RESPOSTA A INCIDENTES CIBERNÉTICOS EM SISTEMAS CIBER-FÍSICOS: ESTADO DA ARTE E ANÁLISE DE UM CASO NO SETOR ELÉTRICO BRASILEIRO

Wesdres de Santana Teixeira

Dissertação de Mestrado apresentada ao Programa de Pós-graduação em Engenharia de Produção, COPPE, da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Engenharia de Produção.

Orientador: Tharcisio Cotta Fontainha

Rio de Janeiro

28/02/2024

RESPOSTA A INCIDENTES CIBERNÉTICOS EM SISTEMAS CIBER-FÍSICOS: ESTADO DA ARTE E ANÁLISE DE UM CASO NO SETOR ELÉTRICO BRASILEIRO

DISSERTAÇÃO SUBMETIDA AO CORPO DOCENTE DO INSTITUTO ALBERTO LUIZ COIMBRA DE PÓS-GRADUAÇÃO E PESQUISA DE ENGENHARIA (COPPE) DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM CIÊNCIAS EM ENGENHARIA DE PRODUÇÃO.

Examinada por:

_____

Prof. Tharcísio Cotta Fontainha, D.Sc.

_____

Prof. , D.Sc.

_____

Prof. , D.Sc.

RIO DE JANEIRO, RJ - BRASIL

FEVEREIRO DE 2024

Teixeira, Wesdres de Santana

Resposta a incidentes cibernéticos em sistemas ciber-físicos: análise de um caso no Setor Elétrico Brasileiro/ Wesdres de Santana Teixeira. – Rio de Janeiro: UFRJ/COPPE, 2024.

XIII, 140 p.: il.; 29,7 cm.

Orientador: Tharcisio Cotta Fontainha

Dissertação (mestrado) – UFRJ/ COPPE/ Programa de Engenharia de Produção, 2024.

Referências Bibliográficas: p. 114-122.

1. Segurança Cibernética. 2. Sistemas Ciber-Físcios. 3. Resposta a Incidentes Cibernéticos. 4. Operação de Redes Elétricas I. Fontainha, Tharcisio Cotta. II. Universidade Federal do Rio de Janeiro, COPPE, Programa de Engenharia de Produção. III. Título.

:

DEDICATÓRIA

A trajetória é longa e difícil.
Tenho a sorte de ser cercado por pessoas que sempre me apoiaram com amor.
Dedico essa dissertação a todos que acreditaram e que tornam minha vida feliz.

AGRADECIMENTOS

Primeiramente agradeço aos meus pais, José e Roseli. Sei o quanto eles se dedicaram e se esforçaram para que seu filho conseguisse trilhar esse caminho. Sem isso, eu não estaria compartilhando o sentimento de felicidade que tenho hoje por mais uma conquista. O amor e apoio deles foram fundamentais e para sempre os terei como referência em minha vida.

Agradeço aos meus irmãos William e Gabriela, que sempre estiveram juntos comigo e sabem o quanto tenho orgulho deles. A dedicação e esforço deles também é uma inspiração para mim e contribui para o que sou e para o que serei.

Agradeço à Nathália, minha companheira e esposa, por estar há tanto tempo ao meu lado, por sempre acreditar no meu potencial, me ouvir, me entender, por compartilhar as alegrias e me apoiar nos momentos mais difíceis. Sua atenção, carinho e alegria foram fundamentais para que eu conseguisse chegar até aqui.

Agradeço ao meu ex-gestor Antônio Carlos, por ter me oferecido a oportunidade e incentivado ingresso no programa de mestrado. Agradeço aos meus ex-colegas de trabalho e hoje amigos, Leonardo, Alessandra. Ao Leo, por ter me encorajado e sempre estar disponível para discutir e me auxiliar durante a trajetória acadêmica. À Alessandra, responsável também por me auxiliar e colaborar com seus contatos, para que eu conseguisse concretizar o estudo de caso.

Agradeço ao meu orientador Tharcisio Fontainha, por ter oferecido oportunidade de ingressar e fazer parte da sua equipe de orientandos, por toda atenção, motivação e auxílio. Nosso grupo é privilegiado por ter você como orientador. Aproveito e agradeço a todos os colegas do CEPED que de alguma forma contribuíram e me ajudaram ao longo desse caminho.

Agradeço também a todos os profissionais que disponibilizaram parte de seu tempo e contribuíram com sua experiência sobre o tema, em especial ao Geraldo, por ter compartilhado maior parte da atenção e conhecimento técnico sobre o tema.

Por fim, agradeço à banca examinadora por dedicar seu tempo e conhecimento para avaliar o trabalho e me auxiliar em minha formação acadêmica. Agradeço a também a todos que se interessam pelo tema e que de alguma forma possam prosseguir com o

desenvolvimento de trabalhos futuros, ou utilizar os resultados para a promoção da segurança cibernética dos de Sistemas Ciber-Físicos

.

Resumo da Dissertação apresentada à COPPE/UFRJ como parte dos requisitos necessários para a obtenção do grau de Mestre em Ciências (M.Sc.)

RESPOSTA A INCIDENTES CIBERNÉTICOS EM SISTEMAS CIBER-FÍSICOS: ESTADO DA ARTE E ANÁLISE DE UM CASO NO SETOR ELÉTRICO BRASILEIRO

Wesdres de Santana Teixeira

Fevereiro/2024

Orientador: Tharcisio Cotta Fontainha

Programa: Engenharia de Produção

Os Sistemas Ciber-Físicos (CPS) são sistemas responsáveis por conectar dispositivos físicos ao espaço cibernético. A segurança cibernética dos CPS é uma das principais preocupações que emergem em um cenário de alta conectividade e uso de infraestruturas críticas baseadas nesses sistemas, utilizadas para manutenção de serviços essenciais para sociedade. Nesse contexto, esta pesquisa tem como objetivo identificar e compreender as principais abordagens associadas ao processo de resposta a incidentes cibernéticos em CPS. São identificadas as principais fases do processo de resposta a incidentes, as principais formas gráficas de representação do processo e os modelos de relacionamento entre *stakeholders.*

Posteriormente, são avaliadas a aderência e aplicabilidade das abordagens identificadas na literatura no cenário da operação de redes elétricas, a partir de um estudo empírico no contexto de operações de redes elétricas no Setor Elétrico Brasileiro e em setores relacionados. Os resultados indicam aderência e aplicabilidade das principais abordagens identificadas na literatura em relação à prática

Por fim, os resultados são discutidos no que tange a adoção por profissionais da área e por acadêmicos. Sugere-se uma agenda de pesquisas científicas que avancem na discussão sobre segurança cibernética de CPS

Abstract of Dissertation presented to COPPE/UFRJ as a partial fulfillment of the requirements for the degree of Master of Science (M.Sc.)

INCIDENT RESPONSE IN CYBER-PHYSICAL SYSTEMS: STATE OF ART AND ANALYSIS OF A CASE IN THE BRAZILIAN ELECTRICITY SECTOR

Wesdres de Santana Teixeira

February/2024

Advisor: Tharcisio Cotta Fontainha

Department: Production Engineering

Cyber-Physical Systems (CPS) are systems responsible for connecting physical devices to cyberspace. The CPS cybersecurity is one of the main concerns that emerge in a scenario of high connectivity and use of critical infrastructures based on these systems, used to maintain essential services for society. In this context, this research aims to identify and understand the main approaches associated with the cyber incident response process in CPS. This research identifies the main phases of the incident response process, the main graphical forms of representing the process and the models of relationships among stakeholders.

Subsequently, this research performs an empirical study in the context of power grid operations in the Brazilian Electricity Sector and in related sectors, to evaluate the adherence and applicability of the approaches identified in the literature in the scenario of power grid operations. The results indicate adherence and applicability of the main approaches identified in the literature according to practice. Finally, this research discusses the adoption of the results by professionals and academics. An agenda of scientific research is suggested to promote the discussion on CPS cybersecurity.

Sumário

1. INTRODUÇÃO 1

1.1 TEMA DE PESQUISA 1

1.2 OBJETIVOS DA PESQUISA 4

1.3 JUSTICATIVA DE PESQUISA 7

1.1 OBJETO DE ESTUDO 8

1.2 ESTRUTURA DO DOCUMENTO 9

2. MÉTODOS UTILIZADOS NA PESQUISA 10

2.1 REVISÃO SISTEMÁTICA DA LITERATURA 10

2.1.1 Planejamento da revisão 10

2.1.2 Condução da revisão 14

2.1.3 Análise 15

2.1.4 Apresentação dos resultados 19

2.2 ESTUDO DE CASO 19

3. RESPOSTA A INCIDENTES CIBERNÉTICOS EM CPS 23

3.1 ANÁLISE BIBLIOMÉTRICA DA LITERATURA 23

3.1.1 Evolução da produção científica 24

3.1.2 Análise dos artigos mais citados pela literatura 25

3.1.3 Principais termos de pesquisa 28

3.2 RESPOSTA A INCIDENTES CIBERNÉTICOS EM CPS 29

3.2.1 Setores de aplicação dos CPS 29

3.2.2 Análise dos *frameworks* sobre resposta a cibernéticos em CPS - processos e relacionamento entre stakeholders 33

3.2.3 Fases do processo de resposta a incidentes cibernéticos 39

3.2.4 Formas de representações de processos de resposta a incidentes cibernéticos em CPS 47

3.2.5 Representações da relação de Stakeholders no processo de gestão de incidentes 54

4. ESTUDO DE CASO SOBRE O PROCESSO DE RESPOSTA A INCIDENTES NO CONTEXTO DA OPERAÇÃO DE REDES ELÉTRICAS NO SEB 57

4.1 AVALIAÇÃO DO PROCESSO DE RESPOSTA A INCIDENTES CIBERNÉTICOS – NÍVEL BRASIL E SEB 58

4.1.1 Fases do processo de resposta a incidentes - Nível Brasil e SEB ... 59

4.1.2 Formas de representações do processo de resposta a incidentes.. 79

4.2 AVALIAÇÃO DO PROCESSO DE RESPOSTA A INCIDENTES NO CONTEXTO DO PROCESSO DE OPERAÇÃO DE INSTALAÇÕES DO SIN 81

4.2.1 Fases do processo de resposta a incidentes 81

4.2.2 Representações do processo de resposta a incidentes cibernéticos 97

4.3 RELACIONAMENTO ENTRE OS STAKEHOLDERS 99
5. CONTRIBUIÇÕES E PROPOSTAS DE TRABALHOS FUTUROS 108
5.1 CONTRIBUIÇÕES ACADÊMICAS E PARA PROFISSIONAIS DA ÁREA . 108
5.2 PROPOSTAS DE TRABALHOS FUTUROS 109
6. CONSIDERAÇÕES FINAIS 111
REFERÊNCIAS BIBLIOGRÁFICAS 115
APÊNDICE 1 - PROTOCOLO DE PESQUISA 121
APÊNDICE 2 – REGISTRO DAS ENTREVISTAS – ESTUDO DE CASO 126

ÍNDICE DE FIGURAS

Figura 1 - Processo de definição do tópico de pesquisa 5
Figura 2 - Processo de busca da RSL 12
Figura 3 - Resultados da condução da RSL 15
Figura 4 - Processo de criação do mapa de relação de palavras no VOSviewer 17
Figura 5 - Etapas do Estudo de Caso 20
Figura 6 - Evolução do número de publicações por ano 24
Figura 7 - Número de citações e valores atípicos (outliers) por autor 26
Figura 8 - Evolução das palavras-chave por ano 28
Figura 9 - Setores de Aplicação dos CPS 30
Figura 10 - Legislação e regulamentação associada a Segurança Cibernética 62
Figura 11 - Evolução publicação legislação e regulamentação 68
Figura 12 - Relacionamento entre stakeholders na REGIC 101
Figura 13 - Relacionamento entre stakeholders no SEB 103
Figura 14 - Relacionamento entre stakeholders - SEB e REGIC 104
Figura 15 - Notificação de incidentes - REGIC e SEB 105
Figura 16 - Instituições que compõem ou se relacionam com o SEB 121

ÍNDICE DE TABELAS

Tabela 1 - Organizações entrevistadas - Nível Brasil e SEB 21
Tabela 2 - Áreas entrevistadas na organização objeto de estudo (contexto do específico de operação de instalações do SIN)..... 22
Tabela 3 - Publicações em periódicos 24
Tabela 4 - Número de artigos classificados como outliers 25
Tabela 5 - Cálculo estratificado de outliers por grupo em intervalos de tempo 27
Tabela 6 - Fases do processo de resposta a incidentes mais abordadas 42

ÍNDICE DE QUADROS

Quadro 1 - Seleção das palavras-chave 13
Quadro 2 - Critérios de inclusão e exclusão para inspeção dos artigos 14
Quadro 3 - Período de realização da coleta..... 16
Quadro 4 - Síntese do procedimento de análise da pesquisa bibliográfica 16
Quadro 5 - Palavras relacionadas à metodologia de pesquisa excluídas da análise 18
Quadro 6 - Frameworks com representação de abordagens para resposta a incidentes cibernéticos 35
Quadro 7 - Fases do processo de resposta a incidentes na literatura..... 40
Quadro 8 - Frameworks de processos – representações gráficas 48
Quadro 9 - Frameworks de representações da relação entre stakeholders 54
Quadro 10 - Perspectiva geral sobre o processo de resposta a incidentes no contexto do Brasil e SEB. 60
Quadro 11 - Detalhamento sobre a legislação e regulamentação publicadas sobre Segurança Cibernética no Brasil 63
Quadro 12 - Disposições sobre a constituição de equipes de segurança..... 69
Quadro 13 - Análise sobre a fase (1) Planejamento e Preparação - Contexto Brasil e SEB 72
Quadro 14 - Análise sobre às fases (2) Monitoramento e (3) Detecção - Contexto Brasil e SEB 74
Quadro 15 - Análise sobre às fases (4) Avaliação/Análise (5) Decisão e (6) Contenção/Recuperação – Nível Brasil e SEB 76
Quadro 16 - Análise sobre à fase (6) Atividades pós-incidente – Contexto Brasil e SEB . 78
Quadro 17 - Análise sobre a representação gráfica do processo de resposta a incidentes - Contexto Brasil e SEB 80
Quadro 18 - Perspectiva geral sobre o processo de resposta a incidentes no contexto do específico de operação de instalações do SIN 82
Quadro 19 - Instrumentos Normativos - contexto do específico de operação de instalações do SIN 85
Quadro 20 - Análise sobre a fase (1) Planejamento e Preparação – contexto do específico de operação de instalações do SIN 87
Quadro 21 - Análise sobre as fases (2) Monitoramento e (3) Detecção – contexto do específico de operação de instalações do SIN 89
Quadro 22 - Análise sobre as fases de (4) Avaliação/Análise (5) Decisão e (6) Contenção/Recuperação – contexto do específico de operação de instalações do SIN .. 93
Quadro 23 - Análise sobre a fase (6) Atividades pós incidente – contexto do específico de operação de instalações do SIN 96
Quadro 24 - Análise sobre a representação gráfica do processo de resposta a incidentes – contexto do processo de operação do SEB..... 98
Quadro 25 - Relacionamento entre os stakeholders – REGIC e SEB 106
Quadro 26 - Questões do Estudo de Caso 122

LISTA DE SIGLAS

AIQ – Amplitude Interquartil
ANEEL – Agência Nacional de Energia Elétrica
CCEE – Câmara de Comercialização de Energia Elétrica
CERT – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança
CNPE – Conselho Nacional de Política Energética
CPS – *Cyber-Physical Systems*
CSIRT – *Computer Security Incident Response Team*
CTIR Gov – Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Governo
DPO - *Data Protection Officer*
EPE – Empresa de Pesquisa Energética
GCN – Gestão da Continuidade do Negócio
GSI – Gabinete de Segurança Institucional
IA – Inteligência Artificial
ICS – *Industrial Control Systems*
IDS – *Intrusion Detection Systems*
ISAC – *Information Sharing and Analysis Center*
ML – *Machine Learning*
MME – Ministério de Minas e Energia
NT – Nota Técnica
ONS – Operador Nacional do Sistema Elétrico
PGI – Plano de Gestão de Incidentes
PLANGIC – Plano de Gestão de Incidentes Cibernéticos
PPSP – Plano de Preservação dos Serviços Prioritários
REGIC – Rede Federal de Gestão de Incidentes Cibernéticos
REN – Resolução Normativa
RSL – Revisão Sistemática da Literatura
SCADA – *Supervisory Control and Data Acquisition*
SEB – Setor Elétrico Brasileiro
SIEM – *Security Information and Event Management*
SIN – Sistema Interligado Nacional
SOC – *Security Operations Center*
TI – Tecnologia da Informação

1. INTRODUÇÃO

O primeiro capítulo tem como objetivo contextualizar o tema de pesquisa: resposta a incidentes cibernéticos no contexto dos Sistemas Ciber-Físicos. Além da apresentação do tema, são abordados os objetivos gerais e específicos, as justificativas, o objeto de estudo e a estrutura deste documento.

1.1 TEMA DE PESQUISA

A segurança cibernética pode ser definida como um conjunto de ações que visa proteger o ciberespaço de qualquer ameaça cibernética ou ataque cibernético (LEZZI, *et al.*, 2018) Dentre as principais preocupações associadas à segurança cibernética, destaca-se o crescimento exponencial dos Sistemas Ciber-Físicos, em inglês *Cyber Physical Systems* (CPS), sistemas capazes de monitorar e controlar o mundo físico. (HUMAYED *et al*., 2017).

A magnitude da preocupação se eleva quando infraestruturas críticas, responsáveis pelo fornecimento de serviços essenciais à sociedade, como os setores de energia, fornecimento de água, saúde e transporte podem ter seu comprometimento afetado devido algum incidente ou ataque cibernético. Alguns incidentes possuem potencial de desativar sensores, computadores e conexões de rede e incidentes de maior magnitude podem provocar uma cadeia de consequências graves, como perdas econômicas, danos ambientais e perda de vidas (JAATUN, *et al.*, 2009). Um impacto no setor de energia elétrica, por exemplo, que integra sistemas de geração, transmissão e distribuição em nível nacional, pode afetar infraestruturas críticas de outros setores (SALVI, *et al.*, 2022), reverberando em diversos setores críticos à sociedade.

Em um estudo sobre ataques cibernéticos em Sistemas de Controle Industriais, em inglês *Industrial Control Systems* (ICS), considerado um tipo de CPS, Staves *et al.* (2022) identificaram 29 ataques relevantes entre 1999 e 2019 que colocaram em risco infraestruturas críticas de diferentes países. Em 2000, o sistema de supervisão e controle da rede de esgoto de uma cidade australiana foi comprometido. Em 2003, um ataque cibernético penetrou uma rede de computadores de uma usina nuclear nos Estados Unidos (LIANG, *et al.*, 2017).

Em dezembro de 2015, um ataque cibernético ao sistema elétrico da Ucrânia é apontado como a causa de uma interrupção de energia durante horas, que causou impacto a mais de dez milhares de residências (SUN *et al.*, 2016). No Brasil, em fevereiro de 2021, um ataque cibernético afetou a área administrativa da Eletronuclear, sem prejuízos à operação das usinas de Angra 1 e Angra 2 (CNN-BRASIL, 2021)

A mudança do foco dos ataques cibernéticos de sistemas de Tecnologia da Informação (TI) tradicionais para infraestruturas críticas é uma questão observada com atenção pelas instituições governamentais (STAVES, *et al.*, 2022). Agências e órgãos reguladores no mundo se empenham para promover a segurança cibernética de setores críticos. No Reino Unido, o Centro de Cibersegurança Nacional do Reino Unido fornece assistência a organizações críticas do país, incluindo o setor público na instituições privadas, oferendo assistência para o processo de resposta e recuperação de incidentes cibernéticos (NCSC, 2023). Nos Estados Unidos, a Agência de Cibersegurança e Segurança de Infraestrutura dos Estados Unidos (CISA) tem como missão proteger e fortalecer a segurança cibernética e a resiliência da infraestrutura crítica do país (CISA, 2018).

No Brasil, apesar de não existir uma agência específica com responsabilidade definida para regulação do tema, identifica-se avanço na discussão a partir da publicação da Estratégia Nacional de Segurança Cibernética, que possui como objetivo promover a garantia da implementação de políticas, mudanças contínuas, tecnológicas, educacionais, legais e internacionais no âmbito da segurança cibernética (BRASIL, 2020a) e da Política Nacional de Segurança Cibernética, publicada em 2023 com a finalidade de orientar a atividade de segurança cibernética no País (BRASIL, 2023). No Setor Elétrico Brasileiro (SEB), a Agência Nacional de Energia Elétrica (ANEEL) publica Resolução Normativa (REN) 964/2021 que dispõe sobre a política de segurança cibernética a ser adotada pelos agentes do setor de energia elétrica e estabelece diretrizes e conteúdo mínimo para políticas de segurança cibernéticas que devem ser adotadas pelos agentes do setor (ANEEL, 2021b). Com objetivo de aumentar o nível de segurança cibernética do Operador Nacional do Sistema Elétrico (ONS), responsável pela operação da transmissão e geração de energia do Brasil, estabelece a partir da publicação da Rotina

Operacional RO-CB.BR.01, controles de segurança cibernética a serem implementados nos centros de operação dos agentes e em seus equipamentos de infraestrutura (ONS, 2023)

O elevado índice de eventos aumenta a dificuldade de proteção e garantia da segurança de infraestrutura críticas, devido à maior complexidade para análise e resposta aos incidentes (HAN, *et al.*, 2019), especialmente em um cenário que se altera rapidamente e em que novas ameaças são introduzidas (HE, *et al.*, 2022). O surgimento de novas ameaças traz a necessidade do desenvolvimento da capacidade de resposta a incidentes indesejados (LINE, *et al.*, 2016) e, nesse contexto, é fundamental que organizações reconheçam a necessidade de estarem preparadas, para resposta e aprendizado a partir de incidentes (PATTERSON, *et al.*, 2023).Independentemente da causa ou origem de um incidente cibernético, o planejamento da resposta deve prever a elaboração de planos de contingência para gerenciar os impactos negativos sobre equipamentos e operações críticas (SMITH, *et al.*, 2021). O processo de resposta a incidentes surge como uma das medidas propostas para promoção da segurança cibernética dos CPS (LEZZI, *et al.*, 2018) e pode ser compreendido como um conjunto atividades iniciadas quando um ataque é iminente, suspeito, está em andamento ou já concluído (AMOROSO, 2011, p.193). As atividades de preparação, detecção, análise e recuperação compõem um *framework* típico de resposta a incidentes (HE, *et al.*, 2022). Além das atividades de resposta, o compartilhamento de informações, o aumento da consciência situacional e relacionamento entre *stakeholders* são abordagens discutidas no contexto da proteção aos ataques cibernéticos (LESZCZYNA, *et al.*, 2019).

Diante do contexto teórico e prático apresentados, a identificação e investigação as principais abordagens associadas à resposta a incidentes cibernéticos na operação dos CPS surge como uma oportunidade de análise compreensão a partir do estudo de referenciais teóricos e da investigação empírica de um caso real que evidencia um problema prático da sociedade. Essa pesquisa visa identificar e compreender as principais abordagens associadas ao processo de resposta a incidentes cibernéticos em CPS na literatura e avaliar a aderência e aplicabilidade partir de um estudo empírico no contexto de operações de redes elétricas SEB e em setores relacionados.

1.2 OBJETIVOS DA PESQUISA

A definição de um tema de pesquisa depende da identificação de sua necessidade primária e função. Booth; Colomb; Willians (2008, p.10), argumentam que “uma pesquisa deve ser realizada quando é necessário coletar informações para responder uma questão ou resolver um problema”. No campo da engenharia, o acervo de conhecimentos disponível é utilizado em função da intervenção na realidade, de modo a atender uma demanda de mudança pela sociedade a partir de um projeto que encaminhe uma solução para determinado problema identificado (SILVA e PROENÇA JR., 2015). A engenharia precisa lidar com problemas atuais que a sociedade deseja solucionar e esse processo precisa ser desenvolvido de forma consistente de acordo com os recursos disponíveis (KOEN, 2003, p10).

A necessidade de identificação e investigação das principais abordagens associadas ao processo de resposta a incidentes cibernéticos em CPS surge como uma oportunidade de análise e compreensão, a partir do estudo de referenciais teóricos e da investigação empírica de um caso real que evidencia um problema prático da sociedade. Reconhece-se, a partir do contexto apresentado, que os possíveis impactos dos ataques cibernéticos aos CPS podem ser enquadrados como um problema típico de engenharia, em um contexto em que a existência de um problema prático e os custos da sua existência geram uma condição que tende a gerar insatisfação a todos os impactados por esse problema, conforme indicado por Booth; Colomb; Williams (2008).

Os objetivos da presente pesquisa podem ser classificados como objetivos gerais e específicos. O objetivo geral da pesquisa deve ser a síntese do que se pretende alcançar (SILVA e MENEZES, 2005). Diante da necessidade de responder uma questão ou resolver um problema, Both; Colomb; Willians (2008, p.61) propõem que uma pesquisa deve ser realizada a partir da coleta de informações, com a definição de um tópico a partir de um campo específico que deve ser desdobrado em um projeto. Ainda de acordo com os autores, em uma pesquisa aplicada, a solução deve possuir consequências práticas e deve seguir um processo conforme demonstrado na Figura 1.

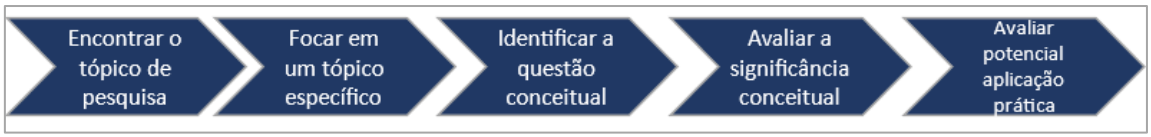


Figura 1 - Processo de definição do tópico de pesquisa
Fonte: Adaptado de Booth; Colomb e Williams (2008)

De acordo com a proposta de Booth; Colomb; Williams (2008), para definição do objetivo geral da pesquisa é necessário desdobrar o tópico de pesquisa, avaliar a questão conceitual e significância. Portanto, na presente pesquisa, estão definidos como:

- **Tópico de pesquisa:** segurança cibernética de CPS;
- **Tópico específico:** resposta a incidentes cibernéticos no contexto de CPS;
- **Questão Conceitual:** identificar e compreender as principais abordagens relacionadas ao processo de resposta a incidentes cibernéticos de CPS, a partir da análise de *frameworks*, e investigar esse fenômeno no contexto da operação de redes elétricas.
- **Significância Conceitual:** os resultados da pesquisa podem auxiliar profissionais da área de operação de redes elétricas e de outros tipos de CPS a compreenderem melhor os avanços relacionados ao processo de resposta a incidentes cibernéticos.
- **Potencial de aplicação prática:** a partir da investigação teórica e do desenvolvimento da pesquisa empírica, espera-se que os resultados deste trabalho possam ser utilizados no desenvolvimento de pesquisas futuras e na utilização por profissionais, como referência para promoção da segurança cibernética na operação dos CPS.

Booth; Colomb; Williams (2008, p101) sugerem ainda que o planejamento do projeto seja guiado em função das questões e problemas que a pesquisa procura responder. Desse modo, os autores propõem que o projeto seja analisado em relação à seguinte afirmação: trabalha-se em **X** para que se aprenda mais sobre **Y**, para que os leitores possam entender melhor sobre **Z**. Na presente pesquisa, as definições de X, Y e Z podem ser definidas do seguinte modo:

- **X** – Trabalha-se na identificação de abordagens sobre segurança cibernética de CPS na literatura, a partir da análise de *frameworks* que tratem sobre processo de resposta a incidentes, assim como na investigação desse fenômeno no contexto da operação específica de um CPS (redes elétricas).
- **Y** – Para que se aprenda sobre a possibilidade de aplicabilidade e aderência das abordagens identificadas na literatura no contexto prático e específico da operação dos CPS.
- **Z** – Para que os leitores: (a) profissionais de segurança cibernética possam obter insumos para a promoção de operação mais segura dos CPS; e (b) pesquisadores se situem sobre os principais avanços e questões relacionadas ao tema.

A partir da discussão do tópico, da questão conceitual e das definições de X, Y e Z, é definido o seguinte objetivo de pesquisa:

- **Objetivo geral:** Identificar e analisar as principais abordagens associadas ao processo de resposta a incidentes cibernéticos em CPS e investigar esse fenômeno no contexto do SEB e em setores relacionados.

Definido o objetivo geral, os objetivos específicos da pesquisa devem explicitar os detalhes e desdobramentos do objetivo geral (SILVA e MENEZES, 2005). A partir da definição do objetivo geral, tem-se como necessidade o alcance dos seguintes objetivos específicos:

- **Objetivos específicos:**
  - Identificar o contexto atual da discussão sobre resposta a incidentes em CPS;
  - Identificar abordagens apresentadas pela literatura para o processo de resposta a incidentes cibernéticos, a partir da identificação e análise de *frameworks*;
  - Avaliar a aderência e aplicabilidade das abordagens identificadas na literatura em relação processo de resposta a incidentes cibernéticos no cenário da operação de redes elétricas, a partir de um estudo empírico no SEB e em setores relacionados;

- Propor uma agenda para que próximas pesquisas científicas possam avançar na discussão sobre segurança cibernética de CPS.

1.3 JUSTICATIVA DE PESQUISA

Para resolver um problema prático, Both; Colomb; Willians (2008, p.53), argumentam que primeiramente é necessário resolver um problema de pesquisa a partir da definição de um problema conceitual que deve trazer respostas a questões que auxiliam no melhor entendimento do problema e do objeto de pesquisa.

