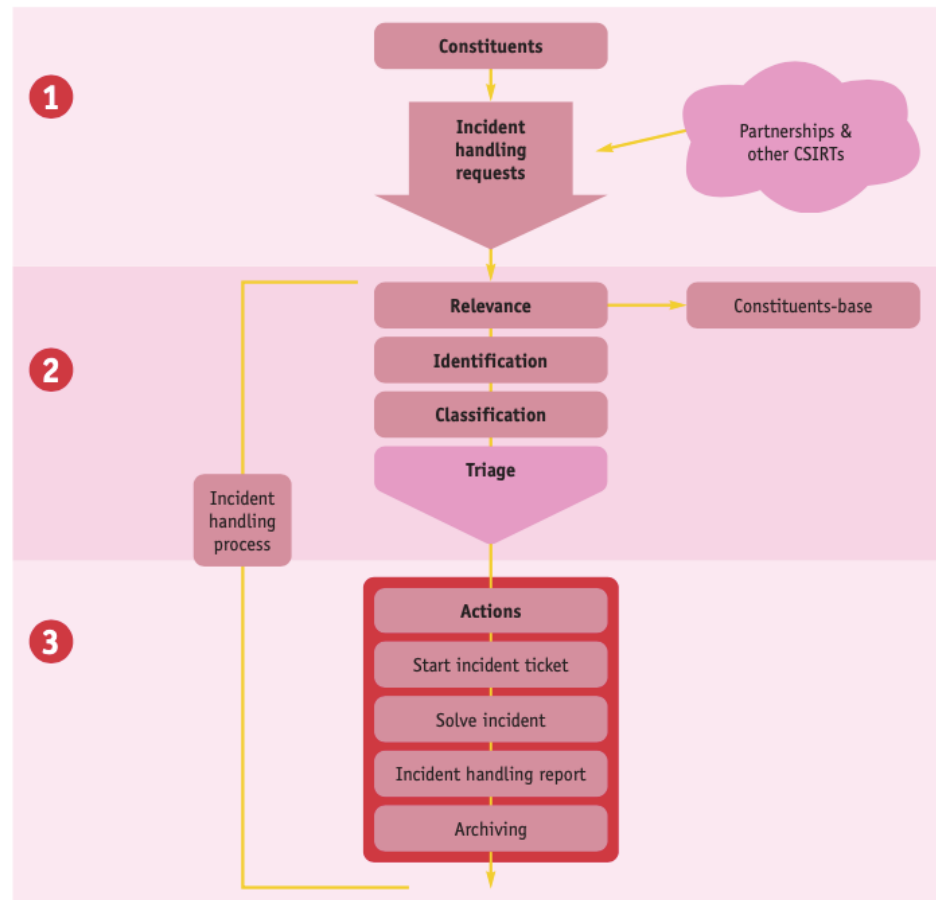
Figura 7 Gerenciamento de Incidente e Tratamento de Incidente da ENISA



Fonte: (MAJ; REIJERS; STIKVOORT, 2010)

A **Figura 6** e a **Figura 7** ilustram como são os chamados processos tradicionais de resposta a incidentes de segurança da informação.

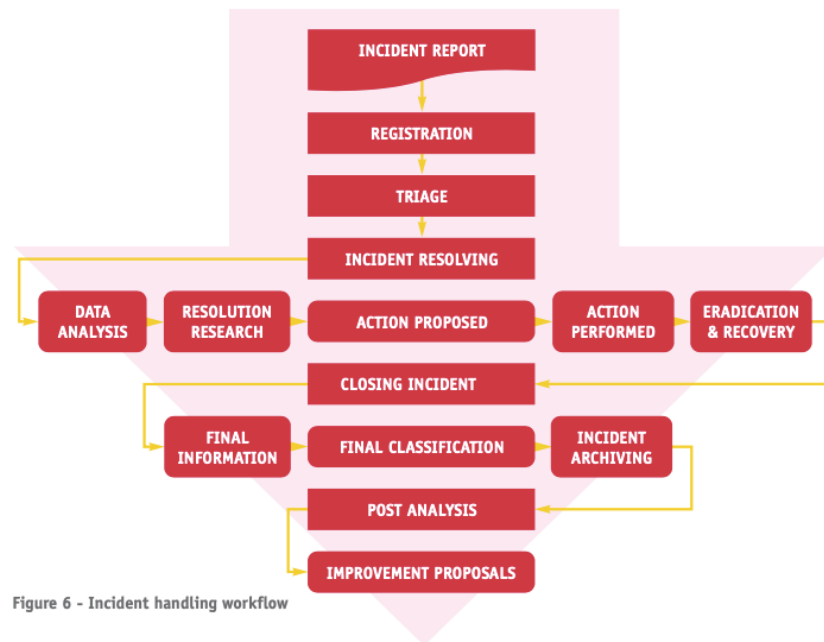
Figura 8 Fluxo de Processo de Tratamento de Incidente da ENISA



Fonte:(MAJ; REIJERS; STIKVOORT, 2010)

Mais um exemplo dado por Maj et al. (2010) é ilustrado na **Figura 8**, apresentando os processos seguindo linearmente, em três etapas e destacando o processo de tratamento de incidentes.

Por fim, explorando o processo de tratamento de incidentes com um nível de detalhamento maior, a **Figura 9** apresenta o *workflow* do tratamento de incidentes pode ser sugerido como o seguinte processo linear.

Figura 9 *Workflow* de Tratamento de Incidentes da ENISA

Fonte: (MAJ; REIJERS; STIKVOORT, 2010)

Ao utilizarem um modelo em cascata para o tratamento e resposta de incidentes de segurança da informação fica inerente aos processos internos a ocorrência dos mesmos problemas que afligiram a indústria de *software* por anos, entre eles a dificuldade de lidar com mudanças, complexidades e relação da equipe com o projeto todo. A próxima seção trata dos princípios ágeis e ajuda a responder porque eles são úteis neste contexto.

1.5 Princípios ágeis

Inicialmente, é preciso esclarecer que esta pesquisa não trata de desenvolvimento seguro de *software* que utiliza o método ágil. Beznosov & Kruchten (2004) fazem isso em um dos primeiros trabalhos focados na garantia da segurança e no exame de como práticas de segurança da informação se encaixam ou não no contexto dos métodos ágeis.

Baca & Carlsson (2011) investigaram se o método ágil cria *softwares* menos seguros analisando as atividades de segurança dos processos tradicionais de engenharia de *software* em um processo ágil de desenvolvimento. A implementação de um *security backlog* no

desenvolvimento de *software* foi proposto por Ghani et al. (2014) para melhorar o problema crítico da segurança.

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 por meio de melhorias contínuas.

1.5.1 Práticas ágeis além do desenvolvimento de *software*

O sucesso que o método ágil promoveu na indústria de desenvolvimento de *software* naturalmente passou a ser utilizado fora dela. Conforme Rigby et al. (2016), após o aumento nas taxas de sucesso no desenvolvimento de *software*, na melhoria da qualidade e da velocidade e no incentivo à motivação e produtividade de times de TI, os métodos ágeis estão se espalhando por meio de uma ampla faixa de indústrias e funções, incluindo a alta gestão. Por exemplo, citam-se: produção de máquinas agrícolas, 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 para fabricantes de produtos físicos B2B. Enquanto Amorim et al. (2018) utilizaram uma abordagem híbrida 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.

Algumas organizações, como Apple, Google e Zara, chamadas de Economia Criativa por fazerem as coisas de forma diferente, mudaram o objetivo de toda a organização, trocando a maximização de valor para o acionista por encantar o cliente. Criaram ambientes amigáveis aos princípios ágeis. Nessas empresas, as práticas de gerenciamento no nível da equipe, como o ágil, tornam-se evidentes. Paradoxalmente, ganhar dinheiro torna-se o resultado, não o objetivo da organização (DENNING, 2015).

Nesse espírito é que se propõe a utilização dos princípios ágeis na resposta a ciberincidentes no ambiente do Poder Judiciário, como será tratado na próxima seção.

1.5.2 Princípios ágeis na resposta a incidentes de segurança da informação

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

Grispos et al. (2014) indicam que poucas pesquisas investigavam a integração de princípios e práticas ágeis dentro dos processos de resposta de incidente de segurança da informação. Os autores sugerem mais estudos para trabalhos futuros chamando de *Agile Incident Response (AIR)*.

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 & 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*, ou seja, após a resolução do incidente, representam uma fase crítica no processo de resposta a incidentes. Os autores apontam a aplicação de aprendizado de *loop* duplo para questionar processos e princípios fundamentais, uma forma semelhante à retrospectiva do *Scrum*.

Grispos et al. (2015) voltam ao tema de utilização dos princípios ágeis propondo uma melhoria nos processos de resposta a incidentes de segurança da informação com o chamado *Security Incident Response Criteria (SIRC)*. Identificam seis critérios essenciais que um processo de resposta a incidente de segurança bem-sucedido precisa endereçar.

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 et al. (2017) destacam a sua fase final: o *feedback/follow-up*. Eles nos trazem que organizações encontram dificuldades em aprender com os incidentes e desse modo 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*. A implementação do uso de retrospectiva afeta e é afetada por um processo cultural na organização, podendo ajudar a implementar melhores práticas e influenciar a disseminar o aprendizado de incidente de segurança.

Também fora do domínio do desenvolvimento de *software*, Anantharaman (2018) sugere o uso do método ágil no gerenciamento de incidentes de serviços do ITIL com o uso de quadros *Kanban* para auxiliar a visualizar, distribuir e priorizar tíquetes e reduzir o tempo de resposta de incidentes.

Naseer et al. (2021), argumentam que (1) as organizações devem desenvolver agilidade em seus processos 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.

Assim, os exemplos trazidos pela literatura científica validam o prosseguimento da pesquisa visando a utilização de princípios ágeis na resposta a incidentes de segurança da informação no Poder Judiciário, a qual seguirá a metodologia descrita no próximo capítulo.

2 METODOLOGIA

A metodologia de pesquisa escolhida para conduzir este estudo é a *Design Science Research Methodology* - DSRM, que tem embasamentos na produção de pesquisa com o processo de *Design Science* (DS) e na apresentação por meio de modelo mental para tratar da realidade construída a partir da compreensão do problema (HEVNER; CHATTERJEE, 2010; LACERDA et al., 2013; PEFFERS et al., 2007).

A DSRM incorpora princípios, práticas e procedimentos necessários para a pesquisa e compreende três objetivos: é consistente com a literatura anterior, fornece um modelo de processo nominal para fazer pesquisa em DS e fornece um modelo mental para apresentar e avaliar a pesquisa em DS em Sistemas de Informação. O processo DS inclui seis etapas: identificação e motivação do problema, definição dos objetivos para uma solução, *design* e desenvolvimento, demonstração, avaliação e comunicação (PEFFERS et al., 2007).

Para Lacerda et al. (2013), a DSRM tem apresentado uma grande evolução como abordagem nas áreas de ciências exatas. Esta evolução se deve a sua característica em constituir um processo rigoroso para projetar artefatos para resolver problemas, avaliar o que foi projetado ou o que está funcionando, e comunicar os resultados obtidos.

Em seu livro sobre as “ciências do artificial”, Simon (2019), contrasta a ciência natural com a ciência do artificial. A primeira, descreve um conjunto de conhecimentos sobre uma classe de objetos e/ou fenômenos naturais no mundo, observa sobre suas características, como se comportam e como interagem, pesquisando como as coisas são e como funcionam, aplicando esse raciocínio para o estudo dos fenômenos naturais (biologia, química, física) e sociais (economia e sociologia). A segunda, define o artificial, aquilo criado ou produzido pelo homem sujeito assim às suas intervenções, como por exemplo máquinas, sistemas de informação, equipamentos, organizações, modelos econômicos e aspectos da própria sociedade e suas instituições. Em outros termos, “O mundo em que vivemos hoje é muito mais artificial, fabricado pelo homem, do que natural [...]” (SIMON, 2019, p. 2)

Van Aken (2005) propõe que a principal atribuição da *Design Science* é modelar e organizar o conhecimento, para a concepção e desenvolvimento de artefatos.

Romme (2003) afirma que os sendo as organizações fruto da atividade criativa do homem, os estudos relacionados a estas, devem ter na *Design Science* e a *Design Science Research*, um dos principais modos de gerar o conhecimento e de realizar pesquisas científicas.

A realização do presente estudo visa a dar subsídio para discutir a seguinte questão norteadora: Como os princípios ágeis podem ser aplicados nos processos de resposta a incidentes de segurança da informação?

Para se realizar a pesquisa com esta pergunta norteadora observou-se ser necessário encontrar instrumentos metodológicos que não necessariamente seguem direções de pesquisa convencional. É requerido que a metodologia traga contribuição teórica do conhecimento e aplicabilidade prática baseada em experiências, incluindo contribuição do autor ao estudo.

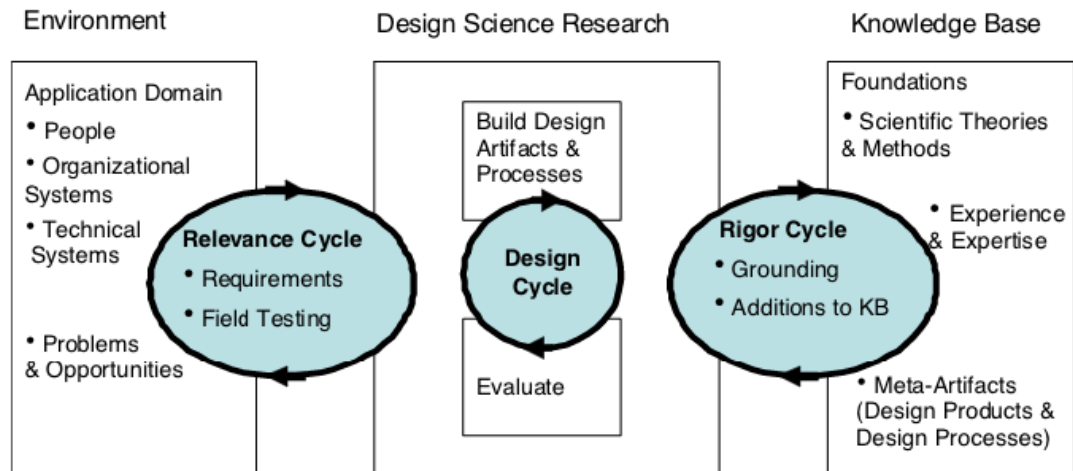
A *design science* foi analisada por Hevner (2007) incorporando três ciclos de atividades intimamente relacionados:

- O *Ciclo de Relevância* insere os requisitos do ambiente contextual na pesquisa e introduz os artefatos de pesquisa nos testes de campo ambientais;
- O *Ciclo do Rigor* fornece base teórica e métodos juntamente com experiência de domínio e competência dos fundamentos da base de conhecimento para a pesquisa e adiciona o novo conhecimento gerado à crescente base de conhecimento;
- O *Ciclo Central do Design* sustenta um ciclo mais estreito de atividade de pesquisa para a construção e avaliação de artefatos e processos de *design*;

O reconhecimento desses três ciclos em um projeto de pesquisa posiciona e diferencia claramente a ciência do *design* de outros paradigmas de pesquisa (HEVNER, 2007).

A **Figura 10** ilustra os três ciclos estudados por Hevner (2007) que os relacionam com o ambiente, a *Design Science Research* e a base de conhecimento. O Ciclo de Relevância conecta o ambiente contextual do projeto de pesquisa com as atividades do *Design Science*. O Ciclo do Rigor, por sua vez, conecta as atividades de *Design Science* com a base de conhecimento de fundamentos científicos, experiência e *expertise* que informam o projeto de pesquisa. O Ciclo de *Design* do centro itera entre as atividades centrais de construção e avaliação dos artefatos de *design* e processos da pesquisa. Hevner (2007) postulou que esses três ciclos devem estar presentes e claramente identificáveis em um projeto de pesquisa em *design science*.

Figura 10 Ciclos da *Design Science Research*



Fonte: (HEVNER, 2007)

A pesquisa em *Design Science* é definida como paradigma de pesquisa que responde a perguntas relevantes a problemas identificados, por meio da criação de artefatos inovadores; o princípio fundamental é ter processo de pesquisa para adquirir conhecimento e compreensão de um problema e construir solução aplicada por artefato (HEVNER; CHATTERJEE, 2010).

O processo DS inclui seis etapas: (Etapa 1) identificação e motivação do problema; (Etapa 2) definição dos objetivos para uma solução; (Etapa 3) *design* e desenvolvimento; (Etapa 4) demonstração; (Etapa 5) avaliação; e (Etapa 6) comunicação (PEFFERS et al., 2007). O **Quadro 5** apresenta o resumo das etapas do processo de *Design Science*.

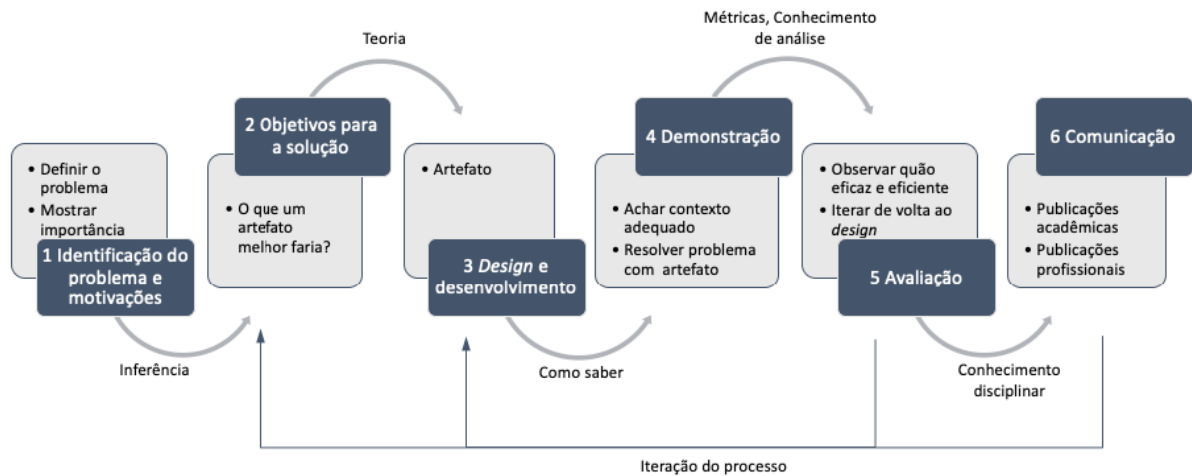
Quadro 5 Resumo das etapas do processo de *Design Science*

Etapas	Descrição	Resumo
Etapa 1	Identificação do problema e motivações	Definir o problema específico da pesquisa e justificar o valor do artefato a ser produzido como solução, que motive pesquisadores e leitores a entenderem a proposta de solução e o raciocínio associado ao entendimento do problema. Os recursos necessários incluem o conhecimento do problema e importância da solução proposta.
Etapa 2	Objetivos para solução	Inferir os objetivos da solução, com base na Etapa 1, com artefato a que seja possível e viável. Os recursos necessários incluem conhecimento dos problemas e possíveis soluções existentes.
Etapa 3	Projeto de desenvolvimento	Criação de artefato de pesquisa por construção, modelo, método ou instanciação, com arquitetura, funcionalidades desejadas. Recursos necessários: conhecimento da teoria a ser aplicada na solução.
Etapa 4	Demonstração	Demonstrar o uso do artefato para resolver uma ou mais instâncias do problema, com experimentação, simulação, estudo de caso, ou outra atividade apropriada. Recursos necessários: conhecimento efetivo de como o artefato é usado para resolver o problema.
Etapa 5	Avaliação	Comparar os objetivos da solução com resultados reais observados do uso do artefato demonstrado, com análises e/ou métricas tecnicamente relevantes, podendo considerar empírico apropriado como evidência. Em iteração esta etapa pode voltar à Etapa 3 para tentar melhorar a eficácia do artefato ou continuar à etapa seguinte.
Etapa 6	Comunicação	Comunicar em publicações de pesquisas acadêmicas, para que pesquisadores e públicos relevantes conheçam a importância do problema, a utilidade e novidade do artefato, o rigor de seu design e sua eficácia.

Fonte: Adaptado de (PEFFERS et al., 2007).

Peffers et al. (2007) sintetizou o modelo de processo composto de seis atividades em uma sequência nominal. Vários pesquisadores em SI e outras disciplinas contribuíram com ideias para elementos de processo e concordam substancialmente em elementos comuns. O resultado desta síntese está descrito graficamente na **Figura 11**.

Figura 11 Modelo do processo da *Design Science Research Methodology* (DSRM)



Fonte: Adaptado de (PEFFERS et al., 2007).

As próximas seções descrevem brevemente cada uma das seis etapas do DSRM.

2.1 Etapa de identificação do problema e motivações

Esta primeira etapa direciona a definição do problema de pesquisa específico e justificativa o valor de uma solução. Uma vez que a definição do problema será usada para desenvolver um artefato que possa efetivamente fornecer uma solução, pode ser útil atomizar o problema conceitualmente para que a solução possa capturar sua complexidade. Justificar o valor de uma solução ajuda produzir duas coisas: motiva o pesquisador e o público da pesquisa a buscar a solução e a aceitar os resultados e ajuda a entender o raciocínio associado à compreensão do problema pelo pesquisador. (PEFFERS et al., 2007).

Os recursos necessários para esta atividade incluem o conhecimento do estado do problema e a importância de sua solução, para no sequenciamento da DSRM endereçar a etapa de objetivos para a solução, obtida com a construção e aplicação de um artefato, que é construído na DSRM em etapas subsequentes (HEVNER; CHATTERJEE, 2010)

Formalmente, um problema da organização pode ser definido como a diferença entre o estado da meta e o estado atual. A resolução de problemas se dá pela redução, restrição ou

eliminação dessas diferenças, relacionadas à utilidade. A relevância da DSRM para resolução do problema refere-se à interação e motivações da comunidade na organização, no planejamento, gerenciamento, projeto de desenvolvimento, implementação, operação e avaliação das suas atividades (HEVNER et al., 2004).

As motivações dessa comunidade é que permitem que problemas sejam endereçados, para pensar em artefatos como constructos, modelos pelos quais representar, explorar métodos para analisar ou otimizar, e instanciações demonstradas (HEVNER et al., 2004).

A etapa seguinte descreve os objetivos para a construção do produto da DSRM.

2.2 Etapa de objetivos para a solução

Esta etapa trata dos objetivos da solução, pela inferência racional embasada na Etapa 1, com artefato que seja possível e viável, podendo ser quantitativo ou qualitativo. Os recursos necessários para isso incluem conhecimento dos problemas e possíveis soluções existentes e suas eficácias (HEVNER; CHATTERJEE, 2010).

Pretende-se inferir os objetivos de uma solução a partir da definição do problema e do conhecimento do que é possível e viável. Os objetivos podem ser quantitativos ou qualitativos. Os objetivos devem ser inferidos racionalmente a partir da especificação do problema. Os recursos necessários para isso incluem o conhecimento do estado dos problemas e das soluções atuais, se houver, e sua eficácia (PEFFERS et al., 2007).

A próxima etapa representa o *core* do *Design Science*, o *Design* e Desenvolvimento.

2.3 Etapa de *design* e desenvolvimento

Os termos *design*, delineamento, plano de pesquisa, protocolo de pesquisa, projeto de pesquisa e modelo operatório, acabam designando a mesma coisa, quase com poucas nuances. De uma forma geral, esses termos se referem ao documento no qual o pesquisador apresenta a pesquisa que ele pretende realizar e o modo como ele procederá (POUPART; NASSER, 2008).

O objetivo desta etapa é criar o artefato. Eles podem ser constructos, modelos, métodos ou instanciações (cada um amplamente definido) (HEVNER et al., 2004), como resumido no **Quadro 6**, ou novas propriedades de recursos técnicos, sociais e/ou informacionais.

Conceitualmente, um artefato de pesquisa de *design* pode ser qualquer objeto projetado no qual uma contribuição de pesquisa esteja incorporada ao *design*. Essa atividade inclui determinar a funcionalidade desejada do artefato e sua arquitetura e, em seguida, criar o artefato real. Os recursos necessários para passar de objetivos para projeto e desenvolvimento incluem conhecimento de teoria que pode ser usado em uma solução (PEFFERS et al., 2007).

O princípio fundamental é ter processo de pesquisa para adquirir conhecimento e compreensão de um problema, reconhecer os recursos necessários para passar dos objetivos ao projeto, sendo que o desenvolvimento inclui o conhecimento da teoria que possa ser aplicada por artefato (HEVNER; CHATTERJEE, 2010).

O **Quadro 6** resume as descrições dos tipos de artefatos documentados na DSRM.

Quadro 6 Tipos de Artefatos da DSRM

Tipo	Descrição
Constructos	Constructos ou conceitos formam o vocabulário de um domínio. Eles constituem uma conceituação utilizada para descrever os problemas dentro do domínio e para especificar as respectivas soluções. Conceituações são extremamente importantes em ambas as ciências, natural e de <i>design</i> . Eles definem os termos usados para descrever e pensar sobre as tarefas e podem ser valiosos para <i>designers</i> e pesquisadores.
Modelos	Um modelo é um conjunto de proposições ou declarações que expressam as relações entre os constructos. Em atividades de <i>design</i> , modelos representam situações como problema e solução. Ele pode ser visto como uma representação de como as coisas são. Cientistas naturais muitas vezes usam o termo ‘modelo’ como sinônimo de ‘teoria’, ou ‘modelos’ como as teorias ainda incipientes. Na <i>Design Science</i> , no entanto, a preocupação é a utilidade de modelos, não a aderência de sua representação à Verdade. Embora tenda a ser impreciso sobre detalhes, um modelo precisa sempre capturar a estrutura da realidade para ser uma representação útil.

Tipo	Descrição
Métodos	Conjunto de passos (um algoritmo/orientação) usado para executar uma tarefa. Métodos baseiam-se em um conjunto de constructos subjacentes (linguagem) e uma representação (modelo) em um espaço de solução. Os métodos podem ser ligados aos modelos, nos quais as etapas do método podem utilizar partes do modelo como uma entrada que o compõe. Além disso, os métodos são, muitas vezes, utilizados para traduzir um modelo ou representação em um curso para resolução de um problema. Os métodos são criações típicas das pesquisas em <i>Design Science</i> .
Instanciações	Uma instanciação é a concretização de um artefato em seu ambiente. Instanciações operacionalizam constructos, modelos e métodos. No entanto, uma instanciação pode, na prática, preceder a articulação completa de seus constructos, modelos e métodos. Demonstram a viabilidade e a eficácia dos modelos e métodos que elas contemplam.

Fonte: Adaptado de (LACERDA et al., 2013; MARCH; SMITH, 1995)

Cabe aqui uma explicação adicional sobre o termo “artefato”, uma vez que será usado em outros contextos no texto. Quando estiver sendo usado como parte da DSRM, o seu significado será o explicado nos parágrafos acima.

Entretanto, em segurança da informação, um artefato malicioso é uma evidência, como um texto ou referência a um recurso, ou uma informação deixada por um invasor em um sistema comprometido, como programas, *scripts*, ferramentas, *logs* e arquivos. Também pode ser qualquer programa de computador, ou parte dele, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes.

Na engenharia de *software*, artefato é um dos vários tipos de subprodutos concretos produzido durante o desenvolvimento de *software*. Nos modelos UML, os artefatos são elementos que representam as entidades físicas em um sistema de *software*, como por exemplo arquivos executáveis, bibliotecas, componentes de *software*, documentos e bancos de dados.

Neste trabalho, o termo artefato será também utilizado como resultado dos eventos do método ágil *Scrum* permitindo transparência, a obtenção do controle do projeto e sua adaptação. São artefatos do *Scrum* o *Backlog* do Produto e o *Backlog* do *Sprint*.

A Seção 3.3 deste trabalho ilustra esta etapa de *design* e desenvolvimento.

2.4 Etapa de demonstração

Demonstrar o uso do artefato para resolver uma ou mais instâncias do problema. Isso pode envolver seu uso em experimentação, simulação, estudo de caso, prova ou outra atividade apropriada. Os recursos necessários para a demonstração incluem conhecimento efetivo de como usar o artefato para resolver o problema (PEFFERS et al., 2007).

O artefato originado da DSRM é obtido dos resultados da pesquisa na fundamentação teórica, sendo necessário cuidados que minimizem o viés nos resultados gerados pelo artefato.

Demonstrar a viabilidade do artefato, de certa maneira ajuda a justificar o esforço da pesquisa teórica realizada e faz a solução fornecer resultados esperados a partir dos estudos de campo. A pesquisa teórica é utilizada para explicar (1) por que o projeto do artefato pode funcionar e (2) especificar eventuais contingências resultantes de princípios que possam fazer parte de práticas recomendadas. A importância do projeto como modo de pesquisa é reconhecida na literatura acadêmica para melhorar o desempenho organizacional (HEVNER; CHATTERJEE, 2010).

Os artefatos produzidos podem ser observados na Seção 3.5 deste trabalho.

2.5 Etapa de avaliação

O objetivo desta etapa é observar e medir quão bem o artefato sustenta uma solução para o problema. Esta atividade envolve a comparação dos objetivos de uma solução com os resultados reais observados do uso do artefato na demonstração (PEFFERS et al., 2007).

Requer conhecimento de métricas relevantes e técnicas de análise e dependendo da natureza do local do problema e do artefato, a avaliação pode assumir muitas formas. Pode incluir itens como uma comparação da funcionalidade do artefato com os objetivos da solução da atividade dois acima, medidas de desempenho quantitativas objetivas, como orçamentos ou itens produzidos, resultados de pesquisas de satisfação, *feedback* de clientes ou simulações.

Pode incluir medidas quantificáveis de desempenho do sistema, como tempo de resposta ou disponibilidade (PEFFERS et al., 2007).

Conceitualmente, tal avaliação pode incluir qualquer evidência empírica apropriada ou prova lógica. A natureza do local de pesquisa pode ditar se tal iteração é viável ou não (PEFFERS et al., 2007).

Para Lacerda et al. (2013), a avaliação final do artefato não dispensa que, em cada etapa do método da *Design Science Research*, sejam realizadas avaliações parciais dos resultados. Isso se faz necessário para se certificar de que a pesquisa está no sentido dos objetivos propostos. Autores como Hevner et al., (2004) propõem alguns métodos que podem ser utilizados para a avaliação dos artefatos gerados pela *Design Science Research*, conforme descrito no **Quadro 7**.