A mudança do foco dos ataques cibernéticos de sistemas de Tecnologia da Informação (TI) tradicionais para infraestruturas críticas apontada por Staves *et al.* (2022) e a rigidez dos *frameworks* existentes para resposta a incidentes em um contexto de aumento no número de registros, apontados por He *et al.* (2022), são desafios apontados no contexto da segurança cibernética dos CPS. Adiciona-se à essa conjuntura a quantidade limitada de trabalhos relacionados à autoproteção de CPS (KHOLIDY, 2021),o crescimento exponencial desses sistemas (HUMAYED, *et al.*, 2017) e os desafios organizacionais relacionados à implementação de lições aprendidas a partir do histórico de incidentes (PATTERSON, *et al.*, 2023)

A partir da análise do contexto teórico, que fornece insumos para delimitação do problema conceitual, é possível fornecer soluções para um problema prático. No Brasil, devido ao aumento da preocupação com uso e segurança do espaço cibernético, observa-se o desenvolvimento da legislação e discussão regulatória sobre segurança cibernética, com a instituição da Estratégia Nacional de Segurança Cibernética a partir do Decreto 10.222/2020, que possui como objetivo promover a garantia da implementação de políticas, mudanças contínuas, tecnológicas, educacionais, legais e internacionais no âmbito da segurança cibernética (BRASIL, 2020a).No contexto específico do SEB, a ANEEL publica a Resolução Normativa (REN) 964/2021, que dispõe sobre a política de segurança cibernética a ser adotada pelos agentes do setor de energia elétrica (ANEEL, 2021b)

A presente pesquisa parte da investigação teórica sobre o processo de resposta a incidentes cibernéticos em CPS e analisa esse fenômeno em um contexto empírico em um cenário onde órgãos e instituições brasileiras debatem sobre políticas, critérios e requisitos para a promoção da segurança cibernética. Dado o potencial impacto de incidentes cibernético no contexto dos CPS e a possibilidade de realização de um estudo empírico no SEB e setores relacionados, constata-se a relevância do desenvolvimento de uma dissertação de mestrado que avalie medidas que possam ser aplicadas para o aumento da segurança cibernética dos CPS. Desse modo é vislumbrada a oportunidade de avanço teórico em relação ao tema de pesquisa e potencial aplicação prática.

1.4 OBJETO DE ESTUDO

A organização selecionada como objeto principal de estudo empírico é uma organização do SEB responsável por operar instalações de geração e transmissão de energia elétrica do Sistema Interligado Nacional (SIN). A organização opera instalações e nível nacional, a partir de centros de operações em diferentes regiões do Brasil. O processo de operação do sistema é realizado partir do uso de sistemas supervisão e controle denominados *Supervisory Control And Data Acquisition* (SCADA) que, de modo abrangente, são constituídos de componentes de *hardware* e *software* e de uma rede de conexão para monitorar e controlar ativos distribuídos em grandes áreas geográficas (CHERDANTSEVA, *et al.*, 2016).

Além de realizar a operação de instalações do SIN, a instituição se empenha na promoção do aumento da segurança cibernética no SEB a partir do envio de contribuições regulatórias para o setor, com propostas de ações para monitoramento e resposta a incidentes e controles mínimos de segurança..

Além do foco primário da pesquisa na avaliação dessa instituição, como foco secundário são avaliadas outras instituições relevantes na estrutura de governança do SEB, para compreensão do contexto geral do setor. Adicionalmente, também é avaliado o cenário da discussão sobre segurança cibernética no Brasil, especialmente no que tange o desdobramento da legislação sobre o tema. Essa análise se faz necessária devido interdependência

entre as organizações do SEB e relação da regulamentação do setor com a evolução sobre o tema no país.

O método de estudo de caso adotado para avaliação do objeto de estudo é detalhado no Capítulo 2 e os resultados da análise são apresentados no Capítulo 4.

1.5 ESTRUTURA DO DOCUMENTO

Esta dissertação está dividida em seis capítulos. O Capítulo 1 é a seção introdutória, que apresenta o tema de pesquisa, os objetivos gerais e específicos, as justificativas e o objeto de estudo. O Capítulo 2 detalha os princípios metodológicos adotados, que são expostos de acordo com sua natureza e abordagem, sob o ponto de vista de seus objetivos, concepção metodológica e métodos técnicos de pesquisa empregados.

O Capítulo 3 apresenta os resultados da análise do referencial teórico, de modo a identificar e apresentar o estado da arte da literatura sobre as abordagens relacionadas ao processo de resposta a incidentes cibernéticos no contexto dos CPS. Esse capítulo é dividido em dois subcapítulos: o primeiro relata os resultados da análise bibliométrica, com apresentação os indicadores de produção da comunidade científica sobre o tema. O segundo foca na análise temática do referencial teórico, com apresentação dos resultados da investigação do conteúdo da discussão da literatura.

O Capítulo 4 apresenta os resultados do estudo e é dividido em dois subcapítulos. O primeiro subcapítulo avalia o contexto geral sobre o processo de resposta a incidentes cibernéticos no Brasil e no SEB e o segundo subcapítulo avalia o contexto específico da instituição avaliada, responsável pela operação de instalações do SIN.

O Capítulo 5 discute as principais contribuições acadêmicas para pesquisadores e profissionais da área de segurança cibernética, além de sugerir uma proposta de agenda futura de pesquisa.

Por fim, o Capítulo 6, apresenta as considerações finais da pesquisa. Ao final do documento constam as referências bibliográficas, o apêndice e anexos

2. MÉTODOS UTILIZADOS NA PESQUISA

A presente pesquisa está estruturada a partir de uma abordagem multimetodológica. São utilizados dois métodos: Revisão Sistemática da Literatura (RSL) e estudo de caso. A adoção de uma abordagem multimetodológica é justificada pela possibilidade de contribuição para o desenvolvimento de uma pesquisa que contribua com resultados cientificamente sólidos e relevantes sob o ponto de vista prático (CHOI, *et al*. 2016).

2.1 REVISÃO SISTEMÁTICA DA LITERATURA

O relacionamento de uma pesquisa com o conhecimento existente é o elemento básico de todas as atividades de pesquisa acadêmica, independentemente da disciplina estudada (SNYDER, 2019). De acordo com o autor, a RSL é uma das abordagens de revisão da literatura que tem como objetivo a identificação de evidências empíricas que se ajustam a um pré-determinado critério de inclusão para resposta a uma questão de pesquisa particular.

A RSL pode ser definida como

> uma metodologia específica que localiza estudos existentes, avalia suas contribuições, sintetiza dados e reporta evidências de tal forma que permite a obtenção de conclusões razoavelmente claras sobre o que é e o que não é conhecido (DENYER; TRANFIELD, 2009, p.671)

A execução da RSL desta pesquisa toma como base o método proposto por Snyder (2019). Desse modo, seguidas as seguintes fases: (1) Planejamento da revisão; (2) Condução da revisão; (3) Análise; (4) Apresentação dos resultados. Além do método proposto por Snyder (2019) esta pesquisa considera recomendações adicionais de Thomé, *et al.* (2016), de Denyer e Tranfield (2009) e de Proença Jr. e Silva, (2016).

2.1.1 Planejamento da revisão

Na primeira fase, planejamento da revisão, são destacados o potencial de contribuição da realização da RSL, a estratégia de busca a ser adotada, a

seleção das palavras-chave e os critérios de inclusão e exclusão. Essa fase depende da definição dos principais desafios, lacunas e questões relacionadas ao tema de pesquisa (THOMÉ *et al.,* 2016). Snyder (2019) recomenda que sejam avaliados os seguintes pontos: a potencial contribuição da revisão de literatura, a potencial audiência, os objetivos de pesquisa que devem ser respondidos e a estratégia de pesquisa que deve ser adotada.

No âmbito desta pesquisa, espera-se a contribuição acadêmica na identificação e compreensão as principais abordagens associadas ao processo de resposta a incidentes cibernéticos em CPS, a partir da análise de *frameworks* propostos na literatura. Em relação à audiência, a pesquisa dirige-se a profissionais da área de operação e segurança dos CPS e pesquisadores do tema. Quanto aos objetivos específicos, já descritos no subcapítulo 1.2, essa RSL auxilia na identificação de abordagens relacionadas ao processo de resposta incidentes cibernéticos em CPS.

A Figura 2 apresenta o processo para condução da pesquisa bibliográfica. A RSL realizada a partir de dois caminhos diferentes que se unem ao final do processo.

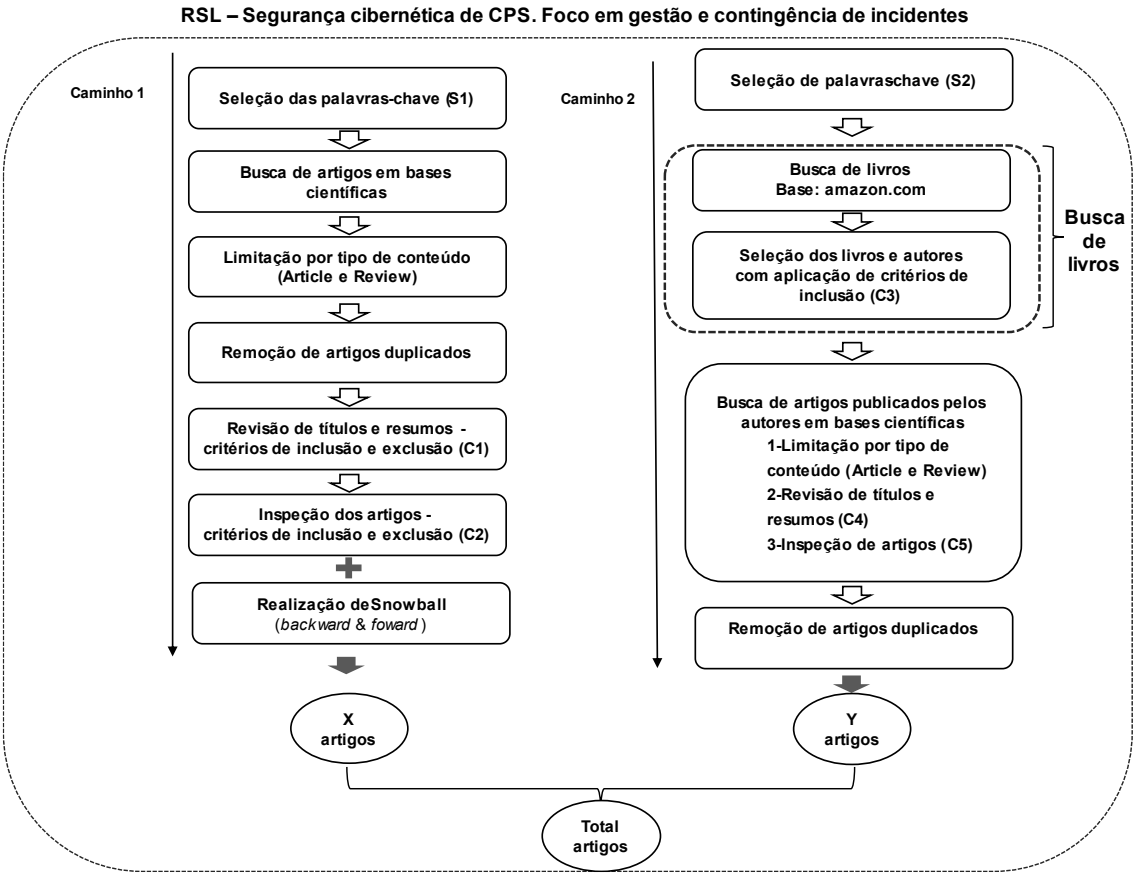


Figura 2 - Processo de busca da RSL
Fonte: o autor

O caminho 1 tem o processo originado na seleção de palavras-chave e busca por artigos em bases científicas e segue recomendações propostas por Snyder (2019) e Thomé, *et al.* (2016). O caminho 2 é originado pela seleção de palavras-chave, busca em livros e posteriormente busca de artigos publicados pelos autores dos livros. O caminho 2 permite uma melhor ambientação no assunto e segue recomendações propostas por Proença Jr. e Silva (2016).

Conforme processo proposto por Snyder (2019), esta pesquisa bibliográfica considera a seleção de termos apropriados. Thomé *et al.* 2016 sugerem a consulta em bases científicas que possuem a capacidade de agregar coleções, bancos de dados de fornecedores como editores acadêmicos e títulos de periódicos. A consulta de livros é realizada de acordo com a recomendação de Proença Jr. e Silva (2016).

O agrupamento de palavras-chave é organizado seguindo recomendações de Denyer e Tranfield (2009), conforme Quadro 1. A busca nas

bases científicas considera a relação entre os grupos de palavras de interesse e relevância para a pesquisa.

Quadro 1 - Seleção das palavras-chave

Grupo	Palavras-Chave	Processo da pesquisa bibliográfica que as utiliza	Referências que apoiam na definição dos termos
(1) Segurança Cibernética	Cybersecurity OR “Cyber security” OR “Cyber Attack” OR “Cyber Threat” OR “Information Security” OR “Security Services”	Caminho 1	(HUMAYED *et al.*, 2017) (KURE *et al.*, 2018) (KHOLIDY, 2021)
(2) Gestão de Riscos e Recuperação de desastres	“Risk Management” OR “Risk Analysis” OR “Vulnerability” OR “Risk Assessment” OR “disaster recovery” OR “live recovery” or “contingency plan” OR “response plan”	Caminho 1	(DIOGENES, OZKAYA, 2019) (KURE *et al.*, 2018)
(3) Sistemas Ciber-físicos, infraestrutura crítica e sistemas de supervisão	“Critical Infrastructure” OR “Cyber Physical System*” OR “Industrial Control System*” OR SCADA OR “Supervisory Control and Data Acquisition”	Caminho 1	(ECKHART, BRENNER, *et al.*, 2019) (HUMAYED *et al.*, 2017) (KURE *et al.*, 2018) (KURE e ISLAM, 2019) (SUN *et al.* , 2016)
(4) Gestão e contingência de incidentes	“incident response” OR “disaster recovery” OR “live recovery” or “contingency plan” OR “response plan”	Caminho 1 e Caminho 2	(DIOGENES, OZKAYA, 2019) (NIST, 2018)
(5) Palavras-chave associadas à busca de livros que tratam de segurança cibernética de CPS	"Cyber Physical System"; "Industrial Control System"; "Supervisory Control and Data Acquisition"; SCADA; "Critical Infrastructure"; Infrastructure; “Cybersecurity”;"Cyber security"	Caminho 2	(HUMAYED *et al.*, 2017) (KURE *et al.*, 2018) (KHOLIDY, 2021)
(6) Palavras-chave associadas à busca de livros, conforme Proença Jr. e Silva (2016)	Principles; introduction, handbook, foundations	Caminho 2	Proença Jr. e Silva (2016)

Fonte: o autor

Além da seleção dos termos, na formulação da estratégia devem ser definidos critérios de inclusão e exclusão para a seleção dos artigos (SNYDER,

2019). De acordo com o autor, o planejamento da pesquisa ainda prevê que os resumos e títulos dos artigos sejam revisados para confirmar a inclusão de estudos que atendam aos critérios de busca e aos critérios de inclusão. Nesta pesquisa, os critérios de inclusão e exclusão para inspeção dos artigos e livros estão detalhados no Quadro 2.

Quadro 2 - Critérios de inclusão e exclusão para inspeção dos artigos

Etapa da pesquisa Bibliográfica	Fase	Critérios de Inclusão (atendimento a pelo menos um dos três itens)	Critérios de Exclusão
RSL (caminho 1)	(C1) Revisão de títulos e resumos de artigos	Tem como foco a abordagem sobre segurança cibernética de: -Sistemas ciberfíscos, ou -Infraestrutura crítica, ou -SCADA, ou -Indústria 4.0	Não aborda sobre segurança cibernética ou resposta a incidentes cibernéticos
		Aborda sobre resposta a incidentes cibernéticos	
	(C2) Inspeção dos artigos	Trata sobre alguma fase de resposta a incidente ou plano de contingência, com apresentação de um *framework*/processo	Não apresenta *framework*/processo
RSL (caminho 2)	(C3) Revisão de títulos e inspeção de livros e seus capítulos	Deve conter capítulo que aborda sobre gestão de incidentes cibernéticos / Plano de contingência	Não aborda sobre CPS, ou SCADA, ou ICS, ou Infraestrutura crítica
			Não aborda sobre segurança cibernética ou resposta a incidentes cibernéticos / Plano de contingência
	(C4) Revisão de títulos e resumos de artigos	Tem como foco a abordagem sobre segurança cibernética de: -Sistemas ciber-físcos, ou -Infraestrutura crítica, ou -SCADA, ou -Indústria 4.0	Pesquisas que não abordam sobre segurança cibernética ou resposta a incidentes cibernéticos
		Aborda sobre gestão de incidentes cibernéticos	
	(C) Inspeção dos artigos	Trata sobre alguma fase de resposta a incidente ou plano de contingência, com apresentação de um *framework*/processo	Não possui *framework* sobre gestão de incidente ou plano de contingência

Fonte: o autor

2.1.2 Condução da revisão

A segunda fase da RSL, condução da revisão, deve testar a aplicação dos termos de busca e os critérios de inclusão e exclusão, além de prever uma

abordagem de condução do processo de leitura de resumos e seleção de artigos para leitura e análise em etapa posterior (SNYDER, 2019).

Nessa dissertação o processo e resultados da condução são apresentados na Figura 3.

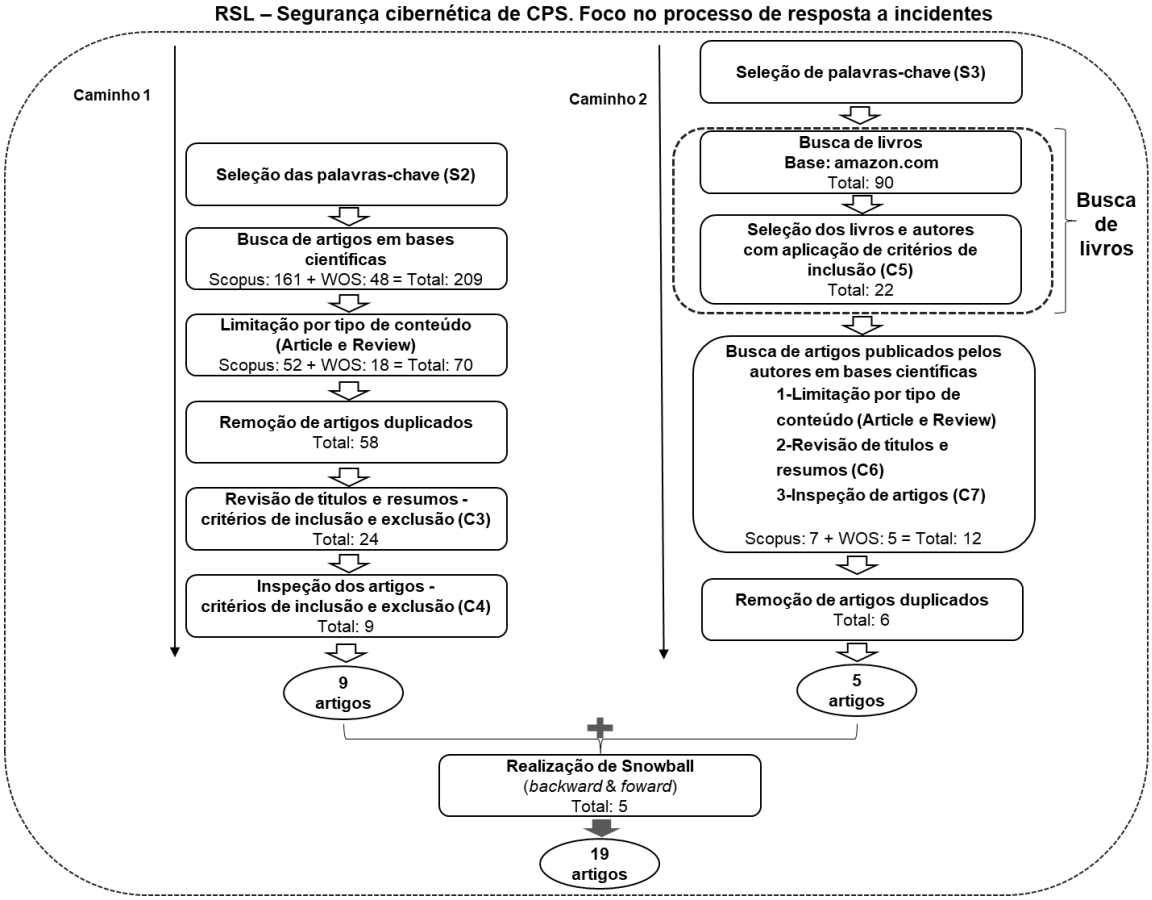


Figura 3 - Resultados da condução da RSL
Fonte: o autor

2.1.3 Análise

A terceira fase da RSL, análise, deve partir da coleta de dados e da adoção de procedimentos de análise. Os dados e informações do material acadêmico selecionado devem ser avaliados de acordo com proposta de pesquisa (SNYDER, 2019). A coleta de dados deve considerar a criação de templates e esquemas para facilitar a classificação e identificação dos dados (THOMÉ, *et al*. 2016). Nesta pesquisa, a coleta é realizada e consolidada a partir do uso de tabelas em planilhas eletrônicas. O período de realização de cada coleta é apresentado no Quadro 3.

Quadro 3 - Período de realização da coleta

Etapa da pesquisa bibliográfica	Fase da coleta	Data da coleta
RSL - Caminho 1	Busca de artigos em bases científicas	Abril /2022
RSL - caminho 2	Busca de livros	Janeiro / 2022
	Busca de artigos publicados pelos autores em bases científicas	Junho/2022

Fonte: o autor

Snyder (2019) sugere a adoção de medidas para garantir a qualidade dos dados obtidos. Para atingir esse objetivo, são adotadas duas medidas no âmbito desta dissertação:

- a realização da pesquisa de acordo com as fases e orientações de Snyder (2019) e Thomé *et al.* (2016);
- a consideração apenas de artigos revisados por pares em periódicos, a partir da limitação de conteúdo na busca das bases, classificados como *articles* e *reviews*, conforme recomendação de Thomé *et al.* (2016)

O Quadro 4 sintetiza o procedimento de análise e síntese da pesquisa bibliográfica realizada.

Quadro 4 - Síntese do procedimento de análise da pesquisa bibliográfica

Procedimento	Objetivo
Análise da potencial contribuição da realização de uma RSL para o tópico de pesquisa	Espera-se que os resultados deste trabalho possam ser utilizados no desenvolvimento de pesquisas futuras e na utilização por profissionais, como referência para promoção da segurança cibernética na operação dos CPS.
Processo de busca	Busca de livros no site amazon.com e busca de artigos científicos nas bases Scopus e Web of Science
Coleta de dados	A coleta de dados é consolidada conforme os processos, fases e etapas dispostos em *frameworks* e modelos conceituais propostos pela literatura
Análise dos dados	A1) Análise bibliométrica: Análise bibliométrica de acordo com métodos propostos Dawson (2011) e Van Eck & Waltman (2017) A2) Análise de frameworks / modelos conceituais: identificação dos principais *frameworks* / modelos para resposta a incidentes cibernéticos no contexto dos CPS. Análise realizada tendo como base a discussão promovida por Purchase (2014). A3) Consolidação dos resultados e proposta de agenda: classificação conceitual das abordagens sobre o processo e

Procedimento	Objetivo
	resposta a incidentes cibernéticos e propostas de trabalhos futuros, conforme Torraco (2005).
Apresentação dos resultados	Os resultados da pesquisa são apresentados no Capítulo 3 desta pesquisa. A propostas de trabalhos futuros são apresentadas no Capítulo 5.

Fonte: o autor

A1) Análise bibliométrica

A análise bibliométrica dos dados coletados é realizada a partir da extração de informações estatísticas sobre a evolução do número de publicações ao longo dos anos, periódicos mais populares, publicações por autores, obras mais citadas e análise das palavras-chave utilizadas pelos autores. Para análise das obras mais citadas, são considerados os valores de citações atípicos, em inglês *outliers*, de cada artigo, conforme método estatístico proposto por Dawson (2011). Para análise das palavras-chave, é utilizado o software VOSviewer, que admite análises bibliométricas em nível agregado e permite o agrupamento de termos a partir de sua relação (VAN ECK e WALTMAN, 2017). O processo e critérios adotados (Figura 4) para a criação do mapa de análise de palavras nesta pesquisa considera a construção da base de análise, a seleção do tipo de análise e ajustes para consolidação de palavras.

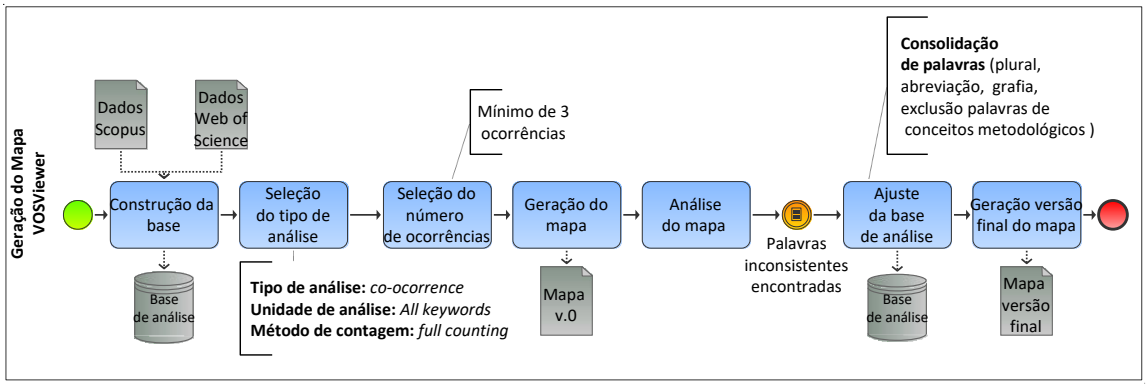


Figura 4 - Processo de criação do mapa de relação de palavras no VOSviewer
Fonte: o autor

Os ajustes necessários para a geração da base de análise, considera a consolidação de palavras no plural, abreviações e grafia além da exclusão de palavras relacionadas à metodologia de pesquisa adotada nesses artigos,

conforme Quadro 5. Deste modo, a análise bibliométrica realizada no VOSviewer reflete apenas termos relacionados ao tema central de pesquisa dos autores.

Quadro 5 - Palavras relacionadas à metodologia de pesquisa excluídas da análise

Palavras-Chave
systematic literature review, snowballing; survey; systematic mapping, comprehensive analysis; literature review*; systematic mapping studies; systematic review; mapping; systematic mapping; review*; research challenges; state of the art

Fonte: o autor

A2) Análise de *frameworks* / modelos conceituais

Os trabalhos selecionados na RSL são analisados de acordo com as representações diagramáticas dos *frameworks* apresentados pelos autores analisados. Os diagramas são ferramentas de comunicação de informação e possuem a capacidade de aumentar o processamento visual, fornecendo um meio flexível para representar a informação de forma objetiva e direta (PURCHASE, 2014). Os diagramas são catalogados em uma tabela e descritos de acordo com:

- Tipo de representação diagramática do *framework*/modelo conceitual proposto
- Representação abstrata do diagrama proposto
- Descrição do *framework* / modelo conceitual

A3) Consolidação dos resultados e proposta de agenda

Torraco (2005) argumenta como possíveis resultados de uma síntese de revisão da literatura a consolidação de resultados a partir de uma classificação conceitual de constructos e a proposta de uma agenda futura que provoque novas questões ou proposições. Nessa dissertação, a partir da análise das principais abordagens sobre a resposta a incidentes cibernéticos, no Capítulo 3 é realizada uma classificação conceitual e uma discussão a partir da síntese da literatura selecionada. A agenda de pesquisa futura é discutida no Capítulo 5.

2.1.4 Apresentação dos resultados

Na quarta fase, apresentação dos resultados, Snyder (2019) sugere que os dados sejam sintetizados e reportados de forma clara pelo autor. Thomé *et al.* (2016) recomenda que a interpretação dos resultados seja realizada com exposição e discussão dos principais resultados obtidos, de modo a contribuir para maior compreensão do estado da arte sobre o assunto. Os são apresentados no Capítulo 3 desta pesquisa. No Capítulo 5, conforme proposição de Snyder (2019) e Thomé *et al.* (2016), são discutidas sugestões de trabalho futuro como modo de contribuição para atualização e revisão desta pesquisa.

2.2 ESTUDO DE CASO

O estudo de caso é “um trabalho de pesquisa de caráter empírico que investiga um dado fenômeno dentro de um contexto real contemporâneo por meio da análise aprofundada de um ou mais objetos de análise”(CAUCHIK-MIGUEL, SOUZA, 2018, p.131). O estudo de caso permite que o pesquisador obtenha uma perspectiva holística do mundo real, o auxiliando na análise de alguma circunstância presente (YIN, 2015). Para Yin (2015) para a estruturação do método, deve-se utilizar como insumos os resultados obtidos na etapa de revisão da literatura, após a investigação das questões e objetivos de pesquisa.

A presente pesquisa utiliza como referência as principais etapas para a realização de um estudo de caso abordadas por Yin (2015), conforme Figura 5: (1) planejamento, o (2) projeto, a (3) preparação, a (4) coleta, a (5) análise dos dados e o (6) -compartilhamento dos resultados. Além das etapas sugeridas por YIN (2015) este trabalho também considera orientações apresentadas por Cauchik-Miguel e Souza (2018)

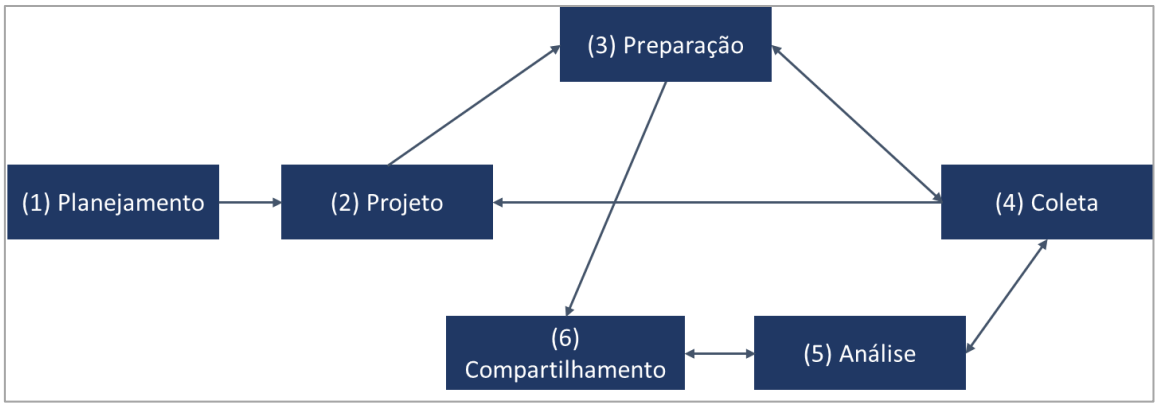


Figura 5 - Etapas do Estudo de Caso
Fonte: Adaptado de Yin (2015)

Na primeira etapa, planejamento, Yin (2015, p.10), recomenda a identificação da situação relevante para a qual deve se fazer o estudo. Para Yin (2015), o estudo de caso deve ser utilizado quando a questão de pesquisa se configura a partir das perguntas “como” e “por que”. Nesta dissertação, a questão de pesquisa se sustenta na necessidade de identificação e análise das principais abordagens associadas à resposta a incidentes cibernéticos em CPS, assim como na possibilidade de investigação desse fenômeno no contexto da operação de redes elétricas.