Quadro 7 Métodos para avaliação dos artefatos

Forma de avaliação	Métodos propostos
Observacional	<p><i>Estudo de Caso</i>: Estudar o artefato existente, ou não, em profundidade no ambiente de negócios.</p> <p><i>Estudo de Campo</i>: Monitorar o uso do artefato em projetos múltiplos. Esses estudos podem, inclusive, fornecer uma avaliação mais ampla do funcionamento dos artefatos configurando, dessa forma, um método misto de condução da pesquisa.</p>
Analítico	<p><i>Análise Estatística</i>: Examinar a estrutura para qualidades estáticas.</p> <p><i>Análise da Arquitetura</i>: Estudar o encaixe do artefato na arquitetura técnica do sistema técnico geral.</p> <p><i>Otimização</i>: Demonstrar as propriedades ótimas inerentes ao artefato ou então os limites de otimização no comportamento do artefato.</p> <p><i>Análise Dinâmica</i>: Estudar o artefato durante o uso para avaliar suas qualidades dinâmicas (por exemplo, desempenho).</p>
Experimental	<p><i>Experimento Controlado</i>: Estudar o artefato em um ambiente controlado para verificar suas qualidades (por exemplo, usabilidade).</p> <p><i>Simulação</i>: Executar o artefato com dados artificiais.</p>

Forma de avaliação	Métodos propostos
Teste	<p><i>Teste Funcional (Black Box):</i> Executar as interfaces do artefato para descobrir possíveis falhas e identificar defeitos.</p> <p><i>Teste Estrutural (White Box):</i> Realizar testes de cobertura de algumas métricas para sua implementação (por ex., caminhos para a execução).</p>
Descritivo	<p><i>Argumento informado:</i> Utilizar a informação das bases de conhecimento (por exemplo, das pesquisas relevantes) para construir um argumento convincente a respeito da utilidade do artefato.</p> <p><i>Cenários:</i> Construir cenários detalhados em torno do artefato, para demonstrar sua utilidade</p>

Fonte: Adaptado de (HEVNER et al., 2004; LACERDA et al., 2013)

Ao final desta etapa o pesquisador deste estudo pode decidir iterar à etapa de projeto e desenvolvimento para tentar melhorar a eficácia do artefato ou continuar à etapa seguinte para obter melhoria adicional por meio de projetos subsequentes (HEVNER; CHATTERJEE, 2010).

2.6 Etapa de comunicação

Esta etapa tem como objetivo comunicar o problema e sua importância, bem como o artefato, sua utilidade e novidade, o rigor de seu *design* e sua eficácia para pesquisadores e outros públicos relevantes, como profissionais atuantes, quando apropriado e em publicações de pesquisa acadêmica, os pesquisadores podem usar a estrutura desse processo para estruturar o artigo, assim como a estrutura nominal de um processo de pesquisa empírica (definição do problema, revisão da literatura, desenvolvimento de hipóteses, coleta de dados, análise, resultados, discussão e conclusão). É uma estrutura comum para trabalhos de pesquisa empírica. A comunicação requer o conhecimento da cultura disciplinar.

3 PESQUISA EMPÍRICA

Conforme apresentado no Capítulo 2, a pesquisa foi conduzida pela metodologia DSRM, cujos resultados são apresentados a seguir.

A etapa de identificação do problema e motivações para a pesquisa referenciadas na DSRM estão cobertas pelo capítulo de fundamentação teórica, por meio da literatura científica estudada e da aderência à questão da pesquisa, conforme apresentado nas Seções 1.1 a 1.4.

A etapa de objetivos para a solução são apresentados na Introdução do trabalho e nas Seções 1.1 a 1.4. As próximas seções discutem as etapas de *design* e desenvolvimento, demonstração, avaliação e comunicação.

3.1 *Design* e desenvolvimento

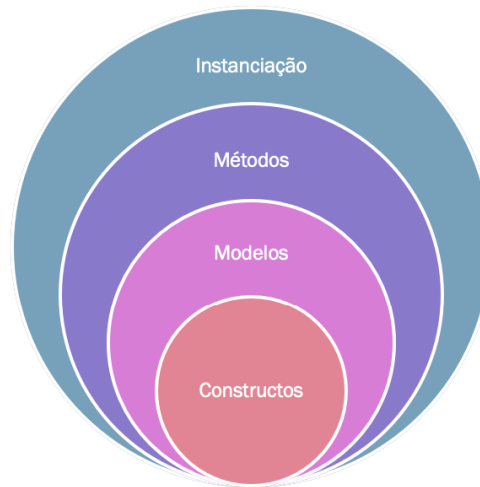
Enquanto a Seção 2.3 Etapa de *design* e desenvolvimento, do capítulo anterior, trouxe a descrição teórica das atividades da presente etapa, esta Seção representa a Etapa 3 do DSRM e detalha como a solução foi projetada e desenvolvida para alcançar os objetivos identificados descritos no início do trabalho.

3.1.1 *As relações entre os artefatos constructo, modelo, método e instanciação*

Retomando os conceitos dos artefatos produzidos pelo DSRM, resumidos no **Quadro 6** da Seção 2.3, a **Figura 12** ilustra de maneira simplificada a relação entre eles. Esta relação será a maneira pela qual se construirá a explicação do *design* e desenvolvimento desta pesquisa.

O trabalho desenvolvido utiliza algumas práticas ágeis para complementar e melhorar os processos tradicionais de resposta a incidentes de informação com ênfase nas fases de pré-incidente, triagem, análise e resolução do incidente. A este modelo chamamos de **AIR-Jud**, de *Agile Incident Response* aplicado ao judiciário brasileiro.

Figura 12 Relação entre constructos, modelos, métodos e instanciação conforme o DSRM



Fonte: Adaptado de (LACERDA et al., 2013; MARCH; SMITH, 1995)

A **Figura 13** ilustra os constructos tratados pela pesquisa: Incidentes de Segurança, Tratamento de Incidentes e Princípios Ágeis. As práticas e princípios ágeis e o tratamento de incidentes atuam no contexto do gerenciamento de riscos relacionados aos incidentes de segurança de uma instituição do Poder Judiciário.

Figura 13 Constructos da pesquisa



Fonte: Resultado da pesquisa

Os conceitos apresentados na **Figura 13** pertencem ao domínio de estudo deste trabalho. Conforme a DSRM, eles podem ser classificados como um artefato do tipo **constructo**. Retomando a sua descrição, constructos constituem uma conceituação utilizada para descrever os problemas dentro do domínio e para especificar as respectivas soluções.

O constructo *Incidente de Segurança* é definido como um evento de segurança ou um conjunto deles, confirmado ou sob suspeita de impactar a disponibilidade, integridade,

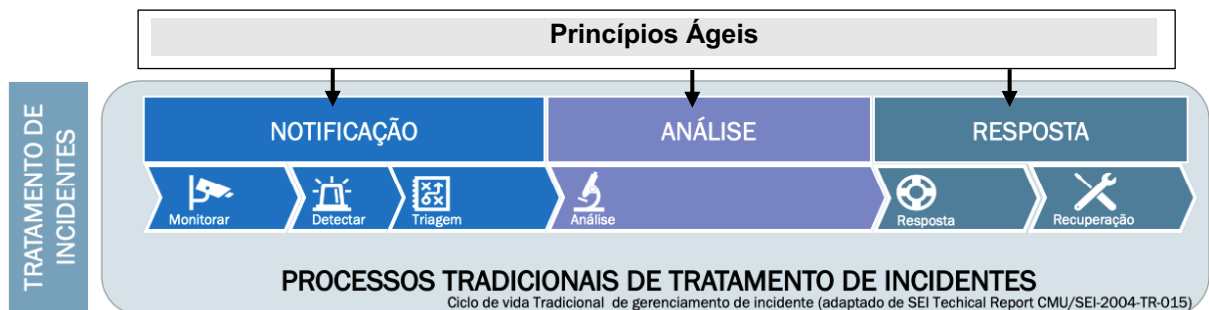
confidencialidade ou a autenticidade de um ativo de informação, bem como qualquer violação da política de segurança da informação.

O *Tratamento de Incidentes* é composto por notificação do incidente, análise do incidente e resposta ao incidente, contendo os processos tradicionais de resposta a incidentes.

O constructo *Princípios Ágeis* trata da adaptação dos princípios ágeis aos processos de resposta a incidentes, como os papéis, eventos e artefatos do *Scrum*, explicados na sequência. Princípios ágeis são os conceitos, ferramentas e práticas oriundas do manifesto e método ágil.

No DSRM, um **modelo** é um conjunto de proposições ou declarações que expressam as relações entre os constructos. Em atividades de *design*, modelos representam situações como problema e solução, podendo ser visto como uma representação de como as coisas são e na sua utilidade (LACERDA et al., 2013). Desse modo, as relações entre os constructos definidos nesta pesquisa são exemplificados na **Figura 14**, ilustra o modelo representando o ciclo de vida do experimento, relacionando os constructos do tratamento de incidente.

Figura 14 Modelo dos processos de tratamento de incidentes com métodos ágeis



Fonte: Resultado da pesquisa

Notificação de incidente é o que habilita um CSIRT a servir como um ponto central de contato para notificação de problemas locais. Isto permite que todas as atividades e os incidentes reportados sejam coletados em um único local, onde esta informação pode ser analisada e correlacionada por meio da organização ou comunidade sendo atendida. É subdividida geralmente em monitoramento, detecção e triagem.

Análise de incidente envolve analisar a fundo uma notificação ou uma atividade observada para determinar o escopo, prioridade e ameaça representada pelo incidente, bem como pesquisar acerca de possíveis estratégias de resposta e erradicação;

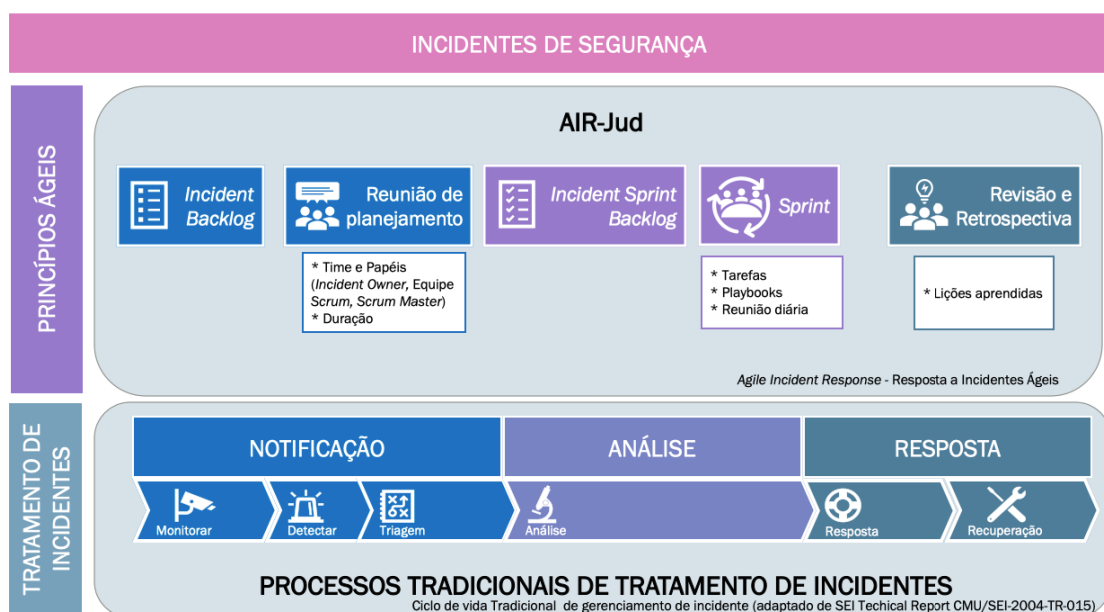
Resposta a incidente pode assumir formas variadas. Um CSIRT pode elaborar e divulgar recomendações para recuperação, contenção e prevenção, que são enviadas para os membros da comunidade por ele atendida e para os administradores de redes e sistemas que serão responsáveis por implementar os passos referentes à resposta ao incidente. A resposta pode envolver também o compartilhamento de informações e lições aprendidas com outros grupos de resposta a incidentes e com outras organizações e sites;

Avançando no DSRM, um **método** é um conjunto de passos usado para executar uma tarefa. Métodos baseiam-se em um conjunto de constructos subjacentes (linguagem) e uma representação (modelo) em um espaço de solução (LACERDA et al., 2013).

Os métodos podem ser ligados aos modelos, nos quais as suas etapas podem utilizar partes do modelo como uma entrada que o compõe. Dessa maneira, os métodos ágeis, como o *Scrum* e o *Kanban*, são utilizados para traduzir o modelo em um curso para resolução do problema estudado nesta pesquisa. Ou seja, a adaptação dos processos tradicionais de resposta a incidentes passa a utilizar os métodos ágeis do *Scrum* e *Kanban* para o modelo representado.

Ilustrado na **Figura 15** temos o método ágil *Scrum* utilizado para adaptar o ciclo de vida tradicional de gerenciamento de incidentes. É possível observar o método *Scrum* adaptado, o AIR-Jud, e o modelo do ciclo de vida tradicional, alinhado ao método cascata.

Figura 15 O modelo de resposta a incidentes adaptado com o método *Scrum*



Fonte: Resultado da pesquisa

As principais práticas ágeis que inspiraram a adaptação dos processos tradicionais de resposta incidentes foram os métodos do *Scrum* e do *Kanban*. Desse modo, é necessário adotar algumas regras específicas derivadas dos seus valores de transparência, inspeção e adaptação, conforme proposto por Schwaber & Sutherland (2017):

- i. Um time *Scrum* consiste em três papéis principais: *Product Owner*, *Scrum Master* e Time de Desenvolvimento. Esses papéis serão adaptados ao contexto de cibersegurança.
- ii. O projeto é dividido em *Sprints* de período de 1 a 4 semanas, devendo ser entregue algum incremento de produto valioso no final de cada *Sprint*. Aqui também será adaptado o período para a entrega de valor de um incidente.
- iii. Os eventos formais do Scrum asseguram a inspeção e adaptação: no início de cada *Sprint* (*Sprint Planning*), no final de cada dia (*Daily Meeting*) e no final de cada *Sprint* (*Sprint Review* e *Sprint Retrospective*). Estes eventos podem ser encaixados no fluxo de um tratamento e resposta a incidentes de segurança da informação.
- iv. Os artefatos produzidos fornecem transparência e oportunidades de inspeção e adaptação: *Product Backlog*, *Sprint Backlog* e Incremento, são itens que necessitam ser adaptados ao contexto de cibersegurança.

Uma **instanciação** é a concretização de um artefato em seu ambiente. Instanciações operacionalizam constructos, modelos e métodos. No entanto, ela pode, na prática, preceder a articulação completa de seus constructos, modelos e métodos (LACERDA et al., 2013).

A instanciação proposta neste trabalho visa demonstrar a viabilidade e a eficácia dos modelos e métodos que ela contempla, utilizando para isso um exemplo prático real situado no contexto da resposta a incidentes de segurança da informação do Poder Judiciário. Na seção da Etapa de Demonstração compreende-se melhor este artefato.

3.1.2 Processos adaptados do método Scrum

Como proposto por SMITH et al. (2021) em seu *framework* AIR4ICS, os processos de resposta a incidentes apresentado neste trabalho são estruturados em breves rajadas de atividade

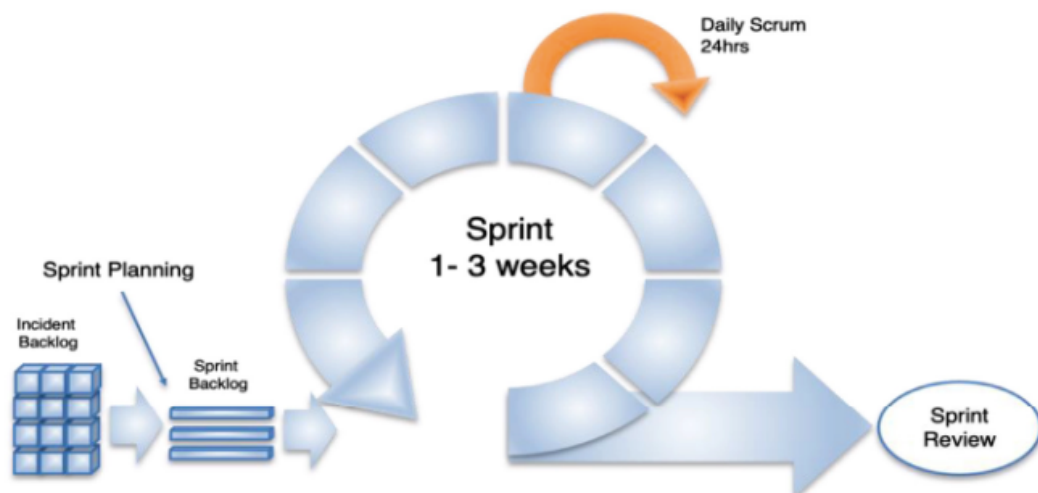
análogas às *Sprints* do *Scrum* durante as quais os objetivos das fases tradicionais serão parcialmente alcançados e etapas para a resolução sendo adicionadas etapas interativas.

Considerando que a dinâmica de um ataque cibernético complexo pode exigir várias edições e revisões da estratégia de resposta, dependendo das informações obtidas durante o ataque, o modelo proposto utiliza uma abordagem interativa aos processos dando ênfase na melhoria contínua do processo de resposta a incidentes (SMITH et al., 2021).

A equipe responsável por incidentes é multifuncional e conduz o planejamento e revisão da *Sprint* pelo melhor curso de ação, podendo escalar os incidentes aos negócios ou às organizações externas, como outros CSIRTs ou CERTs nacionais. Diferentemente dos projetos de desenvolvimento, essas *Sprints* são mais curtas em duração – diminuindo a equipe para responder e se adaptar à ação adversária ou às mudanças imprevistas no ambiente de operação como consequência dos efeitos do ataque ao ambiente. A abordagem para identificar o objetivo para o próximo *Sprint* é impulsionada pelo valor da resposta e pelo risco associado aos termos de probabilidade de sucesso e impacto no negócio (SMITH et al., 2021).

A **Erro! Fonte de referência não encontrada.** de Smith et al. (2021), ilustra o método *Scrum* adaptado ao contexto de resposta a incidentes. É possível observar que vários “blocos” de *Incident Backlog* originam os *Sprint Backlogs*. Durante o *Sprint* de duração variável, as *Daily Scrum* podem ser menores que 24h, dependendo do caso. O *Sprint Review* incorpora a função de Retrospectiva do *Sprint*.

Figura 16 O método *Scrum* adaptado para o modelo de resposta a incidentes



Fonte: (SMITH et al., 2021)

A **Erro! Fonte de referência não encontrada.** exemplifica o conceito de método do DSRM ao agrupar constructos e modelos e exhibe o conjunto de passos para execução conforme descreve o método *Scrum*. Neste caso, os constructos, modelos e métodos estão adaptado ao domínio do objeto deste estudo. Em seguida trataremos dos papéis, eventos e artefatos adaptado do método *Scrum*.

3.1.3 Papéis

As equipes tradicionais de resposta a incidentes muitas vezes seguem uma estrutura rígida e hierárquica. Os indivíduos são realocados para uma função especializada, como *firewalls*, ameaças etc. Essa segregação de tarefas muitas vezes leva à criação de silos de informações e conhecimentos, onde as tentativas de passar informações e habilidades para outras unidades relevantes podem ser abaixo do ideal. Os princípios ágeis visam quebrar esses silos criando equipes mais integradas (SMITH et al., 2021).

Para isso, existem apenas três papéis distintos dentro de uma equipe de resposta a incidentes ágeis, conforme descrito no **Quadro 8**. A primeira coluna identifica o papel, a segunda coluna se baseia nas definições originais do *Scrum* pelos autores Schwaber & Sutherland (2017), enquanto a terceira coluna é a proposta de adaptação pelo modelo AIR-Jud, inspirado no trabalho de Smith et al. (2021).

Quadro 8 Papéis de uma equipe ágil de resposta a incidentes

Papel	Descrição original <i>Scrum</i>	Descrição no AIR-Jud
<i>Incident Owner</i>	Originalmente <i>Product Owner</i> , papel que representa o cliente durante todo o projeto e responsável por criar e gerenciar o conteúdo do <i>Product Backlog</i> , ordenando os itens para trazer o incremento mais valioso ao final de cada <i>Sprint</i> (SCHWABER; SUTHERLAND, 2017)	Essa função geralmente é desempenhada por um gerente de resposta a incidentes experiente ou líder técnico. Possui a visão/estratégia do incidente. Atua como ponto de contato com a alta administração e em nome do cliente (quando diferente de organização). Controla e prioriza o <i>Backlog de Incidentes</i> (SMITH et al., 2021)

Papel	Descrição original <i>Scrum</i>	Descrição no AIR-Jud
<i>SCRUM Master</i>	O <i>Scrum Master</i> é responsável por promover e apoiar o <i>Scrum</i> entre membros e não membros da equipe, pois também deve treinar a equipe de desenvolvimento. (SCHWABER; SUTHERLAND, 2017)	Igualmente à descrição original, é um líder servidor da equipe de Resposta a Incidentes, ajudando a remover obstáculos, melhorar a resposta a incidentes e o desempenho da equipe para maximizar o valor (SMITH et al., 2021).
Membro da equipe	Equipe de desenvolvimento auto-organizada e multifuncional cuja função é transformar os itens do <i>Product Backlog</i> em Incrementos de Produto tangíveis. Decide de forma autônoma qual parte do <i>Product Backlog</i> é feita em cada <i>Sprint</i> . (SCHWABER; SUTHERLAND, 2017)	Profissionais que fazem o trabalho de dar a resposta para minimizar e mitigar o impacto de um incidente. Eles são estruturados e capacitados pela organização para organizar e gerenciar seu próprio trabalho. São auto-organizados, <i>cross functional</i> , sem títulos e responsáveis como um todo (SMITH et al., 2021).

Fonte: Adaptado de (SCHWABER; SUTHERLAND, 2017; SMITH et al., 2021)

3.1.4 Eventos

Adaptando os conceitos do *Scrum*, o modelo de resposta a incidentes ágil pode incorporar os eventos de um *Sprint*. Os *Sprints* são processos cíclicos que se iniciam com o *Incident Backlog* que é então dissecado para criar um *Sprint Backlog*. Isso é então usado como entrada para as *Daily Scrums* até o final do *Sprint*, quando as revisões e retrospectivas ocorrem. Quaisquer lições aprendidas alimentam as ações no próximo *Sprint*.

Os eventos da *Sprint* são descritos no **Quadro 9**. Novamente, a primeira coluna descreve o evento *Scrum*, a segunda coluna se baseia nas definições originais do *Scrum* pelos autores Schwaber & Sutherland (2017), enquanto a terceira coluna é a proposta de adaptação pelo modelo AIR-Jud, inspirado no trabalho de Smith et al. (2021).

Quadro 9 Os eventos do método *Scrum* adaptados
para uma equipe de resposta a incidentes ágeis

Evento	Descrição original <i>Scrum</i>	Descrição no AIR-Jud
Planejamento do <i>Sprint</i>	Reunião de planejamento do próximo <i>Sprint</i> , criado pelo trabalho colaborativo de toda equipe <i>Scrum</i> . Cada membro da equipe de desenvolvimento seleciona algumas histórias de usuário do <i>Product Backlog</i> para implementar na próxima iteração e o resultado é o <i>Sprint Backlog</i> . (SCHWABER; SUTHERLAND, 2017)	Reunião em que as partes interessadas e os membros da equipe definem com eficiência e eficácia o trabalho a ser executado na iteração atual. Ela tem dois objetivos: (1) o que pode ser entregue na atualização resultante do próximo <i>Sprint</i> ? (2) como o trabalho será realizado? Os itens <i>Incident Backlog</i> a serem trabalhados durante o <i>Sprint</i> serão identificados criando um <i>Sprint Backlog</i> , com os membros da equipe assumindo a propriedade das tarefas (SMITH et al., 2021)
Reuniões <i>Scrums</i>	Originalmente <i>Daily Scrum</i> , é uma reunião em pé de duração máxima de 15 minutos, todos os dias no mesmo local à mesma hora. O objetivo é que cada membro exponha todos os conflitos ou problemas com o restante da equipe. Os membros geralmente se reúnem imediatamente após o <i>Daily Scrum</i> para discussões detalhadas ou para adaptar ou replanejar o restante do trabalho da <i>Sprint</i> . (SCHWABER; SUTHERLAND, 2017)	A frequência ideal para Reuniões <i>Scrum</i> é altamente dependente do contexto, exigindo um equilíbrio entre atualizar o conhecimento da equipe e interromper o trabalho no meio da tarefa. Recomenda-se que ocorram uma ou duas vezes ao dia com o <i>Scrum Master</i> decidindo a cadência mais apropriada. Como o Agile incentiva a adaptabilidade e a resposta à situação, as reuniões podem ocorrer com mais regularidade durante os momentos em que o incidente está mudando rapidamente. A reunião gira em torno de três questões: (1) O que eu fiz ontem? (2) O que vou fazer hoje? (3) Vejo algum impedimento? (SMITH et al., 2021).

Evento	Descrição original <i>Scrum</i>	Descrição no AIR-Jud
Fluxo de trabalho	Fluxo de trabalho organizado e gerenciado pela própria equipe. A sinergia resultante otimiza a eficiência e eficácia geral. (SCHWABER; SUTHERLAND, 2017)	É o trabalho de triagem, análise, mitigação e resposta aos incidentes realizado pelo <i>Scrum Team</i> por meio dos <i>playbooks</i> de resposta a ciberincidentes e demais técnicas.
Revisão da <i>Sprint</i>	Reunião no final de cada <i>Sprint</i> , onde o <i>Scrum Team</i> e as partes interessadas relevantes inspecionam o incremento e concordam com as mudanças no <i>Backlog</i> do Produto. O objetivo principal é mostrar os itens “feitos” e obter <i>feedback</i> sobre o incremento, que pode ser aceito ou rejeitado pelo cliente. (SCHWABER; SUTHERLAND, 2017)	A Revisão do Sprint é uma oportunidade para inspecionar o progresso feito durante o Sprint atual e adaptar o <i>Backlog do Incidente</i> , se necessário. Os resultados da reunião incluirão: (1) Identificação do que deu certo e melhores práticas para levar adiante em <i>Sprints</i> subsequentes; (2) Identificação de eventuais bloqueios à investigação e potenciais estratégias de mitigação; (3) Informações estratégicas necessárias para a sessão de planejamento da <i>Sprint</i> subsequente. (SMITH et al., 2021)
Retrospectiva da <i>Sprint</i>	Reunião ao final do <i>Sprint</i> , onde o time faz uma autoinspeção e o trabalho realizado e cria um plano com melhorias para aplicar no próximo sprint. Ocorre após cada <i>Sprint Review</i> e antes de cada <i>Sprint Planning</i> (SCHWABER; SUTHERLAND, 2017).	Como a versão original, mas destacando fatores humanos por meio de uma Matriz de Aprendizagem para identificar lições aprendidas para os próximos e futuros <i>Sprints</i> . Objetivos: (1) Inspecionar como foi o <i>Sprint</i> anterior em relação a pessoas, relacionamentos, processos e ferramentas; (2) Identificar e ordenar os principais itens que correram bem e potenciais melhorias; (3) Criar um plano para implementação de melhorias nos processos operacionais da equipe <i>Scrum</i> (SMITH et al., 2021).

Fonte: Adaptado de (SCHWABER; SUTHERLAND, 2017; SMITH et al., 2021)

3.1.5 Artefatos do Scrum

Os artefatos do *Scrum* e *Kanban* adaptados para o uso nos processos da CSIRT são descritos no **Quadro 10**:

Quadro 10 Artefatos do *Scrum* e *Kanban* adaptados ao contexto da resposta a incidentes de segurança cibernética

Artefato	Descrição original Scrum	Descrição no AIR-Jud
<i>Incident Backlog</i> (IB)	Originalmente, o <i>Product Backlog</i> é uma lista ordenada de todas as funcionalidades, requisitos, melhorias e correções que representam uma mudança no produto. É responsabilidade do <i>Product Owner</i> durante todo o projeto, incluindo sua criação, gerenciar seu conteúdo, disponibilidade e ordenação de seus itens (SCHWABER; SUTHERLAND, 2017).	O <i>Incident Backlog</i> é uma lista ordenada de incidentes, incluindo todos os aspectos de identificação, proteção, detecção, resposta e recuperação. É a única fonte de requisitos e quaisquer alterações devem ser refletidas nele. Inicialmente são incluídos os únicos requisitos conhecidos e mais bem compreendidos, mas à medida que a situação avança, eles serão expandidos e novos serão criados conforme e quando necessário (SMITH et al., 2021).
<i>Incident Sprint Backlog</i>	<i>Sprint Backlog</i> é uma lista de itens selecionados do <i>Product Backlog</i> para uma <i>Sprint</i> específica, resultado da seleção da equipe de desenvolvimento a partir de histórias de usuários para trabalhar nessa iteração (SCHWABER; SUTHERLAND, 2017).	Os itens do <i>Incident Sprint Backlog</i> devem facilitar a priorização das tarefas durante o incidente. Para garantir que o <i>backlog</i> possa ser gerenciado de forma eficaz, cada item deve ser: (1) detalhado; (2) evolutivo ao longo do tempo; (3) ter estimativa de esforço; (4) ter controle de prioridade (SMITH et al., 2021).
<i>Incident Board</i> (quadro <i>Kanban</i>)	Originalmente chamado de <i>Board</i> , ele implementa a transparência do <i>Scrum</i> fornecendo visualmente as informações sobre quem é	O <i>Incident Board</i> é um documento vivo e o ponto focal para as reuniões do <i>Scrum</i> e é usado em todo o processo extensivamente. Permite a fácil

Artefato	Descrição original Scrum	Descrição no AIR-Jud
	responsável pelas tarefas e quando elas são concluídas. Existem três níveis de status de tarefas: “a fazer”, “fazendo” e “feito”. Pode ser implementado com <i>post-its</i> em um quadro branco ou por <i>softwares</i> que fornecem métricas e análises (SUTHERLAND; SUTHERLAND, 2019)	identificação da situação atual dos <i>Incident Sprint Backlogs</i> dividido em diferentes fases. O <i>Incident Owner</i> e o <i>Scrum Master</i> são os principais usuários do quadro, utilizando-o para manter a consciência situacional do progresso da equipe, permitindo que a equipe melhore sua eficiência removendo potenciais gargalos (SMITH et al., 2021).
Fonte: Adaptado de (SCHWABER; SUTHERLAND, 2017; SMITH et al., 2021)		

A próxima seção avança para a parte demonstrativa do processo AIR-Jud.

3.2 Demonstração

Esta seção cobre a Etapa 4 Demonstração do método DSRM, enquanto a Seção 2.4 trouxe a descrição teórica das atividades desta etapa. Pode-se dizer que a demonstração da utilização do processo AIR-Jud contempla a sua instanciação, uma vez que os constructos, modelos e métodos já apresentados se concretizam em um exemplo prático, neste caso aplicado a um órgão do Poder Judiciário.

O experimento em realização neste trabalho propõe analisar os casos de incidentes de *phishing* que são reportados para a Comissão Local de Resposta a Incidentes do Tribunal Regional Federal da Terceira Região (CLRI-TRF3).

3.2.1 O Tribunal Regional Federal da 3ª. Região

A razão para a escolha do Tribunal Regional Federal da 3ª. Região (TRF3) foi devido a existência neste órgão do judiciário de um time de resposta a incidentes de segurança da informação já implantado e da necessidade de aprimoramento dos seus processos de trabalho.

O TRF3 foi criado juntamente com os outros quatro Tribunais Regionais Federais, pela Constituição de 1988 (artigo 27, § 6º), com o objetivo de substituir e regionalizar a jurisdição do extinto Tribunal Federal de Recursos (TFR). Os Tribunais Regionais Federais foram inaugurados simultaneamente, com suas sedes em São Paulo, Brasília, Rio de Janeiro, Porto Alegre e Recife no dia 30 de março de 1989.

Figura 17 Estados e Regiões da Justiça Federal brasileira



Fonte: Conselho da Justiça Federal

As cinco unidades da Justiça Federal brasileira com seus respectivos estados são ilustrados na **Figura 17**, sendo possível observar que a Justiça Federal da Terceira Região (JF3R) é composta pelos estados de Mato Grosso do Sul e São Paulo. Esta região atinge uma população de mais de 49 milhões de pessoas, cerca de 23% da população do país. Mato Grosso do Sul e São Paulo detem 33% do PIB brasileiro, cerca de R\$ 2,4 trilhões, conforme dados do painel da Justiça em Números (CNJ, 2021c).

Os dados do painel da Justiça em Números mostram que em 2020, período mais recente disponível dos dados, a Justiça Federal da Terceira Região foi responsável por receber mais de 764 mil novas ações ajuizadas na Justiça Federal do país. São mais de 3,3 milhões de processos pendentes de julgamento e mais de 744 mil sentenças proferidas em 2020.

O número total de servidores públicos na JF3R em 2020 chegou a 8.293, sendo que 531 são de magistrados do 1º. e do 2º. Grau e 6.664 são servidores. O número de usuários ativos dos recursos de informática somam 7.260 e o número de computadores chegam a quase 10 mil, dando uma média de 1,37 computadores por usuário. Entretanto, os dados mostram que apenas 127 servidores são da área de tecnologia da informação.

São 169 varas federais distribuídas entre 51 cidades sedes das chamadas de Subseções Judiciárias que tem a sua jurisdição sobre as cidades ao seu redor.

A JF3R teve em 2020 o registro de orçamento para despesas no total de R\$ 2,7 bilhões, incluindo despesas de pessoal e outras despesas. Das outras despesas, 12,6% dos valores foram destinados a despesas de informática, um valor de mais de R\$ 11,5 milhões.

3.2.2 *A Comissão Local de Resposta a Incidentes de Segurança da Informação*

A Comissão Local de Resposta a Incidentes do Tribunal Regional Federal da Terceira Região (CLRI-TRF3) é composta por grupo de servidores de diferentes áreas do Tribunal e da Seção Judiciária de Mato Grosso do Sul, cuja missão precípua é o gerenciamento de incidentes de segurança da informação – um conjunto de ações proativas e reativas cujo objetivo é a prevenção e o tratamento desses incidentes.

A criação da CLRI-TRF3 objetiva atender à determinação contida na Política de Segurança da Informação da Justiça Federal, descrita na Resolução CJF nº 6, de 7 de abril de 2008. Além da Justiça Federal da 3ª Região, todas as demais Regiões da Justiça Federal, e o Conselho da Justiça Federal, possuem suas CLRIs.

A *constituency*, isto é, o público-alvo da CLRI-TRF3 é composto dos magistrados, servidores e demais colaboradores dos órgãos da Justiça Federal nas Seções Judiciárias de São Paulo e de Mato Grosso do Sul, incluindo os Juizados Especiais Federais.

Entre as atividades proativas prestadas pela comissão, podem-se citar:

1. Acompanhamento da tecnologia: monitoramento das principais fontes de informação de tecnologia e segurança sobre as principais ameaças, riscos e vulnerabilidades;
2. Avaliações de segurança da informação: opinar sobre a segurança de produtos e serviços relacionados à TI, por meio de análises, pesquisa de reputação de segurança do fornecedor dos produtos e/ou serviços, e outros métodos;
3. Avisos: emitir avisos e recomendações relativas à segurança da informação considerados de valor para o seu público-alvo;

4. Cooperação com outros grupos de gerenciamento e de resposta a incidentes: colaborar e trocar informações com outros grupos, sejam estes governamentais ou privados;
5. Educação e conscientização: divulgar informação sobre segurança da informação para seu público-alvo, ajudando a aumentar a conscientização sobre o tema.

Entre os serviços reativos da CLRI-TRF3, podem ser citados:

- i. Alertas: emitir alertas sobre ameaças cibernéticas, na forma de mensagens de correio eletrônico, alertas no site da Internet e intranet e outros meios;
- ii. Análise de artefatos: Artefatos maliciosos que atinjam as redes e sistemas da instituição;
- iii. Tratamento e resposta a incidentes: Este é o trabalho mais importante da Comissão: receber as notificações, fazer a sua triagem, e executar, por sua própria iniciativa ou em parceria com outros órgãos, as ações para a mitigação do incidente;
- iv. Tratamento de vulnerabilidades: analisar os comunicados de vulnerabilidades pertinentes e orientar as áreas de TI e de outros órgãos envolvidos para que tomem as ações adequadas para evitar que essa vulnerabilidade seja explorada.

O presente trabalho se pauta na atividade reativa de tratamento e resposta a incidentes, conforme descrito acima e detalhado na sequência.

3.2.3 Detalhamento dos incidentes analisados no experimento

Existem diversos tipos de incidentes que podem ocorrer, entre os mais comuns estão: negação de serviço (DoS – *Denial of Service*), ataque de *phishing*, atividades de propagação de códigos maliciosos na rede (*worm*), invasão em computador ou rede, fraude ou tentativa de fraude, ataque de varredura de rede (*scan*), entre tantos outros.

A escolha de analisar esse tipo de incidente, *phishing*, em vez de demais permite que se faça uma análise mais homogênea da base de dados do incidente. Além disso, ataques de *phishing* já produziram danos ao judiciário. O TRF3 investigou um incidente de segurança da informação que indicou por meio de um *phishing* houve a recuperação de senhas de diversos usuários do TRF3 ao principal sistema de processo eletrônico, o PJe, o que possibilitou a

alteração de documentos de vários processos judiciais, incluindo o recebimento dos valores levantados (CONJUR, 2021a).

Em resumo, o trabalho proposto seguiu as seguintes diretivas:

- i. Utilizando como teste a base de casos de incidentes de *phishing report*;
- ii. Definir um time *scrum* de resposta a incidentes dentro da equipe CLRI;
- iii. Fazer triagem dos incidentes em um *Incident Backlog*;
- iv. Planejar e iniciar o *Sprint* de resolução dos incidentes;
- v. Revisar e realizar a retrospectiva da resolução dos incidentes;
- vi. Avaliar o desempenho do *Sprint* com a equipe CLRI;
- vii. Repetir o experimento agregando melhorias ao modelo;

A fonte de dados utilizada se baseia qualitativamente em dados reais obtidos da base de casos de incidentes de *phishing report*.

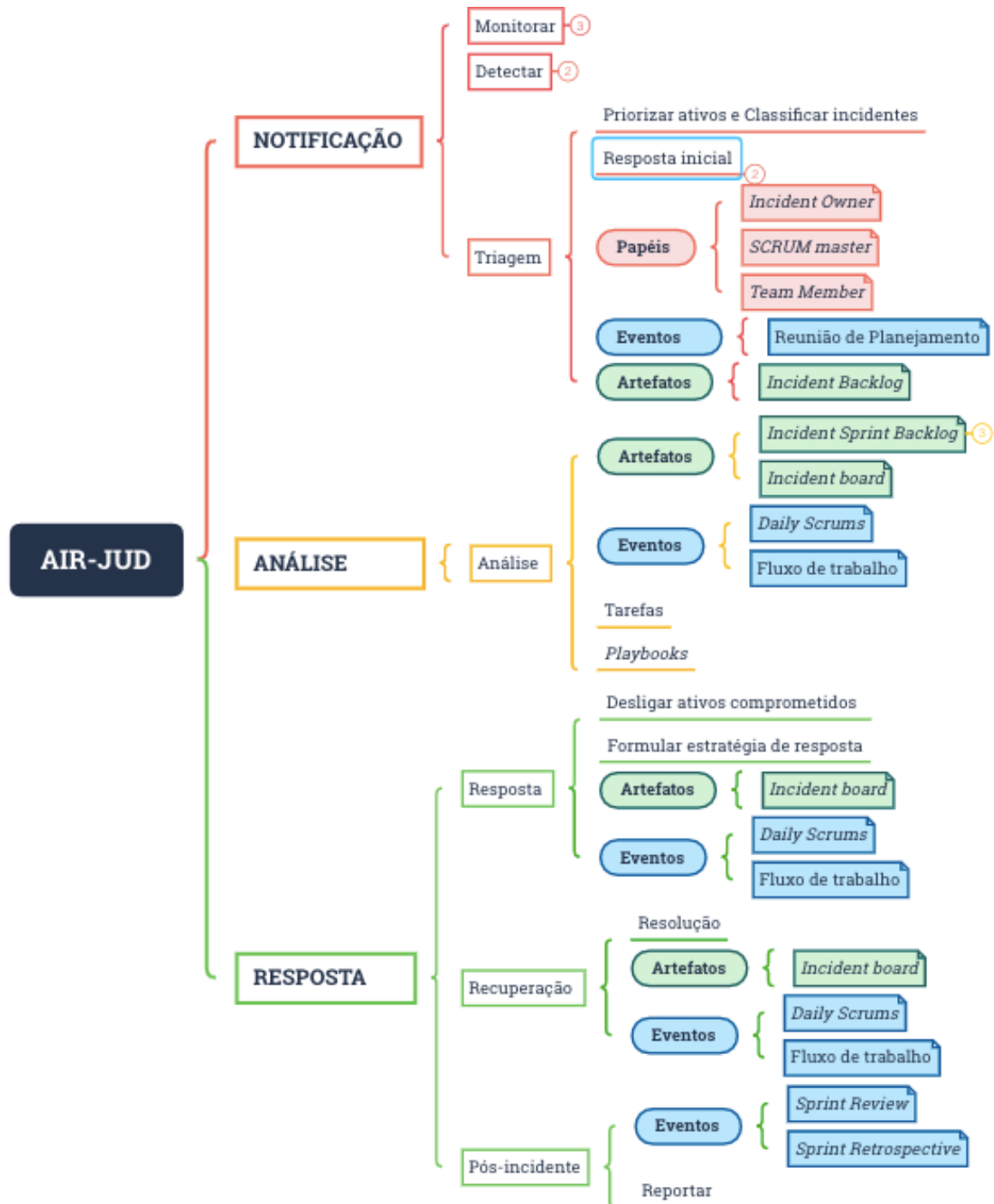
Seguindo a ideia de utilizar no modelo dos processos tradicionais de resposta a incidentes os métodos ágeis *Scrum* e *Kanban* foram espalhados ao longo das fases tradicionais, conforme mostrado na **Figura 18**. São ilustrados o mapeamento das práticas ágeis mencionadas anteriormente de maneira que estão incorporadas nos processos de resposta a incidentes tradicionais.

Os processos tradicionais de resposta a incidentes podem ser identificados na primeira e segunda camada na árvore da **Figura 18**, com as formas em retângulo. Estes processos são, como descritos anteriormente, notificação, análise e resposta. As práticas ágeis adaptadas podem ser vistas nas folhas da árvore, com a forma de retângulo elíptico e preenchido. Os papéis dos membros da equipe *Scrum* adaptada para resposta a incidentes, na cor vermelha, se encaixam na fase de Triagem, quando há tarefas de detecção, classificação de incidentes e priorização de ativos. Artefatos adaptados do *Scrum*, na cor verde, podem ser utilizados nas fases de Triagem, Análise, Resposta e Recuperação. E os eventos do *Sprint* do incidente, na cor azul, se encaixa nas fases de Triagem, Análise, Resposta, Recuperação e Pós incidentes.

Seguindo essas adaptações do método ágil, mesmo utilizando modelo tradicional de tratamento de incidentes, o processo de trabalho não segue um fluxo de plano de ação linear ou cascata, mas da forma como foi descrito na etapa de *design* e desenvolvimento: com a definição e auto organização da equipe ágil de resposta a incidente, a partir do *Incident Backlog* elabora-

se o *Incident Sprint Backlog*, que são usados como entrada para as *Daily Scrums* até o final do *Sprint*, quando as revisões e retrospectivas ocorrem.

Figura 18 Mapeamento das práticas ágeis no processo de resposta a incidentes



Fonte: Resultado da pesquisa

3.2.4 Demonstração do novo processo

Um primeiro ciclo de teste foi realizado em fevereiro de 2022, por meio de 40 casos de incidentes de *phishing* que foram distribuídos para um time de quatro indivíduos membros da CLRI-TRF3. A origem desses incidentes foi obtida de notificações de *phishing* encaminhadas ao e-mail institucional da CLRI. Os dados utilizados são, dessa forma, qualitativos.

Uma vez que o time *Scrum* foi definido, durante a reunião inicial de planejamento da *Sprint*, foi estabelecido o tempo de três semanas para a conclusão do primeiro *Sprint*, uma reunião por dia com os membros por meio de videoconferência e a divisão dos 40 casos para atribuição de um caso para cada membro.

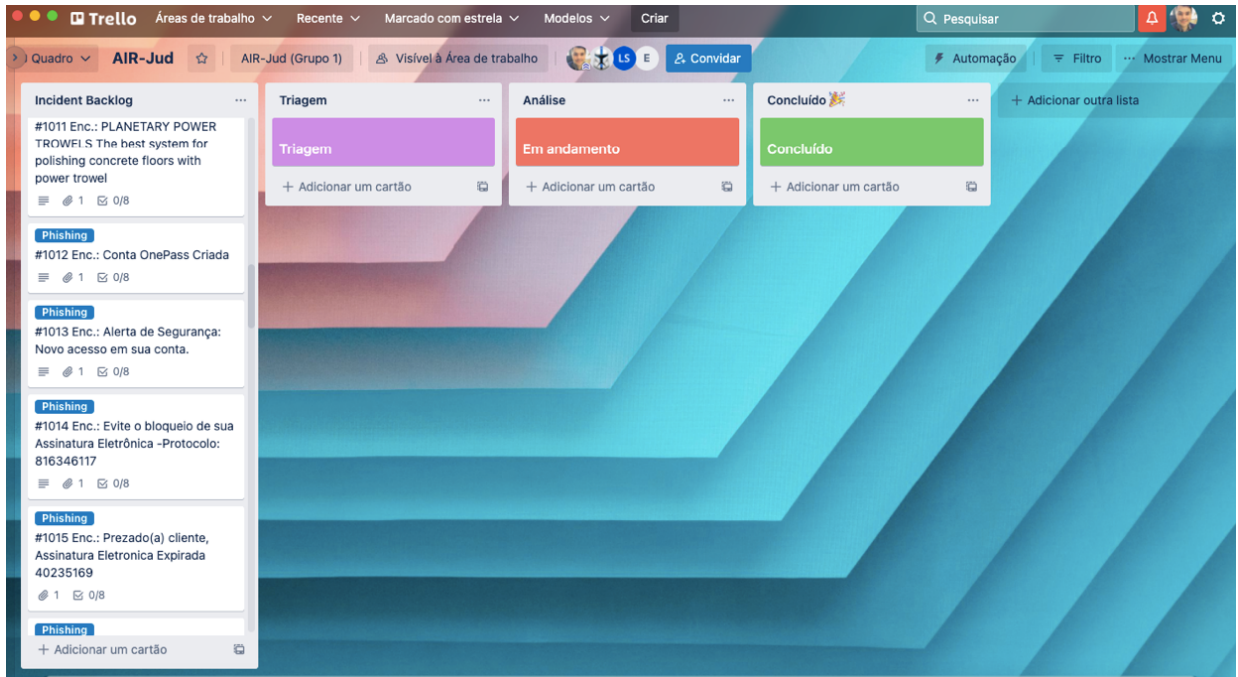
Foi utilizada a ferramenta *Trello* para gerenciar o quadro *Kanban* por sua familiaridade de uso entre os integrantes da equipe. O *Trello* é uma ferramenta flexível de gerenciamento de trabalho em equipes que permite idealizar planos, colaborar em projetos, organizar fluxos de trabalho e acompanhar o progresso de maneira visual. Os membros da equipe ingressaram por meio de convites de participação ao quadro e tiveram uma explicação sobre ele.

Cada notificação de *phishing* foi recebida como um incidente para ser analisado, passando previamente por uma triagem. Os incidentes foram inicialmente distribuídos no *Kanban board*, ilustrados na **Figura 19**. As fases das atividades foram classificadas como:

- i. *Incident Backlog*, por onde os incidentes foram primariamente alocados;
- ii. Triagem ou *Incident Sprint Backlog*, na qual os incidentes foram atribuídos a cada membro da equipe;
- iii. Análise, fase em que cada membro executa a devida análise em seu item atribuído;
- iv. Encerramento, para a realização de parte das tarefas; e
- v. Concluído, para depositar os casos já resolvidos.

Em sua versão inicial, ilustrada na **Figura 19**, não foi considerada a fase encerramento. Entretanto, ao longo do processo e das reuniões diárias, verificou-se a necessidade de criar mais essa fase que poderia ser atendida por um único membro da equipe. Assim, esse membro poderia ter a opção de realizar as atividades de encerramento de vários incidentes analisados por outro membro da equipe.

Figura 19 Quadro *Kanban* inicial com os incidentes a serem analisados



Fonte: Resultado da pesquisa

Cada quadro do *Kanban* representa um caso e foi estabelecido uma sequência de atividades para cada um deles, conforme ilustrado na **Figura 20**. As tarefas para este tipo de análise de suspeita de *phishing* podem ser descritas da seguinte maneira:

- i. Analisar o cabeçalho do e-mail suspeito;
- ii. Descobrir o nome e IP do servidor que originou o e-mail;
- iii. Descobrir a conta de contato (ABUSE) do servidor que originou o e-mail;
- iv. Pesquisar a reputação do servidor (IP) que originou o e-mail;
- v. Analisar links e arquivos anexados ao e-mail suspeito;
- vi. Notificar servidor que originou o e-mail;
- vii. Bloquear internamente o IP e/ou domínio que estiverem comprometidos;
- viii. Responder ao usuário que reportou o e-mail suspeito;

As tarefas de i a v são geralmente realizadas na fase de Análise, enquanto o restante, da vi a viii são tarefas da fase de Encerramento. Como os times *Scrum* são auto-organizáveis, eles podem decidir que as tarefas possam ser realizadas por um ou mais membro.

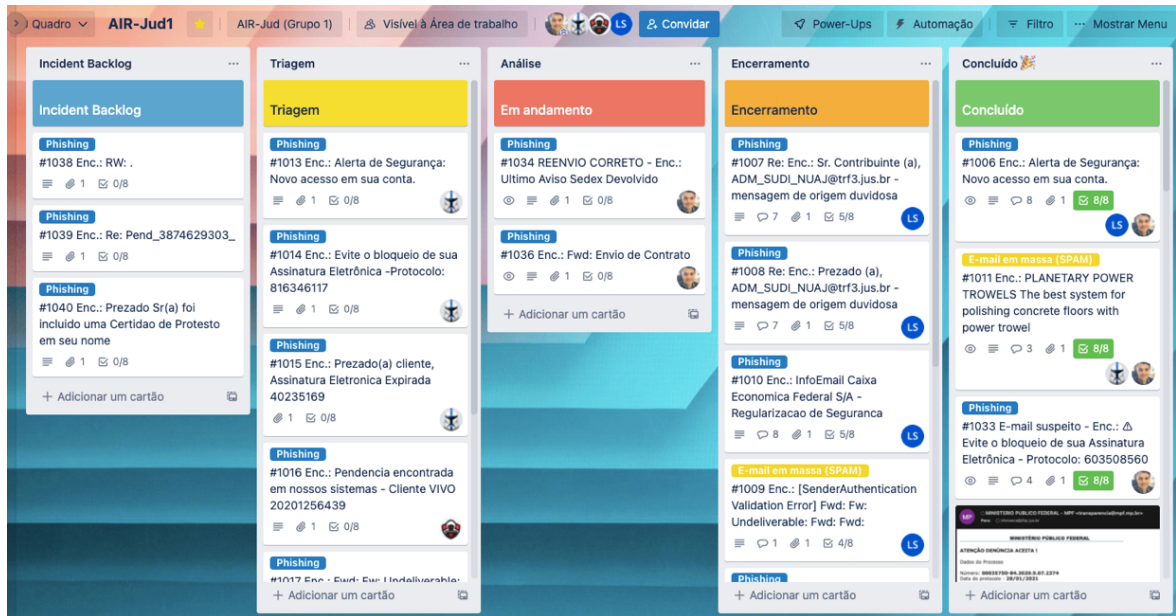
Figura 20 Exemplo de atividades constantes em cada item de *Incident Backlog*.



Fonte: Resultado da pesquisa

Considerando a capacidade de autoajustes e adaptações dos times *Scrum*, o quadro *Kanban* foi adaptado para acolher mais a fase Encerramento, posterior à fase Análise para que abarcasse as atividades finais dos incidentes. Assim, a **Figura 21** ilustra essas alterações.

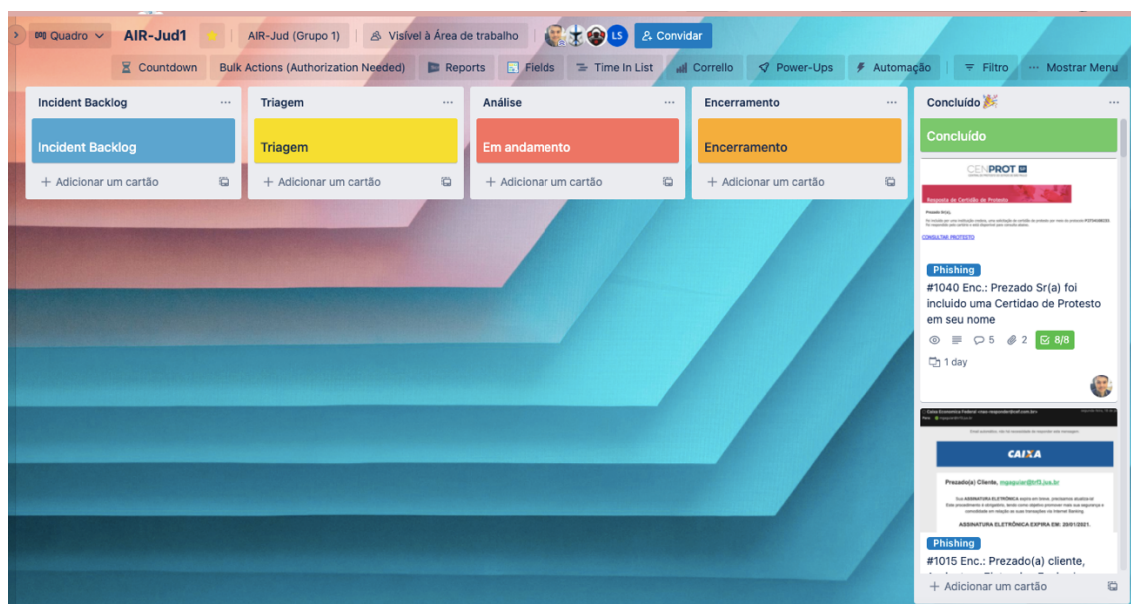
Figura 21 Quadro *Kanban* após autoajuste definido pelo time *Scrum*



Fonte: Resultado da pesquisa

No final da Sprint, os casos foram todos solucionados, deixando o quadro *Kanban* conforme **Figura 22**. O próximo passo é a revisão e retrospectiva do *Sprint* para obter melhorias para o planejar e execução do próximo *Sprint*, assim como prescreve o *Scrum* originalmente.

Figura 22 Resultado do quadro *Kanban* após o ciclo da *Sprint*



Fonte: Resultado da pesquisa

O experimento foi orientado conforme guia do Apêndice B e os resultados foram realizados por meio da avaliação proposta no Apêndice A, detalhadas na Etapa de avaliação a seguir.

3.3 Etapa de avaliação

A Seção 2.5 trouxe a descrição teórica da etapa de avaliação (etapa 5 do DSRM). Esta fase visa medir quão bem um artefato sustenta uma solução para o problema, comparando os objetivos com os resultados observados do uso dos artefatos na demonstração.

A partir da utilização dos princípios ágeis utilizados nos processos de resposta a incidentes de segurança da informação, o guia de avaliação do processo foi direcionado aos participantes:

- i. gestores de segurança da informação;
- ii. integrantes de times de resposta a incidentes de segurança da informação; e
- iii. pesquisadores de segurança da informação.

O método contempla ainda entrevistas semiestruturadas com respondentes dos questionários que assim aceitaram participações com as adequadas iterações, para avaliar se o processo possa ser, eventualmente refinado ou reconstruído. As questões da entrevista semiestruturada constam no Apêndice A.

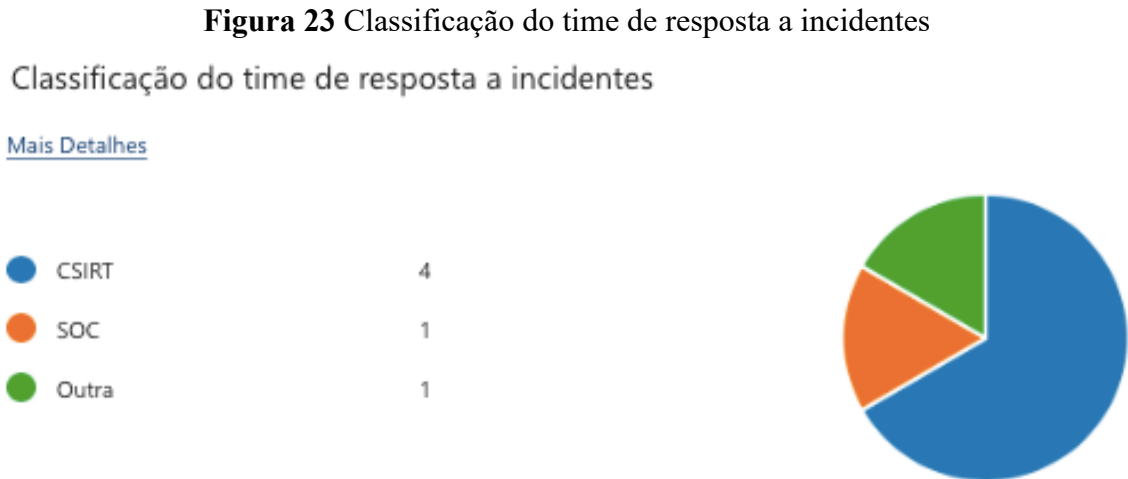
Um guia para a utilização do processo proposto foi desenvolvido para facilitar a replicação e aprendizado do experimento. O Apêndice B apresenta este guia.

Após a realização do experimento, os participantes responderam a entrevista semiestruturada para avaliar o artefato produzido. Os resultados individuais da entrevista semiestruturada de avaliação interna estão no Apêndice C e os de avaliação externa no Apêndice D.

Ressalta-se que os resultados da avaliação externa são iniciais, e pretende-se executar novas avaliações, tendo em vista o prazo para a apresentação desta dissertação.

Os três times de resposta a incidentes resultaram em cinco respostas da entrevista. O time do TRF3 contou com três respostas de avaliação interna, enquanto os outros dois de avaliação externa.

A classificação dos times de resposta a incidentes é ilustrada na **Figura 23**.



Fonte: Resultado da pesquisa

Todo os times utilizaram o tipo de incidente de *Phishing/Spear Phishing* no experimento. A média foi de 29 incidentes selecionados, com duração média de 16 dias. Quanto aos participantes, o número médio foi de três pessoas por time. A duração média da reunião diária (*Daily Scrum*) foi de aproximadamente meia hora por dia.

3.3.1 Avaliação interna

O **Quadro 11** apresenta o perfil da formação acadêmica e experiência profissional dos avaliadores internos.

Quadro 11 Perfil dos avaliadores internos

Avaliador	Formação	Experiência profissional na área e em CSIRTs
<i>Avaliador Interno 1</i>	Bacharel em Física; Mestre em Física Teórica; Pós-Graduado em Engenharia de Sistemas	Profissional de Tecnologia da Informação por 11 anos; Analista Judiciário da área de segurança da Equipe de Tratamento de Resposta a Incidentes de Segurança Cibernética há um ano.
<i>Avaliador Interno 2</i>	Tecnólogo em Processamento de Dados, e Pós-Graduado em Desenvolvimento de Sistemas e Segurança;	Profissional de Tecnologia da Informação como Técnico Judiciário, Especialidade Operação de Computadores por 28 anos; supervisor de Internet e Intranet por sete anos; Diretor da Divisão de Sistemas Web por seis anos e membro da Comissão Local de Resposta a Incidentes há três anos.
<i>Avaliador Interno 3</i>	Bacharel em Ciência da Computação e Pós-Graduado em Governança de TI; formação em <i>Fundamentals of Incident Handling</i> e <i>Advanced Topics of Incident Handling</i>	Profissional de Tecnologia da Informação por 22 anos; Analista Judiciário da área de redes e segurança há oito anos; membro da Comissão Local de Resposta a Incidentes há oito anos

Fonte: Resultado da Pesquisa

Sobre os papéis do *Incident Owner*, Equipe *Scrum* e *Scrum Master*, os resultados médios são apresentados na **Tabela 3**, em que as variações de respostas eram: 1 - Discordo plenamente; 2 - Discordo mais do que concordo; 3 - Não concordo, nem discordo; 4 - Concordo mais do que discordo; 5 - Concordo plenamente.

Tabela 3 Resultado das médias das avaliações INTERNAS dos papéis.

Papel	Avaliação média da relevância do papel no contexto da adaptação do processo de resposta a incidentes	Avaliação média da melhoria obtida pela inclusão do papel comparando ao método tradicional
<i>Incident Owner</i>	5,00	5,00
<i>SCRUM Master</i>	5,00	5,00
Membro da equipe	5,00	5,00

Fonte: Resultado da Pesquisa

Sobre os artefatos do *Incident Backlog*, *Incident Sprint Backlog* e quadro *Kanban Board*, os resultados médios são apresentados na **Tabela 4**, em que as variações de respostas eram: 1 - Discordo plenamente; 2 - Discordo mais do que concordo; 3 - Não concordo, nem discordo; 4 - Concordo mais do que discordo; 5 - Concordo plenamente.

Tabela 4 Resultado das médias das avaliações INTERNAS dos artefatos.

Artefato	Avaliação média da relevância do artefato no contexto da adaptação do processo de resposta a incidentes	Avaliação média da melhoria obtida pela inclusão do artefato comparando ao método tradicional
<i>Incident Backlog</i>	4,67	4,67
<i>Incident Sprint Backlog</i>	4,67	4,67
<i>Kanban Board</i>	5,00	5,00

Fonte: Resultado da Pesquisa

Sobre os eventos do Planejamento do *Sprint*, Reunião Diária, Revisão do *Sprint*, Retrospectiva do *Sprint* e ciclo *Sprint*, os resultados médios são apresentados na **Tabela 5**, em que as variações de respostas eram: 1 - Discordo plenamente; 2 - Discordo mais do que concordo; 3 - Não concordo, nem discordo; 4 - Concordo mais do que discordo; 5 - Concordo plenamente.

Tabela 5 Resultado das médias das avaliações INTERNAS dos eventos.

Eventos	Avaliação média da relevância do evento no contexto da adaptação do processo de resposta a incidentes	Avaliação média da melhoria obtida pela inclusão do evento comparando ao método tradicional
Planejamento do <i>Sprint</i>	5,00	4,67
Reunião Diária	5,00	5,00
Revisão do <i>Sprint</i>	5,00	4,67
Retrospectiva do <i>Sprint</i>	4,67	5,00
ciclo <i>Sprint</i>	4,67	4,67

Fonte: Resultado da Pesquisa

Os resultados das avaliações internas indicam que existe relevância e indicação de melhorias tendo em vista que as notas médias ficaram entre 4,67-5, ou seja, uma concordância com as afirmações indicadas na entrevista semiestruturada.