Na segunda etapa do estudo de caso, o projeto, Yin (2015, p.31) recomenda que seja explicitada a questão de estudo, a unidade de análise assim como a lógica que une os dados às proposições e os critérios para interpretação das constatações.

A partir da investigação teórica de abordagens para resposta a incidentes cibernéticos discutidas pela literatura para promoção da segurança cibernética dos CPS, há a necessidade de avaliação da aderência à unidade de análise. Na presente pesquisa, a análise foca no contexto do SEB, especificamente no processo de operação das instalações do SIN, assim como em setores relacionados, conforme discutido no Capítulo 1. Desse modo, o estudo de caso investiga a situação atual e contribui potencialmente para a construção de um resultado aderente ao contexto prático. As análises do estudo de caso requerem que os dados coletados sejam um reflexo direto das proposições iniciais da pesquisa (Yin. 2015, p.38). Os critérios para interpretação das constatações, juntamente com a lógica de união de dados às proposições devem levar à antecipação da análise do estudo de caso sugerindo o que deve ser feito após a

análise de dados (Yin, 2015, p.39). Assim, a lógica que une os dados às proposições evidencia-se quando as constatações do estudo de caso são confrontadas com os resultados da RSL e quando proposições derivadas da RSL possam ter sua aderência e aplicabilidade verificada na unidade de análise.

Na terceira etapa, a preparação, deve ser explicitada como a coleta de dados deve ser realizada (Yin, 2015, p.75). A partir da seleção do caso deve-se determinar quais instrumentos e métodos para a coleta de dados serão utilizados na pesquisa, podendo ser consideradas múltiplas fontes de evidências, como entrevistas, análise documental, observações e levantamento *survey* (CAUCHIK-MIGUEL e SOUZA, 2018, p.137). Nesta pesquisa, para aumento da confiabilidade dos resultados, é desenvolvido um protocolo de pesquisa, como instrumento de coleta de dados que contém os procedimentos e regras gerais a serem seguidas conforme sugere Yin (2015, p.88). O protocolo de pesquisa consta no Apêndice 1 do documento.

Na quarta etapa, coleta de dados, são evidenciadas as fontes de dados utilizadas (YIN, 2015, p.107). Dentre as fontes de evidência utilizadas nesta pesquisa, utilizam-se a análise documental e entrevistas. A análise documental é realizada a partir da investigação e análise de documentos fornecidos pelas instituições, legislação e regulamentos publicados, que estão associados à unidade de análise considerada. Em relação às entrevistas, são registradas durante cada reunião realizada com as instituições avaliadas. Os profissionais entrevistados desempenham papel relevante na articulação de soluções para a segurança cibernética do SEB. A Tabela 1**Erro! Fonte de referência não encontrada.** apresenta o quantitativo de entrevistados e setor das organizações:

Tabela 1 - Organizações entrevistadas - Nível Brasil e SEB

Organização/Entidade	Setor	Grupo	Integra grupo coordenação setorial SEB?	Quantidade de entrevistados
Organização 1	SEB e Brasil (REGIC)	1	Sim	1
Organização 2	SEB e Brasil (REGIC)	1	Não	2
Organização 3 (objeto de estudo)	SEB	2	Sim	7
Organização 4	SEB	2	Sim	2

Fonte: o autor

Na organização objeto do estudo, são consideradas as percepções de 7 entrevistados de 6 diferentes áreas da organização (Tabela 2), além da análise documental de informações disponibilizadas.

Tabela 2 - Áreas entrevistadas na organização objeto de estudo (contexto do específico de operação de instalações do SIN)

Área	Quantidade de entrevistados
Segurança Cibernética	1
Gestão de Riscos	2
Gestão de Assuntos Regulatírios	1
Normatização da Operação	1
Telecomunicações	1
Comunicação Institucional	1

Fonte: o autor

Na quinta etapa, análise de dados, deve ser desenvolvida uma estratégia analítica geral (YIN, 2015, p.137). “A partir do conjunto de dados coletados, considerando as múltiplas fontes de evidência, o pesquisador deve produzir uma espécie de narrativa geral do caso” (CAUCHIK-MIGUEL e SOUZA, 2018, p.139). Yin (2015, p.136) recomenda que os dados sejam categorizados de modo a produzir descobertas baseados no empirismo. Uma das estratégias apresentadas por Yin (2015, p.140) é seguir com proposições teóricas que levem ao estudo de caso. Desta forma, na presente pesquisa, as proposições teóricas se originam dos resultados da análise do referencial teórico, obtidos na RSL, e fornecem insumos para organizar e guiar a análise do estudo de caso. A orientação teórica é avaliada e combinada com as informações coletadas no estudo de caso a partir do uso da técnica analítica de combinação padrão, conforme sugere Yin (2015, p.147). O resultado é a combinação do padrão teórico e do padrão empírico resultante do estudo de caso no SEB e setores relacionados.

A sexta etapa, compartilhamento, prevê a apresentação dos resultados e constatações ao encerramento do trabalho (YIN, 2015, p. 180). Os resultados do estudo de caso estão apresentados no Capítulo 4 desta pesquisa. As conclusões e contribuições para o público-alvo considera as questões de pesquisa propostas neste trabalho.

3. RESPOSTA A INCIDENTES CIBERNÉTICOS EM CPS

Este capítulo tem como objetivo apresentar os principais resultados da análise do referencial teórico, que apresentam respostas para os seguintes objetivos específicos da pesquisa:

- Identificar o contexto atual da discussão sobre resposta a incidentes em CPS;
- Identificar abordagens apresentadas pela literatura para o processo de resposta a incidentes cibernéticos, a partir da identificação e análise de *frameworks.*

O primeiro subcapítulo apresenta o contexto atual e evolução do tema a partir da apresentação dos resultados da análise bibliométrica dos artigos identificados na RSL. O segundo subcapítulo tem como foco a análise e discussão das principais abordagens apresentadas pela literatura para o processo de resposta a incidentes cibernéticos. São identificados os principais setores de aplicação dos CPS e, a partir da análise dos *frameworks* propostos pela literatura, são identificadas e analisadas como abordagens: o modelos ou representações de processos par resposta a incidentes cibernéticos, as fases do processo de resposta e o formato gráfico de representação do relacionamento entre os *stakeholders.*

3.1 ANÁLISE BIBLIOMÉTRICA DA LITERATURA

Este subcapítulo apresenta os resultados da bibliometria da literatura analisada, a partir da análise dos 19 artigos selecionados. São expostos os indicadores de produção da comunidade científica sobre o tema, como a evolução no número de publicações ao longo dos anos, publicações por periódico, artigos mais citados, análise de palavras-chave e os principais métodos adotados nas pesquisas.

3.1.1 Evolução da produção científica

A análise da evolução da produção científica relacionada à resposta a incidentes cibernéticos em CPS (Figura 6), revela que há uma tendência de aumento no número de publicações de 2009 a 2022..

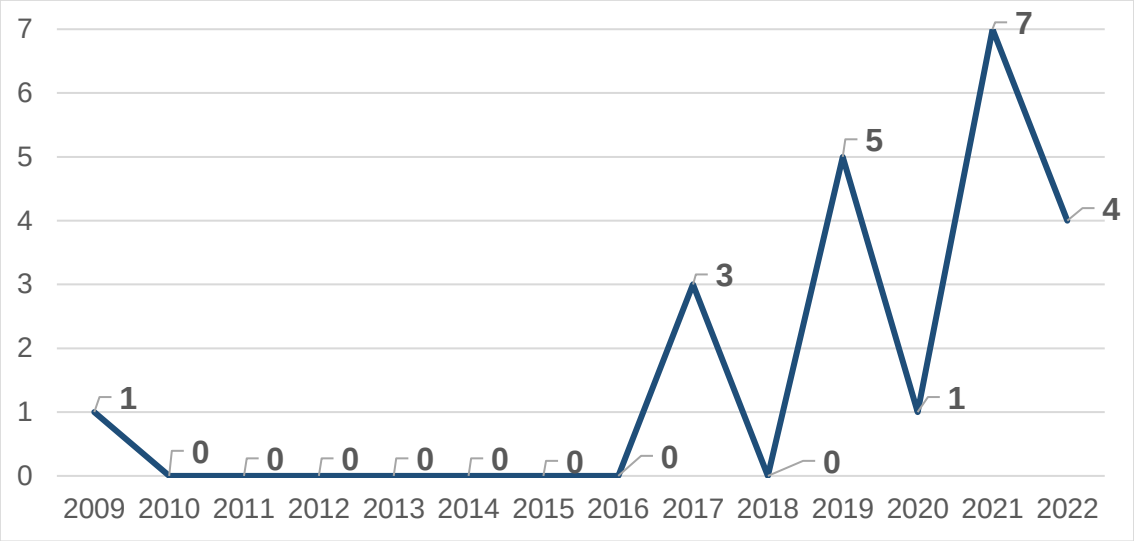


Figura 6 - Evolução do número de publicações por ano
Fonte: Elaborado pelo autor

A primeira publicação identificada data do ano de 2009, entretanto é a partir de 2019 que há crescimento expressivo no número de publicações. Esse resultado indica que o aumento da preocupação com o tema é recente.

Quanto à publicação dos artigos (Tabela 3) observa-se grande diversidade de periódicos que abordam temas associados à computação, tecnologias da informação e comunicação e infraestruturas críticas. Dos 14 periódicos identificados, apenas dois registram, mais de uma publicação: "*Computers and Security*" e "*International Journal of Critical Infrastructure Protection*". O resultado indica que a publicação em diversos periódicos pelos autores pode ser compreendida como reflexo da heterogeneidade das aplicações dos CPS e da atualidade do tema.

Tabela 3 - Publicações em periódicos

Periódico	Nº Publicações
Computers and Security	4
International Journal of Critical Infrastructure Protection	3
International Journal of Information Management	1
Software - Practice and Experience	1
Sensors (Switzerland)	1

Periódico	Nº Publicações
Ingenieria Solidaria	1
Proceedings of the ACM on Human-Computer Interaction	1
IEEE Access	1
Computer Fraud and Security	1
Energies	1
Peer-to-Peer Networking and Applications	1
Decision Support Systems	1
Sensors	1
Computers in Human Behavior Reports	1

Fonte: o autor

3.1.2 Análise dos artigos mais citados pela literatura

O número de citações de cada artigo é apresentado de acordo com o quantitativo de citações realizadas por outros autores, conforme metadados disponíveis nas bases de pesquisa científica Scopus e Web of Science. Os valores atípicos (*outliers*) podem ser calculados estatisticamente, a partir da Amplitude Interquartil (AIQ), definida como a diferença entre o terceiro (Q3) e o primeiro (Q1) quartis, AIQ = Q3 – Q1 (DAWSON, 2011). De acordo o autor, qualquer valor acima de 1,5xAIQ + Q3 deve ser considerado como um valor atípico. Diante do exposto, a partir da análise dos dados (Tabela 4Tabela 4), identificam-se 4 artigos como *outliers*.

Tabela 4 - Número de artigos classificados como *outliers*

Intervalo de tempo (anos)	Nº de artigos no grupo do intervalo	Mediana	AIQ	Limite superior de citações para ser considerado *outlier* (deve ser maior que)	Número de *outliers*
2009 – 2022	19	2,0	7,0	18,5	4

Fonte: o autor

O resultado detalhado da análise (Figura 7) evidencia o número de citações das publicações classificadas como *outliers* e os respectivos autores

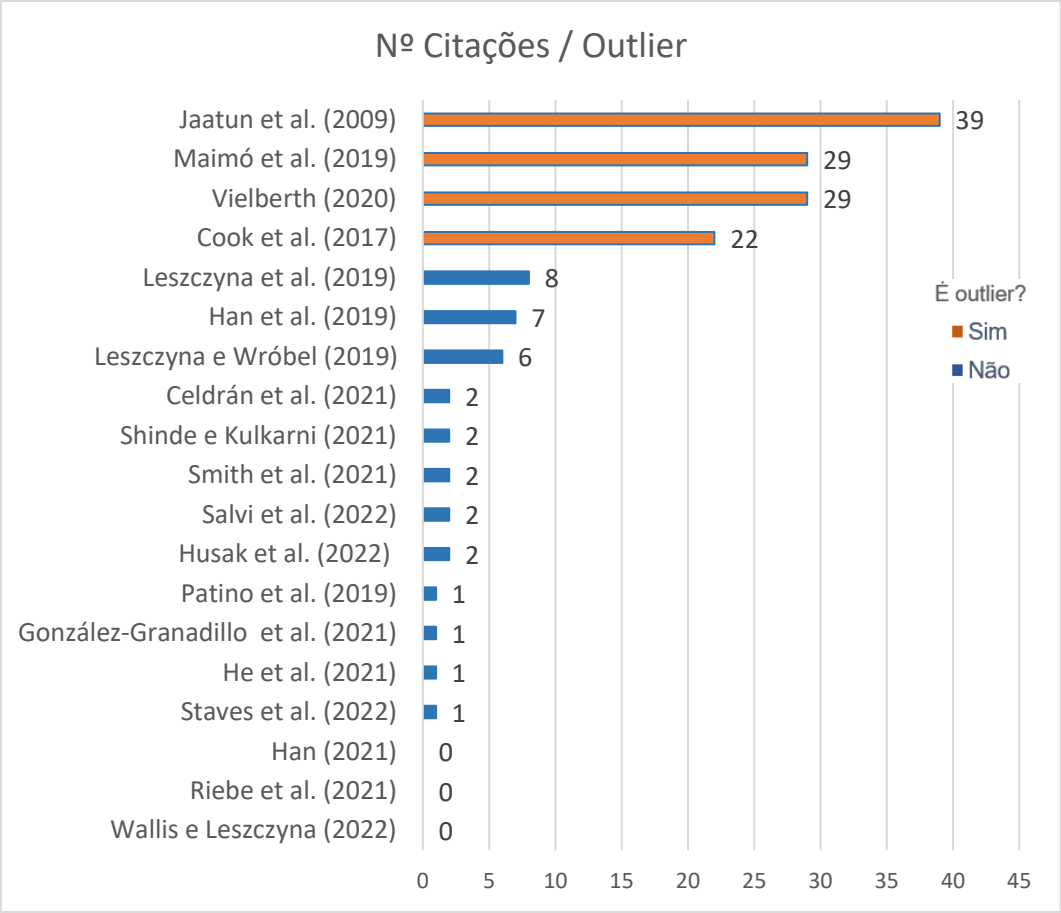


Figura 7 - Número de citações e valores atípicos (*outliers*) por autor
Fonte: o autor

No artigo de Jaatun *et al.* (2009) o modelo de resposta a incidentes é avaliado no contexto da indústria petrolífera, com enfoque no aprendizado contínuo e proativo, sob uma perspectiva sociotécnica no ciclo de resposta à incidentes cibernéticos. Cook, *et al.* (2017) realizam seu estudo no contexto de defesa de sistemas industriais, propondo soluções para triagem de incidentes cibernéticos, em um contexto onde as soluções de segurança de TI tradicional existentes não mais se aplicam ao contexto dos CPS. Maimó *et al.* (2019) abordam o processo de gestão de incidentes no setor de saúde sob uma perspectiva tecnológica, propondo o uso de sistemas automáticos baseados em *Machine Learning* (ML) para apoio à detecção, classificação e mitigação de incidentes. Vielberth (2020) analisam o papel dos Centros de Operação de Segurança, em inglês *Security Operations Center* (SOC), como *stakeholders* centrais responsáveis pela segurança operacional das organizações diante do processo de gestão de incidentes.

Observa-se diversidade nos setores de aplicação dos CPS dentre os artigos mais citados e a diferença nas abordagens adotadas para promoção da segurança cibernética, desde a adoção de uma perspectiva sociotécnica, a partir da gestão de *stakeholders* e da aplicação de tecnologias de Inteligência Artificial (IA).

Para reduzir o efeito do viés da temporalidade na análise dos *outliers*, adicionalmente são criados três grupos, considerando-se diferentes intervalos de tempo, conforme apresentado na Tabela 5. Para criação dos intervalos, pondera-se a melhor distribuição homogênea quantitativa dos artigos, adotando-se como premissa que artigos de um mesmo ano de publicação não podem estar contidos em grupos distintos.

Tabela 5 - Cálculo estratificado de *outliers* por grupo em intervalos de tempo

Intervalo de tempo (anos)	Nº de artigos no grupo do intervalo	Mediana	AIQ	Limite superior de citações para ser considerado outlier (deve ser maior que)	Nº de artigos outliers no grupo
2009 – 2019	7	8,0	1,5	4,25	0
2020 – 2021	8	1,5	1,75	4,75	1
2022	4	1,5	1,75	4,62	0

Fonte: o autor

A partir da análise dos resultados apresentados na Tabela 5, constata-se que o valor para o limite superior é alterado de acordo com cada grupo de artigos, assim como a mediana e o cálculo dos quartis. Quando agrupados de modo homogêneo em relação ao número de publicações nos respectivos intervalos de tempo, no intervalo de 2020 – 2021 apenas o artigo de Vielberth (2020) é identificado como *outlier*, o que demonstra a relevância da publicação, sobre os sistemas automáticos baseados em ML no processo de resposta a incidentes, para a literatura.

3.1.3 Principais termos de pesquisa

Para compreensão da evolução da discussão sobre a segurança cibernética dos CPS ao longo dos últimos anos, é gerado um mapa (Figura 8) de correlação de palavras-chave com auxílio do *software* VOSviewer. São identificados 12 termos com número superior a três ocorrências e os tamanhos. As ligações e cores variam de acordo com a ponderação realizada pelo *software*, e com a ocorrência das palavras-chave indexadas ao longo dos anos. A localização próxima dos termos tende a indicar uma forte relação entre as palavras-chave.

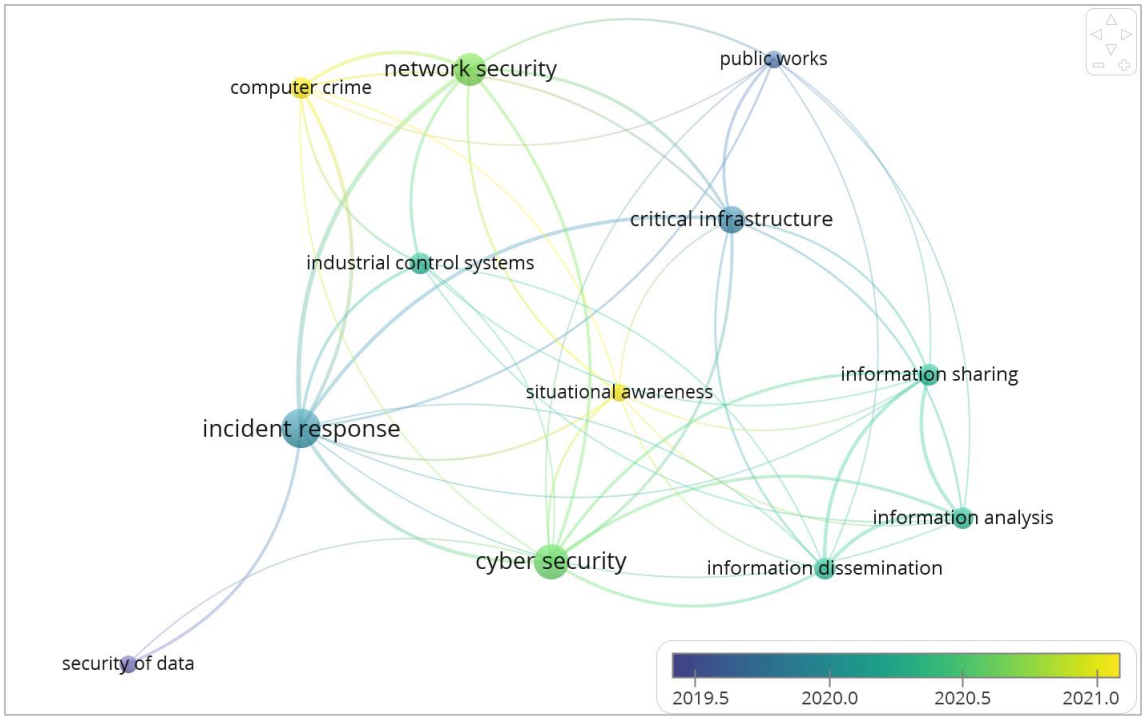


Figura 8 - Evolução das palavras-chave por ano
Fonte: o autor

Nota-se que em 2019 há maior tendência de pesquisas relacionadas a infraestruturas críticas, segurança de dados e resposta a incidentes. Em 2020 surgem como destaque os conceitos de segurança cibernética, análise e compartilhamento de informações. A partir de 2021 as pesquisas tendem a focar em crimes computacionais e consciência situacional. Apesar dos termos relacionados à resposta a incidentes, CPS e infraestruturas críticas se destacarem com maior relevância, a análise revela a evolução da preocupação da literatura para questões associadas a consciência situacional, o que reforça

a necessidade de se entender e avaliar o estado atual da segurança cibernética em um ambiente específico.

3.2 RESPOSTA A INCIDENTES CIBERNÉTICOS EM CPS

Este subcapítulo tem como objetivo apresentar a análise do conteúdo do referencial teórico com foco na análise da discussão da literatura para resposta de incidentes cibernéticos em CPS. Os resultados são classificados de acordo com as abordagens associadas ao processo e resposta e setores envolvidos a partir da análise dos *frameworks* propostos pela literatura selecionada.

São identificados dezesseis artigos que abordam sobre modelos ou representações de processos de resposta a incidentes e três sobre o relacionamento de *stakeholder*s. O subcapítulo é dividido em quatro seções: a primeira apresenta os principais setores de aplicações dos CPS. A segunda seção apresenta as principais abordagens para resposta a incidentes cibernéticos em CPS com a análise dos *frameworks* de processos e de relacionamento entre *stakeholder*s. A terceira seção foca na análise dos *frameworks* de processos, suas fases, os principais elementos e tipos de representação gráfica. A quarta e última seção foca na análise dos *frameworks* que tratam do relacionamento entre *stakeholder*s e as principais formas de representação.

3.2.1 Setores de aplicação dos CPS

Os CPS são sistemas que podem ser aplicados em diferentes setores considerados críticos para sociedade. A partir da análise do referencial teórico, obtém-se maior detalhamento de informações sobre o contexto de setores em que estão sendo desenvolvidas ações para promoção da segurança cibernética dos CPS. Os resultados da análise (Figura 9) indicam que os autores focam especialmente no setor de energia elétrica, indústria, saúde, abastecimento de água, financeiro, petróleo, governo e transporte. Também existem trabalhos que abordam os setores de forma genérica.

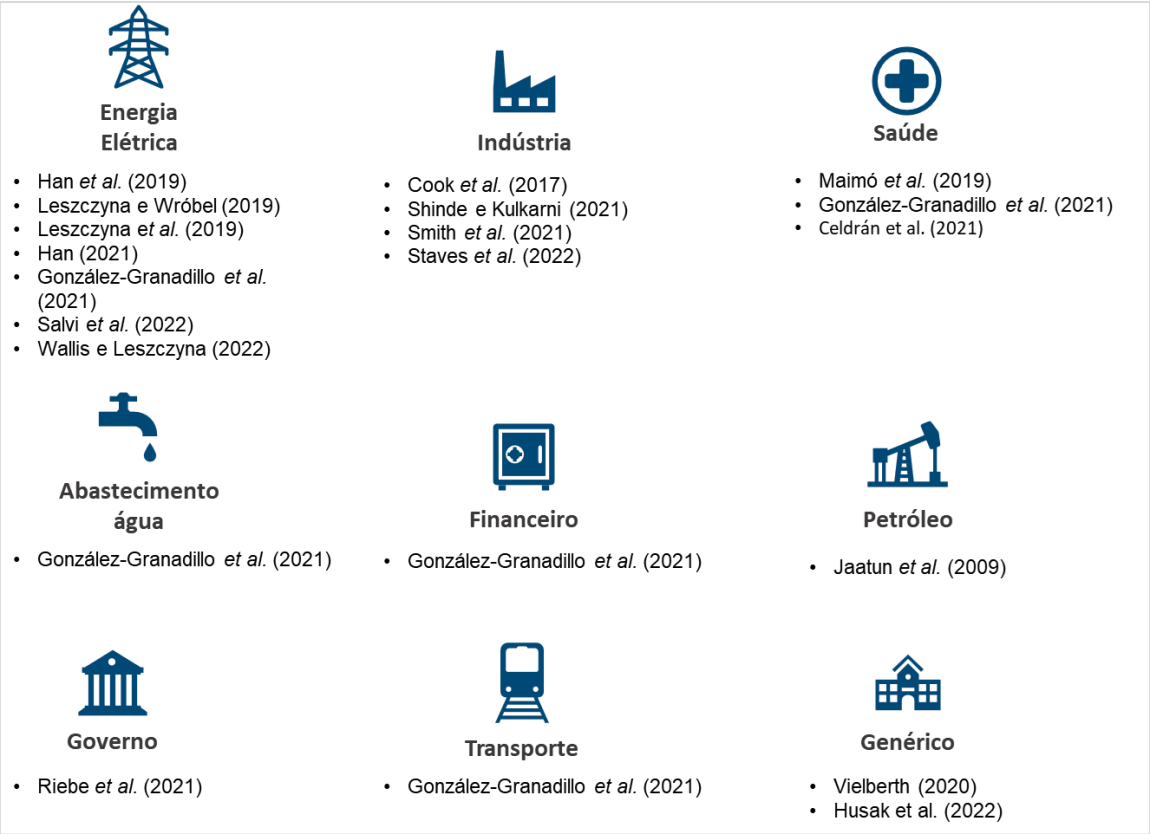


Figura 9 - Setores de Aplicação dos CPS
Fonte: o autor

O setor de energia elétrica é o mais abordado pelos autores, sendo apontado como de alta prioridade devido a dependência de outras infraestruturas (LESZCZYNA, WRÓBEL, 2019). A rede elétrica existente está sendo atualizada para uma rede inteligente, denominada *smart grid* por meio da evolução para infraestruturas de comunicação inteligentes, camadas para troca de informação, bem como tecnologias de computação e sensoriamento (HAN, *et al.*, 2019). Dado o novo cenário, Han *et al.* (2019) realizam estudo para investigar o histórico de ataques ao sistema elétrico coreano e propõem um controle de segurança aprimorado em conjunto com o processo de priorização e bloqueio que deve prever a identificação dos ativos relevantes, execução de processo de bloqueio e de resposta, para proteção de infraestruturas críticas.

O compartilhamento de informações é uma das necessidades mais apontadas para promoção da consciência situacional no setor elétrico, conforme estudos de Leszczyna e Wróbel (2019), Leszczyna *et al.* (2019), Wallis e Leszczyna (2022), Han (2021) e Salvi *et al.* (2022). Nesse contexto, a pesquisa de Leszczyna e Wróbel (2019) sugere um modelo centralizado para troca de

informações entre os *stakeholder*s. A criação de uma base de conhecimento acerca das ameaças emergentes pode ser utilizada para suporte às decisões de defesa cibernética. (LESZCZYNA E WRÓBEL, 2019). Salvi *et al.* (2022) argumentam que o compartilhamento de informações entre *stakeholder*s privados e públicos pode auxiliar na mitigação de riscos cibernéticos no setor elétrico. Han (2021) também defende a explicitação de informações sobre ameaças cibernéticas, no contexto da operação de um SOC.

No setor industrial, a mudança de foco dos ataques de sistemas de TI tradicionais para os Sistemas de Controle Industriais, em inglês *Industrial Control Systems* (ICS) é considerada uma preocupação relevante (STAVES *et al.,* 2022). Cook *et al.* (2017) argumentam que atualizações frequentemente aplicadas em sistemas de TI tradicionais não ocorrem para os ICS, que evoluíram de ambientes isolados que tradicionalmente não dispunham de conectividade externa para arquiteturas integradas. Segundo Cook *et al.* (2017) é de extrema importância a garantia da disponibilidade, confiabilidade e segurança da operação dos ICS. Os autores propõem um conjunto de atividades para investigação e análise de possíveis opções de ataques em uma fase pré-resposta incidente, para aprimoramento da defesa de um ICS. Shinde e Kulkarni (2021) e Staves *et al.* (2022), propõem um *framework* para todas as fases de gestão de um incidente cibernético, prevendo atividades para fases anteriores, durante e após incidentes, ambos em uma estrutura linear de processo de resposta. Smith *et al.* (2021) propõem uma abordagem dinâmica e ágil que permita facilitar o compartilhamento de informações e tornar o processo de resposta mais flexível.