3.3.2 Avaliação externa

O **Quadro 12** apresenta o perfil da formação acadêmica e experiência profissional dos avaliadores internos.

Quadro 12 Perfil dos avaliadores externos

Avaliador	Formação	Experiência profissional na área e em CSIRTs
<i>Avaliador Interno 1</i>	Graduação em Tecnologia da Informação, Pós-graduação em <i>Data Science</i> , formação em <i>Fundamentals of Incident</i>	Consultor de Segurança da Informação por cinco anos; Engenheiro de segurança por quatro anos; Infosec Tech Manager há três anos;

Avaliador	Formação	Experiência profissional na área e em CSIRTs
	<i>Handling e Advanced Topics of Incident Handling</i>	
<i>Avaliador Interno 2</i>	Graduação em Administração de Empresas; Especialização em Análise de Sistemas, MBA Executive em Gestão Empresarial	Analista de Sistemas por dez anos e onze meses; analista de negócio e segurança por três anos e dois meses; analista de negócio em TI por um ano e nove meses; especialista em projetos por dois anos e três meses; <i>product owner</i> há três anos

Fonte: Resultado da Pesquisa

Sobre os papéis do *Incident Owner*, Equipe *Scrum* e *Scrum Master*, os resultados médios são apresentados na **Tabela 6**, em que as variações de respostas eram: 1 - Discordo plenamente; 2 - Discordo mais do que concordo; 3 - Não concordo, nem discordo; 4 - Concordo mais do que discordo; 5 - Concordo plenamente.

Tabela 6 Resultado das médias das avaliações EXTERNAS dos papéis.

Papel	Avaliação média da relevância do papel no contexto da adaptação do processo de resposta a incidentes	Avaliação média da melhoria obtida pela inclusão do papel comparando ao método tradicional
<i>Incident Owner</i>	5,00	5,00
<i>SCRUM Master</i>	4,00	4,00
Membro da equipe	4,00	4,00

Fonte: Resultado da Pesquisa

Sobre os artefatos do *Incident Backlog*, *Incident Sprint Backlog* e quadro *Kanban Board*, os resultados médios são apresentados na **Tabela 7**, em que as variações de respostas eram: 1 - Discordo plenamente; 2 - Discordo mais do que concordo; 3 - Não concordo, nem discordo; 4 - Concordo mais do que discordo; 5 - Concordo plenamente.

Tabela 7 Resultado das médias das avaliações EXTERNAS dos artefatos.

Artefato	Avaliação média da relevância do artefato no contexto da adaptação do processo de resposta a incidentes	Avaliação média da melhoria obtida pela inclusão do artefato comparando ao método tradicional
<i>Incident Backlog</i>	5,00	4,50
<i>Incident Sprint Backlog</i>	4,00	4,00
<i>Kanban Board</i>	4,50	4,50

Fonte: Resultado da Pesquisa

Os eventos do Planejamento do *Sprint*, Reunião Diária, Revisão do *Sprint*, Retrospectiva do *Sprint* e ciclo *Sprint*, os resultados médios são apresentados na **Tabela 8**, em que as variações de respostas eram: 1 - Discordo plenamente; 2 - Discordo mais do que concordo; 3 - Não concordo, nem discordo; 4 - Concordo mais do que discordo; 5 - Concordo plenamente.

Tabela 8 Resultado das médias das avaliações EXTERNAS dos eventos.

Eventos	Avaliação média da relevância do evento no contexto da adaptação do processo de resposta a incidentes	Avaliação média da melhoria obtida pela inclusão do evento comparando ao método tradicional
Planejamento do <i>Sprint</i>	5,00	5,00
Reunião Diária	5,00	5,00
Revisão do <i>Sprint</i>	4,00	4,00
Retrospectiva do <i>Sprint</i>	5,00	5,00
ciclo <i>Sprint</i>	4,50	5,00

Fonte: Resultado da Pesquisa

Os resultados das avaliações externas também indicam que existe relevância e contém melhorias tendo em vista que as notas médias ficaram entre 4-5, ou seja, uma concordância com as afirmações indicadas na entrevista semiestruturada.

Tendo em vista o prazo para a apresentação da dissertação, os resultados ficaram limitados em número de participantes. Entretanto, considerando os indicadores que apresentam a possibilidade de melhorias nos processos, o objetivo é chegar a sete avaliadores externos.

3.4 Comunicação

A Seção 2.6 traz a descrição das atividades da etapa 6 conforme a metodologia DSRM.

Com a conclusão e formalização desta dissertação, com as aprovações e formalização do Programa de Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos, sob a coordenação do Professor Doutor Napoleão Verardi Galegale, do Centro Estadual de Educação Tecnológica Paula Souza, o pesquisador desenvolverá o processo de comunicação dos resultados submetidos para publicações de pesquisas acadêmicas, para que pesquisadores e profissionais envolvidos no contexto deste estudo, conheçam a importância do problema, a utilidade e novidade do artefato, do que se propõe a resolver do problema, o rigor de seu *design* e sua eficácia em equipes de resposta a incidentes de segurança da informação, e que possa proporcionar contribuições para futuras iterações de pesquisas.

O Apêndice E contém o Relatório Técnico Conclusivo desta produção intelectual atendendo decisão do Colegiado do PPG do Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos.

4 CONSIDERAÇÕES FINAIS

Esta pesquisa começa com a seguinte questão que é “*Como os princípios ágeis podem ser aplicados nos processos de resposta a incidentes de segurança da informação no Poder Judiciário?*”. Assim, foi realizada uma pesquisa bibliométrica seguida por uma revisão da literatura que procurou apresentar os achados sobre o tema nas bases de dados científicas. Além disso, a adaptação e avaliação do processo proposto foi realizada.

Em sua fundamentação teórica foi apresentado o escopo sobre o tema investigado, incluindo a justificativa da pesquisa indicada com a informatização do Poder Judiciário brasileiro, a importância dos times de resposta a incidentes de segurança da informação e as práticas ágeis utilizadas no contexto da resposta a ciberincidentes.

Para a realização desta pesquisa seguiu-se a metodologia do DSRM, que compreende seis fases de desenvolvimento, os quais foram discutidos no Capítulo 2, na teoria, e no Capítulo 3, na prática.

O objetivo principal foi atingido tendo em vista que este trabalho examinou como adaptar e avaliar um processo baseado na aplicação dos princípios ágeis nos processos de tratamento e resposta de incidentes de segurança da informação no Poder Judiciário.

Os objetivos específicos foram alcançados, conforme lista abaixo:

- i. O problema e motivação foram identificados por meio do levantamento bibliométrico e revisão da literatura recente e da identificação dos problemas e questões em processos de resposta a incidentes e da aderência à questão da pesquisa, conforme apresentado nas Seções 1.1 a 1.4.;
- ii. Os objetivos da solução para melhoria nos processos de um CSIRT do Poder Judiciário foram definidos, conforme apresentado na introdução do trabalho e nas Seções 1.1 a 1.4;
- iii. A adaptação dos processos de um CSIRT do Poder Judiciário foi projetada e desenvolvida por meio da identificação dos princípios e práticas do método ágil, por intermédio do processo AIR-Jud;

- iv. A utilização de práticas ágeis nos processos de resposta a incidentes de segurança de informação em uma instituição do Poder Judiciário foi demonstrada, por meio da aplicação do processo AIR-Jud no CSIRT do TRF3;
- v. O processo foi avaliado com os atores envolvidos, por intermédio de entrevistas semiestruturadas com avaliadores internos e externos;
- vi. Os resultados da pesquisa foram comunicados por meio desta dissertação, do relatório técnico e do futuro artigo a ser produzido;

Para demonstrar que a solução pode ser usada para atingir os objetivos propostos, a abordagem foi aplicada em um projeto real de resposta a incidentes. Conforme observado no Capítulo 3, um ciclo de utilização dos princípios ágeis na resposta a incidentes de segurança do Poder Judiciário trouxe alguns benefícios, como o aprimoramento dos processos de resposta a incidentes e a melhor integração da equipe.

Para avaliação da metodologia, foram realizadas entrevistas com especialistas em segurança da informação que avaliaram a viabilidade da solução, bem como a existência de melhorias em relação aos processos tradicionais de resposta a incidentes.

Os resultados da avaliação do processo proposto foram realizados após a realização do experimento com um pequeno grupo de incidentes em um período curto. As avaliações apresentaram a existência de relevância e a indicação de melhorias nos processos, considerando que as notas médias ficaram entre 4-5, ou seja, uma concordância com as afirmações indicadas na entrevista semiestruturada.

As limitações encontradas na realização da pesquisa devem ser consideradas tendo em vista a pandemia de COVID-19 que inicialmente paralisou atividades e limitou os acessos à recursos, pessoas, serviços, entre outros. Além disso, o processo adaptado proposto para atender os setores de segurança da informação do poder judiciário somente pode ser testado no TRF3 e ainda com a limitação de ter os acessos indisponíveis devido ataque cibernético ocorrido durante o desenvolvimento do trabalho. Desse modo, novos testes do experimento poderiam ser realizados para a proposição de novas melhorias e aperfeiçoamento. Também poderiam ser testados em diversos tipos de incidentes, não apenas para os casos de *phishing* e *spear phishing*.

Como trabalhos futuros podem ser sugeridas a realização da aplicação da pesquisa em equipes de resposta a incidentes de segurança da informação de outras áreas como o setor bancário, universidades, comércio, energia, indústrias e demais setores produtivos.

REFERÊNCIAS

ABNT. **ABNT NBR ISO/IEC 27002**. [s.l: s.n.].

ABNT. **ABNT NBR ISO/IEC 27005**. [s.l: s.n.].

AGÊNCIA BRASIL. **Tribunal de Justiça gaúcho é alvo de ataque hacker**. Disponível em: <<https://agenciabrasil.ebc.com.br/justica/noticia/2020-11/tribunal-de-justica-gaucha-e-alvo-de-ataque-hacker>>. Acesso em: 4 mar. 2022a.

AGÊNCIA BRASIL. **Superior Tribunal de Justiça reinicia hoje sessões virtuais | Agência Brasil**. Disponível em: <<https://agenciabrasil.ebc.com.br/justica/noticia/2020-11/superior-tribunal-de-justica-reinicia-hoje-sessoes-virtuais>>.

AGÊNCIA BRASIL. **STJ é alvo de ataque hacker e Polícia Federal investiga o sistema**. Disponível em: <<https://agenciabrasil.ebc.com.br/justica/noticia/2020-11/stj-e-alvo-de-ataque-de-hacker-e-policia-federal-investiga-o-sistema>>. Acesso em: 5 mar. 2022c.

AHMAD, A.; HADGKISS, J.; RUIGHAVER, A. B. **Incident Response Teams-Challenges in Supporting the Organisational Security Function**. [s.l: s.n.].

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, 2012b.

ALCÁCER, V.; CRUZ-MACHADO, V. **Scanning the Industry 4.0: A Literature Review on Technologies for Manufacturing Systems**. *Engineering 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.

ANANTHARAMAN, N. **Agile Incident Management using Kanban Board for data Visualization**. [s.l.] SIMSR, 2018. Disponível em: <www.iosrjournals.org>.

AXELOS. **ITIL® Foundation ITIL**. Norwich: [s.n.].

BACA, D.; CARLSSON, B. **Agile Development with Security Engineering Activities**. [s.l.].

BAGUETE. **TRT4 sofre ataque hacker**. Disponível em: <<https://www.baguete.com.br/noticias/05/10/2021/trt4-sofre-ataque-hacker>>. Acesso em: 4 mar. 2022.

BECK, K.; BEEDLE, M.; VAN BENNEKUM, A.; COCKBURN, 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.

BEZNOSOV, K.; KRUCHTEN, P. Towards Agile Security Assurance. **Proceedings of the 2004 workshop on New security paradigms**, p. 47–54, 2004.

BRAS, J. C.; RIBEIRO, R. Business Continuity and Disaster Recovery: An Overview, Trends and Challenges. **13th CONTECSI**, p. 1698–1719, jun. 2016.

BRITISH STANDARDS INSTITUTE. **BS 25999-1: Code of Practice for Business Continuity Management**. London: [s.n.].

CERT.BR. **CSIRT FAQ**. Disponível em: <https://www.cert.br/certcc/csirts/csirt_faq-br.html>. Acesso em: 30 maio. 2022.

CERT.BR. **Tradução: CERT/CC CSIRT FAQ**. Disponível em: <https://www.cert.br/certcc/csirts/csirt_faq-br.html>. Acesso em: 26 fev. 2022a.

CERT.BR. **Estatísticas dos Incidentes Reportados ao CERT.br**. Disponível em: <<https://www.cert.br/stats/incidentes>>. Acesso em: 26 fev. 2022b.

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.

CNJ. **Juízo 100% Digital tudo o que você precisa saber**. Disponível em: <www.cnj.jus.br>.

CNJ. **Nova estratégia nacional atua contra-ataques cibernéticos no Judiciário**. Disponível em: <<https://www.cnj.jus.br/cnj-regulamenta-estrategia-nacional-contra-ataques-ciberneticos-ao-judiciario/>>. Acesso em: 9 mar. 2022b.

CNJ. **Justiça em Números 2021**. [s.l: s.n.]. Disponível em: <www.cnj.jus.br>.

CNJ. **Tecnologia 5G tornará mais robusta infraestrutura do Judiciário - Portal CNJ**. Disponível em: <<https://www.cnj.jus.br/tecnologia-5g-tornara-mais-robusta-infraestrutura-do-judiciario/>>. Acesso em: 9 mar. 2022d.

CNJ. **Exigência do uso de processo eletrônico deve acelerar extinção dos processos em papel**. Disponível em: <<https://www.cnj.jus.br/exigencia-do-uso-de-processo-eletronico-deve-acelerar-desaparecimento-dos-processos-em-papel/>>. Acesso em: 9 mar. 2022a.

CNJ. **Resultado do Questionário de TIC - Portal CNJ**. Disponível em: <<https://www.cnj.jus.br/tecnologia-da-informacao-e-comunicacao/com...comunicacao-do-poder-judiciario/resultado-do-questionario-de-tic/>>. Acesso em: 9 mar. 2022b.

COHEN, D.; LINDVALL, M.; COSTA, P. An Introduction to Agile Methods. **Advances in Computers**, v. 62, n. C, p. 1–66, 2004.

CONBOY, K.; FITZGERALD, B. Toward a Conceptual Framework of Agile Methods: A Study of Agility in Different Disciplines. **WISER**, 2004.

CONJUR. **TRF-3 recebe denúncia contra hacker que invadiu sistema do tribunal**. Disponível em: <<https://www.conjur.com.br/2021-jul-13/trf-recebe-denuncia-hacker-invadiu-sistema-tribunal>>. Acesso em: 4 mar. 2022a.

CONJUR. **TJ do Rio Grande do Sul volta a ser alvo de ataque hacker**. Disponível em: <<https://www.conjur.com.br/2021-abr-30/tj-rio-grande-sul-volta-alvo-ataque-hacker>>. Acesso em: 4 mar. 2022b.

CONJUR. **Após ataque hacker, sistemas do TRF-3 continuam fora do ar**. Disponível em: <<https://www.conjur.com.br/2022-abr-06/ataque-hacker-sistemas-trf-continuum-fora-ar>>. Acesso em: 30 maio. 2022.

COOPER, R. G.; SOMMER, A. F. Agile-Stage-Gate: New idea-to-launch method for manufactured new products is faster, more responsive. **Industrial Marketing Management**, v. 59, p. 167–180, 1 nov. 2016.

DE JESUS, I. R. D.; COSTA, H. G. A Nova Gestão Pública como indutora das atividades de Engenharia de Produção nos órgãos públicos. **Production**, v. 24, n. 4, p. 887–897, 2014.

DENNING, S. How To Make The Whole Organization Agile. **Forbes**, 2015.

DINGSØYR, T.; NERUR, S.; BALIJEPALLY, V.; MOE, N. B. A decade of agile methodologies: Towards explaining agile software development. **Journal of Systems and Software**, v. 85, n. 6, p. 1213–1221, 2012.

DOROFEE, A.; RUEFLE, R.; ZAJICEK, M.; MCINTERE, D.; ALBERTS, C.; CARLY, S. P.; HUTH, L.; WALTERS, P. **Incident Management Capability Assessment**. [s.l: s.n.]. Disponível em: <<http://www.sei.cmu.edu>>.

FOLHA. **Ataque hacker ao STJ não é sinal de ameaça à segurança das urnas - 15-11-2020 - Poder - Folha**. Disponível em: <<https://www1.folha.uol.com.br/poder/2020/11/ataque-hacker-ao-stj-nao-e-sinal-de-ameaca-a-seguranca-das-urnas.shtml>>. Acesso em: 4 mar. 2022.

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

G1. **Supremo investiga suposto ataque hacker a sistema da Corte | Política | G1**. Disponível em: <<https://g1.globo.com/politica/noticia/2021/05/07/supremo-investigatentativa-de-ataque-hacker-a-sistema-da-corte.ghtml>>. Acesso em: 5 mar. 2022.

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 Ciência da Informação**, v. 22, n. 3, p. 75–97, 1 jul. 2017.

GHANI, I.; AZHAM, Z.; JEONG, S. R. Integrating Software Security into Agile-Scrum Method. **KSII Transactions on Internet and Information Systems (TIIS)**, v. 8, n. 2, p. 646–663, 2014.

GRISPOS, G.; GLISSON, W. B.; STORER, T. Rethinking Security Incident Response: The Integration of Agile Principles. **20th Americas Conference on Information Systems (AMCIS 2014)**, 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)**, 2015a.

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

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

HE, Y.; ZAMANI, E. D.; LLOYD, S.; LUO, C. Agile incident response (AIR): Improving the incident response process in healthcare. **International Journal of Information Management**, v. 62, 1 fev. 2022.

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

HEINO, O.; TAKALA, A.; JUKARAINEN, P.; KALALAHTI, J.; KEKKI, T.; VERHO, P. Critical infrastructures: The operational environment in cases of severe disruption. **Sustainability (Switzerland)**, v. 11, n. 3, 6 fev. 2019.

HEVNER, A.; CHATTERJEE, S. **Design science research in information systems**. [s.l.] Springer, 2010. v. 22

HEVNER, A. R.; MARCH, S. T.; PARK, J.; RAM, S. **Design Science In Information Systems Research**. [s.l: s.n.].

HEVNER, A. R. A Three Cycle View of Design Science Research. **Scandinavian journal of information systems**, v. 19, n. 4, 2007.

IMONIANA, J. O. Validity of information security policy models. **Transinformação**, v. 16, n. 3, p. 263–274, 2004.

ISACA. **COBIT 5**. [s.l: s.n.].

KLIEM, R. L.; RICHIE, G. D. **Business Continuity Planning a Project Management Approach**. Boca Raton, FL: CRC Press, 2015.

LACERDA, D. P.; DRESCH, A.; PROENÇA, A.; VALLE, J. A.; JÚNIOR, A. Design Science Research: método de pesquisa para a engenharia de produção. **Gestão & Produção**, v. 20, n. 4, p. 741–761, 2013.

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.

MAJ, M.; REIJERS, R.; STIKVOORT, D. Good Practice Guide for Incident Management. **European Network and Information Security Agency (ENISA)**, 2010.

MARCH, S. T.; SMITH, G. F. **Design, and natural science research on information technology Decision Support Systems**. [s.l: s.n.].

MOHER D.; LIBERATI, A.; TETZLAFF, J.; ALTMAN, DG. T. Principais itens para relatar Revisões sistemáticas e Meta-análises: A recomendação PRISMA. **Epidemiologia e Serviços de Saúde**, v. 24, n. 2, p. 335–342, jun. 2015.

NASEER, A.; NASSER, H.; AHMAD, A.; MAYNARD, S. B.; SIDDIQUI, A. M. 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.

PEFFERS, K.; TUUNANEN, T.; ROTHENDERGER, M. A.; CHATTERJEE, S. A design science research methodology for information systems research. **Journal of Management Information Systems**, v. 24, n. 3, p. 45–77, dez. 2007.

PFLEEGER, S. L. **Improving Cybersecurity Incident Response Team (Csirt) Skills, Dynamics And Effectiveness**. Rome, NY: [s.n.]. Disponível em: <<http://www.dtic.mil>>.

POUPART, J.; NASSER, A. C. **A pesquisa qualitativa: enfoques epistemológicos e metodológicos**. [s.l.] Vozes, 2008.

REIS, L.; AMARAL, L. Gestão de Riscos num contexto de Planeamento da Contingência e Recuperação. **Atas da Conferência da Associação Portuguesa de Sistemas de Informação**, v. 3, n. 3, 2016.

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

ROMME, A. G. L. Making a Difference: Organization as Design. **Organization Science**, v. 14, n. 5, p. 558–573, 2003.

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.

SAMONAS, S.; COSS, D. The CIA strikes back: redefining confidentiality, integrity and availability in security. **Journal of Information System Security - JISSec**, v. 10, n. 3, p. 21–45, 2014.

SCHWABER, K.; SUTHERLAND, J. **The Scrum Guide™ the Definitive Guide to Scrum: The Rules of the Game**. [s.l.: s.n.].

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

SIMON, H. A. **The Sciences of the Artificial, reissue of the third edition with a new introduction by John Laird**. [s.l.] MIT Press, 2019.

SMITH, R.; JANICK, 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.

SNEDAKER, S. **Business Continuity and Disaster Recovery Planning for IT Professionals**. 2. ed. [s.l.] Syngress, 2014.

SOUZA, J. G. S.; ARIMA, C. H.; DE OLIVEIRA, R. M. N.; AKABANE, G. K.; GALEGALE, N. V. Gestão de Riscos de Segurança da Informação numa Instituição Pública Federal: Um Estudo de Caso. **ENIAC Projetos**, v. 5, n. 2, 2016.

STEFANI, C. E.; FEITOSA, M. D. COLABORAÇÃO NO DESENVOLVIMENTO ÁGIL DE SOFTWARE: UM ESTUDO A PARTIR DA VISÃO DOS PARTICIPANTES DO PROCESSO PRODUTIVO. 2019.

STIKVOORT, D. SIM3: Security Incident Management Maturity Model. **Open CSIRT Foundation (OCF)**, 2015.

STJ. **Comunicado da Presidência do STJ**. Disponível em:

<<https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/11112020-Comunicado-da-Presidencia-do-STJ.aspx>>. Acesso em: 4 mar. 2022.

SUTHERLAND, J.; SUTHERLAND, J. **Scrum - A arte de fazer o dobro do trabalho na metade do tempo**. Rio de Janeiro: Sextante, 2019.

SYMANTEC. **ISTR Internet Security Threat Report Volume 24**. [s.l.: s.n.]. Disponível em: <<https://docs.broadcom.com/docs/istr-24-2019-en>>. Acesso em: 26 fev. 2022.

TASHI, I.; GHERNAOUTI-HÉLIE, S. **Information Security Evaluation a Holistic Approach**. Boca Raton, FL: EPFL Press, 2011.

TERRA. **Depois de STJ, TJRS é alvo de ataque hacker**. Disponível em:

<<https://www.terra.com.br/noticias/brasil/politica/depois-de-stj-t>>.

TORRACO, R. J. Writing Integrative Literature Reviews: Guidelines and Examples. **Human Resource Development Review**, v. 4, n. 3, p. 356–367, 2005.

TRF3. **Tribunal Regional Federal da 3a Região**. Disponível em:

<<https://www.trf3.jus.br/index.html>>.

UOL. **Fachin: Justiça Eleitoral pode estar sob ataque hacker, inclusive da Rússia**.

Disponível em: <<https://www.uol.com.br/eleicoes/2022/02/16/entrevista-edson-fachin-stf-tse-eleicoes.htm>>. Acesso em: 2 mar. 2022.

VAN AKEN, J. E. Management research as a design science: Articulating the research products of mode 2 knowledge production in management. **British Journal of Management**, v. 16, n. 1, p. 19–36, mar. 2005.

VIEGA, J.; MCGRAW, G. **Building secure software: how to avoid security problems the right way**. [s.l.] Addison-Wesley, 2008.

WEST-BROWN, M. J.; STIKVOORT, D.; KOSSAKOWSKI, K-P.; KILLCRECE, G.; RUEFLE, R.; ZAJICEK, M. **Handbook for Computer Security Incident Response Teams (CSIRTs)**. [s.l.: s.n.].

APÊNDICE A – ROTEIRO DE AVALIAÇÃO INTERNA E EXTERNA DO PROCESSO

1. Dados profissionais

1.1. Nome e Local do CSIRT: _____

1.2. Nome do contato: _____

1.3. E-mail: _____

1.4. Telefone com DDD: _____

1.5. Formação: _____

1.6. Experiência: _____

2. Dados do experimento

2.1. Quais os tipos de incidentes escolhidos para o experimento? (*Phishing, Spear Phishing, DoS, DDoS, Malware, Forensic, etc.*): _____

2.2. Quantos incidentes foram selecionados para o experimento?

2.3. Qual a duração da Sprint para o experimento?

2.4. Quantas pessoas e quais papéis foram utilizados para o experimento?

2.5. Qual a duração e periodicidade da Reunião do Scrum do experimento?

3. Sobre o papel do *Incident Owner*:

3.1. Considero relevante o papel do *Incident Owner* (membro da equipe que é responsável pelo incidente) no contexto da adaptação do processo de resposta a incidentes.

1 Discordo plenamente	2 Discordo mais do que concordo	3 Não concordo, nem discordo	4 Concordo mais do que discordo	5 Concordo plenamente
-----------------------	---------------------------------	------------------------------	---------------------------------	-----------------------

3.2. A inclusão do papel do Incident Owner representa uma maneira melhor de responder um incidente comparando ao método tradicional.

1 Discordo plenamente	2 Discordo mais do que concordo	3 Não concordo, nem discordo	4 Concordo mais do que discordo	5 Concordo plenamente
-----------------------	---------------------------------	------------------------------	---------------------------------	-----------------------

4. Sobre o papel da Equipe Scrum

4.1. Considero relevante o papel da Equipe Scrum (membro da equipe que realizam o tratamento e análise do incidente) no contexto da adaptação do processo de resposta a incidentes.

1 Discordo plenamente	2 Discordo mais do que concordo	3 Não concordo, nem discordo	4 Concordo mais do que discordo	5 Concordo plenamente
-----------------------	---------------------------------	------------------------------	---------------------------------	-----------------------

4.2. A inclusão do papel da Equipe Scrum representa uma maneira melhor de responder um incidente comparando ao método tradicional.

1 Discordo plenamente	2 Discordo mais do que concordo	3 Não concordo, nem discordo	4 Concordo mais do que discordo	5 Concordo plenamente
-----------------------	---------------------------------	------------------------------	---------------------------------	-----------------------

5. Sobre o papel do Scrum Master

5.1. Considero relevante o papel do Scrum Master (membro da equipe que treinará o resto da equipe na estrutura do Scrum e ajudará os integrantes a eliminarem os obstáculos que

diminuam o desempenho do tratamento do incidente) no contexto da adaptação do processo de resposta a incidentes.

1 Discordo plenamente	2 Discordo mais do que concordo	3 Não concordo, nem discordo	4 Concordo mais do que discordo	5 Concordo plenamente
-----------------------	---------------------------------	------------------------------	---------------------------------	-----------------------

5.2. A inclusão do papel do Scrum Master representa uma maneira melhor de responder um incidente comparando ao método tradicional.

1 Discordo plenamente	2 Discordo mais do que concordo	3 Não concordo, nem discordo	4 Concordo mais do que discordo	5 Concordo plenamente
-----------------------	---------------------------------	------------------------------	---------------------------------	-----------------------

6. Sobre o artefato Incident Backlog

6.1. Considero relevante o artefato Incident Backlog (lista ordenada de incidentes, incluindo todos os aspectos de identificação, proteção, detecção, resposta e recuperação) no contexto da adaptação do processo de resposta a incidentes.

1 Discordo plenamente	2 Discordo mais do que concordo	3 Não concordo, nem discordo	4 Concordo mais do que discordo	5 Concordo plenamente
-----------------------	---------------------------------	------------------------------	---------------------------------	-----------------------

6.2. A inclusão do artefato Incident Backlog representa uma maneira melhor de responder um incidente comparando ao método tradicional.

1 Discordo plenamente	2 Discordo mais do que concordo	3 Não concordo, nem discordo	4 Concordo mais do que discordo	5 Concordo plenamente
-----------------------	---------------------------------	------------------------------	---------------------------------	-----------------------

7. Sobre o artefato Incident Sprint Backlog

7.1. Considero relevante o artefato Incident Sprint Backlog (lista ordenada de incidentes derivada do Incident Backlog, que contém o(s) membro(s) responsável, tarefas e demais detalhes do incidente) no contexto da adaptação do processo de resposta a incidentes.

1 Discordo plenamente	2 Discordo mais do que concordo	3 Não concordo, nem discordo	4 Concordo mais do que discordo	5 Concordo plenamente
-----------------------	---------------------------------	------------------------------	---------------------------------	-----------------------

7.2. A inclusão do artefato Incident Sprint Backlog representa uma maneira melhor de responder um incidente comparando ao método tradicional.

1 Discordo plenamente	2 Discordo mais do que concordo	3 Não concordo, nem discordo	4 Concordo mais do que discordo	5 Concordo plenamente
-----------------------	---------------------------------	------------------------------	---------------------------------	-----------------------

8. Sobre o quadro Kanban Board

8.1. Considero relevante o quadro Kanban (instrumento para tornar o trabalho visível e transparente) no contexto da adaptação do processo de resposta a incidentes.

1 Discordo plenamente	2 Discordo mais do que concordo	3 Não concordo, nem discordo	4 Concordo mais do que discordo	5 Concordo plenamente
-----------------------	---------------------------------	------------------------------	---------------------------------	-----------------------

8.2. A inclusão do quadro Kanban representa uma maneira melhor de responder um incidente comparando ao método tradicional.

1 Discordo plenamente	2 Discordo mais do que concordo	3 Não concordo, nem discordo	4 Concordo mais do que discordo	5 Concordo plenamente
-----------------------	---------------------------------	------------------------------	---------------------------------	-----------------------

9. Sobre o evento de Planejamento do Sprint

9.1. Considero relevante o evento de Planejamento do Sprint (primeira reunião do time Scrum em que o Sprint é planejado e o Incident Sprint Backlog é criado) no contexto da adaptação do processo de resposta a incidentes.

1 Discordo plenamente	2 Discordo mais do que concordo	3 Não concordo, nem discordo	4 Concordo mais do que discordo	5 Concordo plenamente
-----------------------	---------------------------------	------------------------------	---------------------------------	-----------------------

9.2. A inclusão do evento de Planejamento do Sprint representa uma maneira melhor de responder um incidente comparando ao método tradicional.

1 Discordo plenamente	2 Discordo mais do que concordo	3 Não concordo, nem discordo	4 Concordo mais do que discordo	5 Concordo plenamente
-----------------------	---------------------------------	------------------------------	---------------------------------	-----------------------

10. Sobre o evento de Reunião Diária (Daily Scrum)

10.1. Considero relevante o evento de Reunião Diária (rápida reunião periódica, sempre no mesmo horário e local, em que a equipe e o Scrum Master se encontram) no contexto da adaptação do processo de resposta a incidentes.