No setor de saúde, dispositivos médicos integrados não foram desenvolvidos de acordo com requisitos de segurança cibernética (CELDRÁN *et al.,* 2021; MAIMÓ *et al.*, 2019). De acordo com Celdrán *et al.* (2021) a segurança cibernética da infraestrutura da rede hospitalar é uma das questões mais críticas que os ambientes clínicos atuais precisam enfrentar. Os CPS médicos (MCPS) referem-se aos sistemas médicos interligados de segurança crítica que analisam os sinais vitais dos pacientes coletados a partir de dispositivos médicos. Os MCPS inferem o estado de saúde do paciente e permitem o compartilhamento automático informações clínicas para médicos ou sistemas automatizados (MAIMÓ, CELDRÁN, *et al.*, 2019). Os autores propõem modelo para detecção,

classificação e mitigação de ameaças de *ramsomware* em ambientes clínicos. De acordo com os autores, as tecnologias atuais de antivírus, *firewalls* e detecção de intrusão são insuficientes para identificação de ameaças em ambientes clínicos. É proposta uma arquitetura com uso de tecnologias de ML para apoio ao processo de análise e decisão Celdrán *et al.*, (2021) propõem uma arquitetura para detecção de ataques e ameaças nas redes dos ambientes clínicos em tempo real que integra componentes de rede com atividades de monitoramento, análise, decisão e reação.

O Governo é abordado no trabalho de Riebe *et al.* (2021) como possível gestor do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança (CERT). De acordo com os autores, os CERT têm papel importante no compartilhamento de informações e aumento do nível de consciência situacional. Os CERT podem ser públicos ou privados e devem ser um ponto focal no desempenho de atividades de prevenção, recebimento de informações e resposta a incidentes de segurança cibernética. Papeis alternativos dos CERT incluem coordenação e compartilhamento com parceiros externos, resolução colaborativa de problemas. compartilhamento de informações sobre incidentes e incentivo ao aprendizado organizacional e sobre incidentes.

No setor de petróleo, Jaatun *et al.* (2009) apresentam uma abordagem sistemática (ciclo de processo) de resposta a incidentes e de aprendizado proativo no setor petrolífero e tratam da necessidade de aprimoramento do processo resposta a incidentes e da necessidade de desenvolvimento de funções gerais de segurança da informação (tecnológica, humana e administrativa) a fim de melhorar o desempenho geral da segurança da informação.

De modo transversal aos setores de abastecimento de água, financeiro e transporte e energia, González-Granadillo *et al.* (2021), pesquisam sobre a solução de Gerenciamento de Informações e Eventos de Segurança, em inglês *Security Information and Event Management* (SIEM) e sua capacidade de coleta, agregação, e armazenamento de eventos gerados por uma infraestrutura crítica gerida. Nesses setores, as infraestruturas críticas são consideradas estruturas organizacionais e físicas cuja falha e/ou degradação pode resultar em perturbações significativas da segurança pública. (GONZÁLEZ-GRANADILLO *ET AL.*, 2021).

De modo genérico, Vielberth (2020) realizam uma análise da literatura para identificação dos principais desafios e aspectos humanos e tecnológicos relacionados aos *Security Operations Center* (SOC) e sua relevância como *stakeholder* responsável pela segurança operacional das organizações no processo de gestão de incidentes. Husak *et al.* (2022) abordam sobre a complexidade da rede de computadores, que dificulta a manutenção da consciência situacional nas organizações. Os autores propõem ferramentas e métodos para os times de segurança com objetivo de aumentar a consciência situacional cibernética em um ambiente amplo e heterogêneo para suporte ao processo de decisão e tratamento de incidentes.

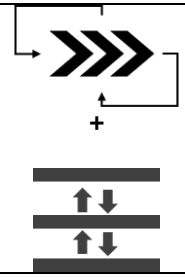
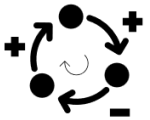
3.2.2 Análise dos *frameworks* sobre resposta a cibernéticos em CPS - processos e relacionamento entre stakeholders

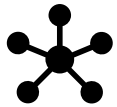
A análise dos *frameworks* que representam abordagens associadas à resposta a incidentes cibernéticos em CPS revela uma diversidade de representações gráficas. São identificados *frameworks* que tratam sobre o processo de resposta a incidentes e que abordam sobre a forma de relacionamento dos diferentes *stakeholder*s envolvidos.

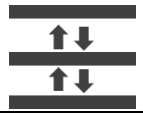
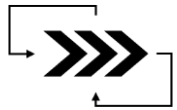
No que tange às representações do processo de resposta a incidentes cibernéticos, são identificados fluxos de processos lineares, cíclicos e com retroalimentação ágil. A maior parte dos artigos identificados apresenta um fluxo sequencial de atividades, com modelo início-fim, ou ponta a ponta, sem retroalimentação intermediária entre as fases do processo de gestão. Alguns autores abordam sobre a necessidade de uma representação de processo com elementos ágeis, com retroalimentação dinâmica e constante entre as diferentes fases. Em relação ao relacionamento entre os *stakeholder*s, identifica-se a predominância de representações gráficas que sugerem interação a partir de um foco central, com representação de estruturas hierárquicas, apesar de alguns autores apontarem a possibilidade de relacionamento entre todos os *stakeholder*s de forma lateral ou *peer-to-peer*. A necessidade de compartilhamento de informação entre os *stakeholder*s é um dos pontos mais destacados pelos autores, devido à necessidade de aumento da consciência situacional.

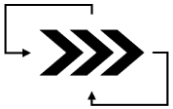
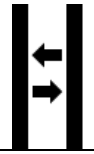
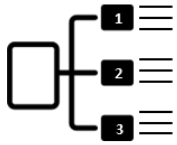
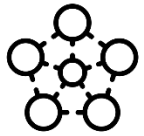
O Quadro 6 apresenta a síntese dos *frameworks* identificados na literatura analisada e descreve os principais objetivos e representações gráficas adotadas pelos autores.

Quadro 6 - *Frameworks* com representação de abordagens para resposta a incidentes cibernéticos

Autor	Foco da representação do *Framework*	Descrição do *Framework* apresentado	Tipo de Representação gráfica	Representação abstrata do *framework*
Jaatun *et al.* (2009)	Resposta a incidentes, com foco na segurança da informação	Processo com fases dispostas de forma cíclica e sequencial que considera possibilidade de alimentação e ajustes em função de mudanças no contexto externo	**Representação Principal** Fluxo de processos cíclico **Elementos adicionais** Setas	
Cook *et al.* (2017)	Fase de pré-resposta a incidentes cibernéticos	Processo com fases dispostas de forma linear e sequencial com fluxograma de atividades pré-resposta a incidentes que alimentam o plano de resposta;	**Representação Principal** Fluxo processos linear **Elementos adicionais** Setas	
Han *et al.* (2019)	Atividades de segurança desempenhadas por um SOC	Processo com fases dispostas de forma linear para resposta a incidentes, com possibilidade de retroalimentação entre as fases. Há representação para troca de informações a partir de fluxo de dados entre as entradas e saídas de cada fase e entre atores/responsáveis por acompanhar cada fases.	**Representação Principal** Fluxo processos linear e Diagrama abstrato de fluxo de dados **Elementos adicionais** Setas, figuras geométricas, como retângulos para agrupamento	
Patiño *et al.* (2019)	Ciclo de vida de resposta a incidente	Diagrama de loop causal. Estabelece a relação entre fases e etapas do ciclo de resposta a incidentes, a partir de uma perspectiva de dinâmica de sistemas. As fases são dispostas de forma cíclica e as etapas de cada fase são representadas a partir do diagrama causal.	**Representação Principal** Diagrama de loop causal, com sequência processual **Elementos adicionais** Setas, retângulos para agrupamento de atividades	
Leszczyna e Wróbel (2019)	Relacionamento entre *stakeholder*s para troca de informações no setor de energia	*Framework* com um foco centralizado, para compartilhamento de informações. Possibilidade de interação *peer-to-peer* apontada pelo autor. O elemento central é plataforma tecnológica para compartilhamento de informações.	**Representação Principal** Interação com foco central **Elementos adicionais** Setas	

Autor	Foco da representação do *Framework*	Descrição do *Framework* apresentado	Tipo de Representação gráfica	Representação abstrata do *framework*
Leszczyna *et al.* (2019)	Relacionamento entre *stakeholder*s. Comunidades para compartilhamento de informação.	*Framework* com um foco centralizado para compartilhamento de informações. Possibilidade de interação *peer-to-peer* apontada pelo autor. O elemento central é um ator com hierarquia superior em relação aos demais stakeholderes	**Representação Principal** Interação com foco central	
Maimó *et al.* (2019)	Ciclo de vida para mitigação de ataques cibernéticos (*ransomware*)	Processo cíclico e sequencial com fases de monitoramento, análise e decisão. Fases de monitoramento e decisão alimentam um modelo de ML que retroalimenta fase de análise.	**Representação Principal** Fluxo de processos cíclico **Elementos adicionais** Setas	
Vielberth (2020)	Alerta e gestão de incidentes	Processo sequencial com ciclo de vida de gestão de incidentes.	**Representação Principal** Fluxo de processos cíclico **Elementos adicionais** Setas	
Han (2021)	Segurança cibernética. Elementos para bloqueio, detecção e resposta.	Processo cíclico e sequencial, para defesa contra ameaças cibernéticas, sem retroalimentação entre fases	**Representação Principal** Fluxo de processos cíclico **Elementos adicionais** Setas	
González-Granadillo *et al.* (2021)	Gestão de eventos de segurança da informação	Processo linear, sequencial e sem retroalimentação entre fases. O processo de gestão de eventos de um SIEM deve apoiar o processo de resposta a incidentes.	**Representação Principal** Fluxo processos linear **Elementos adicionais** Setas	
Riebe *et al.* (2021)	Resposta a incidentes cibernéticos de um CERT	O processo é predominantemente linear e sequencial. Apresenta uma estrutura de troca de informações para coleta de evidências.	**Representação Principal**	

Autor	Foco da representação do *Framework*	Descrição do *Framework* apresentado	Tipo de Representação gráfica	Representação abstrata do *framework*
			Fluxo processos linear e Diagrama abstrato de fluxo de dados **Elementos adicionais** Setas, figuras geométricas	+ 
Shinde e Kulkarni (2021)	Gestão de incidentes	Processo com fases dispostas de forma linear e sem retroalimentação entre as fases. Para cada fase do processo, há descrição de atividades.	**Representação Principal** Fluxo processos linear **Elementos adicionais** Setas e figuras geométricas	
Smith *et al.* (2021)	Resposta ágil a incidentes cibernéticos	Aborda sobre um *framework* ágil. Utiliza artefatos do Scum para o processo de resposta a incidentes, com definição de responsabilidades e ferramentas. Ex.: Sprint, Learning Matrix Incident Backlog, Personas e histórias de usuário.	**Representação Principal** Processo ágil / Scrum	
Celdrán *et al.* (2021)	Arquitetura para segurança cibernética em ambientes clínicos	O processo de resposta a incidentes é abordado de forma linear e está contido em um *framework* de tecnologias de funções virtualizadas de um SDN (Software Defined Network) para promoção da segurança cibernética.	**Representação Principal** Fluxo processos linear e Arquitetura TI **Elementos adicionais** Setas, figuras geométricas	 + 
He *et al.* (2022)	Resposta ágil a incidentes cibernéticos	Processo linear de resposta a incidentes, com fases dispostas de forma linear e prevê a retroalimentação entre as fases. Informações devem ser compartilhadas entre as diferentes fases para aumentar a agilidade durante a resposta a um incidente cibernético.	**Representação Principal** Fluxo processos linear com retroalimentação **Elementos adicionais** Setas	

Autor	Foco da representação do *Framework*	Descrição do *Framework* apresentado	Tipo de Representação gráfica	Representação abstrata do *framework*
Husak *et al.* (2022)	Segurança cibernética durante um incidente	O *framework* proposto utiliza o método OODA (Observar, Orientar, Decidir, Agir). Para cada uma das fases são detalhadas as etapas para gestão de um incidente cibernético. O *framework* apresenta a possibilidade de retroalimentação de informações entre as fases.	**Representação Principal** Fluxo processos linear com retroalimentação **Elementos adicionais** Setas e figuras geométricas	
Salvi *et al.* (2022)	Resposta a incidentes cibernéticos	O *framework* apresenta um processo predominantemente cíclico com duas fases (prevenção e resposta). Cada fase possui 3 camadas hierárquicas. (Ecossistema geral, operacional e técnica.) Existe troca de informações entre as etapas de cada camada.	**Representação Principal** Predominantemente cíclico e Diagrama abstrato de fluxo de dados r **Elementos adicionais** Setas, figuras geométricas	 + 
Staves *et al.* (2022)	Processo de resposta e recuperação de incidentes	As fases do processo são dispostas de forma linear com conotação sequencial, sem retroalimentação. Os processos são classificados a partir de uma taxonomia. É elaborado a partir da análise de padrões técnicos e de um estudo empírico.	**Representação Principal** Classificação de processos, com lógica linear entre as fases	
Wallis e Leszczyna (2022)	Compartilhamento de informações entre *stakeholder*s	*Framework* com múltiplas interações entre os atores. Possibilidade de interação *peer-to-peer,* para compartilhamento de informações.	**Representação Principal** Interação múltipla	

Fonte: o autor

3.2.3 Fases do processo de resposta a incidentes cibernéticos

A partir da análise do processo de resposta a incidentes cibernéticos no contexto dos CPS é realizada consolidação a partir de uma classificação conceitual, conforme Quadro 7. Nessa pesquisa, assume-se que cada fase do processo compreende um conjunto de etapas e que que as etapas compreendem um conjunto de atividades. Dessa forma, é avaliado o conjunto das principais fases do processo de gestão de incidentes cibernéticos de acordo com os processos abordados pela literatura analisada. O processo é avaliado de acordo com seis fases: (1) Planejamento e Preparação; (2) Monitoramento; (3) Detecção; (4) Avaliação/Análise e Decisão; (5) Contenção e Recuperação e (6) Atividades pós incidente.

Quadro 7 - Fases do processo de resposta a incidentes na literatura

Autor	1- Planejamento e preparação	2-Monitoramento	3-Detecção	4-Avaliação/Análise e Decisão	5- Contenção e Recuperação	6-Atividades pós incidente
Jaatun *et al.* (2009)	Preparação		Detecção		Recuperação	Aprendizado
Cook *et al.* (2017)	Triagem para defesa					
Han *et al.* (2019)		Coleta de dados	Detecção		Resposta e Reporte	
Patiño *et al.* (2019)	Preparação		Detecção	Análise	Contenção; Eliminação e Recuperação	Atividades pós incidente
Maimó *et al.* (2019)		Monitorar; treinar modelos de IA	Detectar	Analisar; Decidir	Reagir; Mitigar	Realimentar modelos de IA
Vielberth (2020)	Preparação e coleta de dados	Preparação e coleta de dados	Detecção e análise	Detecção e análise Alerta e priorização	Contenção; Erradicação e Recuperação	Ações pós incidente
Han (2021)	Bloqueio de ameaças		Detecção		Resposta	
González-Granadillo *et al.* (2021)		Coleta; Armazenamento de dados e Monitoramento				
Riebe *et al.* (2021)		Monitoramento	Detecção		Reporte	
Shinde e Kulkarni (2021)	Preparação			Identificação; Investigação	Encerramento e Comunicação	Auditoria e treinamentos
Smith *et al.* (2021)			Detecção	Resposta Inicial ; Formulação da Estratégia de resposta; Investigação	Reporte	
Celdrán *et al.* (2021)		Monitoramento		Análise; Decisão	Reação	
He *et al.* (2022)	Preparação		Detecção	Análise	Contenção; Erradicação; Recuperação	Atividades Pós incidente

Autor	1- Planejamento e preparação	2-Monitoramento	3-Detecção	4-Avaliação/Análise e Decisão	5- Contenção e Recuperação	6-Atividades pós incidente
Husak *et al.* (2022)		Monitorar e coletar dados; Análise e síntese		Decisão	Ação	
Salvi *et al.* (2022)	Prevenção				Resposta	
Staves *et al.* (2022)	Planejamento e preparação			Avaliação dos recursos	Reporte; contenção; Erradicação; Recuperação e Coleta de Evidências	Análise de causa-raíz; Lições aprendidas

Fonte: o autor

A Tabela 6 apresenta o quantitativo de trabalhos que abordam sobre cada fase do processo de resposta a incidentes cibernéticos. A análise do resultado revela a fase de “Contenção e Recuperação” como a mais abordada pela literatura. As fases de “Monitoramento” e “Análise pós incidente” são as menos abordadas apesar de ainda possuírem significativo número de publicações relacionadas.

Tabela 6 - Fases do processo de resposta a incidentes mais abordadas

Fase do processo de resposta a incidentes	Quantitativo de artigos identificados que abordam sobre cada fase
1- Planejamento e preparação	9
2-Monitoramento	7
3-Detecção	9
4-Avaliação/Análise e Decisão	9
5- Contenção e Recuperação	14
6-Atividades pós incidente	7

Fonte: o autor

1. Planejamento e Preparação

A fase de Preparação se refere às atividades de elaboração de planos e preparação para a resposta ao incidente (JAATUN, *et al.* 2009). Nessa fase são constituídas políticas, normas, equipes de segurança e devem ser previstas a elaboração e execução de planos de treinamento, a análise de risco, a avaliação de ativos e aquisição de ferramenta de softwares e hardware (JAATUN, *et al.* 2009; PATIÑO *et al.* 2019; SHINDE & KULKARNI 2021; HE *et al.* 2022). Adicionalmente, nessa devem ser definidos papeis e responsabilidades dos atores envolvidos no processo (STAVES *ET AL.*, 2022). Devido ao dinamismo e necessidade de adaptação aos cenários de incidente, a fase de preparação deve ser executada observando-se as alterações externas ao ambiente organizacional, com aprendizado proativo (JAATUN, *et al.* 2009). Para Cook *et al.* (2017), um plano de resposta a incidente não pode ser desenvolvido apenas com base em medidas protetivas, mas deve considerar a possibilidade de ataques por adversário inteligente e adaptativo.

Quanto ao estabelecimento de políticas, Salvi *et al.* (2022) argumentam as políticas e requisitos normativos devem ser previstas a partir de uma camada

estratégica da organização e os requisitos de prevenção devem ser previstos nas camadas operacionais. O estabelecimento de políticas pode apoiar no bloqueio de ameaças de fontes indesejáveis, de forma a limitar o fluxo de vulnerabilidades já identificadas (HAN, 2021). A análise histórica de dados sobre incidentes cibernéticos (VIELBERTH, *et al.*, 2020) e a implementação de ações a partir de lições aprendidas de outros incidentes cibernéticos (HE *et al,* 2022) também são abordadas como atividades fundamentais para a retroalimentação do processo.

A preparação é a fase inicial do processo de resposta a incidentes cibernéticos, demanda uma análise e entendimento do ambiente externo e da análise histórica de incidentes ocorridos. Nessa fase são definidas as principais políticas organizacionais e responsabilidades e esses instrumentos de gestão devem ser desdobrados em atividades que permitam a identificação de principais vulnerabilidades e execução ações para antecipação aos ataques.

2. Monitoramento

No contexto dos CPS, o monitoramento de incidentes cibernéticos pode ser definido como a fase em que dados gerados por diferentes dispositivos são coletados em tempo real a partir de tecnologias que utilizadas para supervisão da rede (MAIMÓ *et al*. 2019; CELDRÁN *et al.,* 2021). A coleta de dados deve permitir a identificação de eventos de segurança a partir de diferentes fontes (HAN *et al.* 2019; RIEBE *et al.*, 2021). No monitoramento os SIEM desempenham papel fundamental na coleta, armazenamento e correlação de eventos de uma infraestrutura gerida (GONZÁLEZ-GRANADILLO *et al.*, 2021). Apesar de Vielberth (2020) argumentar que a atividade de coleta pode estar associada à fase de preparação, na literatura analisada nessa pesquisa Husak *et al.* (2022), González-Granadillo *et al.* (2021) e Maimó *et al.* (2019) a coleta de dados como uma etapa associada ao monitoramento e observação, que produz insumos para as fases posteriores de Detecção ou de Análise de um processo de resposta a incidentes cibernéticos.

O compartilhamento de eventos e informações obtidos na fase de monitoramento são abordadas por Han *et al*. (2019) e Riebe *et al.* (2021). Han *et al*. (2019) apontam a necessidade de troca de informações entre um ecossistema de SOC em nível nacional. Para Riebe *et al.* (2021). os CERT

devem atuar como instituições que devem assumir o papel de compartilhamento de informações sobre incidentes e incentivas o aprendizado organizacional. Essa abordagem tangencia dificuldades associadas à coordenação e competição entre *stakeholder*s (RIEBE *et al.,* 2021) e expõe dificuldades associadas à sensibilidade dos dados que podem ou deveriam ser compartilhados para aumento da consciência situacional de um determinado grupo de *stakeholder*s.

3. Detecção

A detecção pode ser compreendida como a fase em que os eventos e informações coletados na fase de Monitoramento são analisados de acordo com seus padrões. Esses eventos podem ser analisados por operadores especializados que atuam no monitoramento de sistemas, redes, aplicações e serviços (HAN *et al.*, 2019; HAN, 2021). Incidentes podem detectados com a ajuda de humanos ou por procedimentos automáticos (VIELBERTH, 2020).

Dentre os procedimentos automáticos de detecção e segurança, são destacados sistemas de detecção de intrusão, em inglês *intrusion detection systems* (IDS) (JAATUN *et al.* 2009; SMITH *et al.* 2021) e sistemas de gestão de *log* e *endpoint protection* (SMITH *et al.* 2021). Quanto à detecção realizada a partir de humanos, diferentes canais podem ser utilizados pelos usuários finais para comunicação e reporte às equipes que gerenciam os incidentes, como telefone e e-mail (RIEBE *et al,* 2021). Nesse caso, papeis e responsabilidades devem estar claros para todos os envolvidos que devem ter a consciência sobre a responsabilidade de envio de avisos e alertas quando irregularidades são identificadas (JAATUN *et al.* 2009).

No contexto da operação de Infraestruturas Críticas, Patiño *et al.* (2019) reforçam que o tempo de detecção deve ser o menor possível, de forma a minimizar o impacto causado pelos incidentes. Conforme o volume da ocorrência de incidentes aumenta, maior deve se o nível de vetores de(PATIÑO, *et al.* 2019). Como resultado do processo de detecção de eventos, devem ser coletadas as evidências do incidente (HE *et al.,* 2022) e identificadas as principais vulnerabilidades (HAN *et al.*, 2019), que posteriormente serão utilizadas como insumo na fase de Avaliação/Análise parra tomada de decisão.

4. Avaliação/Análise e Decisão

A literatura aborda a fase de Avaliação/Análise e Decisão como o momento em que as informações obtidas nas fases de monitoramento e detecção devem ser analisadas para a tomada de decisão em resposta ao incidente detectado. A análise é essencialmente um meio de dar sentido ao que é coletado (VIELBERTH, 2020). A opção de seguir com a decisão de conter o incidente ou apenas continuar o monitoramento deve estar embasada nas políticas de segurança estabelecidas (HUSÁK, *et al.*, 2022).

Patiño *et al.* (2019) argumentam que durante a análise, devem ser avaliadas todas as informações disponíveis sobre o incidente detectado. De acordo com os autores, devem ser realizadas correlações com outros ataques e incidentes já registrados para que sejam sugeridos os próximos passos a serem seguidos. Sob o ponto de vista tecnológico, Maimó *et al.* (2019) defendem o uso de tecnologias de ML para apoio à fase de análise de incidentes. Celdrán *et al.* (2021) sugerem o uso de tecnologias de rede que permitam o processamento de pacotes e extração de métricas relevantes a partir da detecção de ataques na rede cibernética.

Shinde e Kulkarni (2021) adotam uma abordagem processual e defendem que os incidentes sejam identificados, priorizados, escalados e investigados de acordo com as causas raízes e possível impacto. Staves *et al.* (2022) ainda abordam sobre a necessidade de avaliação dos recursos disponíveis, diante de um incidente cibernético. He *et al.* (2022) destacam a análise de forma processual e reforçam a importância da priorização de ativos e identificação dos principais *stakeholder*s envolvidos.

He *et al.* (2022) defendem que as fases de Contenção e Recuperação devem ser acionadas mesmo que todo o processo de análise ainda não tenha sido finalizado, de modo que o ciclo de gestão de incidente seja executado e retroalimentado de forma ágil e adaptativa ao cenário do incidente. A abordagem de He *et al.* (2022) permite que as equipes de segurança possam investigar qualquer ativo comprometido assim que há alguma identificação, sem que haja necessidade de acionamento e finalização de todo o processo de gestão de incidente. Além de He *et al.* (2022), Smith *et al.* (2021) também defendem a incorporação de princípios ágeis, para análise de incidentes cibernéticos, devido ao grande nível de incertezas e imprevisibilidade dos ataques aos CPS.

5. Contenção e Recuperação

A fase de Contenção e Recuperação compreende atividades relacionadas à defesa contra a ameaça cibernética externa (Han, 2021). Essa fase abrange um conjunto de ações que devem ser executadas para mitigação, supressão e erradicação do incidente do incidente cibernético (HUSAK *et al.*, 2022; PATIÑO *et al.*, 2019; STAVES *et al.*; 2022). Nessa fase, conforme Husak *et al.* (2022), as ações devem ser executadas por operadores humanos com auxílio de softwares para execução de atividades passíveis de automação para recuperação dos sistemas. Han *et al.* (2019) argumentam que as atividades dessa fase são de difícil padronização e a criação de procedimentos automatizados de defesa contra ameaças sem a interação entre humanos para normalização de padrões, discussões e decisão são de extrema importância. Mesmo com o apoio de softwares de IA para suporte à decisão, a resposta e tomada de ações para contenção do incidente devem ser tomadas a partir de ação humana (MAIMÓ *et al.*, 2019).

Após erradicação do incidente, devem ser desempenhadas ações para recuperação ao estágio normal (VIELBERTH, 2020). Nessa fase devem ocorrer a recuperação dos ativos (PATIÑO *et al.*, 2019), a coleta de evidências (STAVES *et al.*; 2022), a documentação e modificação da infraestrutura existente (SHINDE & KULKARNI; 2021), o reporte e comunicação aos *stakeholder*s externos (HAN *et al.*, 2019; RIEBE *et al.*; 2021; STAVES *et al.*; 2022)

Apesar da literatura analisada convergir para o conjunto de ações que devem ser tomadas durante essa fase, alguns autores questionam o fluxo linear tradicional e apontam a necessidade de atuação ágil do processo de resposta e recuperação. A dinâmica de um ataque cibernético complexo pode exigir várias interações e revisões da estratégia de resposta, dependendo das informações obtidas durante o ataque. A hierarquia tradicional de um processo de resposta pode afetar a eficiência do processo no contexto dos CPS (SMITH *et al.* 2021). Desde 2009 Jaatun *et al.* (2009) argumentam que um processo de resposta a incidentes não opera isoladamente dentro de uma organização e deve ser sempre ajustado à dinâmica externa da organização.

Nesse contexto, Salvi *et al.* (2022) defendem uma coordenação ágil entre os times de resposta a incidentes. Smith *et al.* (2021) e He *et al.* (2022),

entendem que a integração de princípios do *Agile* pode acelerar e tornar mais efetivo o processo, tonando a comunicação mais efetiva entre os *stakeholder*s e acelerando a tomada de ações para contenção mesmo que todas as outras fases anteriores ainda não tenham sido totalmente concluídas. Entretanto, em ambas as pesquisas os processos de resposta ágil não foram testados em grandes organizações ou em um contexto real de resposta a incidente e carecem de validação quanto a sua efetiva aplicação em casos reais de gestão de incidentes cibernéticos em CPS.

6. Atividades pós incidente

Durante a fase pós incidente, devem ser discutidas lições aprendias e analisadas as causas raízes dos incidentes cibernéticos (STAVES *et al.*; 2022). A fase de aprendizado depende da coleta de informações (PATIÑO *et al.*, 2019) e da documentação dos incidentes e deve cobrir questões organizacionais e fatores humanos (JAATUN, *et al*. 2009). Shinde e Kulkarni (2021) apontam para a necessidade de auditorias e treinamentos para os envolvidos Shinde e Kulkarni (2021). Sob o ponto de vista do uso ferramentas de aprendizagem de IA, Maimó *et al.* (2019) argumentam que os modelos de dados devem ser retroalimentados com informações dos incidentes, para que possam suportar novos ciclos detecção e análise.

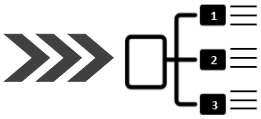
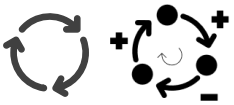
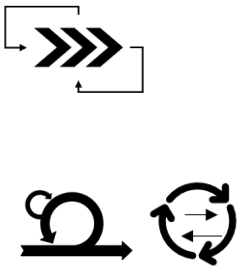
A necessidade de retroalimentação da fase de preparação pelas atividades pós incidentes é abordada Jaatun *et al.* (2009), Patiño *et al.* (2019) e Vielberth (2020), que deixam claro em seus *frameworks* a constituição de um ciclo fechado e contínuo de resposta a incidentes cibernéticos. Desse modo, o processo de resposta pode se aprimorar continuamente, a partir de informações obtidas pelas atividades executadas e da constante observação e análise do ambiente em que os CPS estão inseridos

3.2.4 Formas de representações de processos de resposta a incidentes cibernéticos em CPS

Os *frameworks* apresentados pelos autores para representação gráfica do processo de resposta a incidentes cibernéticos em CPS podem ser classificados em três grupos temáticos (Quadro 8): (a) Linear sequencial, sem

retroalimentação entre as fases intermediárias; (b) Cíclico sequencial com retroalimentação após fase final; (c) Linear ou cíclico com retroalimentação entre as fases intermediárias / ágil.

Quadro 8 - *Frameworks* de processos – representações gráficas

Forma do Processo	Representações abstratas	Autores	Total de representações
(a) Linear sequencial, sem retroalimentação entre as fases intermediárias		Cook *et al.* (2017); González-Granadillo *et al.* (2021); Riebe *et al.* (2021); Shinde e Kulkarni (2021); Celdrán *et al.* (2021).	5
(b) Cíclico sequencial com retroalimentação após fase final		Jaatun *et al.* (2009); Patiño *et al.* (2019); Maimó *et al.* (2019); Vielberth (2020); Han (2021)	5
(c) Linear ou cíclico com retroalimentação entre as fases intermediárias / ágil		Han *et al.* (2019); He *et al.* (2022); Husak *et al.* (2022); Smith *et al.* (2021); Salvi *et al.* (2022)	5

Fonte: o autor

(a) Linear sequencial, sem retroalimentação entre as fases intermediárias

Os processos lineares, sem retroalimentação, são apresentados como uma sequência de atividades ponta a ponta, com início e fim. Todos os modelos representam as atividades a partir de fluxogramas simples e é identificado elevado nível de divergência no escopo de atividades tratadas por cada um dos autores analisados, conforme descrito a seguir:

- Atividades pré-incidente no contexto de um ICS (COOK *et al.*, 2017);
- Atividades de detecção e análise para monitoramento (GONZÁLEZ-GRANADILLO, *et al.*, 2021);
- Atividades de resposta de incidentes desempenhadas por um CERT (RIEBE, *et al.*, 2021);

- Atividades de Gestão de incidentes a partir de análise de normas técnicas e estudo empírico com consultorias (SHINDE, KULKARNI, 2021);
- Atividades de resposta a incidentes cibernético no contexto em ambiente clínico (CELDRÁN *et al.*, 2021).

Cook et al (2017) apresentam uma sequência de atividades que devem ser observadas na fase de pré-resposta a um incidente, com objetivo de preparação e elaboração de um plano de resposta, para defesa de um ICS. As atividades propostas têm como objetivo identificar as principais rotas de ataques que podem ser exploradas por um invasor, para investigação e análise de possíveis opções de resposta. Apesar de Cook et al (2017) defenderem a necessidade de se considerar o adversário como um ator adaptativo, o *framework* apresentado não aborda como o processo poderia ser retroalimentado com dados reais de um eventual ataque cibernético. As rotas de um possível ataque são estudadas apenas a partir de testes e monitoramento.

González-Granadillo *et al.* (2021) realizam uma análise da tecnologia dos SIEM, que possuem a capacidade de coletar, agregar, armazenar e correlacionar eventos gerados por uma infraestrutura gerida. O processo proposto pressupõe atividades que permitem o monitoramento de dispositivos de infraestruturas críticas e servem como ferramenta para prevenção, deteção e reação contra ataques cibernéticos (GONZÁLEZ-GRANADILLO *ET AL.*, 2021). A dificuldade para análise de grande quantidade e dados coletados é apontada como desafio pelos autores.

Riebe *et al.* (2021) apresentam um processo de resposta a incidentes de um CERT e citam as fases de aquisição, análise e resposta como as principais fases de um processo de resposta a incidente. O *framework* evidencia de forma mais clara atividades de coleta, detecção e reporte e não explicita as fases de análise e resposta. Além do fluxo de atividades, Riebe *et al.* (2021) abordam sobre o fluxo de informações que devem ser trocadas a partir de uma estrutura de comunicação para coleta. Embora Riebe *et al.* (2021) citem CERTs como um ponto focal nas atividades de prevenção, recebimento de informação e resposta a incidentes de segurança cibernética, não apresentam visualmente como essa interação poderia ser realizada, de modo a explicitar as eventuais as relações e estruturas de coordenação para compartilhamento de informações.

Shinde e Kulkarni (2021) realizam um estudo empírico com consultorias organizacionais e propõem um *framework* de gestão de incidentes focados nas fases de preparação, identificação, investigação, encerramento e comunicação. O *framework* proposto uma combinação das fases em comum de padrões técnicos da Organização Internacional de Normalização, do Instituto Nacional de Padrões e Tecnologia dos Estados Unidos e do *Information Technology Infrastructure Library.* O fluxo é linear, as fases não são detalhadas e não há uma discussão de como as organizações responsáveis por operar um ICS podem adaptá-lo ao seu contexto.

Celdrán *et al.* (2021) propõem uma arquitetura para detectar e mitigar ataques cibernéticos em infraestruturas móveis de ambientes clínicos. O *framework* é focado em aspectos técnicos das tecnologias de rede e, portanto, não detalha fases de processos de resposta a incidentes. As tecnologias de virtualização são abordadas de forma prioritária em relação ao processo.

(b) Cíclico sequencial com retroalimentação após fase final

Os *frameworks* de estrutura cíclica, identificados na literatura analisada, apresentam a disposição das fases do processo de resposta a incidentes de modo mais homogêneo quando comparado aos *frameworks* lineares sequenciais. As fases são dispostas como um clico de vida de resposta, que perpassa pelas fases pré-incidente, durante e pós incidente. Os processos cíclicos apresentam um conceito de continuidade para a resposta a incidentes, onde os resultados sempre alimentam as fases pré-incidentes, o que mantém processo atualizado. Entretanto, retroalimentação do processo é realizada apenas após toda a execução do fluxo, não havendo previsão de interações intermediárias para troca de informações nos *frameworks* analisados.

Jaatun *et al.* (2009) apresentam um *framework* cíclico de gestão de incidentes de informação com foco em sistemas SCADA e prevê as fases de preparação, detecção, recuperação e aprendizado. O trabalho foca em aspectos socio-técnicos, considerando a relação entre indivíduos e tecnologias e aborda sobre a importância do aprendizado contínuo e proativo na fase de preparação ou pré-incidente. A relação de aprendizado também é abordada por Patiño *et al.* (2019), que argumentam sobre a necessidade de manutenção de uma equipe e permanente treinada, para lidar com a complexidade dos ataques cibernéticos.

Em seu *framework* propõem um diagrama de *loop* causal que procura representar a complexidade da relação de causa e efeito das etapas de cada fase de um processo de resposta a um incidente. Entretanto, o fluxo em nível macro, com as principais fases de resposta que preveem a preparação, detecção e análise, contenção e atividades pós incidentes são representadas de forma cíclica e sequencial, sem análise de causa e efeito, o que reduz a profundidade da análise de relação e complexidade entre as diferentes fases

O *framework* proposto por Maimó *et al.* (2019), prevê as fases de monitoramento, análise, decisão e reação e é apoiado pelo uso de tecnologia de IA que utiliza dados derivados da fase de decisão para treinamento do modelo. Os resultados do modelo de ML fornecem padrões e informações adicionais para as fases de análise do processo de resposta a incidentes, apoiando na detecção de anomalias e classificação dos ataques. Diferentemente das abordagens de Jatatun *et al.* (2009) e Patiño *et al.* (2019), os autores não consideram a dimensão humana durante o ciclo de vida de gestão de incidentes e direcionam o foco para componentes tecnológicos que podem prover insumos para o processo e consequentemente aumentar a segurança cibernética dos CPS.

Han (2021) apresentam um *framework* cíclico composto pelas fases de bloqueio, detecção e resposta, no contexto de operação de um SOC. O bloqueio pode ser interpretado como uma fase de preparação pré-incidente, onde os autores sugerem que ameaças devem ser identificadas e o acesso a conteúdo identificado como suspeito deve ser previamente bloqueado. O *framework* proposto não aborda as fases pós incidente e como os dados resultantes do processo poderiam retroalimentar o ciclo.

(c) Linear ou cíclico com retroalimentação entre as fases intermediárias / ágil

Os *frameworks* identificados na literatura com estrutura linear ou cíclico com retroalimentação entre as fases intermediárias apresentam as fases do processo de resposta de incidentes de modo similar. Em uma crítica aos processos lineares e sequenciais, He *et al.* (2022) argumentam que a estrutura rígida consome tempo elevado para resposta. De modo similar, Smith *et al.*(2012) ponderam que os processos rígidos tradicionais tornam o processo de

proteção das infraestruturas e funções do negócio mais difícil, em um contexto de ataques multifacetados.

Para Salvi et al (2021), o cenário é dinâmico e novas ameaças são introduzidas enquanto um complexo incidente ainda está sendo tratado. Ainda de acordo com os autores, a coordenação ágil deve ser considerada como instrumento de gestão para promover o aumento da consciência situacional cibernética. Apesar de se aproximarem e fornecerem elementos para que um contexto de maior dinamismo de resposta a um incidente cibernético, as interações intermediárias entre as fases para troca de informações ou mudança de ações representam maior complexidade para execução empírica desses modelos. Quanto à representação gráfica do processo, Han *et al.* (2019); He *et al.* (2022); Husak *et al.* (2022); Salvi *et al.* (2022) constroem *frameworks* seguindo uma estrutura linear. Salvi *et al.* (2022) apresenta uma estrutura cíclica e Smith *et al.* (2021) preveem o uso de artefatos ágeis do Sistema Ágil de Gerenciamento de Projetos denominado Scrum para o processo de resposta a incidentes;

No modelo de processo apresentado por Han *et al.* (2019) são previstas as fases de Coleta, Detecção e Análise, Resposta e Reporte. Os autores têm como objetivo apresentar essas atividades no escopo de um SOC do sistema elétrico. O *framework* prevê a troca de dados e informações entre a fase de resposta e detecção, de modo que a análise detalhada de um incidente possa gerar insumos para detecção de novas vulnerabilidades. Apesar de prever a troca de informações durante a operação de segurança de um SOC, o processo representado pelo *framework* não detalha como os resultados das atividades pós incidente poderiam retroalimentar todo o processo.

He *et al.* (2022) propõem um *framework* ágil para resposta a incidentes no setor de saúde e fazem críticas ao processo de resposta a incidentes como um processo linear de resposta a incidentes, devido sua rigidez, morosidade e previsibilidade. O processo apresentado no *framework* é composto pelas fases de Preparação, Detecção/Análise, Contenção (que retroalimenta a fase anterior), Erradicação/Recuperação (que retroalimenta as duas fases anteriores) e Atividades Pós Incidente. De acordo com He *et al.* (2022), um *framework* ágil, ou híbrido, aumenta a possibilidade de retorno rápido à normalidade e melhoria no processo de lições aprendidas. Para atingir esse objetivo, devem ser previstas a

interação e comunicação efetiva com os *stakeholder*s envolvidos com entregas ágeis e incrementais, de modo que não seja necessária aguardar a conclusão de todas as atividades de uma determinada fase do processo de resposta a incidentes para que as demais fases sejam iniciadas. Apesar do *framework* proposto estar mais aderente ao contexto complexo da gestão de incidentes cibernéticos, existem dificuldades para avaliação empírica do *framework* (HE *et al.*, 2022).

Husak *et al.* (2022) abordam sobre dificuldade de manutenção da consciência situacional devido complexidade da rede cibernética, o que dificulta o processo de tomada de decisões. A consciência situacional pode ser definida como “a habilidade de perceber e compreender o ambiente cibernético e estar preparado para projetar uma condição ou situação futura” (HUSAK *ET AL.*, 2022). O *framework* proposto por Husak *et al.* (2022) prevê as fases de Monitoramento, Análise, Decisão e Supressão do Incidente. Todas as fases devem retroalimentar o monitoramento, de modo que se possa ter uma maior consciência situacional durante essa fase. Husak *et al.* (2022) apontam aspectos técnicos relacionados ao volume e performance de dados como um desafio e, apesar de destacarem a importância do fator humano no processo de decisão, não avaliam os desafios relacionados à essa dimensão. Além disso, o *framework* não aborda fases de pré e pós incidente.

Salvi et al (2021) focam nas fases de prevenção e resposta e o modelo proposto visa minimizar e reduzir os impactos dos ataques cibernéticos. A tecnologia de gêmeos digitais é utilizada para coleta e processamento de dados, de modo a prover feedbacks de forma ágil. Na camada técnica, as fases de prevenção e resposta alimentam o modelo de aprendizado, que pode funcionar como uma plataforma de testes para geração de informações para deteção e recuperação. Na camada organizacional, apesar de citarem a importância de colaboração entre organizações, a representação do *framework* apresentado pelos autores limita-se à discussão de aspectos regulatórios.

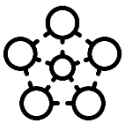
Smith *et al.* (2021) propõem o uso de artefatos e processos ágeis do Scrum para criar uma dinâmica que permita maior flexibilidade e decisão coletiva na resposta de um incidente cibernético em um ambiente ICS. O aumento da consciência situacional a partir da construção decisão coletiva e uma resposta com maior flexibilidade é um dos objetivos propostos pelos autores. Embora

critiquem o modelo linear de resposta a incidentes, os autores não chegam a propor um novo processo, limitando-se apenas a utilização de forma adaptada do método Scrum e seus artefatos no processo de resposta a incidentes.

3.2.5 Representações da relação de Stakeholders no processo de gestão de incidentes

As representações gráficas de relacionamento entre *stakeholder*s, identificadas na literatura analisada, podem ser classificadas de acordo com o seu modelo de interação: (A) Interação entre *stakeholder*s com centralização (B) Interação múltipla entre os *stakeholder*s. O Quadro 9 detalha as representações de acordo com a forma de interação.

Quadro 9 - *Frameworks de* representações da relação entre stakeholders

Forma da interação	Representações abstratas	Autores	Total de representaçõ es
(A) Interação entre *stakeholder*s com centralização		Leszczyna e Wróbel (2019); Leszczyna *et al.* (2019)	2
(b) Interação múltipla entre os *stakeholder*s		Wallis e Leszczyna (2022)	1

Fonte: o autor

(a) Interação entre *stakeholder*s com centralização

Em relação à representação com interação centralizada, Leszczyna e Wróbel (2019) abordam sobre compartilhamento de informações no setor de energia partir de uma plataforma centralizada. Os autores defendem a existência de duas topologias básicas de compartilhamento de informações: nodal centralizado e descentralizado. Adicionalmente, preveem um terceiro modo de interação denominado confederado, que pressupõe o compartilhamento de informação entre grupos nodais centralizados. Quanto ao modo de comunicação, preveem o envio de informações de modo unidirecional ou bidirecional entre os atores do grupo e o nó central.

Leszczyna e Wróbel (2019) apresentam uma plataforma para troca de informações entre os principais *stakeholder*s. Apesar de abordarem sobre a possibilidade de troca de informações de forma bilateral entre os atores, o *framework* proposto prevê uma plataforma central para compartilhamento de dados de detecção de ameaças, reporte de incidentes e análise de incidentes objetivando o aumento da consciência situacional. A plataforma proposta deve ficar sob gestão central de uma parceria público privada, o Centro de Análise e Compartilhamento de Informações, em inglês, *Information Sharing and Analysis Center* (ISAC). Apesar dos benefícios desse modelo de compartilhamento, Leszczyna e Wróbel (2019) apontam dificuldades associadas à resistência de alguns atores no compartilhamento de dados sensíveis e apontam a anonimização de dados como um pré-requisito para essa arquitetura. O *framework* apresentado por Leszczyna e Wróbel (2019) prevê o uso da plataforma de compartilhamento de informações entre os seguintes *stakeholder*s: governo, institutos de padrão/ normatização, centros de pesquisa, vendedores, *utilities* e o ISAC. Leszczyna *et al.* (2019) também utilizam representação de um ISAC como um gestor central do compartilhamento de informações, apesar de argumentarem que a troca de informações pode ser realizada de forma *peer-to-peer*. Para os autores, o *stakeholder* central deve atuar como um moderador da comunicação e garantidor da distribuição por toda a comunidade de *stakeholder*s. Entretanto, o modelo proposto não detalhe como o processo de moderação deve ser realizado.

(b) Interação múltipla entre os *stakeholder*s

Wallis & Leszczyna, (2022) evoluem a discussão sobre compartilhamento de informações para o nível mais operacional entre centros de operação do setor elétrico. Em seu modelo, prevê a centralização a partir de um Grupo de Resposta de Incidentes de Segurança da Computação, em inglês, *Computer Security Incident Response Team* (CSIRT), que são destacados em níveis nacionais para promover o para compartilhamento de informações entre diferentes SOC e provedores de serviços de segurança. No modelo proposto por Wallis e Leszczyna (2022) é o *framework* apresentado prevê de troca de informações de forma lateral entre os atores. Os CSIRT aparecem apenas como possíveis receptores de todas as informações, tornando a comunicação mais interativa, o

que diverge dos modelos centralizados propostos por Leszczyna e Wróbel (2019) e Leszczyna *et al.* (2019)

4. ESTUDO DE CASO SOBRE O PROCESSO DE RESPOSTA A INCIDENTES NO CONTEXTO DA OPERAÇÃO DE REDES ELÉTRICAS NO SEB

O presente capítulo apresenta os resultados do estudo de caso sobre o processo de resposta a incidentes no contexto da operação de redes elétricas no SEB e setores relacionados. Os resultados do estudo contribuem para avaliação da aderência e aplicabilidade das abordagens para proteção de CPS identificadas na literatura e apresentadas no Capítulo 3, a partir de um estudo empírico em organização responsável por operação de instalações de geração e transmissão de energia elétrica do SIN. A supervisão e controle da operação são realizadas com apoio sistemas de supervisão denominados SCADA, considerados um tipo de CPS e que demandam alto grau de disponibilidade e segurança.

Adicionalmente, o estudo de caso também considera o contexto da discussão da segurança cibernética em âmbito nacional e no SEB. Conforme abordado no Capítulo 1, observa-se o desenvolvimento da legislação e discussão regulatória sobre segurança cibernética no Brasil e no SEB. Os resultados dessa discussão também refletem no desenvolvimento de medidas de segurança no âmbito da:

- coordenação de ações setoriais no SEB;
- Rede Federal de Gestão de Incidentes Cibernéticos (REGIC), que envolve a participação de órgãos e entidades da administração pública em nível nacional.

Dessa forma, o primeiro subcapítulo trata sobre elementos da perspectiva geral da legislação e regulamentação sobre o tema no Brasil e da perspectiva do SEB, a partir de análise documental e de entrevistas. O segundo subcapítulo trata sobre os elementos do contexto específico das ações desempenhadas pela instituição avaliada. Por fim, o terceiro subcapítulo trata sobre o relacionamento entre *stakeholders* no processo de resposta a incidentes cibernéticos abordando a relação entre diferentes entidades e órgãos no contexto geral do Brasil e do SEB.

No que tange à lógica que une os dados às proposições, o primeiro e segundo subcapítulos abordam individualmente sobre a avaliação do processo

de resposta a incidentes e relação aos seguintes elementos discutidos no Capítulo 3 do presente trabalho:

- Fases do processo de resposta a incidentes;
- Formas de representações do processo de resposta a incidentes;

O terceiro subcapítulo trata das representações da relação de stakeholders no processo de resposta a incidentes

Assim, as três subseções deste capítulo apresentam resultados correspondentes aos três grupos de análise abordados no Capítulo 3 e apresentam a percepção dos entrevistados e o resultado da análise documental em relação aos elementos questionados e busca responder o seguinte objetivo específico de pesquisa:

- Avaliar a aderência e aplicabilidade das abordagens identificadas na literatura em relação processo de resposta a incidentes cibernéticos no cenário da operação de redes elétricas, a partir de um estudo empírico no Setor Elétrico Brasileiro (SEB) e em setores relacionados;

As questões elaboradas, assim como o detalhamento da condução do estudo de caso são apresentadas no Protocolo de Pesquisa, no Apêndice I da presente pesquisa.

4.1 AVALIAÇÃO DO PROCESSO DE RESPOSTA A INCIDENTES CIBERNÉTICOS – NÍVEL BRASIL E SEB

Neste subcapítulo são analisadas a aderência e aplicabilidade das abordagens e fases do processo de resposta a incidentes cibernéticos no contexto brasileiro e no SEB. São consideradas as percepções dos entrevistados de quatro diferentes organizações e entidades do SEB, assim como a análise documental da legislação e regulamentação associada ao tema. Adicionalmente, para análise de aderência e aplicabilidade, são utilizados como referência a síntese das fases do processo de resposta a incidentes cibernéticos, apresentadas na seção 3.2.3 e os resultados da consolidação das representações de processos de resposta a incidentes abordadas na seção 3.2.4.

4.1.1 Fases do processo de resposta a incidentes - Nível Brasil e SEB

Em relação à perspectiva geral do processo de resposta a incidentes, todos os entrevistados concordam que as fases do processo de resposta a incidentes cibernéticos, consolidadas a partir da análise da literatura, estão aderentes ao contexto das organizações. Um entrevistado do Grupo 1 reportou que sua instituição desempenha importante papel no SEB nas fases de Detecção, Avaliação/Análise e Decisão, Contenção e Recuperação e Atividades pós incidente, obtendo e consolidando informações de demais agentes do setor e entende que cultura de segurança cibernética ainda está em fase de desenvolvimento no Brasil

Outro entrevistado do Grupo 1 informou que sua organização, pertencente à esfera pública federal e ao SEB, está focada em atender os dispositivos de regulamentos que são publicados pelo Poder Concedente, a exemplo do Plano de Gestão de Incidentes Cibernéticos (PLANGIC). A Portaria estabelece que os órgãos e as entidades participantes da Rede Federal de Gestão Incidentes utilizem o PLANGIC como orientação (GSI, 2022).

Um entrevistado do Grupo 2 afirmou que sua organização possui processo de resposta a incidentes implementada, entretanto não enxerga um processo de resposta a incidentes consolidado como referência no SEB. Outro entrevistado do Grupo 2 reportou que que sua instituição está focada internamente nas fases de prevenção, monitoramento e detecção.

No que tange à análise da regulamentação sobre o tema, no SEB não foi identificado um dispositivo regulatório definidor de um processo de resposta a incidentes para orientação agentes do setor, a exemplo do PLANGIC na esfera pública federal. O Conselho Nacional de Política Energética (CNPE) é responsável por definir estratégia e política de desenvolvimento do setor de energia elétrica (BRASIL, 1997), publica a Resolução nº 24/2022, que sugere o estabelecimento de uma estrutura de coordenação setorial e o estabelecimento de procedimentos para identificação continuada de instalações estratégicas críticas (CNPE, 2021a). A ANEEL, a partir da publicação da REN ANEEL 964/2021, dispõe sobre a política de segurança cibernética a ser adotada pelos agentes (ANEEL, 2021b) e o ONS, a partir da publicação da Rotina Operacional

RO-CB.BR.01, estabelece requisitos mínimos a serem implementados pelos agentes do SEB (ONS, 2023).

Apesar de não existirem disposições que tratem de forma específica sobre um processo de resposta a incidentes cibernéticos no contexto do SEB, a REN ANEEL 964/2021 trata da necessidade de os agentes do setor notificarem incidentes que afetem que de maneira substancial a segurança das instalações e compartilharem informações (ANEEL, 2021b). Durante as entrevistas, a necessidade de atendimento a esses requisitos foi abordada e confirmada por três entrevistados, representantes das organizações 1, 3 e 4. O Quadro 10 sintetiza os resultados obtidos em relação à perspectiva geral sobre o processo de resposta a incidentes no contexto do Brasil e do SEB.

Quadro 10 - Perspectiva geral sobre o processo de resposta a incidentes no contexto do Brasil e SEB.

Perspectiva de Análise	Resultados análise documental e entrevistas	Avaliação em relação à literatura
Há um processo para resposta a incidentes cibernéticos?	No nível da esfera pública federal, o PLANGIC é um plano orientativo para instituições que está sendo adotado por organizações desse grupo No contexto do SEB, não foi identificado um processo de resposta a incidentes ou instrumento regulatório orientativo. Entretanto foi identificada a necessidade notificação e compartilhamento de informações sobre incidentes relevantes pelos agentes do setor para grupo centralizado.	A literatura não aborda sobre a necessidade de criação de um processo comum para um setor específico, como o de energia. Entretanto, a necessidade de consciência situacional e de compartilhamento de informações, é abordada por Leszczyna et al. (2019).
As fases do processo de resposta do referencial teórico se aplicam ao contexto do SEB ou em sua instituição?	Todos os entrevistados concordam que as fases do processo se aplicam ao contexto de sua instituição e/ou do SEB. Na esfera federal, as fases do PANGIC se assemelham as fases do processo do referencial teórico	As fases de resposta a incidentes, abordadas pela literatura e sintetizadas da seção 3.2.3 são aplicáveis ao contexto empírico do SEB e se assemelham ao contexto do PLANGIC.

Fonte: o autor

Conforme destacado no Quadro 10, na esfera pública federal existe um plano orientativo que descreve as principais fases do processo de resposta a incidentes. Entretanto esse plano é mais abrangente e não é específico para o

contexto de CPS ou infraestruturas críticas. No SEB, foi identificado um grupo coordenação setorial para recebimento de informações sobre incidentes cibernéticos. Esse resultado indica que há intenção de criação de uma estrutura para aumento da consciência situacional do setor a partir de notificação de incidentes, apesar de não estarem explícitos os processos e tecnologias que serão utilizados para alcance desse objetivo.

Em relação às fases específicas do processo de resposta a incidentes cibernéticos, todos os entrevistados consideram que as fases de (1) Planejamento e Preparação; (2) Monitoramento; (3) Detecção; (4) Avaliação/Análise e Decisão; (5) Contenção e Recuperação e (6) Atividades pós incidente se aplicam ao contexto de resposta a incidentes cibernéticos, o que demonstra uma aderência da abordagem da literatura em relação à prática executada pelas organizações.

Na fase (1) Planejamento e Preparação, são avaliados os requisitos associados ao estabelecimento de regulamentos, políticas planos e normas; constituição de equipes de segurança, estabelecimento de processo de gestão de risco, análise do histórico de lições aprendidas e relacionamento com outras instituições.

Em relação ao estabelecimento de políticas, normas e regulamentos foi identificado a partir das entrevistas que, no âmbito nacional, a publicação do Decreto 10.222, de 2020 que estabelece a Estratégia Nacional de Segurança Cibernética e, no âmbito do SEB, a publicação da Rotina Operacional do ONS, RO-CB.BR.01 e a REN ANEEL 964/2021 são considerados importantes marcos.

A partir da análise documental da evolução regulatória sobre o tema, são identificados 12 instrumentos regulatórios que estabelecem diretrizes e orientações normativas diretamente relacionadas ou associadas à segurança cibernética no Brasil e no do SEB. A Figura 10 destaca os principais instrumentos publicados entre os anos de 2018 e 2023.

Figura 10 - Legislação e regulamentação associada a Segurança Cibernética
Fonte: o autor

O Quadro 11 apresenta a síntese dos objetivos da legislação e regulamentação identificadas, com detalhes sobre o escopo, foco, objetivos e observações relevantes sobre abordagens relacionadas à resposta a incidentes cibernéticos.