1 Discordo plenamente	2 Discordo mais do que concordo	3 Não concordo, nem discordo	4 Concordo mais do que discordo	5 Concordo plenamente
-----------------------	---------------------------------	------------------------------	---------------------------------	-----------------------

10.2. A inclusão do evento de Reunião Diária representa uma maneira melhor de responder um incidente comparando ao método tradicional.

1 Discordo plenamente	2 Discordo mais do que concordo	3 Não concordo, nem discordo	4 Concordo mais do que discordo	5 Concordo plenamente
-----------------------	---------------------------------	------------------------------	---------------------------------	-----------------------

11. Sobre o evento de Revisão do Sprint (Sprint Review)

11.1. Considero relevante o evento de Revisão do Sprint (reunião em que a equipe mostra o que realizou durante o Sprint) no contexto da adaptação do processo de resposta a incidentes.

1 Discordo plenamente	2 Discordo mais do que concordo	3 Não concordo, nem discordo	4 Concordo mais do que discordo	5 Concordo plenamente
-----------------------	---------------------------------	------------------------------	---------------------------------	-----------------------

11.2. A inclusão do evento de Revisão do Sprint representa uma maneira melhor de responder um incidente comparando ao método tradicional.

1 Discordo plenamente	2 Discordo mais do que concordo	3 Não concordo, nem discordo	4 Concordo mais do que discordo	5 Concordo plenamente
-----------------------	---------------------------------	------------------------------	---------------------------------	-----------------------

12. Sobre o evento de Retrospectiva do Sprint (Sprint Retrospective)

12.1. Considero relevante o evento de Retrospectiva do Sprint (reunião em que a equipe discute o que deu certo e o que poderia ser melhorado para o próximo Sprint) no contexto da adaptação do processo de resposta a incidentes.

1 Discordo plenamente	2 Discordo mais do que concordo	3 Não concordo, nem discordo	4 Concordo mais do que discordo	5 Concordo plenamente
-----------------------	---------------------------------	------------------------------	---------------------------------	-----------------------

12.2. A inclusão do evento de Retrospectiva do Sprint representa uma maneira melhor de responder um incidente comparando ao método tradicional.

1 Discordo plenamente	2 Discordo mais do que concordo	3 Não concordo, nem discordo	4 Concordo mais do que discordo	5 Concordo plenamente
-----------------------	---------------------------------	------------------------------	---------------------------------	-----------------------

13. Sobre o ciclo Sprint

13.1. Considero relevante o ciclo Sprint (todo o processo, desde o planejamento do Sprint até a retrospectiva) no contexto da adaptação do processo de resposta a incidentes.

1 Discordo plenamente	2 Discordo mais do que concordo	3 Não concordo, nem discordo	4 Concordo mais do que discordo	5 Concordo plenamente
-----------------------	---------------------------------	------------------------------	---------------------------------	-----------------------

13.2. A inclusão do ciclo Sprint representa uma maneira melhor de responder um incidente comparando ao método tradicional.

1 Discordo plenamente	2 Discordo mais do que concordo	3 Não concordo, nem discordo	4 Concordo mais do que discordo	5 Concordo plenamente
-----------------------	---------------------------------	------------------------------	---------------------------------	-----------------------

APÊNDICE B – GUIA PARA UTILIZAÇÃO DO PROCESSO

Vol 1 | Versão 0.1
Maio/2022

Práticas Ágeis na Resposta a Incidentes de Segurança da Informação

Objetivo

Você está sendo convidado a participar da pesquisa “Práticas Ágeis na Resposta a Incidentes de Segurança da Informação”. Sua contribuição muito enriquecerá nosso trabalho, pois participando desta pesquisa, você nos trará uma visão específica pautada na sua experiência sobre o assunto.

O presente guia apresenta resumidamente o método AIR – *Agile Incident Response* e como aplicá-lo. Os passos a serem adotados são:

O modelo apresentado se encaixa no ciclo de vida de gerenciamento de incidente nas fases de triagem, análise, resposta e recuperação.



Grupo de Incidentes

Backlog de incidentes

Definir o escopo de incidentes escolhendo um grupo de incidentes semelhantes e de baixa a média complexidade. Esta fase pode ser executada após ou durante a fase de triagem.

De 10 a 40 incidentes de resolução rápida adequados para o tempo de duração do *Sprint*.



Duração do Sprint

Definição do tempo de duração

Para o teste, utilizar a duração de 5 dias.

Duração estabelecida: _____

Time e Papéis



Incident Owner

Incident Owner

Essa função geralmente é desempenhada por um gerente de resposta a incidentes experiente ou líder técnico. Possui a visão/estratégia do incidente. Atua como ponto de contato com a alta administração e em nome do cliente (quando diferente de organização). Controla e prioriza o *Backlog de Incidentes*.



SCRUM Master

Scrum Master

O *Scrum Master* é responsável por promover e apoiar o *Scrum* entre membros e não membros da equipe. É um líder servidor da equipe de Resposta a Incidentes, ajudando a remover obstáculos, melhorar a resposta a incidentes e o desempenho da equipe para maximizar o valor.



Membros do Time

Membros do Time

Profissionais que fazem o trabalho de dar a resposta para minimizar e mitigar o impacto de um incidente. Eles são estruturados e capacitados pela organização para organizar e gerenciar seu próprio trabalho. São auto organizados, *cross functional*, sem títulos e responsáveis como um todo.

Sugere-se que a equipe tenha de 3 a 7 membros.

Reunião de Planejamento do Sprint

Incident Sprint Backlog

Reunião em que as partes interessadas e os membros da equipe definem com eficiência e eficácia o trabalho a ser executado na iteração atual. A reunião tem dois objetivos: (1) o que pode ser entregue na atualização resultante do próximo *Sprint*? (2) como o trabalho necessário para entregar o Incremento será realizado? Os itens *Incident Backlog* a serem trabalhados durante o *Sprint* serão identificados criando um *Sprint Backlog*, com os membros da equipe assumindo a propriedade das tarefas.

A figura abaixo ilustra o processo ágil *Scrum* adaptado ao contexto de resposta a incidentes. É possível observar que vários “blocos” de *Incident Backlog* originam os *Sprint Backlogs*. Durante o *Sprint* de duração variável, as *Daily Scrum* podem ser menores que 24h, dependendo do caso. O *Sprint Review* incorpora a função de Retrospectiva do *Sprint*.

Adaptando os conceitos do *Scrum*, o modelo de resposta a incidentes ágil pode incorporar os elementos de um *Sprint*. Os *Sprints* são processos cíclicos que se iniciam com o *Incident Backlog* que é então dissecado para criar um *Sprint Backlog*. Isso é então usado como entrada para as *Daily Scrums* até o final do *Sprint*, quando as revisões e retrospectivas ocorrem. Quaisquer lições aprendidas alimentam as ações no próximo *Sprint*.

O modelo Scrum é adaptado para incorporar elementos da resposta a incidentes de segurança da informação



Nesta etapa, os incidentes do Incident Backlog são atribuídos aos membros do time e movidos para a fila *Incident Sprint Backlog*.



Adaptando os conceitos do *Scrum*, o modelo de resposta a incidentes ágil pode incorporar os elementos de um *Sprint*. Os *Sprints* são processos cíclicos que se iniciam com o *Incident Backlog* que é então dissecado para criar um *Sprint Backlog*. Isso é então usado como entrada para as *Daily Scrums* até o final do *Sprint*, quando as revisões e retrospectivas ocorrem. Quaisquer lições aprendidas alimentam as ações no próximo *Sprint*.

Fluxo de Trabalho

Reuniões *Scrums*

Os métodos e playbooks utilizados para a resolução de incidentes são realizados nesta etapa.

É o trabalho de triagem, análise, mitigação e resposta aos incidentes realizado pelo *Scrum Team* por meio dos *playbooks* de resposta a ciberincidentes e demais técnicas. O fluxo de trabalho é organizado e gerenciado pela própria equipe.



Reunião Diária (*Daily Scrum*)

Reuniões *Scrums*

A frequência ideal para Reuniões *Scrum* é altamente dependente do contexto, exigindo um equilíbrio entre atualizar o conhecimento da equipe e interromper o trabalho no meio da tarefa. Recomenda-se que ocorram uma ou duas vezes ao dia com o *Scrum Master*.



Revisão e Retrospectiva do *Sprint*

Revisão do *Sprint*

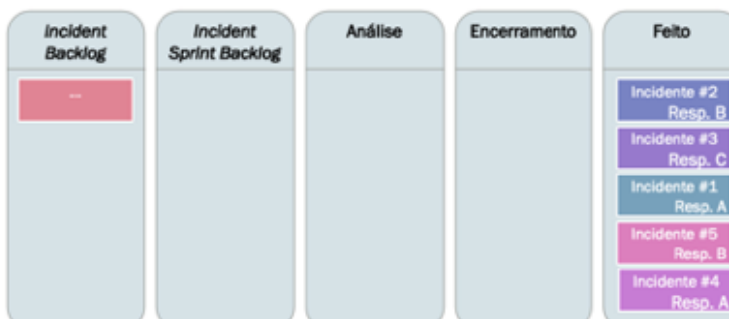
A Revisão do *Sprint* é uma oportunidade para inspecionar o progresso feito durante o *Sprint* atual e adaptar o *Backlog* de Incidente, se necessário. Os resultados da reunião incluirão:

- (1) Identificação do que deu certo e melhores práticas para levar adiante em *Sprints* subsequentes;
- (2) Identificação de eventuais bloqueios à investigação e potenciais estratégias de mitigação;
- (3) Informações estratégicas necessárias para a sessão de planejamento da *Sprint* subsequente.

Retrospectiva do *Sprint*

Reunião ao final do *Sprint*, onde o time faz uma ~~autoinspeção~~ e o trabalho realizado e cria um plano com melhorias para aplicar no próximo *sprint*. Ocorre após cada *Sprint Review* e antes de cada *Sprint Planning*. Os objetivos são:

- (1) Inspecionar como foi o *Sprint* anterior em relação a pessoas, relacionamentos, processos e ferramentas;
- (2) Identificar e ordenar os principais itens que correram bem e potenciais melhorias;
- (3) Criar um plano para implementação de melhorias nos processos operacionais da equipe *Scrum*



APÊNDICE C – RESPOSTAS INDIVIDUALIZADAS DO QUESTIONÁRIO DE AVALIAÇÃO INTERNA

Pergunta	Resp. 1	Resp. 2	Resp. 3
ID	2	4	5
Nome e Local do time de resposta a incidentes CSIRT	TRF3	TRF3	TRF3
Classificação do time de resposta a incidentes	CSIRT;	CLRI;	CSIRT;
Quais os tipos de incidentes escolhidos para o experimento?	Phishing / Spear Phishing	Phishing / Spear Phishing	Phishing / Spear Phishing
Quantos incidentes foram selecionados para o experimento?	40	40	40
Qual a duração do <i>Sprint</i> para o experimento?	4 semanas	Uma semana	4 semanas
Quantas pessoas e quais papéis foram utilizados para o experimento?	4 pessoas	3 pessoas	4 pessoas
Qual a duração e periodicidade da Reunião do <i>Scrum</i> do experimento?	Reuniões diárias de cerca de 30 minutos	A reunião semanal de 1 hora aproxim/	30 minutos e diária.
Sobre o papel do <i>Incident Owner</i> : Considero relevante o papel do <i>Incident Owner</i> (membro da equipe que é responsável pelo incidente) no contexto da adaptação do processo de resposta a incidentes.	5	5	5
Sobre o papel do <i>Incident Owner</i> : A inclusão do papel do <i>Incident Owner</i> representa uma maneira melhor de responder um incidente comparando ao método tradicional.	5	5	5
Sobre o papel da Equipe <i>Scrum</i> : Considero relevante o papel da Equipe <i>Scrum</i> (membro da equipe que realizam o tratamento e análise do incidente) no contexto da adaptação do processo de resposta a incidentes.	5	5	5
Sobre o papel da Equipe <i>Scrum</i> : A inclusão do papel da Equipe <i>Scrum</i> representa uma maneira melhor de responder um incidente comparando ao método tradicional.	5	5	5
Sobre o papel do <i>Scrum Master</i> : Considero relevante o papel do <i>Scrum Master</i> (membro da equipe que treinará o resto da equipe na estrutura do <i>Scrum</i> e ajudará os integrantes a eliminarem obstáculos que diminuam o desempenho do tratamento do incidente) no contexto da adaptação do processo de resposta a incidentes.	5	5	5
Sobre o papel do <i>Scrum Master</i> : A inclusão do papel do <i>Scrum Master</i> representa uma maneira melhor de responder um incidente comparando ao método tradicional.	5	5	5
Sobre o artefato <i>Incident Backlog</i> : Considero relevante o artefato <i>Incident Backlog</i> (lista ordenada de incidentes, incluindo todos os aspectos de identificação, proteção, detecção, resposta e recuperação) no contexto da adaptação do processo de resposta a incidentes.	5	5	4
Sobre o artefato <i>Incident Backlog</i> : A inclusão do artefato <i>Incident Backlog</i> representa uma maneira melhor de responder um incidente comparando ao método tradicional.	5	5	4
Sobre o artefato <i>Incident Sprint Backlog</i> : Considero relevante o artefato <i>Incident Sprint Backlog</i> (lista ordenada de incidentes derivada do <i>Incident Backlog</i> , que contém o(s) membro(s) responsável, tarefas	5	5	4

Pergunta	Resp. 1	Resp. 2	Resp. 3
e demais detalhes do incidente) no contexto da adaptação do processo de resposta a incidentes.			
Sobre o artefato <i>Incident Sprint Backlog</i> : A inclusão do artefato <i>Incident Sprint Backlog</i> representa uma maneira melhor de responder um incidente comparando ao método tradicional.	5	5	4
Sobre o quadro <i>Kanban Board</i> : Considero relevante o quadro <i>Kanban</i> (instrumento para tornar o trabalho visível e transparente) no contexto da adaptação do processo de resposta a incidentes.	5	5	5
Sobre o quadro <i>Kanban Board</i> : A inclusão do quadro <i>Kanban</i> representa uma maneira melhor de responder um incidente comparando ao método tradicional.	5	5	5
Sobre o evento de Planejamento do <i>Sprint</i> : Considero relevante o evento de Planejamento do <i>Sprint</i> (primeira reunião do time <i>Scrum</i> em que o <i>Sprint</i> é planejado e o <i>Incident Sprint Backlog</i> é criado) no contexto da adaptação do processo de resposta a incidentes.	5	5	5
Sobre o evento de Planejamento do <i>Sprint</i> : A inclusão do evento de Planejamento do <i>Sprint</i> representa uma maneira melhor de responder um incidente comparando ao método tradicional.	5	5	4
Sobre o evento de Reunião Diária (<i>Daily Scrum</i>): Considero relevante o evento de Reunião Diária (rápida reunião periódica, sempre no mesmo horário e local, em que a equipe e o <i>Scrum Master</i> se encontram) no contexto da adaptação do processo de resposta a incidentes.	5	5	5
Sobre o evento de Reunião Diária (<i>Daily Scrum</i>): A inclusão do evento de Reunião Diária representa uma maneira melhor de responder um incidente comparando ao método tradicional.	5	5	5
Sobre o evento de Revisão do <i>Sprint</i> (<i>Sprint Review</i>): Considero relevante o evento de Revisão do <i>Sprint</i> (reunião em que a equipe mostra o que realizou durante o <i>Sprint</i>) no contexto da adaptação do processo de resposta a incidentes.	5	5	5
Sobre o evento de Revisão do <i>Sprint</i> (<i>Sprint Review</i>): A inclusão do evento de Revisão do <i>Sprint</i> representa uma maneira melhor de responder um incidente comparando ao método tradicional.	5	5	4
Sobre o evento de Retrospectiva do <i>Sprint</i> (<i>Sprint Retrospective</i>): Considero relevante o evento de Retrospectiva do <i>Sprint</i> (reunião em que a equipe discute o que deu certo e o que poderia ser melhorado para o próximo <i>Sprint</i>) no contexto da adaptação do processo de resposta a incidentes.	5	5	4
Sobre o evento de Retrospectiva do <i>Sprint</i> (<i>Sprint Retrospective</i>): A inclusão do evento de Retrospectiva do <i>Sprint</i> representa uma maneira melhor de responder um incidente comparando ao método tradicional.	5	5	5
Sobre o ciclo <i>Sprint</i> : Considero relevante o ciclo <i>Sprint</i> (todo o processo, desde o planejamento do <i>Sprint</i> até a retrospectiva) no contexto da adaptação do processo de resposta a incidentes.	5	5	4
Sobre o ciclo <i>Sprint</i> : A inclusão do ciclo <i>Sprint</i> representa uma maneira melhor de responder um incidente comparando ao método tradicional.	5	5	4

APÊNDICE D – RESPOSTAS INDIVIDUALIZADAS DO QUESTIONÁRIO DE AVALIAÇÃO EXTERNA

Pergunta	Resp. 1	Resp. 2
ID	1	3
Nome e Local do time de resposta a incidentes CSIRT	Fintech	Atacado
Classificação do time de resposta a incidentes	CSIRT; SOC;	CSIRT;
Quais os tipos de incidentes escolhidos para o experimento?	Phishing / Spear Phishing	Phishing / Spear Phishing
Quantos incidentes foram selecionados para o experimento?	5	20
Qual a duração do <i>Sprint</i> para o experimento?	2 dias	15 dias
Quantas pessoas e quais papéis foram utilizados para o experimento?	3	2
Qual a duração e periodicidade da Reunião do <i>Scrum</i> do experimento?	30min	2 vezes/ semana
Sobre o papel do <i>Incident Owner</i> : Considero relevante o papel do <i>Incident Owner</i> (membro da equipe que é responsável pelo incidente) no contexto da adaptação do processo de resposta a incidentes.	5	5
Sobre o papel do <i>Incident Owner</i> : A inclusão do papel do <i>Incident Owner</i> representa uma maneira melhor de responder um incidente comparando ao método tradicional.	5	5
Sobre o papel da Equipe <i>Scrum</i> : Considero relevante o papel da Equipe <i>Scrum</i> (membro da equipe que realizam o tratamento e análise do incidente) no contexto da adaptação do processo de resposta a incidentes.	4	4
Sobre o papel da Equipe <i>Scrum</i> : A inclusão do papel da Equipe <i>Scrum</i> representa uma maneira melhor de responder um incidente comparando ao método tradicional.	4	4
Sobre o papel do <i>Scrum Master</i> : Considero relevante o papel do <i>Scrum Master</i> (membro da equipe que treinará o resto da equipe na estrutura do <i>Scrum</i> e ajudará os integrantes a eliminarem obstáculos que diminuam o desempenho do tratamento do incidente) no contexto da adaptação do processo de resposta a incidentes.	3	5
Sobre o papel do <i>Scrum Master</i> : A inclusão do papel do <i>Scrum Master</i> representa uma maneira melhor de responder um incidente comparando ao método tradicional.	3	5
Sobre o artefato <i>Incident Backlog</i> : Considero relevante o artefato <i>Incident Backlog</i> (lista ordenada de incidentes, incluindo todos os aspectos de identificação, proteção, detecção, resposta e recuperação) no contexto da adaptação do processo de resposta a incidentes.	5	5
Sobre o artefato <i>Incident Backlog</i> : A inclusão do artefato <i>Incident Backlog</i> representa uma maneira melhor de responder um incidente comparando ao método tradicional.	4	5
Sobre o artefato <i>Incident Sprint Backlog</i> : Considero relevante o artefato <i>Incident Sprint Backlog</i> (lista ordenada de incidentes derivada do <i>Incident Backlog</i> , que contém o(s) membro(s) responsável, tarefas e demais detalhes do incidente) no contexto da adaptação do processo de resposta a incidentes.	4	4
Sobre o artefato <i>Incident Sprint Backlog</i> : A inclusão do artefato <i>Incident Sprint Backlog</i> representa uma maneira melhor de responder um incidente comparando ao método tradicional.	4	4

Pergunta	Resp. 1	Resp. 2
Sobre o quadro <i>Kanban Board</i> : Considero relevante o quadro <i>Kanban</i> (instrumento para tornar o trabalho visível e transparente) no contexto da adaptação do processo de resposta a incidentes.	5	4
Sobre o quadro <i>Kanban Board</i> : A inclusão do quadro <i>Kanban</i> representa uma maneira melhor de responder um incidente comparando ao método tradicional.	5	4
Sobre o evento de Planejamento do <i>Sprint</i> : Considero relevante o evento de Planejamento do <i>Sprint</i> (primeira reunião do time <i>Scrum</i> em que o <i>Sprint</i> é planejado e o <i>Incident Sprint Backlog</i> é criado) no contexto da adaptação do processo de resposta a incidentes.	5	5
Sobre o evento de Planejamento do <i>Sprint</i> : A inclusão do evento de Planejamento do <i>Sprint</i> representa uma maneira melhor de responder um incidente comparando ao método tradicional.	5	5
Sobre o evento de Reunião Diária (<i>Daily Scrum</i>): Considero relevante o evento de Reunião Diária (rápida reunião periódica, sempre no mesmo horário e local, em que a equipe e o <i>Scrum Master</i> se encontram) no contexto da adaptação do processo de resposta a incidentes.	5	5
Sobre o evento de Reunião Diária (<i>Daily Scrum</i>): A inclusão do evento de Reunião Diária representa uma maneira melhor de responder um incidente comparando ao método tradicional.	5	5
Sobre o evento de Revisão do <i>Sprint</i> (<i>Sprint Review</i>): Considero relevante o evento de Revisão do <i>Sprint</i> (reunião em que a equipe mostra o que realizou durante o <i>Sprint</i>) no contexto da adaptação do processo de resposta a incidentes.	4	4
Sobre o evento de Revisão do <i>Sprint</i> (<i>Sprint Review</i>): A inclusão do evento de Revisão do <i>Sprint</i> representa uma maneira melhor de responder um incidente comparando ao método tradicional.	4	4
Sobre o evento de Retrospectiva do <i>Sprint</i> (<i>Sprint Retrospective</i>): Considero relevante o evento de Retrospectiva do <i>Sprint</i> (reunião em que a equipe discute o que deu certo e o que poderia ser melhorado para o próximo <i>Sprint</i>) no contexto da adaptação do processo de resposta a incidentes.	5	5
Sobre o evento de Retrospectiva do <i>Sprint</i> (<i>Sprint Retrospective</i>): A inclusão do evento de Retrospectiva do <i>Sprint</i> representa uma maneira melhor de responder um incidente comparando ao método tradicional.	5	5
Sobre o ciclo <i>Sprint</i> : Considero relevante o ciclo <i>Sprint</i> (todo o processo, desde o planejamento do <i>Sprint</i> até a retrospectiva) no contexto da adaptação do processo de resposta a incidentes.	5	4
Sobre o ciclo <i>Sprint</i> : A inclusão do ciclo <i>Sprint</i> representa uma maneira melhor de responder um incidente comparando ao método tradicional.	5	5

APÊNDICE E – RELATÓRIO TÉCNICO CONCLUSIVO

CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA
UNIDADE DE PÓS-GRADUAÇÃO, EXTENSÃO E PESQUISA
MESTRADO PROFISSIONAL EM GESTÃO E TECNOLOGIA EM SISTEMAS
PRODUTIVOS

LINHA DE PESQUISA: SISTEMAS DE INFORMAÇÃO E TECNOLOGIAS DIGITAIS
PROJETO DE PESQUISA: GESTÃO ESTRATÉGICA DA TECNOLOGIA DA
INFORMAÇÃO

RELATÓRIO TÉCNICO CONCLUSIVO: PRINCÍPIOS ÁGEIS NA RESPOSTA A
INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

RODRIGO SILVA SOTOLANI
NAPOLEÃO VERARDI GALEGALE

São Paulo
Junho/2022

- S718p Sotolani, Rodrigo Silva
Relatório técnico conclusivo: Princípios ágeis na resposta a incidentes de segurança da informação / Rodrigo Silva Sotolani. – São Paulo: CPS, 2022.
52 f. : il.
- Orientador: Prof. Dr. Napoleão Verardi Galegale
Relatório técnico conclusivo apresentado como produto da dissertação do Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos – Centro Estadual de Educação Tecnológica Paula Souza, 2022.
1. Segurança da informação. 2. Princípios ágeis. 3. Resposta a incidente. 4. Poder judiciário. 5. CSIRT. I. Galegale, Napoleão Verardi. II. Centro Estadual de Educação Tecnológica Paula Souza. III. Título.

RESUMO

SOTOLANI, R. S. **PRINCÍPIOS ÁGEIS NA RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO**. nn [52] f. Relatório Técnico Conclusivo (Mestrado Profissional em Gestão e Tecnologia nos Sistemas Produtivos). Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2022.

O objetivo deste trabalho é adaptar e avaliar um processo baseado na aplicação dos princípios ágeis para tratamento e resposta de incidentes de segurança da informação em uma instituição do Poder Judiciário. A pesquisa identificou na literatura, problemas nos processos tradicionais de resposta a incidentes. Foi identificada a existência de lacuna de pesquisa da aplicação de princípios ágeis nestes processos. A metodologia utilizada para conduzir o estudo foi a *Design Science Research Methodology* – DSRM que incorpora princípios, práticas e procedimentos necessários para o *design*, desenvolvimento, demonstração e avaliação do processo em questão. O processo de resposta a incidentes de segurança da informação foi adaptado para utilizar princípios ágeis e implementado com um experimento prático com um time de resposta a incidentes (CSIRT) do TRF3 e nomeado de AIR-Jud. Avaliações interna e externa foram obtidas por meio de entrevistas semiestruturadas com profissionais da área de segurança da informação. Como resultado, o processo AIR-Jud foi avaliado como relevante e considerado contendo melhorias em relação aos processos tradicionais de resposta a incidentes. Como implicação prática, o AIR-Jud pode ser utilizado por CSIRTs do Poder Judiciário que visem a melhoria de seus processos. Como implicações teóricas, o presente trabalho contribui para a literatura preenchendo parte da lacuna sobre este tema.

Palavras-chave: Segurança da Informação. Princípios Ágeis. Resposta a Incidente. Poder Judiciário. CSIRT. DSRM.

ABSTRACT

SOTOLANI, R. S. **Agile principles in security incident handling**. nn [52] f. Relatório Técnico Conclusivo (Mestrado Profissional em Gestão e Tecnologia nos Sistemas Produtivos). Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2022.

The objective of this work is to adapt and evaluate a process based on the use of agile principles for security incident handling in an institution of the Judiciary. The research identified problems in traditional incident response processes in the literature. The existence of a research gap in the application of agile principles in these processes was identified. The methodology used to conduct the study was the Design Science Research Methodology - DSRM, which incorporates principles, practices, and procedures necessary for the design, development, demonstration, and evaluation of the process in question. The information security incident response process was adapted to use agile principles and implemented with a practical experiment with a TRF3 incident response team (CSIRT) named AIR-Jud. Internal and external evaluations were obtained through semi-structured interviews with information security professionals. As a result, the AIR-Jud process was assessed as relevant and considered to contain improvements over traditional incident response processes. As a practical implication, AIR-Jud can be used by CSIRTs of the Judiciary that aim to improve their processes. As theoretical implications, the present work contributes to the literature filling part of the gap on this topic.

Keywords: Computer Security Information. Agile Principles. Incident Response. Judicial Power. CSIRT. DSRM.

LISTA DE QUADROS

Quadro 1 Resumo dos principais achados nas publicações selecionadas.....	124
Quadro 2 Papéis de uma equipe ágil de resposta a incidentes	137
Quadro 3 Os eventos do método <i>Scrum</i> adaptados para uma equipe de resposta a incidentes ágeis.....	138
Quadro 4 Artefatos do <i>Scrum</i> e <i>Kanban</i> adaptados ao contexto da resposta a incidentes de segurança cibernética	139
Quadro 5 Perfil dos avaliadores internos	146
Quadro 6 Perfil dos avaliadores externos	148

LISTA DE TABELAS

Tabela 1 Resultado das médias das avaliações INTERNAS dos papéis.....	147
Tabela 2 Resultado das médias das avaliações EXTERNAS dos papéis.....	148

LISTA DE FIGURAS

Figura 1 Fluxograma do Protocolo PRISMA-P	124
Figura 2 Ciclo de vida de resposta a incidente do NIST	128
Figura 3 Relação entre constructos, modelos, métodos e instanciação conforme o DSRM	132
Figura 4 Constructos da pesquisa.....	133
Figura 5 Modelo dos processos de tratamento de incidentes com métodos ágeis	133
Figura 6 O modelo de resposta a incidentes adaptado com o método <i>Scrum</i>	134
Figura 7 O método <i>Scrum</i> adaptado para o modelo de resposta a incidentes	136
Figura 8 Mapeamento das práticas ágeis no processo de resposta a incidentes.....	141
Figura 9 Quadro <i>Kanban</i> inicial com os incidentes a serem analisados	143
Figura 10 Exemplo de atividades constantes em cada item de <i>Incident Backlog</i>	144
Figura 11 Quadro <i>Kanban</i> após autoajuste definido pelo time <i>Scrum</i>	144
Figura 12 Resultado do quadro <i>Kanban</i> após o ciclo da <i>Sprint</i>	145

LISTA DE SIGLAS

AIR	<i>Agile Incident Response</i>
BCP	<i>Business Continuity Plan</i>
CERT	<i>Computer Emergency Response Team</i>
CJF	Conselho da Justiça Federal
CLRI	Comissão Local de Resposta a Incidente
CNJ	Conselho Nacional de Justiça
CSIRT	<i>Computer Security Incident Response Team</i>
DARPA	<i>US Defense Advanced Research Projects Agency</i>
DRP	<i>Disaster Recovery Plan</i>
DS	<i>Design Science</i>
DSRM	<i>Design Science Research Methodology</i>
ENISA	<i>European Network and Information Security Agency</i>
ENSEC-PJ	Estratégia Nacional de Segurança Cibernética e da Informação do Poder Judiciário
ETIR	Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética
IA	Inteligência Artificial
ICS	<i>Industry Control System</i>
IoT	<i>Internet of Things</i>
ISO	<i>International Organization for Standardization</i>
ITIL	<i>Information Technology Infrastructure Library</i>
NIST	<i>National Institute of Standards and Technology</i>
PJ	Poder Judiciário
RI	Resposta a Incidente
SI	Sistema de Informação
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
TI	Tecnologia da informação
TRF3	Tribunal Regional Federal d Terceira Região
VUCA	Acrônimo de volátil, incerto, complexo e ambíguo

SUMÁRIO

INTRODUÇÃO	118
1 FUNDAMENTOS TEÓRICOS UTILIZADOS NA PESQUISA.....	122
1.1 Revisão da literatura.....	123
1.2 A informatização do Poder Judiciário brasileiro	125
1.3 Continuidade do negócio e recuperação de desastres.....	127
1.4 Resposta a incidentes de segurança da informação	127
1.5 Princípios ágeis.....	129
<i>1.5.1 Princípios ágeis na resposta a incidentes de segurança da informação.....</i>	<i>129</i>
2 CAMINHO METODOLÓGICO	131
3 RESULTADOS (INOVAÇÃO/ INTERVENÇÃO/ RECOMENDAÇÕES)	132
3.1 Design e desenvolvimento	132
<i>3.1.1 As relações entre os artefatos constructo, modelo, método e instanciação</i>	<i>132</i>
<i>3.1.2 Processos adaptados do método Scrum</i>	<i>135</i>
<i>3.1.3 Papéis</i>	<i>136</i>
<i>3.1.4 Eventos.....</i>	<i>137</i>
<i>3.1.5 Artefatos do Scrum</i>	<i>138</i>
3.2 Demonstração	139
<i>3.2.1 O Tribunal Regional Federal da 3ª. Região</i>	<i>139</i>
<i>3.2.2 A Comissão Local de Resposta a Incidentes de Segurança da Informação.....</i>	<i>140</i>
<i>3.2.3 Detalhamento dos incidentes analisados no experimento.....</i>	<i>140</i>
<i>3.2.4 Demonstração do novo processo.....</i>	<i>142</i>
3.3 Etapa de avaliação	145
<i>3.3.1 Avaliação interna.....</i>	<i>146</i>
<i>3.3.2 Avaliação externa</i>	<i>147</i>
3.4 Comunicação	149
4 CONTRIBUIÇÕES PARA A ORGANIZAÇÃO E/OU SOCIEDADE.....	150
REFERÊNCIAS	152
ANEXO 1 – DETALHAMENTO DO PRODUTO (CAPES).....	158
ANEXO II – DECLARAÇÃO EMITIDA PELA EMPRESA/ORGANIZAÇÃO	
OBJETO DA PESQUISA.....	160

INTRODUÇÃO

Os avanços tecnológicos criam, transformam e tratam informações valiosas que precisam ser protegidas para o sucesso da organização e segurança dos sistemas. Neste ambiente complexo, heterogêneo e interconectado, é necessário observar as premissas da integridade, da confidencialidade e da disponibilidade (SAMONAS; COSS, 2014).