Quadro 11 - Detalhamento sobre a legislação e regulamentação publicadas sobre Segurança Cibernética no Brasil

Legislação/ Regulamento	Ano	Escopo	Foco	Objetivos	Observações sobre abordagem em relação Processo de Resposta a incidentes cibernéticos	Referências
Decreto 9.637 /2018 - Política Nacional de Segurança da Informação	2018	Brasil	Segurança da Informação	Institui a Política Nacional de Segurança da Informação com finalidade de assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação em âmbito nacional. O Decreto sugere a divisão do tema em módulos de forma que contemple a segurança e defesa cibernética, a segurança de infraestruturas críticas, à segurança da informação e proteção de dados.	Institui equipe de prevenção, tratamento e resposta a incidentes cibernéticos, coordenada pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) do Departamento de Segurança da Informação do GSI.	(BRASIL, 2018b)
Decreto 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas	2018	Brasil	Proteção das Infraestruturas Críticas	Estabelece a Política Nacional de Segurança de Infraestruturas Críticas, que tem como propósito promover a segurança e a resiliência das infraestruturas críticas do Brasil e a continuidade da prestação de seus serviços	Dentre os instrumentos propostos pela política, estão a Estratégia Nacional de Segurança de Infraestruturas Críticas e o Plano Nacional de Segurança de Infraestruturas Críticas.	(BRASIL, 2018a)

Legislação/ Regulamento	Ano	Escopo	Foco	Objetivos	Observações sobre abordagem em relação Processo de Resposta a incidentes cibernéticos	Referências
Decreto 10.222/2020 - Estratégia Nacional de Segurança Cibernética	2020	Brasil	Segurança Cibernética	Estabelece ações estratégicas com foco no aumento da maturidade sobre a segurança cibernética no Brasil, a partir do fortalecimento de governança, do incentivo ao desenvolvimento do arcabouço legal e do estímulo à ampliação da cooperação entre instituições nacionais e internacionais.	Recomenda o estabelecimento de protocolos e requisitos referentes à prevenção, ao monitoramento, ao tratamento, e à resposta aos incidentes computacionais, voltados às equipes especializadas que tratam das ameaças cibernéticas Sugere a elaboração de planos de resposta a incidentes e de recuperação dos ambientes críticos que podem ser impactados pelos incidentes cibernéticos, a partir da interação conjunta entre Governo e operadores de infraestruturas críticas.	(BRASIL, 2020a)
Decreto 10.748/2021 - Instituição da Rede Federal de Gestão de Incidentes Cibernéticos	2021	Entidades da administração pública federal	Segurança Cibernética	Com foco na administração pública federal, institui REGIC, que cria equipe específica para prevenção, tratamento e resposta a incidentes cibernéticos, coordenada pelo GSI e que deve operar em cooperação por entidades da administra	Dentre os objetivos da REGIC, estão a divulgação de medidas de prevenção, tratamento e resposta a incidentes cibernéticos, o compartilhamento sobre ameaças e vulnerabilidades, divulgação de informações sobre ataques, além da promoção da cooperação entre os participantes da rede	(BRASIL, 2021)
Portaria 120/2022 GSI Aprova o PLANGIC	2022	Entidades da administração pública federal	Segurança Cibernética	Aprova o PLANGIC, com foco administração pública federal e tem como objetivo estabelecer procedimentos de gestão de incidentes cibernéticos para os participantes da REGIC	A Portaria complementa as instruções normativas sobre o tema a serem observados pelos profissionais dos órgãos e entidades. O PLANGIC dispõe sobre as seguintes fases do processo de resposta a incidentes cibernéticos: (1) Preparatória, (2) Prevenção, (3)	(GSI, 2022)

Legislação/ Regulamento	Ano	Escopo	Foco	Objetivos	Observações sobre abordagem em relação Processo de Resposta a incidentes cibernéticos	Referências
					Detecção, (4) Tratamento de incidentes cibernéticos, (5) Resposta, (6) Pós Incidente	
Decreto 10.569/2020 - Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas	2020	Brasil	Proteção das Infraestruturas Críticas	Documento orientador, que organiza os objetivos e iniciativas estratégicas em eixos estruturantes, direciona os esforços a serem empenhados para proteção e sinaliza os resultados a serem alcançados, inclusive sobre a adoção de medidas para segurança cibernética de infraestruturas críticas.	Incentiva a adoção de recursos e de procedimentos voltados para a segurança cibernética nas infraestruturas críticas As atividades associadas a um ativo ou de um sistema envolvem riscos, os quais devem ser identificados, caracterizados e, em seguida, analisados quanto à necessidade e viabilidade de aplicação de controles, de modo a reduzir a probabilidade de ocorrência dos eventos relacionados a tais riscos.	(BRASIL, 2020b)
Decreto 11.200/2022 - Aprova o Plano Nacional de Segurança de Infraestruturas Críticas	2022	Brasil	Proteção das Infraestruturas Críticas	O plano trata do detalhamento das ações estratégicas, com definição de metas, responsáveis e prazos.	Dentre as ações do plano, dispõe sobre a necessidade de integração dos temas Segurança Cibernética e Segurança de Infraestruturas Críticas e define ações para exercícios, conscientização e protocolos de integração entre CTIR Gov e o Sistema Integrado de Infraestruturas Críticas, que deve ser implementado pelo GSI	(BRASIL, 2022)
Resolução CNPE 01/2021	2021	SEB	Segurança Cibernética	Institui Grupo de Trabalho para estabelecimento de diretrizes de Segurança Cibernética no SEB	O Grupo de Trabalho deve abordar sobre os aspectos relativos à prevenção, tratamento, resposta a incidentes e resiliência sistêmica.	(CNPE, 2021b)

Legislação/ Regulamento	Ano	Escopo	Foco	Objetivos	Observações sobre abordagem em relação Processo de Resposta a incidentes cibernéticos	Referências
Resolução CNPE 24/2021	2021	SEB	Segurança Cibernética	Aprova diretrizes para Segurança Cibernética do SEB considerando aspectos de prevenção, tratamento, resposta e resiliência sistêmica.	Dentre as diretrizes definidas, estão a implementação de ações de gerenciamento de riscos e ameaças cibernéticas, o estabelecimento de requisitos e controles mínimos de segurança cibernética, o estabelecimento de políticas que promovam a utilização de recursos tecnológicos e o estímulo à melhoria contínua e estabelecimento de procedimentos para identificação continuada de serviços e instalações estratégicas consideradas críticas.	(CNPE, 2021a)
Rotina Operacional ONS - RO-CB.BR.01 / 2021	2021	SEB	Segurança Cibernética	Estabelece controles mínimos de segurança cibernética para o Ambiente Regulado Cibernético, definindo requisitos mínimos que devem ser implementados pelos agentes do SEB.	Devem ser executadas ações que prevejam o inventário de ativos, gestão de vulnerabilidades e monitoramento e resposta a incidentes. Os agentes devem implementar um plano de resposta a incidentes que contemple a identificação dos cenários de riscos cibernéticos, classificação do impacto, equipes envolvidas, critérios para ativação do plano.	(ONS, 2023)
Resolução Normativa ANEEL 964/2021	2021	SEB	Segurança Cibernética	Estabelece as diretrizes e o conteúdo mínimo das políticas de segurança cibernética a serem adotados pelos agentes do SEB.	Estabelece as diretrizes gerais de segurança cibernética para: -identificação, proteção, diagnóstico, resposta e recuperação dos incidentes cibernéticos Os incidentes devem ser identificados, avaliados, classificados e tradados conforme processo de gestão de	(ANEEL, 2021b)

Legislação/ Regulamento	Ano	Escopo	Foco	Objetivos	Observações sobre abordagem em relação Processo de Resposta a incidentes cibernéticos	Referências
					riscos estabelecidos individualmente por cada agente. Adicionalmente, devem ser estabelecidas políticas de segurança cibernética, que disponham sobre a capacidade para prevenir, detectar, responder e reduzir a vulnerabilidade relacionadas a incidentes cibernéticos.	
Portaria do Ministério de Minas e Energia (MME) 662/2022	2022	SEB - Escopo do MME	Segurança Cibernética	Institui a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) do Ministério de Minas e Energia.	Define a composição da equipe da ETIR.	(MME, 2022)
Decreto 11.856/2023	2023	Brasil	Segurança Cibernética	Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança	Tem como um de seus objetivos estimular a adoção de medidas de proteção cibernética e de gestão de riscos para prevenir, evitar, mitigar, diminuir e neutralizar vulnerabilidades, incidentes e ataques cibernéticos, e seus impactos.	(BRASIL, 2023)

Fonte: o autor

Em relação à publicação dos normas e regulamentos, constata-se que o esforço para legislação e regulamentação sobre segurança cibernética no Brasil é recente, assim como a discussão na literatura acadêmica e que a criação de diretrizes, planos, grupos e definições de responsabilidades ainda está em desenvolvimento. A evolução regulatória evidencia o foco em temas relacionados à segurança da informação, proteção de infraestruturas críticas e segurança cibernética. Existem regulamentos de abrangência nacional, restritos ao setor público federal e ao SEB. A Figura 11 apresenta o quantitativo de publicações ao longo dos anos e sugere evolução recente da discussão sobre o tema assim em linha com o identificado no resultado da análise bibliométrica da RS, apresentado no subcapítulo 3.1.

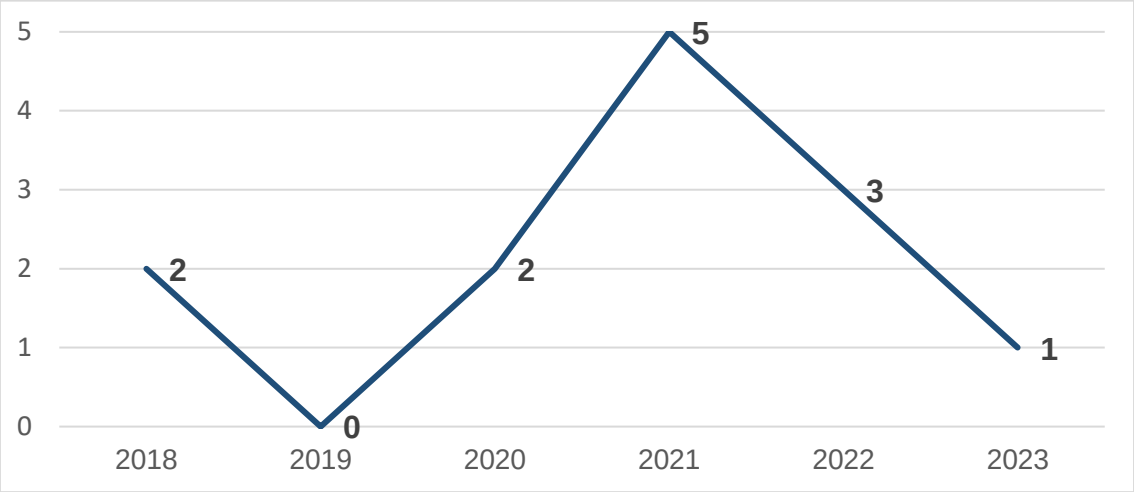


Figura 11 - Evolução publicação legislação e regulamentação
Fonte: o autor

Em contrapartida, apesar da evolução do número de publicações, os entrevistados de uma organização do Grupo 1 entendem que há grande dispersão na discussão normativa e regulatória, o que dificulta a implementação e o acompanhamento pelas instituições impactadas. Além disso, os entrevistados informaram ainda que a discussão normativa não acompanha a necessidade de evolução natural sobre o tema segurança cibernética e que a Estratégia Nacional, estabelecida a partir do Decreto 10.222 de 2020 precisa ser desdobrada. Esses entrevistados informaram que sua organização está focada na observância à legislação sobre o tema.

No que tange ao estabelecimento de planos específicos para resposta a incidentes cibernéticos, foi identificado o PLANGIC, publicado a partir da Portaria GSI 120 de 2022, e que está restrito ao escopo público federal (GSI, 2022).
No contexto específico do SEB, um dos entrevistados do Grupo 2 informou que entende não haver um plano específico no contexto do SEB e que a REN ANEEL 964/2021 publicada pela ANEEL foca no estabelecimento de diretrizes e delega aos agentes o estabelecimento de políticas de segurança cibernética e define a necessidade de comunicação de incidentes à agência reguladora. Um dos entrevistados do Grupo 1 afirmou que entende que a regulamentação do setor e avaliação do regulador desempenha papel mais educativo com sugestão de boas práticas e evolução do aprendizado, com objetivo desenvolvimento do nível de maturidade no setor.

Quanto à constituição de equipes de segurança, em âmbito nacional e no contexto do SEB, a partir da análise documental foram identificadas as seguintes disposições listadas no Quadro 12.

Quadro 12 - Disposições sobre a constituição de equipes de segurança

Legislação/Regulamento	Disposições sobre Equipes de Segurança	Referências
Decreto 9.637 /2018 - Política Nacional de Segurança da Informação	Cria o Comitê Gestor da Segurança da Informação, para assessorar o GSI em atividades relacionadas à segurança da informação. Dispõe da necessidade de cooperação entre as equipes de prevenção, tratamento e resposta a incidentes Cibernéticos com o CTIR Gov.	(BRASIL, 2018b)
Decreto 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas	Estabelece que o GSI deve ser responsável pelo acompanhamento dos assuntos pertinentes às infraestruturas críticas no âmbito da administração pública federal.	(BRASIL, 2018a)
Decreto 10.222/2020 - Estratégia Nacional de Segurança Cibernética	Sugere o estabelecimento de um modelo centralizado de governança no âmbito nacional, por meio da criação de um sistema nacional de segurança cibernética e criação de grupos de debate sob coordenação do GSI.	(BRASIL, 2020a)
Decreto 10.748/2021 - Instituição da Rede Federal de Gestão de Incidentes Ciber (Regic)	Estabelece que o GSI deve ser responsável pela Rede Federal de Gestão de Incidentes Cibernéticos, por meio do CTIR Gov. Equipes de prevenção, tratamento e resposta devem compartilhar informações com o CTIR Gov.	(BRASIL, 2021)
Portaria 120/2022 GSI	Estabelece que o CTIR Gov é responsável pela coordenação da REGIC.	(GSI, 2022)
Decreto 10.569/2020 - Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas	Estabelece que a Segurança de infraestruturas críticas está no rol de competências da Câmara de Relações Exteriores e Defesa Nacional. GSI deve desenvolver o trabalho de identificação e	(BRASIL, 2020b)

Legislação/Regulamento	Disposições sobre Equipes de Segurança	Referências
	análise de riscos das infraestruturas críticas do País.	
Decreto 11.200/2022 - Aprova o Plano Nacional de Segurança de Infraestruturas Críticas	GSI deve implantar e manter o Sistema Integrado de Dados, promover a cooperação com órgãos e entidades nacionais e internacionais, articular e cooperar com órgãos e entidades públicas e privados, coordenar grupos técnicos, integrar grupo de gerenciamento de crise. Ministérios devem elaborar em colaboração com órgãos e entidades do setor público e privado, planos setoriais de segurança de Infraestruturas críticas.	(BRASIL, 2022)
Resolução CNPE 01/2021	Cria Grupo de trabalho para discussão de diretrizes. Define que o grupo é composto por representantes do MME (coordenador), GSI, ONS, ANEEL, Empresa de Pesquisa Energética (EPE) e Câmara de Comercialização de Energia Elétrica (CCEE).	(CNPE, 2021b)
Resolução CNPE 24/2021	Propõe estabelecimento de estrutura de coordenação setorial para atuação em incidentes cibernéticos no SEB (em conformidade com o Decreto 10.748) Órgãos de Coordenação Setorial devem implementar ações. -ANEEL e ONS devem estabelecer requisitos e controles mínimos de segurança. -ANEEL deve estabelecer estrutura de coordenação setorial -ANEEL e ONS devem apoiar na identificação das instalações estratégicas.	(CNPE, 2021a)
Rotina Operacional ONS - RO-CB.BR.01 / 2021	ONS estabelece controle mínimos de segurança para agentes do setor.	(ONS, 2023)
Resolução Normativa ANEEL 964/2021	ANEEL ou equipe de coordenação setorial são responsáveis pelo recebimento de notificação de incidentes cibernéticos de maior impacto pelos agentes do SEB definidos na Resolução.	(ANEEL, 2021b)
Portaria MME 662/2022	Institui Equipe de Prevenção, tratamento e resposta a incidentes cibernéticos do MME.	(MME, 2022)
Decreto 11.856/2023	Institui um Comitê Nacional de Cibersegurança com a finalidade de acompanhar a implantação e evolução da Política Nacional de Cibersegurança	(BRASIL, 2023)

Fonte: o autor

A partir da análise do Quadro 12, identifica-se como estrutura de equipe de segurança em âmbito nacional o CTIR Gov. O CTIR Gov é Grupo de Resposta a Incidentes de Segurança, em inglês "*Computer Security Incident Response Team"* (CSIRT) que tem por objetivo coordenar e integrar as ações destinadas à gestão de incidentes computacionais em órgãos ou entidades da Administração Pública Federal (GSI, 2021).

Em relação ao SEB, identifica-se o grupo de coordenação setorial liderado pela ANEEL para recebimento de notificação de incidentes cibernéticos pelos

agentes do setor (ANEEL, 2021b). Ressalta-se que o papel do grupo de coordenação setorial do SEB não tem a função específica de e não está prevista na regulamentação estrutura específica para coordenação de ações relacionadas à prevenção, monitoramento e análise de incidentes para o setor.

No que tange ao processo de Gestão de Riscos para a proteção das infraestruturas críticas, a Estratégia Nacional de Segurança de Infraestruturas Críticas trata da institucionalização da gestão de riscos na administração pública e entidades privadas como um grande desafio. Dentre as iniciativas estratégicas propostas está a “obrigatoriedade de adoção de medidas para sistematização de práticas relacionadas à gestão de riscos, aos controles internos e à governança”(BRASIL, 2020b). Em relação à Segurança Cibernética, a Estratégia Nacional de Segurança Cibernética trata sobre a gestão de riscos como “um dos principais pontos sustentação da governança cibernética, uma vez que indica a adoção de melhores políticas e metodologias, o que permite gerir, de forma otimizada, os limites aceitáveis” (BRASIL, 2020a).

No SEB, a ANEEL estabelece os agentes do setor devem definir os riscos cibernéticos, com a respectiva forma de tratamento (ANEEL, 2021b). Já o ONS estabelece que os agentes devem implementar planos de resposta a incidentes que contemplem a identificação dos cenários de riscos cibernéticos (ONS, 2023). De acordo com resultados NT 84/2021 publicada pela ANEEL em 2021, a grande maioria dos agentes entrevistados realizam avaliação de riscos para garantir segurança onde houver necessidade de acesso de terceiros, o que indica elevado nível de maturidade (ANEEL, 2021a).

Quanto à ocorrência e análise de histórico de incidentes cibernéticos, sob o ponto de vista regulatório, os órgãos e entidades da administração pública devem notificar o CTIR Gov quando da ocorrência de incidentes cibernéticos graves (BRASIL, 2021). No SEB, os agentes devem enviar os registros de incidentes cibernéticos à ANEEL ou à equipe de coordenação setorial (ANEEL, 2021b).

Durante as entrevistas, apenas um entrevistado de uma das organizações informou já ter corrido incidente cibernético de alta relevância com impacto significante em suas operações. Os entrevistados de todas as outras organizações e entidades informaram desconhecer incidente grave que tenham impactado suas instalações ou atividades. No contexto dos agentes do SEB, os

resultados da NT ANEEL 08/2021 corroboram com esse resultado, onde 100% dos agentes entrevistados informaram que “nunca” ou “raramente” sofreram incidentes cibernéticos nos últimos cinco anos que comprometessem a operacionalização de seu negócio (ANEEL, 2021a).

O Quadro 13 sintetiza os resultados obtidos em relação à fase de (1) Planejamento e Preparação, no contexto brasileiro e do SEB.

Quadro 13 - Análise sobre a fase (1) Planejamento e Preparação - Contexto Brasil e SEB

Perspectiva de Análise	Resultados da análise documental e entrevistas	Avaliação em relação à literatura
Estabelecimento de regulamentos, políticas e normas	A legislação e regulamentação no Brasil e no SEB é recente e o tema está em evolução. São identificados instrumentos que tratam sobre: • Segurança da Informação, • Proteção de Infraestrutura Críticas • Segurança Cibernética em âmbito nacional • Segurança cibernética no SEB Os instrumentos estabelecem políticas, estratégias e diretrizes. Planos e regulamentos de caráter orientativo são propostos. Nas entrevistas, alguns entrevistados afirmaram que há certa dispersão normativa que dificulta a adoção pelos atores envolvidos.	Nessa fase são constituídas políticas, normas e equipes de segurança além da elaboração e execução de planos de treinamento, análise de risco, avaliação de ativos e aquisição de ferramenta de softwares e hardware (JAATUN, et al. 2009; PATIÑO et al. 2019; SHINDE & KULKARNI 2021; HE et al. 2022). É nessa fase que devem ser definidos os papeis e responsabilidades. (STAVES ET AL., 2022) do processo de resposta a incidentes.
Constituição de equipes de segurança	Os regulamentos publicados estabelecem a constituição de equipes de segurança responsáveis por coordenar ou cooperar sobre assuntos relacionados à segurança cibernética, com característica centralizada Na esfera nacional, o GSI, por meio do CTIR GOV é responsável por coordenar a REGIC. No SEB, O CNPE determina que a ANEEL estabeleça uma estrutura de coordenação setorial para recebimento de notificações de incidentes.	
Avaliação sobre o processo de gestão de riscos	A Gestão de Riscos é tratada como importante processo para “sustentação da governança cibernética” (BRASIL, 2020a) para identificação dos limites aceitáveis .	
Histórico de incidentes e lições aprendidas	No âmbito da administração pública, incidentes graves devem ser notificados ao CTIR Gov. No SEB, incidentes graves devem ser notificados à ANEEL ou grupo de coordenação setorial.	A análise histórica de dados sobre incidentes cibernéticos (VIELBERTH, 2020) e a implementação de ações a partir de lições

Perspectiva de Análise	Resultados da análise documental e entrevistas	Avaliação em relação à literatura
	Apenas uma das organizações informou já ter sofrido um incidente grave que tenha afetado de forma relevante suas operações. No SEB, não foram identificados casos graves.	aprendidas de outros incidentes cibernéticos (HE et al, 2022) são abordados como atividades fundamentais para a retroalimentação da fase de preparação

Fonte: o autor

Conforme apresentado no Quadro 13, os regulamentos analisados preveem a constituição de controles de segurança cibernética de forma aderente ao disposto na literatura, apesar de existir percepção de certa dispersão sobre as disposições em diversos instrumentos publicados. A análise histórica sobre incidentes cibernéticos ainda é incipiente e não foi possível avaliar se lições aprendidas estão sendo desenvolvidas a partir do histórico de incidentes.

Em relação às fases (2) Monitoramento e (3) Detecção, são avaliados aspectos associados à coleta de informações sobre incidentes, ao uso de tecnologias e compartilhamento de dados entre instituições.

Na administração pública federal, o CTIR Gov é o órgão responsável por coordenar as atividades das equipes de prevenção, tratamento e resposta a incidentes cibernéticos dos integrantes da Rede Federal (BRASIL, 2021). O PLANGIC define que todo participante da REGIC deve estabelecer o monitoramento contínuo de seus ativos de informação. Caso sejam identificadas anomalias, o evento deve ser encaminhado ao CTIR Gov para triagem. Durante as entrevistas apenas um entrevistado desse contexto (Grupo 1) afirmou que que já foi detectado incidente grave e que a comunicação com as entidades competentes foi realizada, mas não houve um retorno ágil com diretrizes a serem seguidas, a partir do incidente reportado.

No SEB, a REN ANEEL 964/2021 dispõe sobre a necessidade de os agentes do setor estabelecerem políticas que tenham como um dos objetivos a detecção de incidentes. Incidentes cibernéticos de maior impacto devem ser notificados à equipe de coordenação setorial, assim que os agentes tiverem ciência do incidentes (ANEEL, 2021b). Um dos entrevistados (Grupo 1) e integrante do grupo de coordenação setorial do SEB, informou nunca ter recebido notificação de incidentes ou compartilhamento de informação de agentes do setor. Entrevistados de duas instituições do Grupo 2 e integrantes do

grupo de coordenação setorial afirmaram ainda que um sistema informatizado está em desenvolvimento para o recebimento de notificações dos agentes o setor. Um dos entrevistados do Grupo 2 informou que os incidentes do SEB são conhecidos prioritariamente de modo informal. O Quadro 14 sintetiza os resultados obtidos em relação às fases (2) Monitoramento e (3) Detecção.

Quadro 14 - Análise sobre às fases (2) Monitoramento e (3) Detecção - Contexto Brasil e SEB

Perspectiva de análise	Resultados da análise documental e entrevistas	Avaliação em relação à literatura
(1) Monitoramento Como é realizada a coleta de dados das instituições? Há compartilhamento de dados monitorados	Na administração pública federal, o CTIR Gov é responsável por receber as informações de incidentes cibernéticos dos integrantes da REGIC. No SEB, os agentes do setor devem compartilhar os dados de incidentes de alto impacto para o grupo de coordenação setorial. Um sistema para compartilhamento de informações está em desenvolvimento.	O compartilhamento de eventos e informações obtidos na fase de monitoramento são abordadas por Han et al. (2019) e Riebe et al. (2021). Han et al. (2019) apontam a necessidade de troca de informações entre um ecossistema de SOC em nível nacional Para Riebe et al. (2021). os CERT devem atuar como instituições que devem assumir o papel de compartilhamento de informações sobre incidentes e incentivas o aprendizado organizacional
(2) Detecção Como são detectados os incidentes cibernéticos? Há histórico sobre evolução dos incidentes detectados?	Tanto no setor público quanto no SEB, cada organização/entidade é responsável por detectar incidentes relacionados ao seu escopo. Quanto ao histórico de incidentes, uma organização do setor público (Grupo 1) afirmou ter notificado incidente. No SEB, nenhum incidente foi notificado até o presente momento. Incidentes são conhecidos a partir de canais informais.	Papeis e responsabilidades devem estar claros para todos os envolvidos, e cada envolvido deve ter a consciência da responsabilidade de enviar alertas quando irregularidades são identificadas (JAATUN et al. 2009). Leszczyna e Wróbel (2019) apontam dificuldades associadas à resistência de alguns atores no compartilhamento de dados sensíveis

Fonte: o autor

A partir dos resultados apresentados no Quadro 14, é possível verificar que tanto no âmbito do CTIR Gov quanto do grupo de coordenação setorial do

SEB há a previsão de estruturas para recebimento de informações obtidas nas fases de Monitoramento e Detecção. Entretanto, os resultados da análise apontam para dificuldades no processo de compartilhamento e análise de dados de incidentes cibernéticos, ou há poucas informações sobre evidências. Essas dificuldades também são relatadas pela literatura analisada, o que indica aderência em relação aos aspectos abordados.

Em relação às fases de (4) Avaliação/Análise e Decisão e (5) Contenção/Recuperação são avaliados o modo como as informações sobre incidentes são analisadas e como a decisão e contenção de incidentes são administradas no âmbito da administração pública federal e no SEB.

Na administração pública federal, o PLANGIC orienta que os incidentes sejam tratados imediatamente após detecção ou notificação provável e ocorrência e explicita detalhadamente um conjunto de etapas e procedimentos que devem ser executados (GSI, 2022). O processo de tratamento de incidentes compreende as etapas de triagem e análise. Após essas etapas, deve ser executado o processo de resposta, que consiste em ações de contenção, erradicação e recuperação. Um dos entrevistados informou ter experenciado o processo de resposta a um incidente grave, mas que o processo de reporte não foi efetivo.

No SEB, a ANEEL estabelece que os agentes do setor desenvolvam mecanismos de cultura de segurança cibernética, incluindo procedimentos para prevenção tratamento e resposta a incidentes (ANEEL, 2021b). Diferentemente do contexto do setor público, a ANEEL não estabelece um plano ou detalha atividades específicas que devem ser executadas por cada agente, entretanto estabelece que a comunicação deve ser realizada via notificação para equipe de coordenação setorial. Um dos entrevistados, integrante do Grupo 1 e integrante do grupo de coordenação setorial do SEB, informou que todos os incidentes notificados devem ter sua criticidade avaliada. Após avaliação, caso seja identificada alta criticidade, as informações devem ser direcionadas ao conhecimento do GSI. Incidentes de baixa criticidade devem ser registrados e considerados em análises estatísticas. Dependendo do nível de criticidade do evento, a equipe de coordenação setorial deve avaliar a comunicação a outros agentes do SEB. No contexto interno de suas organizações, um dos entrevistados do Grupo 2 afirmou haver processo estabelecido para análise de

incidentes, enquanto outro entrevistado informou que as ações são executadas de forma tácita em sua organização, não havendo procedimentos estabelecidos.

O Quadro 15 sintetiza os resultados obtidos em relação às fases de (4) Avaliação/Análise (5) Decisão e (6) Contenção/Recuperação

Quadro 15 - Análise sobre às fases (4) Avaliação/Análise (5) Decisão e (6) Contenção/Recuperação – Nível Brasil e SEB

Perspectiva de análise	Resultados das entrevistas	Avaliação em relação à literatura
Como as informações sobre incidentes são analisadas? É realizada alguma priorização? Se sim, como? Existem procedimentos definidos para contenção/recuperação	Na administração pública federal, o PLANGIC detalha como cada fase do processo de tratamento de incidentes e contenção devem ser executadas. A priorização deve ser realizada a partir de um processo de triagem. Cada equipe deve considerar suas peculiaridades na priorização. No SEB, a REN ANEEL 964/2021 estabelece que os agentes do setor elaborem procedimentos para tratamento de incidentes, de forma geral. O impacto do incidente deve ser avaliado de acordo com a severidade estabelecida a partir do processo de gestão de riscos.	Shinde e Kulkarni (2021) adotam uma abordagem processual e defendem que os incidentes sejam identificados, priorizados, escalados e investigados de acordo com as causas raízes e possível impacto. He et al. (2022) destacam a análise de forma processual e reforçam a importância da priorização de ativos e identificação dos principais stakeholders envolvidos. Han et al. (2019) argumentam que as atividades dessa fase são de difícil padronização e a criação de procedimentos automatizados de defesa contra ameaças sem a interação entre humanos para normalização de padrões, discussões e decisão são de extrema importância.
Como é realizada a comunicação com stakeholders do setor? Há hierarquia para coordenação dessas atividades?	Na administração pública federal, cada equipe é responsável pela comunicação com o CTIR Gov, via correio eletrônico. O GSI coordena a CTIR Gov. No SEB, a comunicação deve ser realizada via notificação para equipe de coordenação setorial. Dependendo do nível de criticidade, outros agentes do setor precisam ser informados. Incidentes graves devem ser direcionados ao GSI	Leszczyna & Wrobel (2021) apontam para importância da criação de uma plataforma centralizada para compartilhamento de informações Entretanto, a hierarquia tradicional de um processo de resposta pode afetar a eficiência do processo no contexto dos CPS (SMITH et al. 2021). Para Smith et al. (2021) e, para He et al. (2022), a integração de princípios do *Agile* pode acelerar e tornar mais efetivo o processo, tonando a comunicação mais efetiva entre os stakeholders e acelerando a tomada de ações para contenção mesmo que todas as outras fases anteriores ainda não tenham sido totalmente concluídas.

Fonte: o autor

Conforme resultados apresentados no Quadro 15, observa-se que no âmbito da REGIC há uma intenção de padronização de atividades para todas a entidades pertencentes à rede, a partir de procedimentos estabelecidos no PLANGIC. Esse ponto contrasta com argumentação de Han et al. (2019) de que as atividades dessa fase são de difícil padronização. No SEB, a criação de procedimentos para resposta a incidentes fica sob responsabilidade de cada agente do setor, havendo possibilidade de adaptação ao seu contexto e realidade. Quanto à hierarquia para coordenação de atividades, tanto a REGIC quanto no arranjo previsto no SEB, são propostas estruturas centrais para notificação de incidentes, o CTIR Gov. e o Grupo de coordenação setorial respectivamente. Apesar de alguns autores como Leszczyna & Wrobel (2021) argumentarem sobre a importância da criação de uma plataforma centralizada para compartilhamento de informações, outros autores, como Smith et al. (2021), alertam para a ineficiência de uma hierarquia tradicional em um processo de resposta a incidentes cibernéticos. Desse modo, há um desafio para as instituições equilibrarem eventuais benefícios da centralização do recebimento de informações e tomada de decisões em detrimento à necessidade de agilidade em um contexto dinâmico de análise e tratamento de incidentes cibernéticos.

Em relação à fase (6) Atividades pós-incidente, são analisados aspectos relacionados as ações executadas após a ocorrência do incidente, incluindo a análise dos registros e envolvimento dos *stakeholders*;

Na administração pública federal, o PLANGIC orienta a análise da documentação dos incidentes como uma ação com foco na melhoria contínua dos processos, de modo a permitir a elevação do nível de maturidade das entidades participantes da REGIC. Um dos entrevistados do Grupo 1 informou que ainda está aderindo à REGIC e que existem dificuldades para seguimento de todos as normas propostas na PLANGIC e que uma interação lateral entre órgãos e entidades seria importante.

No SEB a avaliação das diretrizes propostas pela ANEEL ainda não foi realizada pela agência. Dois entrevistados, um do Grupo 1 e outro do Grupo 2, informaram que a agência ainda não formalizou intenção de realizar fiscalizações no curto prazo e que o papel da agência é mais orientativo. Um dos

entrevistados inclusive informou que as questões relacionadas à fiscalização estão previstas apenas para o horizonte de médio prazo. Quanto à avaliação da aplicação dos requisitos definidos na Rotina Operacional RO-CB-BR.01 do ONS, um dos entrevistados informou que é responsabilidade de cada a agente a declaração sobre a conformidade em relação aos requisitos propostos e que 2023 foi realizada uma autoavaliação dos agentes a partir de uma declaração de atendimento aos requisitos, entretanto os resultados não foram divulgados.

O Quadro 16 sintetiza os resultados obtidos em relação à fase (7) Atividades pós-incidente.

Quadro 16 - Análise sobre à fase (6) Atividades pós-incidente – Contexto Brasil e SEB

Perspectiva de análise	Resultados das entrevistas	Avaliação em relação à literatura
Como os incidentes são analisadas após ocorrência? Como é o envolvimento dos stakeholders nessa fase?	O PLANGIC é a referência que indica a necessidade de implementação de melhoria contínua. Participante do REGIC informou estar ainda aderindo à rede e, consequentemente, implementando ações e que há dificuldades para adesão a diferentes normativos. Participantes da REGIC devem atualizar suas atividades e realizar ações colaborativas no âmbito da REGIC. No SEB a REN ANEEL 964/2021 explicita que as informações devem ser compartilhadas para a equipe de coordenação setorial. Em relação à adequação à Rotina, os próprios agentes devem fazer autoavaliação.	A necessidade de retroalimentação da fase de preparação pelas atividades pós incidentes é abordada Jaatun et al. (2009), Patiño et al. (2019) e Vielberth (2020), que deixam claro em seus frameworks a constituição de um ciclo fechado e contínuo de resposta a incidentes cibernéticos Uma análise de retrospectiva com todos os stakeholders envolvidos e a identificação de necessidades de alterações nas políticas e processos internos deve ser realizada. (HE et al., 2022).
São realizadas auditorias / fiscalizações?	O tópico foi abordado apenas no âmbito do SEB, Ainda não foram realizadas fiscalizações, pois o papel a da agência reguladora no momento é orientativo.	Shinde e Kulkarni (2021) apontam para a necessidade de auditorias e treinamentos para os envolvidos.

Fonte: o autor

A partir dos resultados apresentados no Quadro 16, identifica-se que ainda não há elementos que evidenciem a execução do processo de análise do histórico de incidentes cibernéticos como insumo para melhoria do processo de resposta, especialmente no SEB. Adicionalmente, apesar de Shinde e Kulkarni

(2021) apontarem para a necessidade de auditorias, ainda não foi observada a adoção desse processo. A atualidade sobre o tema pode justificar a baixa obtenção de informações no contexto prático para a fase de atividades pós-incidente.

4.1.2 Formas de representações do processo de resposta a incidentes

No que tange a representação gráfica aplicável ao processo de resposta a incidentes cibernéticos, os entrevistados de todas as organizações entendem que a representação cíclica, em algum grau, já é aplicada ou se aplicaria ao contexto do SEB ou de sua instituição. Um dos entrevistados abordou que a evolução do nível de maturidade da organização tende à adoção de um modelo com representação ágil, onde a velocidade de resposta ao incidente é a métrica mais importante a ser priorizada. Entretanto, outro entrevistado contratou afirmando que adoção de um modelo ágil poderia trazer maior complexidade e que é difícil aplicabilidade no contexto prático de sua organização. Essa interpretação corrobora com o ponto de vista de outros dois entrevistados, cuja instituição está incluída no contexto da REGIC e do SEB. Eles consideram o processo cíclico como suficiente no âmbito de sua organização. Para esses entrevistados, a adoção de um processo ágil não se configuraria como um avanço primordial e um processo cíclico, implementado com eficácia, seria suficiente para o processo de resposta a incidentes cibernéticos. A percepção dos entrevistados corrobora com o disposto no PLANGIC, que aborda o processo de gestão de incidentes cibernéticos a partir de um *framework* cíclico.

Adicionalmente, tem-se a percepção de outro entrevistado que entende que a segurança cibernética ainda está em desenvolvimento no Brasil e que a representação do processo tende a variar entre as formas lineares e cíclicas no SEB. O entrevistado argumentou que os agentes do SEB possuem diferentes níveis de maturidade e que nas empresas multinacionais há tendência de importação de processo e cultura de suas matrizes internacionais. De acordo com o entrevistado, empresas do setor com maior grau de maturidade já discutem, de algum modo, a ideia de agilidade.

Apesar da predominância da abordagem cíclica do processo nas entrevistas, um dos entrevistados informou que as etapas anteriores a resposta

a incidentes são lineares em sua organização. Esse entrevistado e outro de outra organização do SEB informaram ainda que na fase de análise do incidente, cada incidente é avaliado de forma linear e a partir de processos bem definidos.

O Quadro 17 sintetiza os resultados e a avaliação em relação à abordagem da literatura, sobre a representação do processo.

Quadro 17 - Análise sobre a representação gráfica do processo de resposta a incidentes - Contexto Brasil e SEB

Perspectiva de análise	Resultados das entrevistas	Avaliação em relação à literatura
O formato do processo se assemelha ou difere das representações identificadas na literatura?	O processo cíclico sequencial é abordado como aderente e aplicável ao processo de resposta a incidentes cibernéticos no contexto do SEB. No PLANGIC, o processo é abordado de forma cíclica. A evolução para o processo ágil pode ser enxergada como uma evolução natural. Entretanto, o processo ágil pode trazer maior complexidade	Patiño et al. (2019); Maimó et al. (2019); Vielberth (2020) são autores que abordam o processo de resposta a incidentes como um modelo de ciclo de vida Quanto à aplicação empírica de um modelo ágil para resposta a incidentes cibernéticos, a complexidade é um fator abordado por Salvi et. al. (2021)
Há variação de formatos de processo durante as diferentes fases do processo de resposta a incidentes?	Para fases específicas do processo resposta a incidentes, as atividades podem ser executadas de forma linear, especialmente nas etapas pré-incidentes ou na análise de incidentes mais padronizadas.	Cook et al. (2017) apresentam um fluxo linear para as fases de pré resposta a incidentes. O modelo linear alimenta um plano de resposta. Em relação a análise de incidentes, a gestão de eventos de um SIEM é um dos exemplos abordados como processo linear por González-Granadillo et al. (2021)

Fonte: o autor

A partir da análise do Quadro 17 , entende-se que apesar do processo de gestão de incidentes cibernéticos ser interpretado de forma cíclica, alguns entrevistados entendem que existem variações de representação do processo em cada uma de suas fases, especialmente em processos padronizados e bem definidos. Quanto à adoção de um modelo de ciclo de vida para a resposta a incidentes, há aderência na percepção dos entrevistados e no disposto em documentos investigados em relação à literatura analisada. Patiño et al. (2019); Maimó et al. (2019); Vielberth (2020) são autores que abordam o processo de

resposta a incidentes de forma cíclica. Adicionalmente, a complexidade da adoção de um modelo ágil é abordada tanto pelos entrevistados quanto pela literatura a partir de Salvi et. al. (2021), o que demonstra aderência entre a percepção prática de execução do processo de resposta e a abordagem acadêmica.

4.2 AVALIAÇÃO DO PROCESSO DE RESPOSTA A INCIDENTES NO CONTEXTO DO PROCESSO DE OPERAÇÃO DE INSTALAÇÕES DO SIN

Neste subcapítulo são analisadas a aderência e aplicabilidade das abordagens e fases do processo de resposta a incidentes cibernéticos no contexto do processo de operação realizado pela organização definida no objeto de estudo. Adicionalmente, para análise de aderência e aplicabilidade, são utilizados como referência a síntese das fases do processo de resposta a incidentes cibernéticos, apresentadas na seção 3.2.3 e os resultados da consolidação das representações de processos de resposta a incidentes abordadas na seção 3.2.4.

4.2.1 Fases do processo de resposta a incidentes

Em relação à perspectiva geral do processo de resposta a incidentes, todos os entrevistados da organização concordaram ou apresentaram evidências de que as fases do processo de resposta a incidentes cibernéticos, consolidadas a partir da análise da literatura, se aplicam ou estão aderentes ao contexto da organização. O entrevistado da área de Segurança Cibernética informou que há um processo de resposta a incidentes cibernéticos implementado e que as fases sintetizadas a partir da análise da literatura estão aderentes ao contexto prático. Entretanto, esse entrevistado destacou que existe uma atividade executada em paralelo entre fase de “Detecção” e a fase de “Atividades pós incidente” denominada “Coleta e Retenção de Evidências”. Além disso, o entrevistado informou existir um processo de “Gestão de Vulnerabilidades" que inclui, dentre suas atividades, a realização de inventários, a avaliação de vulnerabilidades e adoção de planos de remediação.

Outros dois entrevistados da área de gestão de riscos informaram que atualmente existem instrumentos que normatizam o processo de segurança cibernética e que esse processo está incluído no escopo da Gestão da Continuidade do Negócio (GCN), que tem como objetivo garantir a continuidade dos processos prioritários da organização.

Em resumo, além dos entrevistados da área de segurança cibernética gestão de riscos, os outros quatro entrevistados, da área de operação, telecomunicação, regulação e comunicação institucional concordam as fases (1) Planejamento e Preparação; (2) Monitoramento; (3) Detecção; (4) Avaliação/Análise e Decisão; (5) Contenção e Recuperação e (6) Atividades pós incidente se aplicam ao contexto da organização, consolidadas a partir da análise da literatura, se aplicam ao contexto da organização.

O Quadro 18 sintetiza os resultados obtidos em relação à perspectiva geral do processo de resposta a incidentes cibernéticos no contexto do processo de operação do SEB.

Quadro 18 - Perspectiva geral sobre o processo de resposta a incidentes no contexto do específico de operação de instalações do SIN

Perspectiva de Análise	Resultados análise documental e entrevistas	Avaliação em relação à literatura
Há um processo para resposta a incidentes cibernéticos no contexto da organização?	Existe um processo de resposta a incidentes cibernéticos na organização. Adicionalmente, existe uma Política de Gestão da Continuidade do Negócio.	Salvi et al. (2022) abordam sobre a importância de se estabelecerem políticas e requisitos normativos em uma camada estratégica e requisitos organizacionais de prevenção em camadas operacionais
As fases do processo de resposta do referencial teórico se aplicam ao contexto do SEB ou em sua instituição?	Todos os entrevistados concordam que as fases do processo de gestão de incidentes cibernéticos, consolidadas a partir da análise da literatura, se aplicam ao contexto da organização. Outras etapas poderiam ser explicitadas, como a coleta de dados e evidências entre as fases de monitoramento e pós incidente e a gestão de vulnerabilidades	As fases de resposta a incidentes, abordadas pela literatura e sintetizadas no Quadro 7 são aplicáveis ao contexto empírico Em relação à etapa de coleta de dados, Han et al. (2019) e González-Granadillo et al. (2021) abordam sobre a importância de coleta de dados durante a fase de monitoramento. Staves et al. (2022) aborda sobre a coleta de evidências durante a “Contenção e Recuperação” Em relação à gestão de vulnerabilidades, Han (2021) argumentam sobre a importância

		de se observar e registrar vulnerabilidades já identificadas. Para Han et al. (2019), as principais vulnerabilidades identificadas devem ser utilizadas como insumo na fase de Avaliação/Análise parra tomada de decisão.

Fonte: o autor

A partir dos resultados identificados no Quadro 18, observa-se que as fases do processo de resposta a incidentes cibernético, sintetizadas a partir do referencial teórico, se aplicam ao contexto da organização. Adicionalmente, elementos adicionais do processo abordados pelos entrevistados, como a coleta de evidências e gestão de vulnerabilidades também são abordados por alguns autores na literatura.

Em relação à fase (1) Planejamento e Preparação, conforme previsto na literatura, são avaliados os aspectos associados ao estabelecimento de políticas, normas e procedimentos; constituição de equipes de segurança, estabelecimento de processo de gestão de risco e análise do histórico de lições aprendidas e relacionamento com outras instituições.

No que tange à implementação de políticas internas, institucionalmente há uma Política de GCN da organização que tem como objetivo formalizar o compromisso da organização com a

> gestão continuidade de seus processos prioritários diante de situações adversas, bem como orientar a atuação de seus conselheiros, diretores, empregados e terceiros com vistas a assegurar o nível adequado de estabilidade organizacional nos momentos posteriores a incidentes que causem interrupção e durante a recuperação desses processos e respectivos recursos.

Apesar de não abordar de forma explícita o tema segurança cibernética, a Política define em seus princípios a necessidade da observância de requisitos associados à segurança da informação. Os entrevistados da área de Gestão de Riscos informaram existir no contexto do GCN um Plano de Gestão de Incidentes Cibernéticos (PGI) que define as etapas de notificação do incidente, documentação, resposta, coleta e manipulação de evidências, erradicação e recuperação. Em complemento, os entrevistados indicaram a existência de

outras 2 políticas: Gestão de Riscos e Segurança da Informação. A política de Gestão de Riscos tem como objetivo

> fomentar ações voltadas para a melhoria da gestão de riscos e de controles internos [...] , tornando a organização mais resiliente em cenários adversos e aprimorando o processo de tomada de decisão de acordo com o perfil e apetite a riscos da organização

A política de Segurança da informação tem como um de seus princípios garantir que a informação deve “ser protegida contra ameaças que comprometam a confidencialidade, a integridade e a disponibilidade”. Apesar de ambas as políticas não tratarem de forma específica sobre riscos cibernéticos, há endereçamento para ações voltadas ao aumento da resiliência e proteção contra ameaças aos sistemas de informação.

No que tange aos procedimentos de comunicação dos incidentes, um entrevistado da área de comunicação informou que existem com foco na proteção da imagem da organização e garantia da transparência às partes interessadas. O Guia de Comunicação publicado no *website* da organização formaliza o compromisso da organização na divulgação ampla de informações e na aproximação com a sociedade. Apesar das diretrizes serem generalistas, o entrevistado afirmou que elas são aplicáveis ao contexto de crise por eventual incidente cibernético e que agilidade no processo de comunicação é um dos principais objetivos de desempenho previstos.

No que tange aos instrumentos normativos que se aplicam contexto de todos os agentes do SEB e, consequentemente ao contexto da organização, foram identificados os seguintes documentos públicos: submódulo dos Procedimentos de Rede “2.16 Requisitos operacionais para centros de operação e instalações da Rede de Operação” (ONS, 2022) e a Rotina Operacional RO-CB-BR-01 “Controles mínimos de segurança cibernética para o Ambiente Regulado Cibernético” (ONS, 2023).

No contexto do processo de operação do sistema, um dos entrevistados indicou que o Submódulo 2.16 define a necessidade dos agentes da rede de operação do SEB adotarem políticas e disporem de recursos tecnológicos para proteção contra ataques cibernéticos. O entrevistado da área de operação afirmou que, como recursos para manutenção da disponibilizada, existem procedimentos internos denominados Planos de Preservação de Serviços

Prioritários (PPSP) elaborados com intuito de fornecer diretrizes para que as salas de controle dos centros de operação da organização preservem seus serviços críticos, diante qualquer cenário de incidente que possa comprometer as atividades da operação. Conforme informado pelo entrevistado, os PPSP possuem relação com os instrumentos normativos no âmbito da GCN e preveem um escopo de cenários de crise além dos cenários de ataques cibernéticos.

Em relação ao disposto na Rotina RO-CB-BR-01, um entrevistado da área de Segurança Cibernética informou que o documento é aplicável ao se contexto e ressaltou sobre a importância do cumprimento de todos os requisitos por todas as organizações incluídas no escopo da Rotina, de modo a promover o aumento da segurança cibernética no SEB.

O Quadro 19 apresenta a síntese dos instrumentos normativos da organização, identificados ou mencionados pelos entrevistados.

Quadro 19 - Instrumentos Normativos - contexto do específico de operação de instalações do SIN

Instrumento Normativo	Objetivos	Contexto
Política de Gestão da Continuidade de Negócios	Política corporativa interna, proteção dos processos prioritários da organização	Interno da organização
Política de Gestão de Riscos e Controles Internos	Política corporativa interna, gestão de riscos corporativos que possam impactar a consecução dos objetivos estratégicos	Interno da organização
Política de Segurança da Informação	Política corporativa interna. Foco na proteção das informações	Interno da organização
Guia de Comunicação	Guia corporativo interno. Formaliza o compromisso da organização na divulgação ampla de informações e aproximação da sociedade.	Interno da organização
Plano de Gestão de Incidentes Cibernéticos	Procedimento interno. Foco na Gestão de Incidentes cibernéticos para garantia da continuidade dos processos prioritários	Interno da organização
Submódulo 2.16 dos Procedimentos de Rede - Requisitos operacionais para centros de operação e instalações da Rede de Operação	Procedimentos de Rede. Foco no SEB, com estabelecimento de requisitos para os centros de operação. Dentre os requisitos, está estabelecimento de políticas para proteção contra ataques cibernéticos	SEB
Plano de Preservação dos Serviços Prioritários	Procedimento interno. Foco na preservação dos serviços prioritários das salas de controle, de forma a garantir a manutenção da operação em caso de incidentes que impactem as salas de controle. O escopo do plano vai além da segurança cibernética	Interno da organização
Rotina Operacional ONS - RO-CB.BR.01 / 2021	Rotina Operacional. Foco no SEB. Estabelece controles mínimos de segurança cibernética para o Ambiente Regulado Cibernético,	SEB

Instrumento Normativo	Objetivos	Contexto
	definindo requisitos mínimos que devem ser implementados pelos agentes do setor.	

Fonte: o autor

Em relação à constituição de equipes de segurança, um dos entrevistados afirmou que as equipes são constituídas durante a decretação de crise quando da ocorrência de um incidente cibernético de alto impacto. De acordo com nível de gravidade do incidente, diferentes equipes podem ser acionadas, incluindo colaboradores da área de Tecnologia da Informação ou ainda outros colaboradores. Outro entrevistado informou que no contexto da operação em tempo real nas salas de controle, simulados são realizados periodicamente a partir da criação de cenários de testes para diferentes tipos de crise. Outra ação destacada por outro entrevistado da área de Regulação é a realização de treinamentos periódicos internos para todos os colaboradores, com objetivo de aumentar o nível de conscientização em relação a ataques cibernéticos.

Quanto ao processo de gestão de riscos, dois entrevistados informaram que o tema relacionado a ataques cibernéticos é priorizado no contexto dos riscos corporativos da organização, sendo tratado como um evento de nível relevante. Outro entrevistado da área de segurança cibernética informou que existe um processo complementar à Gestão de Riscos organizacional no âmbito da TI, com objetivo de avaliar constantemente o nível de maturidade da organização.

No que tange à análise do histórico de incidentes, três entrevistados informaram que não há registros de incidentes cibernéticos relevantes que tenham impactado processos da organização. Um dos entrevistados da área de segurança cibernética informou que na fase monitoramento contínuo, eventuais incidentes de baixo impacto e/ou baixa severidade são detectados e tratados sem necessidade de tomada de ações de maior complexidade ou acionamento da estrutura de governança de GCN.

O Quadro 20 sintetiza os resultados obtidos em relação à fase de (1) Planejamento e Preparação, no contexto da organização objeto de estudo.

Quadro 20 - Análise sobre a fase (1) Planejamento e Preparação – contexto do específico de operação de instalações do SIN

Perspectiva de Análise	Resultados análise documental e entrevistas	Avaliação em relação à literatura
Estabelecimento de regulamentos, políticas e normas	São identificados 7 instrumentos normativos, corporativos ou técnicos, com relação ao processo de gestão de incidentes cibernéticos. Apesar de existirem planos focados no processo de resposta, não foi identificada um Política Organizacional sobre o tema.	Nessa fase são constituídas políticas, normas e equipes de segurança além da elaboração e execução de planos de treinamento, análise de risco, avaliação de ativos e aquisição de ferramenta de softwares e hardware (JAATUN, et al. 2009; PATIÑO et al. 2019; SHINDE & KULKARNI 2021; HE et al. 2022). Nessa fase devem ser definidos os papeis e responsabilidades.
Constituição de equipes de segurança	Há previsão de constituição de equipes de segurança durante a decretação de crise, no âmbito da Gestão da Continuidade do Negócio. Na operação em tempo real existem equipes treinadas para preservação dos serviços prioritários para garantir a continuidade da operação do SIN. Esses planos possuem escopo mais abrangente que o cenário de incidentes cibernéticos	
Avaliação sobre o processo de gestão de riscos	Há política organizacional que endereça compromisso da organização em relação ao tema. Incidentes cibernéticos são priorizados no contexto dos riscos corporativos da organização.	
Histórico de incidentes e lições aprendidas	Não há histórico de incidentes cibernéticos de alto impacto. Incidentes de baixo impacto ou severidade são detectados e tratados sem necessidade de tomada de ações de maior complexidade.	A análise histórica de dados sobre incidentes cibernéticos (VIELBERTH, 2020) e a implementação de ações a partir de lições aprendidas de outros incidentes cibernéticos (HE et al, 2022) são abordados como atividades fundamentais para a retroalimentação da fase de preparação

Os resultados apresentados no Quadro 20 demonstram aderência entre a prática executada pela organização e recomendações endereçadas pela literatura acadêmica quanto à fase de Planejamento e Preparação. Apesar de existirem procedimentos internos que abordem sobre o processo de gestão de incidentes cibernéticos, não foram identificadas políticas específicas que

enderecem o tema de segurança cibernética para o contexto interno à organização. Externamente, no escopo do SEB, os Procedimentos de Rede e Rotinas operacionais endereçam a observação de requisitos e controles mínimos, mas não há abordagem sobre processo de resposta a incidentes cibernéticos para o SEB.

Em relação às fases de (2) Monitoramento e (3) Detecção, conforme identificado na literatura, são avaliados aspectos associados ao monitoramento e tratamento de informações sobre incidentes e tecnologias utilizadas para detecção.

Quanto ao monitoramento, um dos entrevistados, da área de segurança cibernética, informou que é utilizado um serviço contratado de SOC para monitoração contínua dos sistemas de TI da organização. Existem dois tipos de infraestruturas de TI segregadas que estão no escopo do serviço de monitoração: a TI corporativa, relacionada aos sistemas internos da organização e a TI operativa, relacionada aos ativos utilizados para operação dos sistemas que dão suporte à operação do SIN. Além disso, o entrevistado afirmou que é utilizada ferramenta de SIEM para correlação de eventos detectados.

Outro entrevistado, da área de operação, informou que além da supervisão contínua da área de tecnologia, operadores do sistema SCADA, na sala de operação, monitoram o sistema continuamente durante 24h e podem identificar incidentes e notificar eventuais anomalias à área de segurança cibernética. Esse entrevistado reforçou que o ambiente monitorado pela TI operativa é segregado da TI corporativa e que por motivos de segurança existem medidas de controle para acesso aos sistemas de supervisão. Adicionalmente, o acesso aos recursos fora da sala de controle só permite acesso às funções restritas do sistema de supervisão.

No processo de monitoramento da rede elétrica do SEB a partir do sistema SCADA, em caso de problemas relacionados a perda do canal de recebimento de informações de determinado agente do setor, por falha ou eventual incidente cibernético em sua rede, existem ferramentas que possibilitam a estimação do estado de operação da rede, mesmo na ausência parcial de informações. Outro entrevistado, da área de telecomunicações, afirmou que existem níveis de segurança de acordo com o nível de tolerância a falha da rede de comunicação. Adicionalmente, informou que há alta

necessidade de disponibilidade de recursos, que demanda cada vez mais robustez da infraestrutura de rede, visando maior disponibilidade possível.

Quanto à detecção de incidentes, um dos entrevistados afirmou que a ferramenta de SIEM adotada possui tecnologias de ML embarcadas para aumento da capacidade de correlação de dados recebidos. Além disso, existem diversas camadas de *intrusion detection* nas redes internas e tecnologias de gestão de credenciais. Outra área entrevistada, de Gestão de Riscos, reforçou que os normativos implantados preveem que todas as evidências e ações tomadas durante eventual resposta a incidente devem ser coletadas e documentadas.

Em relação à evolução de histórico de incidentes, um dos entrevistados da área de Segurança Cibernética informou que existe uma base reduzida para análise, devido à baixa quantidade de ocorrências identificadas e de pequena severidade. No que tange à comunicação e compartilhamento de informações sobre incidentes no SEB, um dos entrevistados informou que entende que ainda não há processo instituído formalmente para comunicação e compartilhamento e incidentes, apesar dos dispositivos regulatórios já previstos na REN ANEEL 964/2021 que regulam o processo de comunicação dos agentes ao grupo de coordenação setorial. O entrevistado reforçou que os incidentes ocorridos setor são conhecidos informalmente, a partir de interações entre os profissionais das organizações e que não há compartilhamento de dados monitorados entre as instituições do setor.

O Quadro 21 sintetiza os resultados obtidos em relação à fase de (2) Monitoramento e (3) Detecção, no contexto da operação do sistema.

Quadro 21 - Análise sobre as fases (2) Monitoramento e (3) Detecção – contexto do específico de operação de instalações do SIN

Perspectiva de análise	Resultados análise documental e entrevistas	Avaliação em relação à literatura
É realizada a coleta de dados da operação de sistemas por sua instituição e/ou outras instituições do setor?	A área de TI administra um SOC para gestão do monitoramento e detecção de incidentes.	A coleta de dados deve permitir a identificação de eventos de segurança a partir de diferentes fontes (HAN et al. 2019; RIEBE et al., 2021).
Há uso de tecnologias de coleta de dados (Ex.: SIEM, SCADA, ou outros sistemas)?	É utilizada ferramenta de SIEM para gestão de eventos. A solução de SIEM possui tecnologias embarcadas de ML para correlação de eventos.	No monitoramento os SIEM desempenham papel fundamental na coleta, armazenamento e

Perspectiva de análise	Resultados análise documental e entrevistas	Avaliação em relação à literatura
	Na operação em tempo real, a rede de supervisão do SIN é monitorada a partir de sistemas SCADA, que possui tecnologias de estimação de estado em caso de perda de informações.	correlação de eventos de uma infraestrutura gerida (GONZÁLEZ-GRANADILLO *et al.,* 2021).
Há compartilhamento de dados monitorados entre as instituições?	Os dados monitorados não são compartilhados com outras instituições. Os incidentes no setor são conhecimentos de modo informal no setor.	O compartilhamento de eventos e informações obtidos na fase de monitoramento são abordadas por Han et al. (2019) e Riebe et al. (2021). Han et al. (2019) apontam a necessidade de troca de informações entre um ecossistema de SOC em nível nacional
Como são detectados os incidentes cibernéticos?	Os incidentes podem ser detectados a partir do uso de tecnologias de SIEM ou a partir da identificação de anomalias na operação tempo real a partir da supervisão por meio do sistema SCADA. Incidentes cibernéticos podem ser detectados pela equipe SOC ou pelas equipes de operação em Tempo Real.	A detecção é compreendida como a fase em que os eventos e informações coletados na fase de Monitoramento são analisados de acordo com seus padrões e pode ser performada por operadores especializados que monitoram os sistemas, redes, aplicações e serviços (HAN et al., 2019; HAN, 2021). Incidentes podem detectados com a ajuda de humanos ou por procedimentos automáticos (VIELBERTH, 2020).
Há uso de tecnologias para detecção (ex.: IDS)?	Existem camadas de *intrusion detection* nas redes internas e tecnologias de gestão de credenciais. Além disso, a infraestrutura de rede possui níveis de tolerância a falha e a rede operativa é segregada da rede corporativa de TI.	
Há histórico sobre evolução de incidentes detectados em sua instituição? Qual sua avaliação em relação ao histórico?	Não há histórico de evolução de incidentes relevante	

Fonte: o autor

No que tange os resultados apresentados no Quadro 21 , identifica-se que as tecnologias utilizadas para monitoramento e detecção de incidentes cibernéticos estão aderentes às abordagens apresentadas pela literatura acadêmica. Entretanto, no contexto prático da organização não está prevista estrutura de compartilhamento entre informações de incidentes entre SOC de outros agentes e/ou instituições do SEB. O compartilhamento de eventos e informações obtidos na fase de monitoramento são abordadas por Han et al. (2019) e Riebe et al. (2021) e que não se aplicam ao contexto atual da operação do SEB. Adicionalmente, identifica-se histórico restrito de incidentes para avaliação.

Em relação às fases de (4) Avaliação/Análise e Decisão (5) Contenção/Recuperação consideram-se as atividades de avaliação das informações sobre incidentes, as atividades relacionadas ao processo de decisão no contexto da operação e as atividades de contenção e recuperação dos sistemas e processos.

No que tange a avaliação dos incidentes internos à organização, um dos entrevistados da área de Segurança Cibernética informou que existe um processo de priorização adotado pelo SOC que ocorre de forma estruturada. Incidentes pontuais e de menor complexidade são identificados e tratados de forma automatizada, como comportamentos suspeitos associados a uso devido de credenciais. Eventos de maior complexidade ou que podem desencadear um processo crise interna são avaliados pela equipe de segurança cibernética e devem ser reportados para o grupo de decisão no escopo do GCN. Conforme relatado pelo entrevistado, existe um processo de comunicação e criação de “sala de guerra”, que decide o que deve ser priorizado. Atualmente não há aplicação de tecnologias para apoio a decisão e o processo não é pré-definido para eventos de alta complexidades. Os atores envolvidos na situação de crise são os *stakeholders* da área de TI, Riscos, *Data Protection Officer* (DPO), e área de comunicação à sociedade, jurídico e agentes do setor. A hierarquia segue o disposto nos processos de GCN, a partir de um comitê que é formado na detecção de crise.

No contexto da operação em tempo real, para aumento da agilidade e garantia da continuidade dos serviços de supervisão e controle, um entrevistado informou que a decisão pela decretação da crise é tomada no contexto das

próprias equipes de tempo real, não havendo necessidade de espera por decisões no âmbito da hierarquia da GCN.

Quanto à fase de Contenção/Recuperação, no contexto interno, um dos entrevistados informou que, para incidentes de menor complexidade e de maior ocorrência, há procedimentos e tecnologias para contenção automatizados ou padronizados, como soluções de *end point*. *protection* e soluções embarcadas. Além disso, *playbooks* são elaborados em conjunto com o SOC. Para incidentes potenciais geradores de crise, não há padronização de procedimentos. Uma das justificativas foi a possiblidade de diversidade de incidentes que deve ser tratada em conjunto com o grupo do GCN.

No contexto da operação em tempo real, um entrevistado informou que existem procedimentos de *backup* e redundância entre as salas de controle. No cenário indisponibilidade local de um centro, o centro de operação de outra localidade possui a capacidade de assumir as atividades. No caso da ocorrência desse processo, em caso de necessidade outros agentes ou instituições do SEB podem ser comunicados. Durante a contingência, o centro afetado inicia processo de recuperação e passa a assessorar o centro que opera em contingência até o total retorno à normalidade. Todas essas atividades estão previstas no escopo dos PPSP.