No setor privado, os sistemas produtivos caminham para a era da digitalização alavancados pela "Indústria 4.0", um dos temas com maior crescimento de pesquisa nos últimos anos. Nesta nova indústria, tudo está interconectado em um cenário digital com a respectiva representação virtual, permitindo que, em um nível mais alto de automação, muitos sistemas e *softwares* se comuniquem da fábrica utilizando as últimas tendências de tecnologias de informação e comunicação, alcançando todos os elementos da cadeia de valor em um engajamento em tempo real (ALCÁCER; CRUZ-MACHADO, 2019).

Segundo Liu et al. (2019), com a ampla adoção das tecnologias da Internet das Coisas (IoT), a superfície de ataques cibernéticos aumentou drástica e profundidade, fornecendo novos mecanismos para a intrusão e aumentando o potencial 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).

No setor público, o poder judiciário tem avançado na informatização de seus sistemas, inovando e criando soluções para atender a população. Os tribunais têm investido em modernização e tecnologia para manter os sistemas processuais em alta performance e garantir a segurança dos dados com a finalidade de viabilizar um atendimento ágil e seguro. Entretanto, diversas ações de *hackers* têm atingido o Poder Judiciário em seus vários níveis e especialidades (AGÊNCIA BRASIL, 2020a, 2020b, 2020c; BAGUETE, 2021; CONJUR, 2021a, 2021b; FOLHA, 2020; G1, 2021; STJ, 2020; TERRA, 2020; UOL, 2022).

Entre os ataques cibernéticos mais notáveis está o realizado no Superior Tribunal de Justiça (STJ) em novembro de 2020 que causou a interrupção de julgamentos que ocorriam nas suas seis turmas. Os sistemas do tribunal e o site oficial ficaram fora do ar e todos os prazos processuais foram suspensos por dez dias. Todos os funcionários se encontravam em regime de

teletrabalho e tiveram seus acessos suspensos (AGÊNCIA BRASIL, 2020c). Mais de 255 mil processos tramitam na Corte e teriam sido capturados pelo *hacker* que adicionou chaves de criptografia a mais de 1,2 mil máquinas virtuais, além de destruir seus backups com um *ransomware* chamado RansomEXX (BAGUETE, 2021; TERRA, 2020).

A pesquisa aqui realizada vai ao encontro da estratégia do judiciário em elevar o nível de segurança das infraestruturas críticas por meio das equipes de resposta a incidentes de segurança cibernética, conforme Estratégia Nacional de Segurança Cibernética e da Informação do Poder Judiciário aprovada pelo Conselho Nacional de Justiça.

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 e ampliação do desempenho nas organizações.

Os CSIRTs (*Computer Security Incident Response Team*) usam políticas definidas, procedimento e guias para criar processos consistentes, orientados à qualidade e repetíveis (RUEFLE et al., 2014). Os processos são estilo modelo cascata, em que uma fase é seguida de outra, um plano de ação linear. Estes processos rígidos e procedimentais aumentam a previsibilidade dos esforços de defesa e tornam mais difícil proteger a infraestrutura e funções de negócios no contexto de ataques cibernéticos rápidos e multifacetados (SMITH et al., 2021).

Grispos et al. (2014) e Ahmad et al. (2012) destacam que a abordagem de plano de ação linear apresenta alguns problemas, tais como: (1) pouca eficiência para 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) redução dos benefícios da forense digital; (7) enfraquecimento da evidência forense; (8) negligência no uso das lições aprendidas e das funções pós-incidente.

Em face a esses problemas, o paradigma ágil, em especial os princípios do *Scrum*, poderia ser considerado uma opção de solução devido à sua consagrada utilização em áreas fora do desenvolvimento de *software*. De acordo com Stefani & Feitosa (2019), a colaboração em equipes apresentou-se maior quando adotado métodos ágeis. Assim, poderia também atender quando as soluções não são muito claras no início, por focar nas pessoas, em constantes *feedbacks* e na aceitação de constantes mudanças (AMORIM et al., 2018).

Questão da pesquisa:

A questão de pesquisa é “Como os princípios ágeis podem ser aplicados nos processos de tratamento e resposta a incidentes de segurança da informação no Poder Judiciário?”

Objetivo geral:

O objetivo deste trabalho é examinar como adaptar e avaliar um processo baseado na aplicação dos princípios ágeis nos processos de tratamento e resposta de incidentes de segurança da informação no Poder Judiciário.

Os **objetivos específicos** deste trabalho são:

- vii. Identificar o problema e motivação por meio do levantamento bibliométrico e revisão da literatura recente e da identificação dos problemas e questões em processos de resposta a incidentes;
- viii. Definir os objetivos da solução para melhoria nos processos de um CSIRT do Poder Judiciário;
- ix. Projetar e desenvolver a adaptação dos processos de um CSIRT do Poder Judiciário por meio da identificação dos princípios e práticas do método ágil;
- x. Demonstrar a utilização de práticas ágeis nos processos de resposta a incidentes de segurança de informação em uma instituição do Poder Judiciário;
- xi. Avaliar o processo com os atores envolvidos;
- xii. Comunicar os resultados da pesquisa;

Linha de pesquisa:

Este trabalho desenvolvido no Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos do pertence à Linha de Pesquisa de *Sistemas de Informação e Tecnologias Digitais* e ao Projeto de Pesquisa *Gestão Estratégica da Tecnologia da Informação* e explorou os temas da tecnologia da informação e segurança da informação.

Os sistemas produtivos e a engenharia de produção tratam de projetos, aperfeiçoamento e implantação de sistemas integrados de pessoas, materiais, informações, equipamentos e energia, para a produção de bens e serviços. Dentro dessa abordagem cabem não apenas os setores produtivos tradicionais, mas também outras atividades como ONGs, redes de empresas, interfaces colaborativas, e as entidades governamentais (DE JESUS; COSTA, 2014).

Os movimentos da Nova Gestão Pública e da Governança Digital, apesar de algumas diferenças, convergem para um sistema de pensamento caracterizado pela importação de ideias geradas em áreas do setor privado para dentro das organizações do setor público, visando atender às demandas da sociedade por melhores serviços (DE JESUS; COSTA, 2014).

O Poder Judiciário, como os demais órgãos públicos, presta serviços à sociedade, e atualmente são orientados ao cumprimento de metas, melhorias de processos, governança estratégica, orientação a resultados entre outros. Desse modo, se observa uma interface e associação aos preceitos dos sistemas produtivos aos serviços do Poder Judiciário.

Contribuições:

Do ponto de vista da gestão e da tecnologia em sistemas produtivos, a pesquisa contribui para a melhoria dos processos de resposta a incidentes de segurança da informação e dos seus CSIRTs, em especial aos órgãos do Poder Judiciário e aos gestores de segurança da informação.

Pretende-se com este trabalho, contribuir para que as organizações e os membros de CSIRTs possam agregar práticas ágeis em seus processos e com isso trazer outros subsídios para o aprofundamento desta temática.

Sob a perspectiva acadêmica, esta pesquisa colabora com a discussão a respeito da utilização de práticas ágeis em processos da segurança de informação dentro do escopo do Poder Judiciário, possibilitando a abertura de novas oportunidades de pesquisas envolvendo contextos específicos descritos neste trabalho. Por meio de um experimento prático, este estudo contribui para a literatura de resposta a incidentes, mostrando como a integração de princípios ágeis em processos lineares pode melhorar a resposta a incidentes.

1 FUNDAMENTOS TEÓRICOS UTILIZADOS NA PESQUISA

Desde que o manifesto ágil foi criado em 2001, a comunidade de pesquisa dedicou muita atenção ao desenvolvimento ágil de *software*, trazendo mudanças sem precedentes no campo da engenharia de *software* (DINGSØYR et al., 2012). A filosofia ágil permitiu implementar *softwares* de maneira iterativa e incremental, agregando valor ao processo produtivo de maneira que melhorias contínuas são entregues ao produto (BECK et al., 2001; COHEN; LINDVALL; COSTA, 2004; CONBOY; FITZGERALD, 2004; DINGSØYR et al., 2012).

Em termos gerais, muitas áreas fora do desenvolvimento de *software* foram inspiradas a adotar os princípios ágeis: o desenvolvimento colaborativo; a mentalidade predominantemente “enxuta”; a participação ativa dos clientes ou partes interessadas na evolução do produto ou serviço e não mais ficarem à margem do desenvolvimento de *software*; a incerteza como parte integrante do desenvolvimento (DINGSØYR et al., 2012).

Fica demonstrado em alguns trabalhos (GRISPOS; GLISSON; STORER, 2014, 2017, 2015; HE et al., 2022; HE; JANICKE, 2015; NASEER et al., 2021; SMITH et al., 2021), que existe uma lacuna de pesquisa na utilização do método ágil na área de resposta a ciberincidentes.

A resposta a incidentes de segurança da informação, reflete como funciona a política de segurança da informação da organização. A implementação destas políticas, num ambiente de TI, é condição *sine qua non* para o processo de gerenciamento estratégico de qualquer organização (IMONIANA, 2004).

As equipes de segurança da informação devem constantemente atuar, seja de forma proativa ou reativa. Os times de resposta de incidentes das organizações, conhecidos como CSIRTs (*Computer Security Incident Response Team*) ou CERT (*Computer Emergency Response Team*), são responsáveis por receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores (CERT.BR, 2022a).

O processo de resposta a incidentes geralmente é composto por cinco fases: preparação; detecção e análise; contenção; erradicação e recuperação e revisão pós-incidente. No entanto, esta abordagem linear geralmente consome tempo, são ineficazes na resposta a ataques de grande escala, são muito complexas ao lidar com incidentes sofisticados e não têm oportunidades de aprendizado (GRISPOS; GLISSON; STORER, 2014; HE; JANICKE, 2015).

A pesquisa realizada contribui para a solução de alguns dos problemas enfrentados pelos times de tratamento de incidente em face aos desafios atuais. Os princípios ágeis podem

contribuir para aproximar as pessoas, os processos e as ferramentas dentro do escopo da resposta a incidentes de segurança cibernética no Poder Judiciário.

1.1 Revisão da literatura

A realização da pesquisa bibliométrica e da revisão da literatura foi uma das atividades iniciais desse trabalho para apresentar uma análise sistemática e síntese de pesquisa sobre a utilização de práticas ágeis nos processos de resposta a incidentes de segurança da informação.

A metodologia utilizada, de acordo com Prodanov & de Freitas (2013), pode ser classificada quanto à natureza como pesquisa básica. Quanto ao objetivo, pesquisa exploratória e descritiva. E, quanto ao procedimento científico, pesquisa bibliométrica e revisão sistemática.

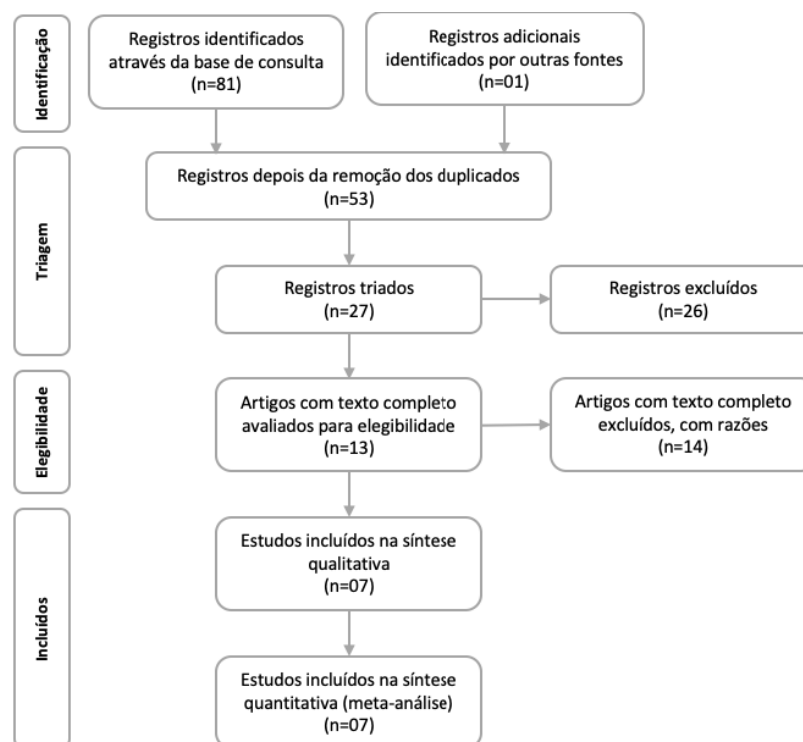
A revisão bibliográfica utilizou as bases de dados SCOPUS, *Web of Science*, *Scielo* e *Google Scholar*, por suas abrangências de cobertura de áreas do conhecimento científico e se integrarem a ferramentas computacionais que auxiliam na recuperação dos metadados.

Os achados foram analisados quantitativa e qualitativamente com o protocolo de pesquisa PRISMA-P (*Preferred Reporting Items for Systematic Review and Meta-Analysis Protocols*) (MOHER D et al., 2015), visando uma revisão sistemática.

Os dados foram coletados em abril de 2021 e depois atualizados em setembro de 2021. Os termos de pesquisa utilizados foram as palavras chaves “*agile principles*”, “*security incident response*” e as variações “*agile method*”, “*security incident handling*”. Foram aplicados os filtros de seleção de documentos publicados entre 2014 e 2021.

Como critérios de exclusão, foram considerados: tipo de publicação (livros, relatórios, *data sets*, citações e matérias jornalísticas); artigos publicados não no idioma inglês ou português; acesso fechados; terminologias não pertinentes ao tema do presente estudo; repetidos nas bases de dados; e resumos que não sejam condizentes com o objeto de estudo.

A **Figura 1** ilustra o fluxograma do protocolo PRISMA-P contendo passo a passo em que, a partir 82 documentos reunidos de todas as fontes de busca, chegou-se ao número de sete artigos incluídos na síntese qualitativa e quantitativa (meta-análise).

Figura 24 Fluxograma do Protocolo PRISMA-P

Fonte: Resultado da pesquisa

O **Quadro 4** apresenta o resultado dos principais achados da pesquisa. São sete estudos incluídos na síntese qualitativa, realizada com a sua leitura e que atendiam o escopo do estudo que trata da utilização de princípios ágeis na resposta a incidentes de segurança da informação.

Quadro 13 Resumo dos principais achados nas publicações selecionadas

Autores	Resumo dos achados
Grispos, WB, Glisson, T Storer	Em (GRISPOS; GLISSON; STORER, 2014) propõem uma integração ágil aos processos de resposta a incidentes de segurança da informação. Indicam que existem poucas pesquisas sobre o tema. Sugerem mais estudos para trabalhos futuros chamando de <i>Agile Incident Response</i> . Em (GRISPOS; GLISSON; STORER, 2015) propuseram que as organizações poderiam se integrar aos princípios e práticas ágeis, identificado como Critérios de Resposta a Incidentes de Segurança (SIRC). Em (GRISPOS; GLISSON; STORER, 2017) investigam a integração de retrospectivas e meta-retrospectivas ágeis leves no processo de resposta a incidentes de segurança, para melhorar o <i>feedback</i> e <i>follow-up</i> .

Autores	Resumo dos achados
Y He, H Janicke	Examinam em (HE; JANICKE, 2015) o procedimento de resposta a incidentes de um <i>Industrial Control System</i> (ICS) sob perspectiva gerencial, identificando características exclusivas de resposta a incidentes de ICS e propõe uma estrutura para melhorar as capacidades da resposta a incidentes.
A Naseer et al.	Propõem em (NASEER et al., 2021) que as organizações podem obter agilidade na resposta a incidentes de segurança com flexibilidade, rapidez e inovação.
R Smith et al.	O <i>framework</i> de Resposta Ágil a Incidentes para Sistemas de Controle Industrial (AIR4ICS) foi desenvolvido para integrar técnicas ágeis ao domínio da resposta a ciberincidentes. O <i>framework</i> fornece uma abordagem dinâmica para melhorar a consciência situacional, o compartilhamento de informações, a tomada de decisão coletiva e a flexibilidade de resposta dentro do contexto do ICS.
He et al.	Neste estudo propõem o <i>framework Agile Incident Response</i> para refinar, ajustar e melhorar o atual processo linear de resposta a incidentes do <i>National Health Service</i> (NHS) do Reino Unido. A atual estrutura linear de resposta a incidentes foi analisada criticamente e demonstrado como ela pode ser transformada em uma estrutura de resposta a incidentes híbrida.

Fonte: Resultado da pesquisa

Ao realizar a construção da síntese dos artigos selecionados neste estudo, identificou-se como lacunas de pesquisa sobre o uso dos princípios ágeis na resposta a incidentes de segurança da informação em sistemas produtivos.

1.2 A informatização do Poder Judiciário brasileiro

O Poder Judiciário brasileiro tem avançado na informatização de seus sistemas. O número de processos eletrônicos de 2009 eram de apenas 11,2% dos processos a julgar enquanto em 2020, o índice saltou para 96,9%, de acordo com estatísticas do CNJ (CNJ, 2022).

O relatório anual Justiça em Números, do Conselho Nacional de Justiça (CNJ), reúne dados dos 90 órgãos do Judiciário. Com informações da Base Nacional de Dados do Poder

Judiciário (DataJud), atualmente representa o armazenamento de mais de 11 bilhões de movimentações processuais de ações em andamento e já baixadas (CNJ, 2021a).

Nos últimos anos, o Judiciário inovou e criou soluções para atender a população em meio à crise sanitária causada pela pandemia da Covid-19. Por meio da tecnologia, iniciativas buscaram garantir a continuidade da prestação jurisdicional de forma célere e eficiente. Entre essas iniciativas estão o Juízo 100% Digital, a Plataforma Digital do Poder Judiciário, a Plataforma Sinapes e Codex e o Balcão Virtual (CNJ, 2021b).

Nos últimos anos, diversas ações de *hackers* têm atingido o Poder Judiciário em seus vários níveis e especialidades (AGÊNCIA BRASIL, 2020a, 2020b, 2020c; BAGUETE, 2021; CONJUR, 2021a, 2021b; FOLHA, 2020; G1, 2021; STJ, 2020; TERRA, 2020; UOL, 2022).

Entre os ataques mais notáveis está o realizado no Superior Tribunal de Justiça (STJ) em novembro de 2020 que causou a interrupção de diversos julgamentos que ocorriam simultaneamente nas seis turmas do STJ. Os sistemas, incluindo o site oficial, ficaram fora do ar e todos os prazos processuais foram suspensos por dez dias (AGÊNCIA BRASIL, 2020c).

O exemplo ilustra a importância na preservação de todo o ecossistema digital do Poder Judiciário, principalmente na pronta resposta aos ciberincidentes que venham a sofrer. Os danos causados por uma resposta a incidentes insatisfatória podem ocasionar enormes prejuízos à vida das pessoas, às organizações, aos operadores do direito, e ao Judiciário como um todo.

O Poder Judiciário julga cerca de 18 milhões de processos por ano, cerca de 77 milhões de processos estão em tramitação (CNJ, 2021a). Uma vez que a maioria desses processos tem tramitação eletrônica, a infraestrutura dos tribunais pode sofrer ataques cibernéticos e ameaças que poderão afetar as premissas da segurança da informação: a integridade, a disponibilidade e a confidencialidade (SAMONAS; COSS, 2014).

Motivado por todos esses acontecimentos recentes, o CNJ aprovou a criação da Estratégia Nacional de Segurança Cibernética e da Informação do Poder Judiciário (ENSEC-PJ), um instrumento para orientar a resposta dos órgãos da Justiça à crescente ameaça de ataques de *hackers* à infraestrutura virtual dos tribunais brasileiros (CNJ, 2021c).

A pesquisa aqui realizada vai ao encontro da estratégia do judiciário em elevar o nível de segurança das infraestruturas críticas. Além disso, o presente trabalho pode contribuir para o objetivo da ENSEC-PJ de estimular uma relação colaborativa entre as cortes no tratamento de incidentes e vulnerabilidades cibernéticas verificadas, e de realizar exercícios em conjunto com as equipes responsáveis por gerenciar crises causadas por ataques *hackers*.

1.3 Continuidade do negócio e recuperação de desastres

O gerenciamento de riscos é fundamental no planejamento de contingências e gerenciamento de continuidade a fim de tratar as interrupções na operação do negócio. Recuperar rápida e eficientemente a atividade depois de um acidente, minimizando os seus efeitos, deverá ser uma preocupação vinculada e real dos decisores (REIS; AMARAL, 2016).

Um plano de continuidade de negócios (*Business Continuity Plan* – BCP) é uma ferramenta essencial que visa garantir a recuperação imediata das atividades críticas e de seus sistemas e aplicativos de suporte, em caso de desastre (BRAS; RIBEIRO, 2016). Seu foco é no planejamento da recuperação de processos e funções de negócios, abrangendo resposta a emergências, continuidade de negócios, recuperação de desastres e gerenciamento de uma situação de crise (KLIEM; RICHIE, 2015; TASHI; GHERNAOUTI-HÉLIE, 2011).

O plano de recuperação de desastres (*Disaster Recovery Plan* - DRP), por sua vez, é o componente técnico do BCP e aborda a recuperação dos sistemas centrais, seus dados e tecnologias de comunicação que suportam o negócio. A recuperação de desastres é um subconjunto da continuidade de negócios (BRAS; RIBEIRO, 2016; SNEDAKER, 2014).

Para Snedaker (2014), além da recuperação de desastres, a recuperação dos serviços de TI envolve responder, interromper e reparar problemas por falhas de sistemas, violações de segurança, corrupção ou destruição de dados. Pode ser necessário ativar uma equipe de resposta a incidentes de segurança da informação (CSIRT), assunto da próxima seção.

A resposta a incidentes de segurança da informação é uma atividade que abrange recuperação de desastres, continuidade de negócios e operações normais. Os membros de um CSIRT devem ter responsabilidades integradas aos BCP e DRP e devem manter suas habilidades atualizadas para que estejam alertas para responderem às ameaças, vulnerabilidades e problemas na área de TI (SNEDAKER, 2014).

1.4 Resposta a incidentes de segurança da informação

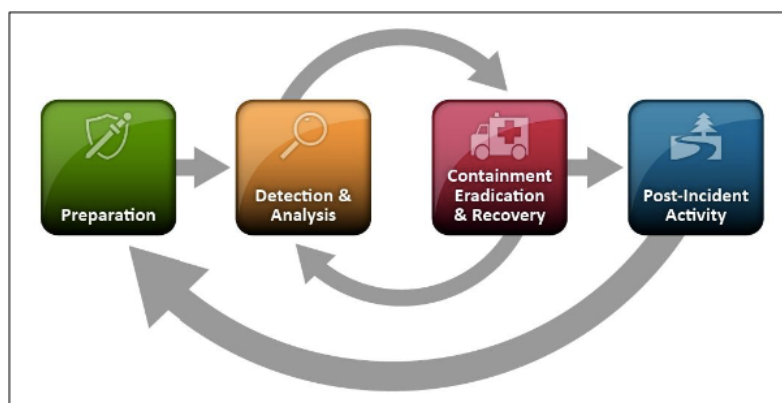
Um incidente de segurança da informação, segundo Cichonski et al. (2012), é uma violação das políticas de segurança, políticas de uso ou práticas padrões de segurança.

Conforme Galeale et al. (2017), a informação tem importância estratégica, é impulsionada com a utilização de TI nos processos organizacionais e deve ter proteção adequada.

O problema a ser analisado e proposto para este trabalho está inserido na área de resposta a incidentes da segurança da informação no Poder Judiciário, os quais são limitados a computadores, dispositivos de redes, redes e informações contidas e transmitidas por eles.

Guias com técnicas, melhores práticas e processos foram publicados pela ENISA (MAJ; REIJERS; STIKVOORT, 2010), NIST (CICHONSKI et al., 2012) e ISO. Em 2015, (STIKVOORT, 2015) propôs um modelo de maturidade de gerenciamento de incidentes de segurança chamado SIM3 e em 2018, a CMU/SEI (DOROFEE et al., 2018) publicou o relatório técnico sobre maturidade *Incident Management Capability Assessment*.

Figura 25 Ciclo de vida de resposta a incidente do NIST



Fonte: (CICHONSKI, MILLAR, GRANCE, & SCARFONE, 2012)

Em geral, o processo de resposta a incidentes de segurança é um plano de ação linear como mostra a **Figura 6**. Esta abordagem de plano de ação linear e tradicional apresentou alguns importantes pontos de atenção e problemas. Conforme (GRISPOS; GLISSON; STORER, 2014): como melhorar os processos tradicionais para que reflitam as necessidades do mundo atual? Como tratar os ciberataques automatizados? Como melhorar as lições aprendidas? Como aplicar um modelo de maturidade na gestão de incidentes? Ainda, existe uma negligência nos aspectos das lições aprendidas de respostas a incidentes e funções pós-incidente? (AHMAD; HADGKISS; RUIGHAVER, 2012b)

Ao utilizarem um modelo em cascata para o tratamento e resposta de incidentes de segurança da informação fica inerente aos processos internos a ocorrência dos mesmos

problemas que afligiram a indústria de *software* por anos, entre eles a dificuldade de lidar com mudanças, complexidades e relação da equipe com o projeto todo. A próxima seção trata dos princípios ágeis e ajuda a responder porque eles são úteis neste contexto.

1.5 Princípios ágeis

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 por meio de melhorias contínuas.

1.5.1 Princípios ágeis na resposta a incidentes de segurança da informação

As práticas e princípios ágeis podem ajudar na solução dos desafios dos processos tradicionais de um CSIRT, tais como os expostos por Grispos et al. (2014): processos que não refletem o dinamismo do mundo atual, que são lentos e que 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 valores ágeis foi proposto por He & Janicke (2015). Grispos et al. (2015) identificaram seis critérios essenciais que um processo de resposta a incidentes bem-sucedido precisa endereçar, com o chamado *Security Incident Response Criteria* (SIRC).

Shedden et al. (2010) propuseram a aplicação de aprendizado de *loop* duplo para acompanhamentos de incidentes e atividades após a resolução do incidente, semelhante à retrospectiva do *Scrum*. E Grispos et al. (2017) destacam essa fase final como implementação de melhores práticas e influenciar a disseminar o aprendizado de incidente de segurança.

Naseer et al. (2021), argumentam que (1) as organizações devem desenvolver agilidade em seus processos 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.

As equipes tradicionais de resposta a incidentes geralmente seguem uma estrutura rígida e hierárquica. A 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).

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.

Assim, os exemplos trazidos pela literatura científica validam o prosseguimento da pesquisa visando a utilização de princípios ágeis na resposta a incidentes de segurança da informação no Poder Judiciário, a qual seguirá a metodologia descrita no próximo capítulo.

2 CAMINHO METODOLÓGICO

A metodologia de pesquisa escolhida para conduzir este estudo é a *Design Science Research Methodology* - DSRM, que tem embasamentos na produção de pesquisa com o processo de *Design Science* (DS) e na apresentação por meio de modelo mental para tratar da realidade construída a partir da compreensão do problema (HEVNER; CHATTERJEE, 2010; LACERDA et al., 2013; PEFFERS et al., 2007).

A DSRM incorpora princípios, práticas e procedimentos necessários para a pesquisa em seis etapas: identificação e motivação do problema, definição dos objetivos para uma solução, *design* e desenvolvimento, demonstração, avaliação e comunicação (PEFFERS et al., 2007).

O processo DS inclui seis etapas: (Etapa 1) identificação e motivação do problema; (Etapa 2) definição dos objetivos para uma solução; (Etapa 3) *design* e desenvolvimento; (Etapa 4) demonstração; (Etapa 5) avaliação; e (Etapa 6) comunicação (PEFFERS et al., 2007).

Conceitualmente, um artefato de pesquisa de *design* pode ser qualquer objeto projetado no qual uma contribuição de pesquisa esteja incorporada ao *design* (PEFFERS et al., 2007). Os artefatos da DSRM podem ser constructos, modelos, métodos ou instanciações (HEVNER et al., 2004).

Demonstrar a viabilidade do artefato, ajuda a justificar o esforço da pesquisa teórica realizada e faz a solução fornecer resultados esperados a partir dos estudos de campo. A pesquisa teórica é utilizada para explicar (1) por que o projeto do artefato pode funcionar e (2) especificar eventuais contingências resultantes de princípios que possam fazer parte de práticas recomendadas. A importância do projeto como modo de pesquisa é reconhecida na literatura acadêmica para melhorar o desempenho organizacional (HEVNER; CHATTERJEE, 2010).

Para Lacerda et al. (2013), a avaliação final do artefato não dispensa que, em cada etapa do método da *Design Science Research*, sejam realizadas avaliações parciais. Autores como Hevner et al., (2004) propõem alguns métodos que podem ser utilizados para a avaliação dos artefatos gerados pela *Design Science Research*.

Ao final desta etapa o pesquisador deste estudo pode decidir iterar à etapa de projeto e desenvolvimento para tentar melhorar a eficácia do artefato ou continuar à etapa seguinte para obter melhoria adicional por meio de projetos subsequentes (HEVNER; CHATTERJEE, 2010).

3 RESULTADOS (INOVAÇÃO/ INTERVENÇÃO/ RECOMENDAÇÕES)

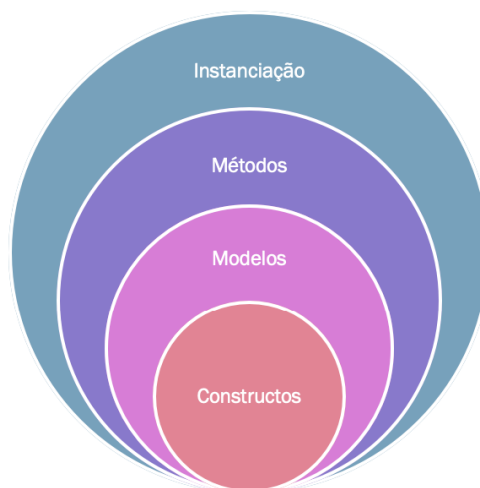
3.1 Design e desenvolvimento

Esta seção detalha como a solução foi projetada e desenvolvida para alcançar os objetivos identificados descritos no início do trabalho.

3.1.1 As relações entre os artefatos constructo, modelo, método e instanciação

A **Figura 12** ilustra de maneira simplificada a relação entre os artefatos. O trabalho utiliza algumas práticas ágeis para complementar e melhorar os processos tradicionais de resposta a incidentes com ênfase nas fases de pré-incidente, triagem, análise e resolução do incidente, o qual é chamado de **AIR-Jud**, de *Agile Incident Response*.

Figura 26 Relação entre constructos, modelos, métodos e instanciação conforme o DSRM



Fonte: Adaptado de (LACERDA et al., 2013; MARCH; SMITH, 1995)

A **Figura 13** ilustra os constructos da pesquisa: Incidentes de Segurança, Tratamento de Incidentes e Princípios Ágeis, os quais atuam no contexto do gerenciamento de riscos relacionados aos incidentes de segurança de uma instituição do Poder Judiciário.

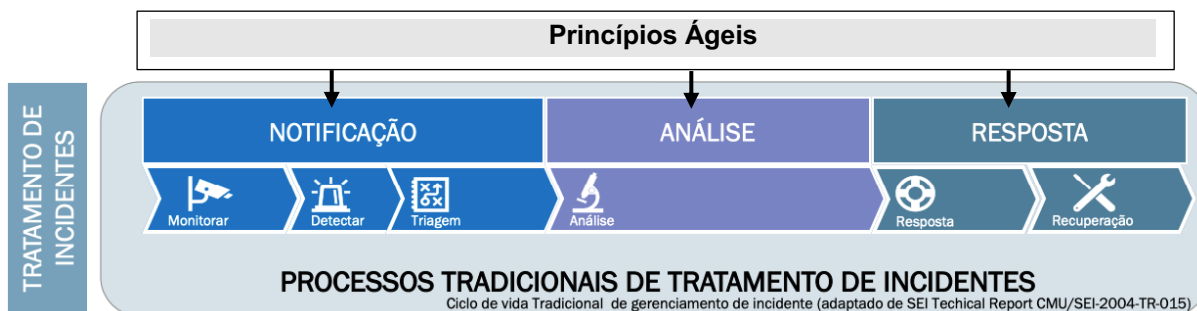
Figura 27 Constructos da pesquisa

Fonte: Resultado da pesquisa

Os conceitos apresentados na **Figura 13** pertencem ao domínio de estudo deste trabalho. Conforme a DSRM, eles podem ser classificados como um artefato do tipo **constructo**.

O constructo *Incidente de Segurança* é definido como um evento de segurança ou um conjunto deles, confirmado ou sob suspeita de impactar a disponibilidade, integridade, confidencialidade ou a autenticidade de um ativo de informação, bem como qualquer violação da política de segurança da informação. O *Tratamento de Incidentes* é composto por notificação, análise e resposta ao incidente, contendo os processos tradicionais de resposta a incidentes. O constructo *Princípios Ágeis* trata da adaptação dos princípios ágeis aos processos de resposta a incidentes, como os papéis, eventos e artefatos do *Scrum*, explicados na sequência. Princípios ágeis são os conceitos, ferramentas e práticas oriundas do manifesto e método ágil.

No DSRM, um **modelo** é um conjunto de proposições ou declarações que expressam as relações entre os constructos. Desse modo, as relações entre os constructos definidos nesta pesquisa são exemplificados na **Figura 14**, ilustra o modelo representando o ciclo de vida do experimento, relacionando os constructos do tratamento de incidente.

Figura 28 Modelo dos processos de tratamento de incidentes com métodos ágeis

Fonte: Resultado da pesquisa

Notificação de incidente é o ponto central de contato para notificação de problemas. Isto permite que todas as atividades e os incidentes reportados sejam coletados em um único local, onde esta informação pode ser analisada e correlacionada por meio da organização ou comunidade sendo atendida. É subdividida geralmente em monitoramento, detecção e triagem.

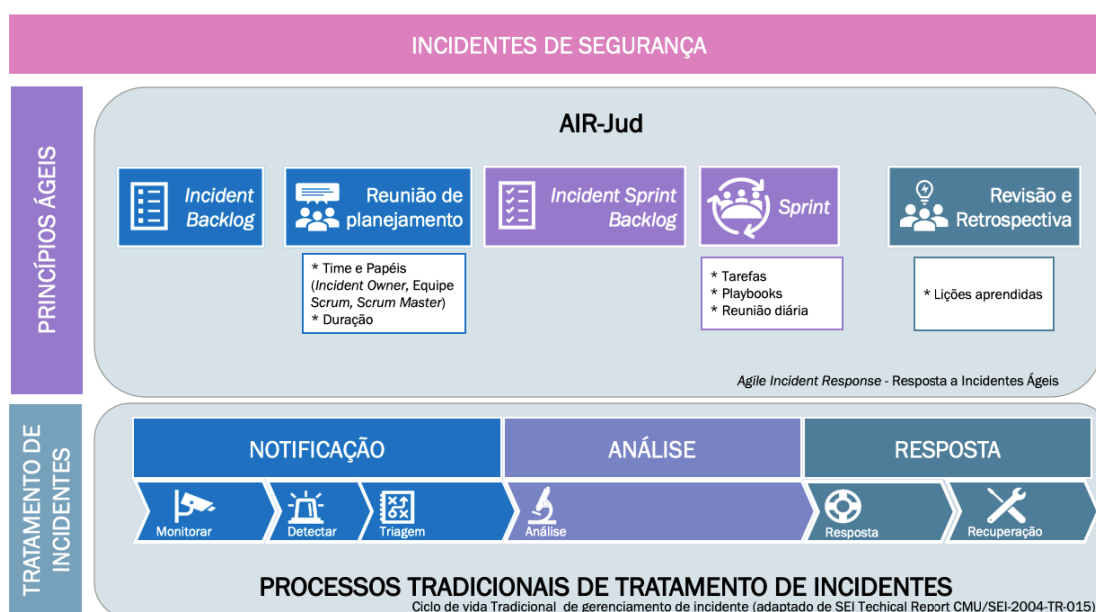
Análise de incidente envolve analisar uma notificação ou uma atividade observada para determinar o escopo, prioridade e ameaça representada pelo incidente, bem como pesquisar acerca de possíveis estratégias de resposta e erradicação;

Resposta a incidente pode assumir formas como divulgação de recomendações para recuperação, contenção e prevenção aos membros da comunidade atendida e aos administradores de redes e sistemas responsáveis. A resposta pode envolver o compartilhamento de informações e lições aprendidas;

Avançando no DSRM, um **método** é um conjunto de passos usado para executar uma tarefa. Dessa maneira, os métodos ágeis, como o *Scrum* e o *Kanban*, são utilizados para traduzir o modelo em um curso para resolução do problema da pesquisa.

Ilustrado na **Figura 15** temos o método ágil *Scrum* utilizado para adaptar o ciclo de vida tradicional de gerenciamento de incidentes.

Figura 29 O modelo de resposta a incidentes adaptado com o método *Scrum*



As principais práticas ágeis que inspiraram o AIR-Jud foram os métodos do *Scrum* e do *Kanban*. Ele adota e adapta ao contexto da cibersegurança algumas regras específicas derivadas dos seus valores de transparência, inspeção e adaptação, conforme proposto por Schwaber & Sutherland (2017):

- v. Um time *Scrum* consiste em três papéis principais: *Product Owner*, *Scrum Master* e Time de Desenvolvimento;
- vi. O projeto é dividido em *Sprints* de período de 1 a 4 semanas, devendo ser entregue algum incremento de produto valioso no final de cada *Sprint*;
- vii. Os eventos formais do Scrum asseguram a inspeção e adaptação: no início de cada *Sprint* (*Sprint Planning*), no final de cada dia (*Daily Meeting*) e no final de cada *Sprint* (*Sprint Review* e *Sprint Retrospective*);
- viii. Os artefatos produzidos fornecem transparência e oportunidades de inspeção e adaptação: *Product Backlog*, *Sprint Backlog* e Incremento;

A instanciação proposta neste trabalho visa demonstrar a viabilidade e a eficácia dos modelos e métodos que ela contempla, utilizando para isso um exemplo prático real situado no contexto da resposta a incidentes de segurança da informação do Poder Judiciário. Na seção da Etapa de Demonstração compreende-se melhor este artefato.

3.1.2 Processos adaptados do método Scrum

Como proposto por SMITH et al. (2021) em seu *framework* AIR4ICS, os processos de resposta a incidentes apresentado neste trabalho são estruturados em breves rajadas de atividade análogas às *Sprints* do *Scrum* durante as quais os objetivos das fases tradicionais serão parcialmente alcançados e etapas para a resolução sendo adicionadas etapas interativas.

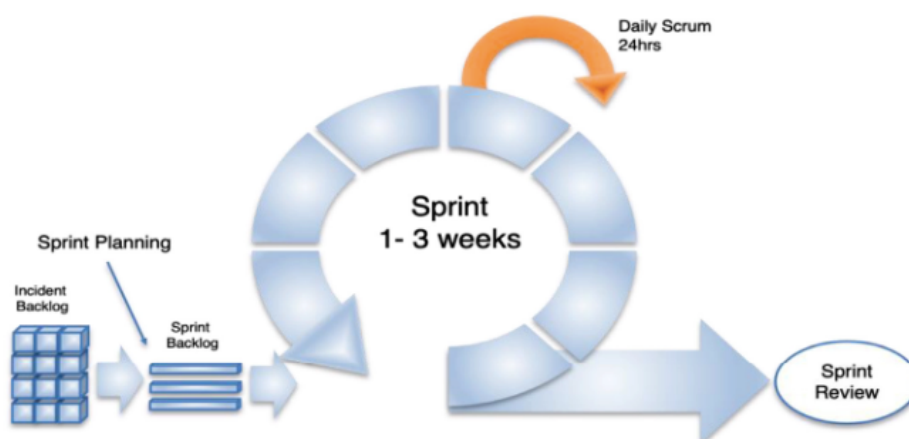
Considerando que a dinâmica de um ataque cibernético complexo pode exigir várias edições e revisões da estratégia de resposta, dependendo das informações obtidas durante o ataque, o modelo proposto utiliza uma abordagem interativa aos processos dando ênfase na melhoria contínua do processo de resposta a incidentes (SMITH et al., 2021).

A equipe responsável por incidentes é multifuncional e conduz o planejamento e revisão da *Sprint* pelo melhor curso de ação, podendo escalar os incidentes aos negócios ou às organizações externas, como outros CSIRTs ou CERTs nacionais. A abordagem para identificar

o objetivo para o próximo *Sprint* é impulsionada pelo valor da resposta e pelo risco associado aos termos de probabilidade de sucesso e impacto no negócio (SMITH et al., 2021).

A **Figura 30** de Smith et al. (2021), ilustra o método *Scrum* adaptado ao contexto de resposta a incidentes. É possível observar que vários “blocos” de *Incident Backlog* originam os *Sprint Backlogs*. Durante o *Sprint* de duração variável, as *Daily Scrum* podem ser menores que 24h, dependendo do caso. O *Sprint Review* incorpora a função de Retrospectiva do *Sprint*.

Figura 30 O método *Scrum* adaptado para o modelo de resposta a incidentes



Fonte: (SMITH et al., 2021)

3.1.3 Papéis

As equipes tradicionais de resposta a incidentes muitas vezes seguem uma estrutura rígida e hierárquica. Os indivíduos são realocados para uma função especializada, como *firewalls*, ameaças etc. Essa segregação de tarefas muitas vezes leva à criação de silos de informações e conhecimentos, onde as tentativas de passar informações e habilidades para outras unidades relevantes podem ser abaixo do ideal. Os princípios ágeis visam quebrar esses silos criando equipes mais integradas (SMITH et al., 2021).

Para isso, existem apenas três papéis distintos dentro de uma equipe de resposta a incidentes ágeis, conforme descrito no **Quadro 8**, conforme Smith et al. (2021).

Quadro 14 Papéis de uma equipe ágil de resposta a incidentes

Papel	Descrição no AIR-Jud
<i>Incident Owner</i>	Função geralmente desempenhada por um gerente de resposta a incidentes experiente ou líder técnico. Possui a visão/estratégia do incidente. Atua como ponto de contato com a alta administração e em nome do cliente (quando diferente de organização). Controla e prioriza o <i>Backlog de Incidentes</i>
<i>SCRUM Master</i>	O <i>Scrum Master</i> é responsável por promover e apoiar o <i>Scrum</i> entre membros e não membros da equipe de Resposta a Incidentes, ajudando a remover obstáculos, melhorar a resposta a incidentes e o desempenho da equipe para maximizar o valor.
Membro da equipe	Profissionais que fazem o trabalho de dar a resposta para minimizar e mitigar o impacto de um incidente. Eles são estruturados e capacitados pela organização para organizar e gerenciar seu próprio trabalho. São auto-organizados, <i>cross funtional</i> , sem títulos e responsáveis como um todo.

Fonte: Adaptado de (SCHWABER; SUTHERLAND, 2017; SMITH et al., 2021)

3.1.4 Eventos

Adaptando os conceitos do *Scrum*, o modelo de resposta a incidentes ágil pode incorporar os eventos de um *Sprint*. Os *Sprints* são processos cíclicos que se iniciam com o *Incident Backlog* que é então dissecado para criar um *Sprint Backlog*. Isso é então usado como entrada para as *Daily Scrums* até o final do *Sprint*, quando as revisões e retrospectivas ocorrem. Quaisquer lições aprendidas alimentam as ações no próximo *Sprint*.

Os eventos da *Sprint* são descritos no **Quadro 9**. Novamente, a primeira coluna descreve o evento *Scrum*, a segunda coluna se baseia nas definições originais do *Scrum* pelos autores Schwaber & Sutherland (2017), enquanto a terceira coluna é a proposta de adaptação pelo modelo AIR-Jud, inspirado no trabalho de Smith et al. (2021).

Quadro 15 Os eventos do método *Scrum* adaptados
para uma equipe de resposta a incidentes ágeis

Evento	Descrição no AIR-Jud
Planejamento do <i>Sprint</i>	Reunião em que as partes interessadas e os membros da equipe definem com eficiência e eficácia o trabalho a ser executado na iteração atual. Ela tem dois objetivos: (1) o que pode ser entregue na atualização resultante do próximo <i>Sprint</i> ? (2) como o trabalho será realizado? Os itens <i>Incident Backlog</i> a serem trabalhados durante o <i>Sprint</i> serão identificados criando um <i>Sprint Backlog</i> , com os membros da equipe assumindo a propriedade das tarefas
Reuniões <i>Scrums</i>	A frequência ideal para Reuniões <i>Scrum</i> depende do contexto do incidente. Como o Agile incentiva a adaptabilidade e a resposta à situação, as reuniões podem ocorrer com mais regularidade durante os momentos em que o incidente está mudando. A reunião gira em torno de três questões: (1) O que fiz ontem? (2) O que farei hoje? (3) Algum impedimento?
Fluxo de trabalho	É o trabalho de triagem, análise, mitigação e resposta aos incidentes realizado pelo <i>Scrum Team</i> por meio dos <i>playbooks</i> de resposta a ciberincidentes e demais técnicas.
Revisão da <i>Sprint</i>	Inspeção do progresso feito durante o <i>Sprint</i> atual e adaptação do <i>Backlog do Incidente</i> , se necessário. Os resultados da reunião incluirão: (1) Identificar as melhores práticas para levar adiante em <i>Sprints</i> seguintes; (2) Identificar bloqueios à investigação e estratégias de mitigação; (3) Informações estratégicas para a sessão de planejamento da <i>Sprint</i> subsequente.
Retrospectiva da <i>Sprint</i>	Identificar lições aprendidas para os próximos e futuros <i>Sprints</i> . Objetivos: (1) Inspecionar o <i>Sprint</i> anterior em relação a pessoas, relacionamentos, processos e ferramentas; (2) Identificar e ordenar os principais itens que correram bem e potenciais melhorias; (3) Criar um plano para implementação de melhorias nos processos operacionais da equipe <i>Scrum</i> .

Fonte: Adaptado de (SCHWABER; SUTHERLAND, 2017; SMITH et al., 2021)

3.1.5 Artefatos do *Scrum*

Os artefatos do *Scrum* e *Kanban* adaptados para o uso nos processos da CSIRT são descritos no **Quadro 10**:

Quadro 16 Artefatos do *Scrum* e *Kanban* adaptados ao contexto da resposta a incidentes de segurança cibernética

Artefato	Descrição no AIR-Jud
<i>Incident Backlog</i> (IB)	É uma lista ordenada de incidentes, incluindo os aspectos de identificação, proteção, detecção, resposta e recuperação. É a única fonte de requisitos e quaisquer alterações devem ser refletidas nele.
<i>Incident Sprint Backlog</i>	Seus itens devem facilitar a priorização das tarefas. Para garantir que possa ser gerenciado de forma eficaz, cada item deve ser: (1) detalhado; (2) evolutivo ao longo do tempo; (3) ter estimativa de esforço; (4) ter controle de prioridade.
<i>Incident Board</i> (quadro <i>Kanban</i>)	É um documento vivo e o ponto focal para as reuniões do <i>Scrum</i> e é usado em todo o processo extensivamente. Permite a fácil identificação da situação atual dos <i>Incident Sprint Backlogs</i> em diferentes fases. É utilizado para manter a consciência situacional do progresso da equipe, permitindo que a equipe melhore sua eficiência removendo potenciais gargalos.

Fonte: Adaptado de (SCHWABER; SUTHERLAND, 2017; SMITH et al., 2021)

3.2 Demonstração

A demonstração da utilização do processo AIR-Jud cobre a Etapa 4 do método DSRM e contempla a sua instanciación, uma vez que os constructos, modelos e métodos já apresentados se concretizam em um exemplo prático, neste caso aplicado a um órgão do Poder Judiciário. O experimento propõe analisar os incidentes de *phishing* reportados para a Comissão Local de Resposta a Incidentes do Tribunal Regional Federal da Terceira Região (CLRI-TRF3).

3.2.1 O Tribunal Regional Federal da 3ª. Região

A razão para a escolha do Tribunal Regional Federal da 3ª. Região (TRF3) foi devido a existência neste órgão do judiciário de um time de resposta a incidentes de segurança da informação já implantado e da necessidade de aprimoramento dos seus processos de trabalho.

A Justiça Federal da Terceira Região (JF3R) é composta pelos estados de Mato Grosso do Sul e São Paulo e atinge uma população de mais de 49 milhões de pessoas, cerca de 23% da população do país, significando 33% do PIB brasileiro, cerca de R\$ 2,4 trilhões, conforme dados do painel da Justiça em Números (CNJ, 2021a).

Os dados do painel da Justiça em Números mostram que em 2020, a JF3R foi responsável por receber mais de 764 mil novas ações ajuizadas. São mais de 3,3 milhões de processos pendentes de julgamento e mais de 744 mil sentenças proferidas em 2020. O número total de servidores públicos na JF3R em 2020 chegou a 8.293, com número de usuários ativos dos recursos de informática de 7.260 e o número de computadores chegam a quase 10 mil.

3.2.2 *A Comissão Local de Resposta a Incidentes de Segurança da Informação*

A Comissão Local de Resposta a Incidentes do Tribunal Regional Federal da Terceira Região (CLRI-TRF3) é composta servidores de diferentes áreas do Tribunal e da SJMS, cuja missão é o gerenciamento de incidentes de segurança – um conjunto de ações proativas e reativas cujo objetivo é a prevenção e o tratamento desses incidentes.

A *constituency* da CLRI-TRF3 é composta dos magistrados, servidores e colaboradores dos órgãos da JF3R. Alguns serviços são: Alertas; Análise de artefatos; Tratamento e resposta a incidentes; e Tratamento de vulnerabilidades. O presente trabalho se pauta na atividade reativa de tratamento e resposta a incidentes, conforme descrito acima e detalhado na sequência.

3.2.3 *Detalhamento dos incidentes analisados no experimento*

Existem diversos tipos de incidentes que podem ocorrer, entre os mais comuns estão: negação de serviço (DoS – *Denial of Service*), ataque de *phishing*, atividades de propagação de códigos maliciosos na rede (*worm*), invasão em computador ou rede, fraude ou tentativa de fraude, ataque de varredura de rede (*scan*), entre tantos outros. A escolha de analisar o tipo de incidente, *phishing* permite que se faça uma análise mais homogênea da base de dados.

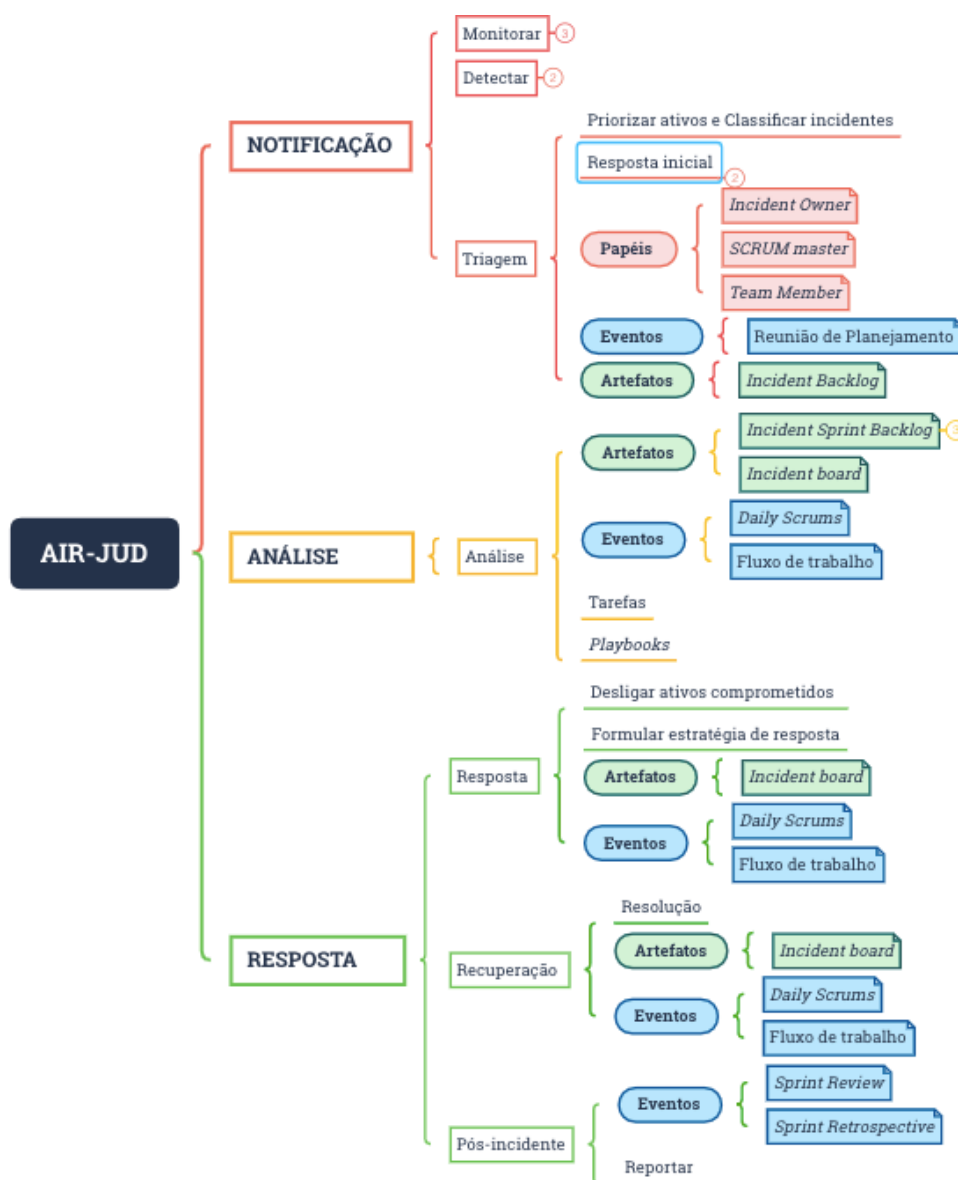
Em resumo, o trabalho proposto seguiu as seguintes diretivas:

- viii. Utilização de base de casos de incidentes de *phishing report*;

- ix. Definição de time *scrum* de resposta a incidentes dentro da equipe CLRI;
- x. Triage dos incidentes em um *Incident Backlog*;
- xi. Planejamento do *Sprint* de resolução dos incidentes;
- xii. Revisão e retrospectiva da resolução dos incidentes;
- xiii. Repetição do experimento agregando melhorias ao modelo;

A fonte de dados utilizada se baseia qualitativamente em dados reais obtidos da base de casos de incidentes de *phishing report*.

Figura 31 Mapeamento das práticas ágeis no processo de resposta a incidentes



Fonte: Resultado da pesquisa

Seguindo a ideia de utilizar no modelo dos processos de resposta a incidentes os métodos *Scrum* e *Kanban* foram usados ao longo das fases, conforme **Figura 18**. Os processos tradicionais podem ser identificados na primeira e segunda camada, com as formas em retângulo. Estes processos são, como descritos anteriormente, notificação, análise e resposta.

As práticas ágeis adaptadas podem ser vistas nas folhas da árvore, na forma de retângulo elíptico e preenchido. Os papéis da equipe *Scrum*, na cor vermelha, se encaixam na fase de Triagem. Artefatos adaptados do *Scrum*, na cor verde, podem ser utilizados nas fases de Triagem, Análise, Resposta e Recuperação. E os eventos do *Sprint* do incidente, na cor azul, se encaixa nas fases de Triagem, Análise, Resposta, Recuperação e Pós incidentes.

Seguindo essas adaptações do método ágil, mesmo utilizando modelo tradicional de tratamento de incidentes, o processo de trabalho não segue um fluxo de plano de ação linear ou cascata, mas com a definição e auto-organização da equipe ágil de resposta a incidente. A partir do *Incident Backlog* elabora-se o *Incident Sprint Backlog*, que são usados como entrada para as *Daily Scrums* até o final do *Sprint*, quando as revisões e retrospectivas ocorrem.

3.2.4 Demonstração do novo processo

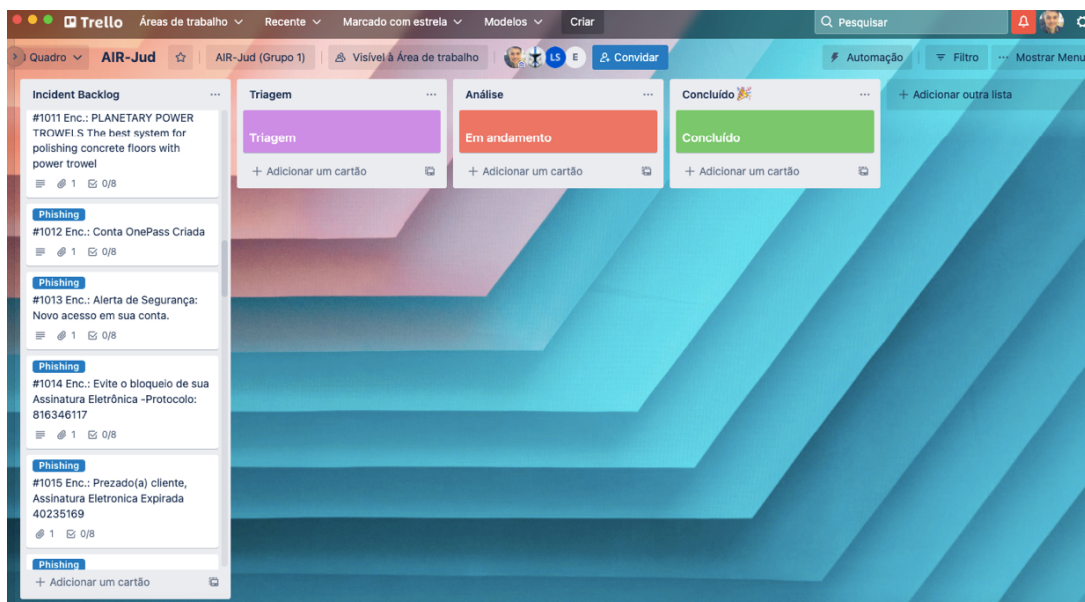
O primeiro ciclo de teste foi realizado por meio de 40 casos de incidentes de *phishing* distribuídos para um time de quatro membros da CLRI-TRF3. Uma vez definido o time *Scrum* na reunião inicial de planejamento da *Sprint*, foi estabelecido o tempo de três semanas para a conclusão do *Sprint*, uma reunião por dia com os membros e a divisão dos 40 casos para atribuição de um caso para cada membro.

Foi utilizada a ferramenta *Trello* para gerenciar o quadro *Kanban*, permitindo colaborar, organizar fluxos de trabalho e acompanhar o progresso de maneira visual. Cada notificação de *phishing* foi recebida como um incidente para ser analisado, passando previamente por uma triagem. Os incidentes foram inicialmente distribuídos no *Kanban board*, ilustrados na **Figura 19**. As fases das atividades foram classificadas como:

- vi. *Incident Backlog*, por onde os incidentes foram primariamente alocados;
- vii. Triagem ou *Incident Sprint Backlog*, na qual os incidentes foram atribuídos a cada membro da equipe;
- viii. Análise, fase em que cada membro executa a análise em seu item atribuído;

- ix. Encerramento, para a realização de parte das tarefas; e
- x. Concluído, para depositar os casos já resolvidos.

Figura 32 Quadro *Kanban* inicial com os incidentes a serem analisados



Fonte: Resultado da pesquisa

Cada quadro do *Kanban* representa um caso e foi estabelecido uma sequência de atividades para cada um deles, conforme ilustrado na **Figura 20**. As tarefas para este tipo de análise de suspeita de *phishing* podem ser descritas da seguinte maneira:

- ix. Analisar o cabeçalho do e-mail suspeito;
- x. Descobrir o nome e IP do servidor que originou o e-mail;
- xi. Descobrir a conta de contato (ABUSE) do servidor que originou o e-mail;
- xii. Pesquisar a reputação do servidor (IP) que originou o e-mail;
- xiii. Analisar links e arquivos anexados ao e-mail suspeito;
- xiv. Notificar servidor que originou o e-mail;
- xv. Bloquear internamente o IP e/ou domínio que estiverem comprometidos;
- xvi. Responder ao usuário que reportou o e-mail suspeito;

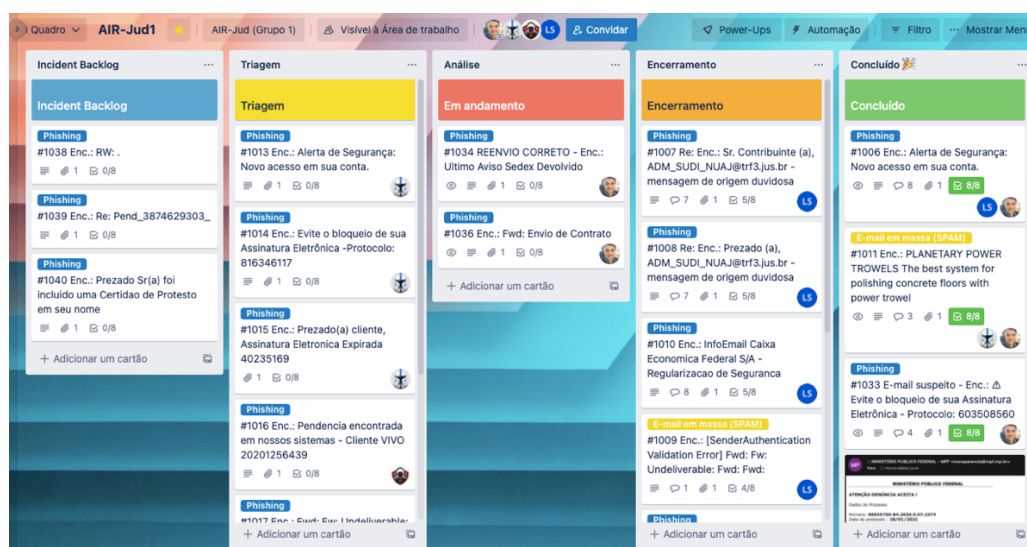
As tarefas de i a v são geralmente realizadas na fase de Análise, enquanto o restante, da vi a viii são tarefas da fase de Encerramento. Como os times *Scrum* são auto-organizáveis, eles podem decidir que as tarefas possam ser realizadas por um ou mais membro.

Figura 33 Exemplo de atividades constantes em cada item de *Incident Backlog*.



Fonte: Resultado da pesquisa

Figura 34 Quadro *Kanban* após autoajuste definido pelo time *Scrum*

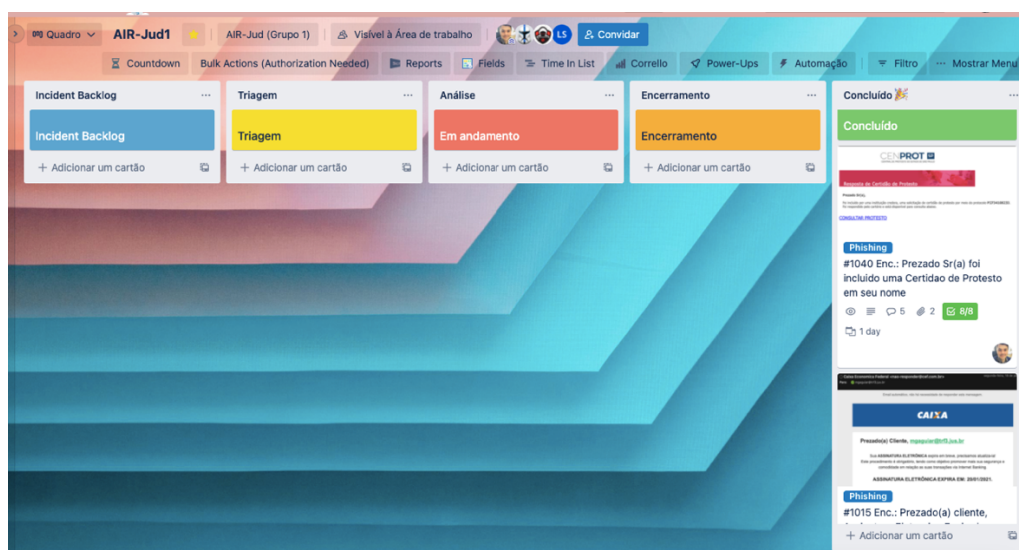


Fonte: Resultado da pesquisa

Considerando a capacidade de autoajustes e adaptações dos times *Scrum*, o quadro *Kanban* foi adaptado para acolher mais a fase Encerramento, mostrado na **Figura 21**.

No final da *Sprint*, os casos foram todos solucionados, deixando o quadro *Kanban* conforme **Figura 22**. O próximo passo é a revisão e retrospectiva do *Sprint* para obter melhorias para o planejar e execução do próximo *Sprint*, assim como prescreve o *Scrum* originalmente.

Figura 35 Resultado do quadro *Kanban* após o ciclo da *Sprint*



Fonte: Resultado da pesquisa

3.3 Etapa de avaliação

Esta fase visa medir quão bem um artefato sustenta uma solução para o problema, comparando os objetivos com os resultados observados do uso dos artefatos na demonstração.

A partir da utilização dos princípios ágeis utilizados nos processos de resposta a incidentes de segurança, o guia de avaliação do processo foi direcionado aos partícipes: gestores de segurança da informação; integrantes de times de resposta a incidentes de segurança da informação; e pesquisadores de segurança da informação.

O método contempla ainda entrevistas semiestruturadas com respondentes dos questionários que assim aceitaram participações. Após a realização do experimento, os participantes responderam a entrevista semiestruturada para avaliar o artefato produzido.

Os times de resposta a incidentes resultaram em três respostas de avaliação interna, enquanto os outros dois de avaliação externa. Todos os times utilizaram o tipo de incidente de *Phishing* no experimento. A média foi de 29 incidentes selecionados, com duração média de 16 dias. Quanto aos participantes, o número médio foi de três pessoas por time. A duração média da reunião diária (*Daily Scrum*) foi de aproximadamente meia hora por dia.

3.3.1 Avaliação interna

O **Quadro 11** apresenta o perfil da formação acadêmica e experiência profissional dos avaliadores internos.

Quadro 17 Perfil dos avaliadores internos

Avaliador	Formação e Experiência profissional na área e em CSIRTs
<i>Avaliador Interno 1</i>	Bacharel em Física; Mestre em Física Teórica; Pós-Graduado em Engenharia de Sistemas. Profissional de TI por 11 anos; Analista Judiciário da área de segurança há um ano.
<i>Avaliador Interno 2</i>	Tecnólogo em Processamento de Dados, e Pós-Graduado em Desenvolvimento de Sistemas e Segurança. Profissional de TI como Técnico Judiciário por 28 anos; supervisor de Internet e Intranet por sete anos; Diretor da Divisão de Sistemas Web por seis anos e membro da CLRI há três anos.
<i>Avaliador Interno 3</i>	Bacharel em Ciência da Computação e Pós-Graduado em Governança de TI; formação em <i>Fundamentals of Incident Handling</i> e <i>Advanced Topics of Incident Handling</i> . Profissional de TI por 22 anos; Analista Judiciário da área de redes e segurança há oito anos; membro da CLRI há oito anos

Fonte: Resultado da Pesquisa

Sobre a avaliação interna dos papéis, artefatos e eventos, os resultados médios são apresentados na **Tabela 3**, em que as variações de respostas eram: 1 - Discordo plenamente; 2 - Discordo mais do que concordo; 3 - Não concordo, nem discordo; 4 - Concorde mais do que discordo; 5 - Concorde plenamente.

Tabela 9 Resultado das médias das avaliações INTERNAS dos papéis.

Grupo	Item	Avaliação média da relevância do item no contexto da adaptação do processo de resposta a incidentes	Avaliação média da melhoria obtida pela inclusão do item comparando ao método tradicional
<i>Papel</i>	<i>Incident Owner</i>	5,00	5,00
	<i>SCRUM Master</i>	5,00	5,00
	Membro da equipe	5,00	5,00
<i>Artefato</i>	<i>Incident Backlog</i>	4,67	4,67
	<i>Incident Sprint Backlog</i>	4,67	4,67
	<i>Kanban Board</i>	5,00	5,00
<i>Eventos</i>	Planejamento do <i>Sprint</i>	5,00	4,67
	Reunião Diária	5,00	5,00
	Revisão do <i>Sprint</i>	5,00	4,67
	Retrospectiva do <i>Sprint</i>	4,67	5,00
	Ciclo <i>Sprint</i>	4,67	4,67

Fonte: Resultado da Pesquisa

Os resultados das avaliações internas indicam que existe relevância e indicação de melhorias tendo em vista que as notas médias ficaram entre 4,67-5, ou seja, uma concordância com as afirmações indicadas na entrevista semiestruturada.

3.3.2 Avaliação externa

O **Quadro 12** apresenta o perfil da formação acadêmica e experiência profissional dos avaliadores internos.

Quadro 18 Perfil dos avaliadores externos

Avaliador	Formação e Experiência profissional na área e em CSIRTs
<i>Avaliador Interno 1</i>	Graduação em TI, Pós-graduação em <i>Data Science</i> , formação em <i>Fundamentals of Incident Handling</i> e <i>Advanced Topics of Incident Handling</i> . Consultor de Segurança da Informação por cinco anos; Engenheiro de segurança por quatro anos; Infosec Tech Manager há três anos;
<i>Avaliador Interno 2</i>	Graduação em Administração de Empresas; Especialização em Análise de Sistemas, MBA Executive em Gestão Empresarial. Analista de Sistemas por dez anos e onze meses; analista de negócio em TI por um ano e nove meses; especialista em projetos por dois anos e três meses; <i>product owner</i> há três anos

Fonte: Resultado da Pesquisa

Sobre a avaliação externa os resultados médios são apresentados na **Tabela 10**.

Tabela 10 Resultado das médias das avaliações EXTERNAS dos papéis.

Grupo	Item	Avaliação média da relevância do item	Avaliação média da melhoria obtida pela inclusão do item
<i>Papéis</i>	<i>Incident Owner</i>	5,00	5,00
	<i>SCRUM Master</i>	4,00	4,00
	Membro da equipe	4,00	4,00
<i>Artefatos</i>	<i>Incident Backlog</i>	5,00	4,50
	<i>Incident Sprint Backlog</i>	4,00	4,00
	<i>Kanban Board</i>	4,50	4,50
<i>Eventos</i>	Planejamento do <i>Sprint</i>	5,00	5,00
	Reunião Diária	5,00	5,00
	Revisão do <i>Sprint</i>	4,00	4,00
	Retrospectiva do <i>Sprint</i>	5,00	5,00
	Ciclo <i>Sprint</i>	4,50	5,00

Fonte: Resultado da Pesquisa

Os resultados das avaliações externas também indicam que existe relevância e contém melhorias tendo em vista que as notas médias ficaram entre 4-5, ou seja, uma concordância com as afirmações indicadas na entrevista semiestruturada.

3.4 Comunicação

A Seção 2.6 traz a descrição das atividades da etapa 6 conforme a metodologia DSRM.

Com a conclusão e formalização desta dissertação, com as aprovações e formalização do Programa de Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos, sob a coordenação do Professor Doutor Napoleão Verardi Galeale, do Centro Estadual de Educação Tecnológica Paula Souza, o pesquisador desenvolverá o processo de comunicação dos resultados submetidos para publicações de pesquisas acadêmicas, para que pesquisadores e profissionais envolvidos no contexto deste estudo, conheçam a importância do problema, a utilidade e novidade do artefato, do que se propõe a resolver do problema, o rigor de seu design e sua eficácia em equipes de resposta a incidentes de segurança da informação, e que possa proporcionar contribuições para futuras iterações de pesquisas.

4 CONTRIBUIÇÕES PARA A ORGANIZAÇÃO E/OU SOCIEDADE

Esta pesquisa começa com a seguinte questão que é “*Como os princípios ágeis podem ser aplicados nos processos de resposta a incidentes de segurança da informação no Poder Judiciário?*”. Assim, foi realizada uma pesquisa bibliométrica seguida por uma revisão da literatura que procurou apresentar os achados sobre o tema nas bases de dados científicas. Além disso, a adaptação e avaliação do processo proposto foi realizada.

Em sua fundamentação teórica foi apresentado o escopo sobre o tema investigado, incluindo a justificativa da pesquisa indicada com a informatização do Poder Judiciário brasileiro, a importância dos times de resposta a incidentes de segurança da informação e as práticas ágeis utilizadas no contexto da resposta a ciberincidentes.

Para a realização desta pesquisa seguiu-se a metodologia do DSRM, que compreende seis fases de desenvolvimento, os quais foram discutidos no Capítulo 2, na teoria, e no Capítulo 3, na prática.

O objetivo principal foi atingido tendo em vista que este trabalho examinou como adaptar e avaliar um processo baseado na aplicação dos princípios ágeis nos processos de tratamento e resposta de incidentes de segurança da informação no Poder Judiciário.

Os objetivos específicos foram alcançados, conforme lista abaixo:

- vii. O problema e motivação foram identificados por meio do levantamento bibliométrico e revisão da literatura recente e da identificação dos problemas e questões em processos de resposta a incidentes e da aderência à questão da pesquisa, conforme apresentado nas Seções 1.1 a 1.4.;
- viii. Os objetivos da solução para melhoria nos processos de um CSIRT do Poder Judiciário foram definidos, descrito na introdução e nas Seções 1.1 a 1.4;
- ix. A adaptação dos processos de um CSIRT do Poder Judiciário foi projetada e desenvolvida por meio da identificação dos princípios e práticas do método ágil, por intermédio do processo AIR-Jud;
- x. A utilização de práticas ágeis nos processos de resposta a incidentes de segurança de informação em uma instituição do Poder Judiciário foi demonstrada, por meio da aplicação do processo AIR-Jud no CSIRT do TRF3;

- xi. O processo foi avaliado com os atores envolvidos, por intermédio de entrevistas semiestruturadas com avaliadores internos e externos;
- xii. Os resultados da pesquisa foram comunicados por meio desta dissertação, do relatório técnico e do futuro artigo a ser produzido;

Para demonstrar que a solução pode ser usada para atingir os objetivos propostos, a abordagem foi aplicada em um projeto real de resposta a incidentes. Conforme observado no Capítulo 3, um ciclo de utilização dos princípios ágeis na resposta a incidentes de segurança do Poder Judiciário trouxe alguns benefícios, como o aprimoramento dos processos de resposta a incidentes e a melhor integração da equipe.

Para avaliação da metodologia, foram realizadas entrevistas com especialistas em segurança da informação que avaliaram a viabilidade da solução, bem como a existência de melhorias em relação aos processos tradicionais de resposta a incidentes.

Os resultados da avaliação do processo proposto foram realizados após a realização do experimento com um pequeno grupo de incidentes em um período curto. As avaliações apresentaram a existência de relevância e a indicação de melhorias nos processos, considerando que as notas médias ficaram entre 4-5, ou seja, uma concordância com as afirmações indicadas na entrevista semiestruturada.

As limitações encontradas na realização da pesquisa devem ser consideradas tendo em vista a pandemia de COVID-19 que inicialmente paralisou atividades e limitou os acessos à recursos, pessoas, serviços, entre outros. Além disso, o processo adaptado proposto para atender os setores de segurança da informação do poder judiciário somente pode ser testado no TRF3 e ainda com a limitação de ter os acessos indisponíveis devido ataque cibernético ocorrido durante o desenvolvimento do trabalho. Desse modo, novos testes do experimento poderiam ser realizados para a proposição de novas melhorias e aperfeiçoamento. Também poderiam ser testados em diversos tipos de incidentes, não apenas para os casos de *phishing* e *spear phishing*.

Como trabalhos futuros podem ser sugeridas a realização da aplicação da pesquisa em equipes de resposta a incidentes de segurança da informação de outras áreas como o setor bancário, universidades, comércio, energia, indústrias e demais setores produtivos.

REFERÊNCIAS

AGÊNCIA BRASIL. **Tribunal de Justiça gaúcho é alvo de ataque hacker**. Disponível em: <<https://agenciabrasil.ebc.com.br/justica/noticia/2020-11/tribunal-de-justica-gaucha-e-alvo-de-ataque-hacker>>. Acesso em: 4 mar. 2022a.

AGÊNCIA BRASIL. **Superior Tribunal de Justiça reinicia hoje sessões virtuais | Agência Brasil**. Disponível em: <<https://agenciabrasil.ebc.com.br/justica/noticia/2020-11/superior-tribunal-de-justica-reinicia-hoje-sessoes-virtuais>>.

AGÊNCIA BRASIL. **STJ é alvo de ataque hacker e Polícia Federal investiga o sistema**. Disponível em: <<https://agenciabrasil.ebc.com.br/justica/noticia/2020-11/stj-e-alvo-de-ataque-de-hacker-e-policia-federal-investiga-o-sistema>>. Acesso em: 5 mar. 2022c.

AHMAD, A.; HADGKISS, J.; RUIGHAVER, A. B. **Incident Response Teams-Challenges in Supporting the Organisational Security Function**. [s.l: s.n.].

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, 2012b.

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

AMORIM, A. C. et al. **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.

BAGUETE. **TRT4 sofre ataque hacker**. Disponível em: <<https://www.baguete.com.br/noticias/05/10/2021/trt4-sofre-ataque-hacker>>. Acesso em: 4 mar. 2022.

BECK, K. et al. **Manifesto for Agile Software Development**. Disponível em: <<http://agilemanifesto.org/>>. Acesso em: 22 ago. 2020.

BRAS, J. C.; RIBEIRO, R. Business Continuity and Disaster Recovery: An Overview, Trends and Challenges. **13th INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS & TECHNOLOGY MANAGEMENT - CONTECSI**, p. 1698–1719, jun. 2016.

CERT.BR. **Tradução: CERT/CC CSIRT FAQ**. Disponível em: <https://www.cert.br/certcc/csirts/csirt_faq-br.html>. Acesso em: 26 fev. 2022a.

CERT.BR. **Estatísticas dos Incidentes Reportados ao CERT.br**. Disponível em: <<https://www.cert.br/stats/incidentes>>. Acesso em: 26 fev. 2022b.

CICHONSKI, P. et al. NIST Special Publication 800-61 Rev 2: Computer Security Incident Handling Guide. **National Institute of Standards and Technology (NIST)**, 2012.

CNJ. **Justiça em Números 2021**. [s.l: s.n.]. Disponível em: <www.cnj.jus.br>.

CNJ. **Juízo 100% Digital tudo o que você precisa saber**. Disponível em: <www.cnj.jus.br>.

CNJ. **Nova estratégia nacional atua contra ataques cibernéticos no Judiciário - Portal CNJ**. Disponível em: <<https://www.cnj.jus.br/cnj-regulamenta-estrategia-nacional-contra-ataques-ciberneticos-ao-judiciario/>>. Acesso em: 9 mar. 2022c.

CNJ. **Exigência do uso de processo eletrônico deve acelerar extinção dos processos em papel - Portal CNJ**. Disponível em: <<https://www.cnj.jus.br/exigencia-do-uso-de-processo-eletronico-deve-acelerar-desparecimento-dos-processos-em-papel/>>. Acesso em: 9 mar. 2022.

COHEN, D.; LINDVALL, M.; COSTA, P. An Introduction to Agile Methods. **Advances in Computers**, v. 62, n. C, p. 1–66, 2004.

CONBOY, K.; FITZGERALD, B. Toward a Conceptual Framework of Agile Methods: A Study of Agility in Different Disciplines. **WISER**, 2004.

CONJUR. **TRF-3 recebe denúncia contra hacker que invadiu sistema do tribunal**. Disponível em: <<https://www.conjur.com.br/2021-jul-13/trf-recebe-denuncia-hacker-invadiu-sistema-tribunal>>. Acesso em: 4 mar. 2022a.

CONJUR. **TJ do Rio Grande do Sul volta a ser alvo de ataque hacker**. Disponível em: <<https://www.conjur.com.br/2021-abr-30/tj-rio-grande-sul-volta-alvo-ataque-hacker>>. Acesso em: 4 mar. 2022b.

COOPER, R. G.; SOMMER, A. F. Agile-Stage-Gate: New idea-to-launch method for manufactured new products is faster, more responsive. **Industrial Marketing Management**, v. 59, p. 167–180, 1 nov. 2016.

DE JESUS, I. R. D.; COSTA, H. G. A Nova Gestão Pública como indutora das atividades de Engenharia de Produção nos órgãos públicos. **Production**, v. 24, n. 4, p. 887–897, 2014.

DENNING, S. How To Make The Whole Organization Agile. **Forbes**, 2015.

DINGSØYR, T. et al. A decade of agile methodologies: Towards explaining agile software development. **Journal of Systems and Software**, v. 85, n. 6, p. 1213–1221, 2012.

DOROFEE, A. et al. **Incident Management Capability Assessment**. [s.l: s.n.]. Disponível em: <<http://www.sei.cmu.edu>>.

FOLHA. **Ataque hacker ao STJ não é sinal de ameaça à segurança das urnas - 15-11-2020 - Poder - Folha**. Disponível em: <<https://www1.folha.uol.com.br/poder/2020/11/ataque-hacker-ao-stj-nao-e-sinal-de-ameaca-a-seguranca-das-urnas.shtml>>. Acesso em: 4 mar. 2022.

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

G1. **Supremo investiga suposto ataque hacker a sistema da Corte | Política | G1**. Disponível em: <<https://g1.globo.com/politica/noticia/2021/05/07/supremo-investiga-tentativa-de-ataque-hacker-a-sistema-da-corte.ghml>>. Acesso em: 5 mar. 2022.

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. **20th Americas Conference on Information Systems (AMCIS 2014)**, 2014.

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

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

HE, Y. et al. Agile incident response (AIR): Improving the incident response process in healthcare. **International Journal of Information Management**, v. 62, 1 fev. 2022.

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

HEVNER, A.; CHATTERJEE, S. **Design science research in information systems**. [s.l.] Springer, 2010. v. 22

HEVNER, A. R. et al. **DESIGN SCIENCE IN INFORMATION SYSTEMS RESEARCH** **1Design Science in IS Research MIS Quarterly**. [s.l: s.n.].

IMONIANA, J. O. Validity of information security policy models. **Transinformação**, v. 16, n. 3, p. 263–274, 2004.

KLIEM, R. L.; RICHIE, G. D. **Business Continuity Planning A Project Management Approach**. Boca Raton, FL: CRC Press, 2015.

LACERDA, D. P. et al. Design Science Research: método de pesquisa para a engenharia de produção Design Science Research: a research method to production engineering. **Gestão & Produção**, v. 20, n. 4, p. 741–761, 2013.

LIU, X. et al. Secure Internet of Things (IoT)-Based Smart-World Critical Infrastructures: Survey, Case Study and Research Opportunities. **IEEE Access**, v. 7, p. 79523–79544, 2019.

MAJ, M.; REIJERS, R.; STIKVOORT, D. Good Practice Guide for Incident Management. **European Network and Information Security Agency (ENISA)**, 2010.

MARCH, S. T.; SMITH, G. F. **Design and natural science research on information technologyDecision Support Systems**. [s.l: s.n.].

MOHER D et al. Principais itens para relatar Revisões sistemáticas e Meta-análises: A recomendação PRISMA. **Epidemiologia e Serviços de Saúde**, v. 24, n. 2, p. 335–342, jun. 2015.

NASEER, A. et al. 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.

PEFFERS, K. et al. A design science research methodology for information systems research. **Journal of Management Information Systems**, v. 24, n. 3, p. 45–77, dez. 2007.

REIS, L.; AMARAL, L. Gestão de Riscos num contexto de Planeamento da Contingência e Recuperação. **Atas da Conferência da Associação Portuguesa de Sistemas de Informação**, v. 3, n. 3, 2016.

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

RUEFLE, R. et al. Computer Security Incident Response Team Development and Evolution. **IEEE Security & Privacy**, v. 12, n. 5, p. 16–26, 2014.

SAMONAS, S.; COSS, D. The CIA strikes back: redefining confidentiality, integrity and availability in security. **Journal of Information System Security - JISSec**, v. 10, n. 3, p. 21–45, 2014.

SCHWABER, K.; SUTHERLAND, J. **The Scrum Guide™ The Definitive Guide to Scrum: The Rules of the Game**. [s.l.: s.n.].

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

SMITH, R. et al. The Agile Incident Response for Industrial Control Systems (AIR4ICS) framework. **Computers and Security**, v. 109, 1 out. 2021.

SNEDAKER, S. **Business Continuity and Disaster Recovery Planning for IT Professionals**. 2. ed. [s.l.] Syngress, 2014.

STEFANI, C. E.; FEITOSA, M. D. COLABORAÇÃO NO DESENVOLVIMENTO ÁGIL DE SOFTWARE: UM ESTUDO A PARTIR DA VISÃO DOS PARTICIPANTES DO PROCESSO PRODUTIVO. 2019.

STIKVOORT, D. SIM3 : Security Incident Management Maturity Model. **Open CSIRT Foundation (OCF)**, 2015.

STJ. **Comunicado da Presidência do STJ**. Disponível em: <<https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/11112020-Comunicado-da-Presidencia-do-STJ.aspx>>. Acesso em: 4 mar. 2022.

SYMANTEC. **ISTR Internet Security Threat Report Volume 24**. [s.l: s.n.]. Disponível em: <<https://docs.broadcom.com/docs/istr-24-2019-en>>. Acesso em: 26 fev. 2022.

TASHI, I.; GHERNAOUTI-HÉLIE, S. **Information Security Evaluation A Holistic Approach**. Boca Raton, FL: EPFL Press, 2011.

TERRA. **Depois de STJ, TJRS é alvo de ataque hacker**. Disponível em: <<https://www.terra.com.br/noticias/brasil/politica/depois-de-stj-t>>.

UOL. **Fachin: Justiça Eleitoral pode estar sob ataque hacker, inclusive da Rússia**. Disponível em: <<https://www.uol.com.br/eleicoes/2022/02/16/entrevista-edson-fachin-stf-tse-eleicoes.htm>>. Acesso em: 2 mar. 2022.

ANEXO I – DETALHAMENTO DO PRODUTO (CAPES)

RELATÓRIO TÉCNICO CONCLUSIVO¹

Organização: Centro Estadual de Educação Tecnológica Paula Souza (CEETEPS)

PPG: Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos

Autores:

Aluno: Rodrigo Silva Sotolani

Professor Orientador: Prof. Dr. Napoleão Verardi Galegale

Demais Autores/Organização:

Dissertação vinculada (título): Princípios Ágeis na Resposta a Incidentes de Segurança da Informação

Data da defesa: 24/06/2022

Setor beneficiado com o projeto de pesquisa, realizado no âmbito do PPG: Segurança da Informação

A produção técnica é constituída pelo próprio produto?

☒ Sim

☐ Não. Qual o grau contribuição diretamente aplicada ao produto:

☐ Excepcional; ☐ Incremental; ☐ Residual

Descrição do produto e finalidade (até 50 palavras): O produto deste trabalho, AIR-Jud, abreviação de *Agile Incident Response* para o Judiciário, tem a finalidade de adaptar processos tradicionais de resposta a incidentes de segurança com princípios ágeis dos métodos *Scrum* e *Kanban* e visa promover melhorias nos processos de resposta a incidentes de um órgão do Poder Judiciário.

Avanços tecnológicos / grau de novidade:

☐ Produção com alto teor inovativo: Desenvolvimento com base em conhecimento inédito;

☒ Produção com médio teor inovativo: Combinação de conhecimentos pré-estabelecidos;

☐ Produção com baixo teor inovativo: Adaptação de conhecimento existente;

☐ Produção sem inovação aparente: Produção técnica.

Conexão com a Pesquisa:

PPG: Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos

Projeto de pesquisa vinculado à produção: Gestão Estratégica da Tecnologia da Informação

Linha de pesquisa vinculada à produção: Sistemas de Informação e Tecnologias Digitais

☐ Projeto isolado, sem vínculo com o PPG

Conexão com a produção científica

a) Título: O método *design science research* e os fatores críticos para sua aplicação na pesquisa de engenharia de produção.

¹ Definição: Texto elaborado de maneira concisa, contendo informações sobre o projeto/atividade, realizada. Indica em seu conteúdo a relevância dos resultados e conclusão em termos de impacto social e/ou econômico e a aplicação do conhecimento produzido. Não se aplica a relatório de projeto de pesquisa financiados por agências de fomento

Periódico: V Simpósio Acadêmico de Engenharia de Produção – SAEPRO (EEL- USP)

Outros dados: Lorena, Editora Even3, Data de Publicação 22/10/2021, DOI: 10.29327/138386

b)Título: Princípios ágeis na resposta a incidentes de segurança da informação de sistemas produtivos: uma bibliometria.

Evento: XXVIII SIMPEP – XXVIII Simpósio de Engenharia de Produção

Anais: Bauru/SP, 10 a 12/11/2021, ISSN 1809-7189

c)Título: Problemas e questões nos processos tradicionais de resposta a incidentes de segurança da informação.

Evento: XVIII SEGeT – Simpósio de Excelência em Gestão e Tecnologia

Anais: nos dias 1 e 2/12/2021, ISSN 1807-409X

d)Título: Identificação de critérios para a utilização de análise multicritério no tratamento de vulnerabilidades de segurança da informação na indústria 4.0.

Evento: IX SINGEP – Simpósio Internacional de Gestão, Projetos, Inovação e Sustentabilidade.

Anais: INSS 2317-8302

e)Título: Princípios Ágeis na Resposta a Incidentes de Segurança nos Sistemas Produtivos: uma Revisão Sistemática.

Evento: XVI Simpósio/Workshop do Centro Paula Souza.

Anais: dias 24 e 25/11/2021, ISSN 2675-8474

Situação atual da Produção:

Coparticipante:

Nome da Empresa/Organização objeto da pesquisa: Comissão Local de Resposta a Incidentes de Segurança da Informação do Tribunal Regional Federal da 3ª Região

Endereço: Av. Paulista 1842. Cidade: São Paulo Estado: SP

Contato na Empresa/Organização objeto da pesquisa:

Nome: Eduardo Carvalho Pereira Cargo: Analista Judiciário Presidente da CLRI/TRF3 e-mail: eduarper@trf3.jus.br Tel (11) 3012-1000

Aplicabilidade da Produção Tecnológica

Descrição da Abrangência realizada: (até 50 palavras) O produto teve abrangência realizada no âmbito de um órgão do Poder Judiciário, em um time de resposta a incidentes de segurança da informação.

Descrição da Abrangência potencial: (até 50 palavras) O produto tem o potencial de ser utilizado por qualquer equipe de resposta a incidentes de segurança da informação de qualquer organização.

Descrição da Replicabilidade: (até 50 palavras) O produto pode ser replicado, com as devidas adaptações, por qualquer equipe de resposta a incidentes de segurança da informação de qualquer organização.

Documentos Anexados (em PDF)

(x) Declaração emitida pela Empresa/Organização objeto da pesquisa.

ANEXO II – DECLARAÇÃO EMITIDA PELA EMPRESA/ORGANIZAÇÃO OBJETO DA PESQUISA

DECLARAÇÃO

Eu, Eduardo Carvalho Pereira, servidor público federal, na qualidade de Presidente da Comissão Local de Resposta a Incidentes de Segurança da Informação do Tribunal Regional Federal da 3ª Região – CLRI/TRF3, certifico a pertinência do Relatório Técnico sobre a aplicação da pesquisa intitulada “Princípios Ágeis na Resposta a Incidentes de Segurança da Informação” desenvolvida pelo então mestrando Rodrigo Silva Sotolani, também integrante da CLRI/TRF3.

O trabalho em estudo foi aplicado em um grupo de incidentes de segurança da informação visando avaliar a adaptação da utilização de princípios ágeis nos tradicionais processos de resposta a incidentes, chamado de AIR-Jud. Os resultados alcançados com a sua utilização se mostraram promissores e apresentaram visíveis melhorias nos tratamentos e respostas aos incidentes analisados ao utilizar os métodos do Scrum e Kanban. O processo AIR-Jud pode ter potencial de ser uma ferramenta útil não somente para os órgãos públicos do judiciário, mas também para que demais organizações possam tratar e responder a incidentes de maneira mais organizada e célere.

São Paulo, 13 de agosto de 2022



Eduardo Carvalho Pereira