Ainda em relação à comunicação durante a fase de contenção e recuperação, um dos entrevistados, responsável por esse processo, informou que durante a crise as ações devem ser tomadas de modo ágil. A ação de comunicação depende do nível do impacto, dimensão e da duração do incidente. Além da preocupação com a preservação dos ativos, existem ações que visam a transparência da comunicação com o setor e a proteção da imagem da organização.

O Quadro 22 sintetiza os resultados obtidos em relação às fases de (4) Avaliação/Análise (5) Decisão e (6) Contenção/Recuperação

Quadro 22 - Análise sobre as fases de (4) Avaliação/Análise (5) Decisão e (6) Contenção/Recuperação – contexto do específico de operação de instalações do SIN

Perspectiva de análise	Resultados análise documental e entrevistas	Avaliação em relação à literatura
Como as informações sobre incidentes são analisadas? É realizada alguma priorização? Se sim, como? Quais são os atores envolvidos.	Para análise de incidentes de baixa complexidade, existe processo padronizado adotado pelo SOC. Incidentes de maior complexidade são direcionados para avaliação no escopo da GCN. No contexto da operação em tempo real, devido agilidade, as próprias equipes de tempo real têm autonomia para decretação de crise e execução de ações em seu ambiente. Em relação à priorização e padronização dos processos, a equipe de segurança cibernética reporta incidentes de grande porte ao escopo do GCN. Em relação aos atores, internamente são envolvidos TI, Riscos, DPO e área de comunicação à sociedade, jurídico e agentes do setor. Se impactar o tempo real, a equipe de operação é envolvida.	Shinde e Kulkarni (2021) adotam uma abordagem processual e defendem que os incidentes sejam identificados, priorizados, escalados e investigados de acordo com as causas raízes e possível impacto. A opção de seguir com a decisão de conter o incidente ou apenas continuar o monitoramento deve estar embasada nas políticas de segurança estabelecidas (HUSAK et al., 2022). Husak et al. (2022), argumentam as ações devem ser executadas por operadores humanos com auxílio de softwares para execução de atividades passíveis de automação para recuperação dos sistemas.

Perspectiva de análise	Resultados análise documental e entrevistas	Avaliação em relação à literatura
Existem procedimentos definidos para contenção/recuperação	Para incidentes cotidianos e de menor complexidade no escopo do SOC, há procedimentos e tecnologias para contenção Para incidentes de crise, não há procedimentos detalhados, devido à diversidade de incidentes. As decisões e priorizações são realizadas no âmbito da GCN. Para incidentes na sala de controle, as equipes de operação possuem autonomia, para maior agilidade. Processos estão definidos no âmbito dos PPSP.	Han et al. (2019) argumentam que as atividades da fase de contenção/recuperação são de difícil padronização e discute sobre a importância da discussão sobre a criação de procedimentos automatizados de defesa contra ameaças.
Como é realizada a comunicação com stakeholders do setor? Há hierarquia para coordenação dessas atividades?	A ação de comunicação depende do nível do impacto, da área impactada e da severidade do incidente. Além da preocupação com a preservação dos ativos, existem ações que visam a transparência ao setor e a proteção da imagem da organização. A hierarquia segue de acordo com o definido nos normativos de GCN.	A hierarquia tradicional de um processo de resposta pode afetar a eficiência do processo no contexto dos CPS (SMITH et al. 2021). Desde 2009 Jaatun et al. (2009) argumentam que um processo de resposta a incidentes não opera isoladamente dentro de uma organização e deve ser sempre ajustado à dinâmica externa da organização

Quanto à análise dos resultados apresentados no Quadro 22, observa-se que na prática existe padronização de atividades de análise e decisão para incidentes de menor complexidade. Incidentes cibernéticos de maior complexidade devem ser submetidos à avaliação e decisão de um comitê, com envolvimento de outros *stakeholders* da organização. Alguns autores como Shinde e Kulkarni (2021) defendem uma análise processual para análise dos incidentes. Entretanto, Han et al. (2019) argumentam que as atividades da fase de contenção/recuperação são de difícil padronização e defendem a criação de

procedimentos automatizados para defesa contra ameaças, o que já vem sendo trabalhado no contexto do SOC. Dessa forma, percebe-se maior aderência do contexto prático às observações de Han et al. (2019). Para o contexto de incidentes de alta complexidade e com potencial de crise, a partir das entrevistas realizadas não foi possível avaliar se a hierarquia atual pode ou não afetar a eficácia do processo de resposta, devido ausência de registros reais desse tipo de incidente.

No que tange à hierarquia para tomada de decisão, Smith et al. (2021) alertam para questões associadas à redução eficiência da tomada de decisão em processos muito hierárquicos. No contexto do processo de operação do SEB, executado pelas salas de controle, identifica-se que no âmbito dos PPSP há maior agilidade e autonomia, com foco na preservação da continuidade do serviço de supervisão controle das instalações do setor. Entretanto, no âmbito do GCN, foi identificado um nível de hierarquia para tomada de decisão para análise do impacto do incidente. Não foi possível mensurar os impactos dessa hierarquia no contexto prático devido à ausência de histórico recente de incidentes cibernéticos que pudessem acionar essa estrutura.

Em relação à fase (6) Atividades pós-incidente, conforme literatura, são avaliadas as lições aprendidas e analisadas as causas raízes, de forma a possibilitar melhoria contínua de todo processo de resposta a incidentes. Essa fase pode incluir ainda ações de auditoria e fiscalizações do processo.

Um dos entrevistados informou que as causas e razões dos incidentes cibernéticos são analisadas pela equipe de TI e que, conforme nível e profundidade de análise, podem ser contratadas empresas terceiras para análise específica. Em relação à fiscalização, esse entrevistado informou que ainda não existe um processo consolidado no setor e que o processo de segurança cibernética da organização nunca foi fiscalizado ou auditado externamente. No que tange à implementação dos controles mínimos de segurança cibernética estabelecidos a Rotina RO-CB.BR.01, o entrevistado informou que todos os agentes realizam uma autoavaliação com entrega de declaração e que o primeiro ciclo desse processo aconteceu em maio de 2023. Com o resultado da análise, o entrevistado afirmou que foi possível ter uma avaliação sobre a maturidade do setor.

Quanto ao contexto da operação em tempo real, outro entrevistado afirmou que as atividades pós-incidente incluem a análise de causas, áreas envolvidas, lições aprendidas e o que pode ser realizado para que o incidente/falha não aconteça. Existem auditorias internas e externas do Sistema de Gestão da Qualidade, mas nunca ocorreu fiscalização do órgão regulador no processo do PPSP.

Na área de comunicação, o entrevistado afirmou que os resultados do aprendizado na fase pós-incidente retroalimentam outros processos, entretanto não há caso histórico sobre incidente cibernético.

O Quadro **23** sintetiza os resultados obtidos em relação à fase (6) Atividades pós incidente.

Quadro 23 **- Análise sobre a fase (6) Atividades pós incidente – contexto do específico de operação de instalações do SIN**

Perspectiva de análise	Resultados análise documental e entrevistas	Avaliação em relação à literatura
Há processos e ferramentas para documentação dos incidentes? São analisadas as causas dos incidentes? Como são discutidas as lições aprendidas?	A causas e razões dos incidentes são analisadas pela equipe de TI e podem ser contratadas empresas terceiras para análise específica, conforme nível e necessidade de análise. No processo de operação em tempo real as atividades pós-incidente incluem a análise de causas, áreas envolvidas, lições aprendidas.	Durante a fase pós incidente, devem ser discutidas lições aprendas e analisadas as causas raízes dos incidentes cibernéticos (STAVES et al.; 2022).
São realizadas auditorias / fiscalizações?	Nunca ocorreu processo fiscalização em relação aso processos de segurança cibernética. Em relação à aplicação da Rotina RO-CB.BR.01, os agentes realizam uma autoavaliação com entrega de declaração e que o primeiro ciclo desse processo aconteceu em maio de 2023 No tempo real existem auditorias internas do Sistema de Gestão da Qualidade, mas nunca ocorreu fiscalização do órgão regulador no processo do PPSP	Shinde e Kulkarni (2021) apontam para a necessidade de auditorias no processo.

Quanto à análise dos resultados apresentados no Quadro **23**, há aderência quanto à intenção e prática da organização em relação ao abordado pela literatura. O estudo de lições aprendidas se aplica tanto ao contexto

específico da segurança cibernética quanto ao processo de operação em tempo real, a partir de um Sistema de Gestão da Qualidade. Quando à realização de fiscalizações, a prática nunca ocorreu para o processo de segurança cibernética. É importante observar que, apesar da aplicabilidade de maior parte dos elementos propostos pela literatura, ainda não há uma avaliação a partir de auditoria e fiscalizações do processo de resposta a incidentes cibernéticos.

4.2.2 Representações do processo de resposta a incidentes cibernéticos

No que tange à análise de representação do processo de resposta a incidentes cibernéticos, os entrevistados de 4 áreas da organização afirmaram que a representação cíclica é a que melhor se aplica ao contexto da organização. Um dos entrevistados, envolvido diretamente em ações de segurança cibernética, afirmou que o processo é executado de forma cíclica, mas que algumas atividades preliminares ao processo de resposta a incidentes são executadas de forma linear, especialmente nas fases de Monitoramento e Detecção. Essas atividades ocorrem de forma ininterruptas, são padronizadas e os resultados são documentados. Adicionalmente, esse entrevistado informou que durante a fase de Análise do Incidente podem existir variações na dinâmica das atividades e que não há uma representação formalizada de forma explícita.

Sobre a adoção de um modelo ágil de processo, esse entrevistado entender que existe alta complexidade para aplicação desse modelo.

Outro entrevistado, da área de Regulação, indicou que, apesar do modelo do processo ser cíclico, há necessidade de atualização do processo mesmo que um ciclo inteiro não seja totalmente finalizado. O entrevistado afirmou que, de certo modo, o processo pode ser atualizado de forma ágil.

Entrevistados da área de Gestão de Riscos informaram que os normativos relacionados à gestão de incidentes cibernéticos representam o processo de forma predominantemente linear, apesar de entenderem que, idealmente, as lições aprendidas desse processo devem retroalimentar o processo de resposta a incidentes como um ciclo. Um dos entrevistados da área de operação, informou que entende que os processos de respostas a incidentes são representados de forma linear, entretanto a gestão do processo é realizada de forma cíclica e periodicamente são realizadas avaliações do processo para melhoria contínua.

Outro entrevistado, da área de Telecomunicações, reforçou essa afirmativa, informando que a representação cíclica se aplica ao contexto, mas que “a todo tempo são necessários ajustes no processo”. Outro entrevistado, da área de Comunicação, informou que o processo cíclico é o que mais se enquadra ao contexto da organização, mas que a comunicação interna e externa sobre a ocorrência de incidentes ocorre a partir de interações constantes com áreas envolvidas.

O Quadro 24 sintetiza os resultados e apresenta a avaliação em relação à abordagem da literatura, sobre a representação do processo de resposta a incidentes cibernéticos na organização.

Quadro 24 - Análise sobre a representação gráfica do processo de resposta a incidentes – contexto do processo de operação do SEB

Perspectiva de análise	Resultados análise documental e entrevistas	Avaliação em relação à literatura
O formato do processo se assemelha ou difere das representações identificadas na literatura?	O processo cíclico sequencial é abordado como aderente e aplicável ao processo de resposta a incidentes cibernéticos no contexto do processo de operação das instalações.	Patiño et al. (2019); Maimó et al. (2019); Vielberth (2020) são autores que abordam o processo de resposta a incidentes como um modelo de ciclo de vida.
Há variação de formatos de processo durante as diferentes fases do processo de resposta a incidentes?	Sob o ponto de vista normativo, normas internas representam o processo de gestão de incidentes de forma linear, apesar de haver um entendimento de que deve haver uma gestão cíclica Em relação à execução, etapas de Detecção e Monitoramento, prévias à ocorrência do incidente, são executadas de forma cadenciada e linear e devem ser documentadas Durante a ocorrência de um incidente, as atividades das fases 4-Avaliação/Análise e Decisão e 5- Contenção e Recuperação podem ser executadas sem padrão específico, priorizando agilidade. Entretanto, a adoção de um modelo ágil é vista como complexo para a organização.	Em relação à normatização. Shinde e Kulkarni (2021) realizam um estudo empírico com consultorias organizacionais e propõem um framework de gestão de incidentes focados nas fases de preparação, identificação, investigação, encerramento e comunicação. O framework proposto uma combinação das fases em comum de padrões técnicos da ISO, NIST e ITIL. O fluxo é linear Em relação as atividades de detecção e análise para monitoramento, Gonzáles-Granadillo, et al. (2021) abordam as atividades/componentes de uma solução de SIEM como lineares e abordam a importância da documentação Em relação à agilidade He et al. (2022) propõem um framework

Perspectiva de análise	Resultados análise documental e entrevistas	Avaliação em relação à literatura
		ágil para resposta a incidentes no setor de saúde e fazem críticas ao processo de resposta a incidentes como um processo linear de resposta a incidentes, devido sua rigidez, morosidade e previsibilidade.

A partir da análise do Quadro 24, constata-se que o processo cíclico é abordado como o mais aplicável ao contexto da organização. Há aderência na percepção dos entrevistados e de autores na literatura quanto a adoção de um modelo de ciclo de vida para a resposta a incidentes, conforme abordado por Patiño et al. (2019); Maimó et al. (2019); Vielberth (2020). Apesar dos instrumentos normativos tratarem do processo como um fluxo linear, há entendimento dos entrevistados de que o processo de resposta a incidentes cibernéticos pode ser representando como um ciclo de vida. Adicionalmente há variações na forma de representação em determinadas etapas de detecção e monitoramento e para a fase de decisão não existe um padrão de forma de processo definido, uma vez que a agilidade é priorizada. A necessidade de agilidade é abordada na literatura por He et al. (2022) que faz críticas ao processo de resposta a incidentes como um processo linear de resposta a incidentes, devido sua rigidez, morosidade e previsibilidade. Na organização entrevistada, entende-se que a adoção de um modelo ágil traz complexidade para a gestão;

4.3 RELACIONAMENTO ENTRE OS STAKEHOLDERS

Nesta seção é analisada a perspectiva de relacionamento entre os *stakeholders* envolvidos nos processos de resposta, notificação e compartilhamento de informações sobre incidentes cibernéticos no âmbito a administração pública federal, a partir da REGIC, e no âmbito do SEB. A seção toma referência as representações gráficas de relacionamento entre *stakeholders*, identificadas na literatura analisada. São consideradas as percepções de 6 entrevistados, 3 da organização objeto de estudo e 3 de outras instituições do SEB, sendo uma integrante da REGIC. Em complemento às

entrevistas, é considerada a análise documental a regulamentação associada ao tema. Adicionalmente, para análise de aderência e aplicabilidade, são utilizados como referência os resultados da consolidação das representações de relacionamento entre *stakeholders* abordadas no subcapítulo 3.2.2.3.

No âmbito da REGIC, o Decreto 10.748 de 2021 estabelece que

> a Rede Federal de Gestão de Incidentes Cibernéticos tem por finalidade aprimorar e manter a coordenação entre órgãos e entidades da administração pública federal direta, autárquica e fundacional para prevenção, tratamento e resposta a incidentes cibernéticos, de modo a elevar o nível de resiliência em segurança cibernética de seus ativos de informação (BRASIL, 2021).

Conforme estabelecido no Artigo 5º do Decreto 10.748 de 2021, a REGIC é composta pelo GSI, órgãos e entidades da administração pública federal direta, autárquica e fundacional, empresas públicas e outras empresas, como sociedades de economia mista e subsidiárias que aderirem à Rede (BRASIL, 2021).No que tange à governança da REGIC, o GSI é responsável pela coordenação por meio da CTIR Gov de forma centralizada (BRASIL, 2021). Os participantes da REGIC devem atuar compartilhando informações por meio de suas equipes de prevenção, tratamento e resposta a incidentes cibernéticos e todas as informações compartilhadas devem observar as restrições legais de acesso a dados (BRASIL, 2021).O Decreto prevê ainda equipes de coordenação setorial do setor regulado, que podem ser coordenadas por agências reguladoras e que devem centralizar as notificações de incidentes das demais equipes.

Dois entrevistados, integrantes de entidade participante da REGIC e do SEB, informaram que, conforme disposto na legislação, o tema é coordenado e centralizado pelo GSI, apesar de existirem estruturas criadas operacionalmente que dificultam o acompanhamento do tema. Os entrevistados afirmaram que no histórico de interações e envio de dados já houve comunicação direta com o CTIR Gov, entretanto existem iniciativas de interações laterais com outras entidades do setor que não estão formalizadas e ocorrem por iniciativa da própria instituição e de seus colaboradores.

Esses entrevistados informaram ainda que atualmente o CTIR Gov está focado na atividade de monitoramento da REGIC. Destacaram que uma possível interação lateral entre os membros da rede poderia promover maior agilidade na

comunicação e compartilhamento de informações e que há a necessidade de evolução regulatória do tema, que atualmente não acompanha a evolução prática sobre o tema segurança cibernética.

A Figura 12 ilustra o relacionamento dos stakeholders na REGIC, a partir da análise regulamentação associada ao tema e consolidação dos resultados das entrevistas.

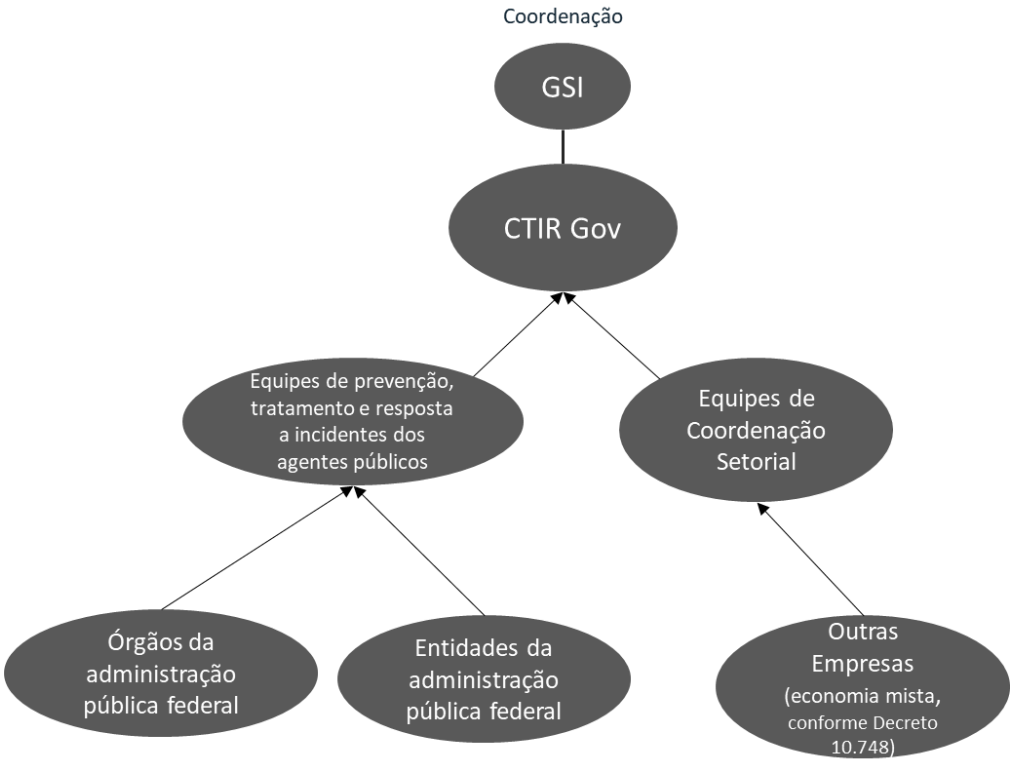


Figura 12 - Relacionamento entre *stakeholders* na REGIC
Fonte: o autor

No SEB a ANEEL é responsável pela coordenação setorial dos temas relacionados à segurança cibernética. A REN 964/2021 aborda sobre a política de segurança cibernética a ser adotada pelos agentes do setor de energia elétrica e estabelece diretrizes e conteúdo mínimo das políticas a serem adotadas pelos agentes do SEB (ANEEL, 2021b). A REN observa o disposto na Estratégia Nacional de Segurança Cibernética, publicada a partir do Decreto 10.222/2022, e o disposto no decreto 10.748 de 2021 que institui a REGIC. A REN ANEEL 964/2021

No escopo do SEB, a REN ANEEL 964/2021, estabelece que os agentes do setor devem

> notificar a equipe de coordenação setorial designada dos incidentes cibernéticos de maior impacto que afetem de maneira substancial a segurança das instalações, a operação ou os serviços aos usuários de dados (ANEEL, 2021b).

Ainda de acordo com a REN ANEEL 964/2021, os agentes devem adotar procedimento de compartilhamento de informações sobre ameaças e outras informações relativas à segurança cibernética de forma sigilosa e não discriminatória, sendo facultado o anonimato (ANEEL, 2021b).

Um dos entrevistados, integrante do grupo de coordenação setorial, entende que há centralização no recebimento de informações de incidentes cibernéticos de agentes do SEB a partir do grupo e que a ANEEL é responsável pela função de coordenação. Esse entrevistado afirmou que apesar da regulamentação sugerir uma atuação centralizadora, há a intenção de que no futuro essa rede possa evoluir para uma rede multilateral.

Outros dois entrevistados reforçaram que o objetivo do grupo é receber informações dos agentes do SEB e que inclusive já ocorreu participação de outras entidades do setor nesse grupo. Um dos entrevistados destacou ainda que o objetivo atual do grupo é receber e analisar a informações enviadas pelos agentes. Um entrevistado inclusive afirmou que uma metodologia para análise de criticidade e classificação de incidentes para apoio na tomada de decisão ainda está sendo desenvolvida.

Adicionalmente, tem-se a indicação de outros três entrevistados, cujas instituições integram ou já participaram do grupo, de que um sistema para coleta de informações de incidentes cibernéticos do SEB está em desenvolvimento e que será sugerida uma matriz de criticidade para classificação dos incidentes recebidos para apoio ao processo de tomada de decisão em relação às ações que deverão ser executadas após notificação de incidentes cibernéticos. Um dos entrevistados informou que entende que o grupo possui o desejo de que o reporte de incidentes pelos agentes do SEB seja ágil, mesmo que os agentes ainda não se tenham todas as informações suficientes para a análise de um eventual incidente cibernético.

Quanto ao envio de informações pelos agentes, um dos entrevistados entende que a cultura de segurança cibernética está se desenvolvendo no Brasil e que os agentes do setor ainda possuem moderado receio para envio de

informações relacionadas à incidentes cibernéticos. Essa afirmação corrobora com o resultado de pesquisa realizada pela ANEEL com agentes do SEB, publicada a partir de Nota Técnica Nº 84/2021, que identificou que 38% dos agentes entrevistados não realizam contato com órgãos regulamentadores, autoridades policiais e provedores de serviços de telecomunicação para apoio em caso de incidentes cibernéticos (ANEEL, 2021a). Apesar do baixo índice de envio de informações, outro entrevistado que já participou do grupo entende que atualmente não há a proposta de ação fiscalizatória da agência regulatória, mas de obtenção de uma visão do mercado de energia.

A Figura 13 ilustra o relacionamento dos *stakeholders* no SEB a partir da análise documentação e resultado das entrevistas. As setas indicam o sentido de envio de informações para o grupo de coordenação setorial.

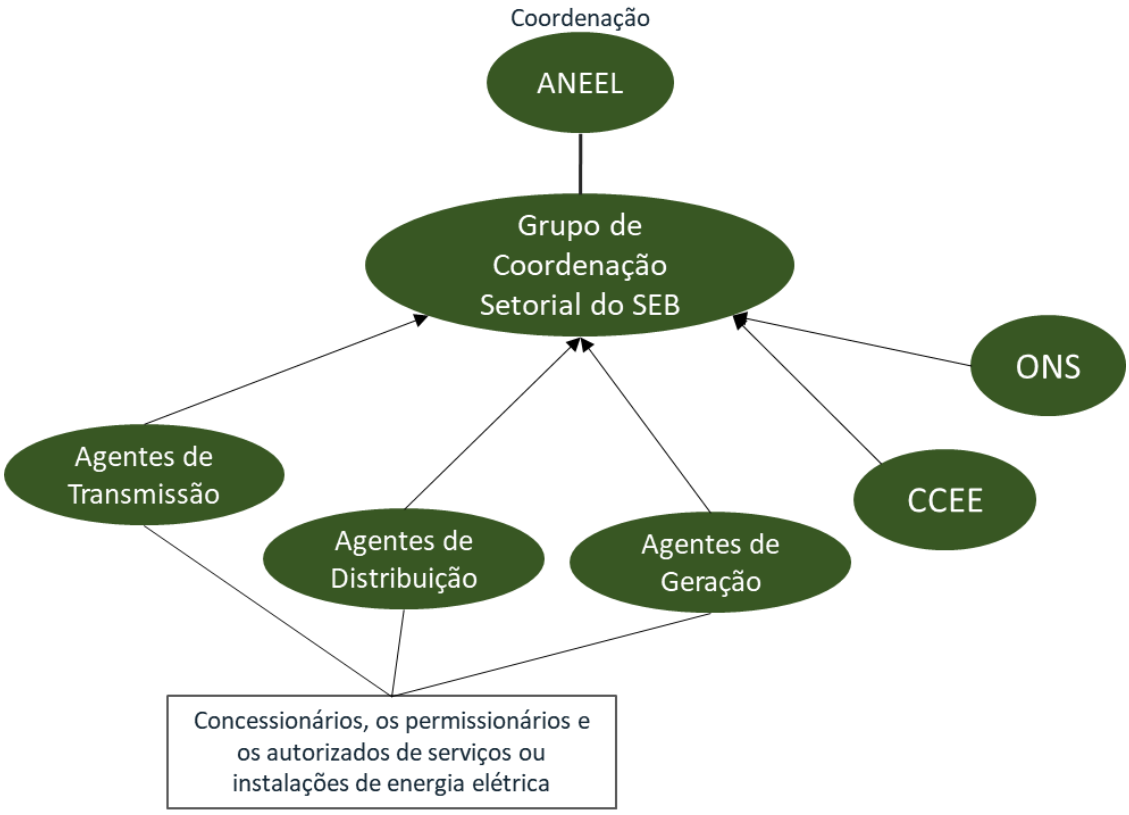


Figura 13 - Relacionamento entre *stakeholders* no SEB
Fonte: o autor

Ressalta-se que no SEB, além da estrutura formal constituída para compartilhamento de informações sobre incidentes cibernéticos, um dos entrevistados, integrante de um grupo de comunicação institucional de uma

organização do setor, informou que existe um grupo de comunicação informal criado para comunicação entre algumas entidades do SEB. A estrutura do grupo não prevê centralização e foca na discussão de questões gerais do setor, não sendo restrito a assuntos de segurança cibernética. É um grupo colaborativo e a interação é múltipla que pode aumentar a agilidade da roca de informações.

Além de classificar os incidentes, outra atribuição do grupo de coordenação setorial, destacada em uma das entrevistas, é a de “comunicar ao GSI incidentes de maior impacto” estabelecendo uma colaboração multilateral. Os eventos de maior impacto devem ser direcionados do grupo de coordenação setorial ao GSI. Dessa forma, a Figura 14 ilustra o modelo de relacionamento entre *stakeholders* incluindo a o relacionamento entre o Grupo de Coordenação Setorial do SEB e a REGIC. As setas indicam o fluxo do compartilhamento de informações entre os *stakeholders*.

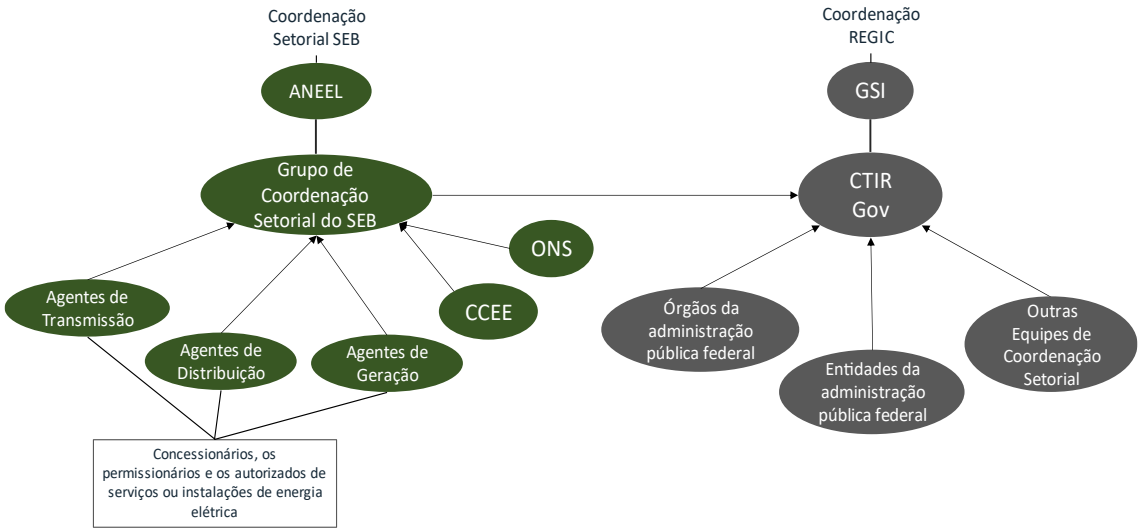


Figura 14 - Relacionamento entre stakeholders - SEB e REGIC
Fonte: o autor

Enquanto Figura 14 detalha as responsabilidades e obrigações de cada ator no âmbito da segurança cibernética do SEB e da REGIC, a Figura 15 considera as obrigações dos *stakeholders* em relação à notificação de incidentes cibernéticos conforme disposições da legislação e regulamentação apresentadas no Quadro 11 da subseção 4.1.1. As setas destacadas na cor vermelha indicam o sentido do envio das notificações. As setas na cor preta indicam responsabilidades e atribuições dos *stakeholders.*

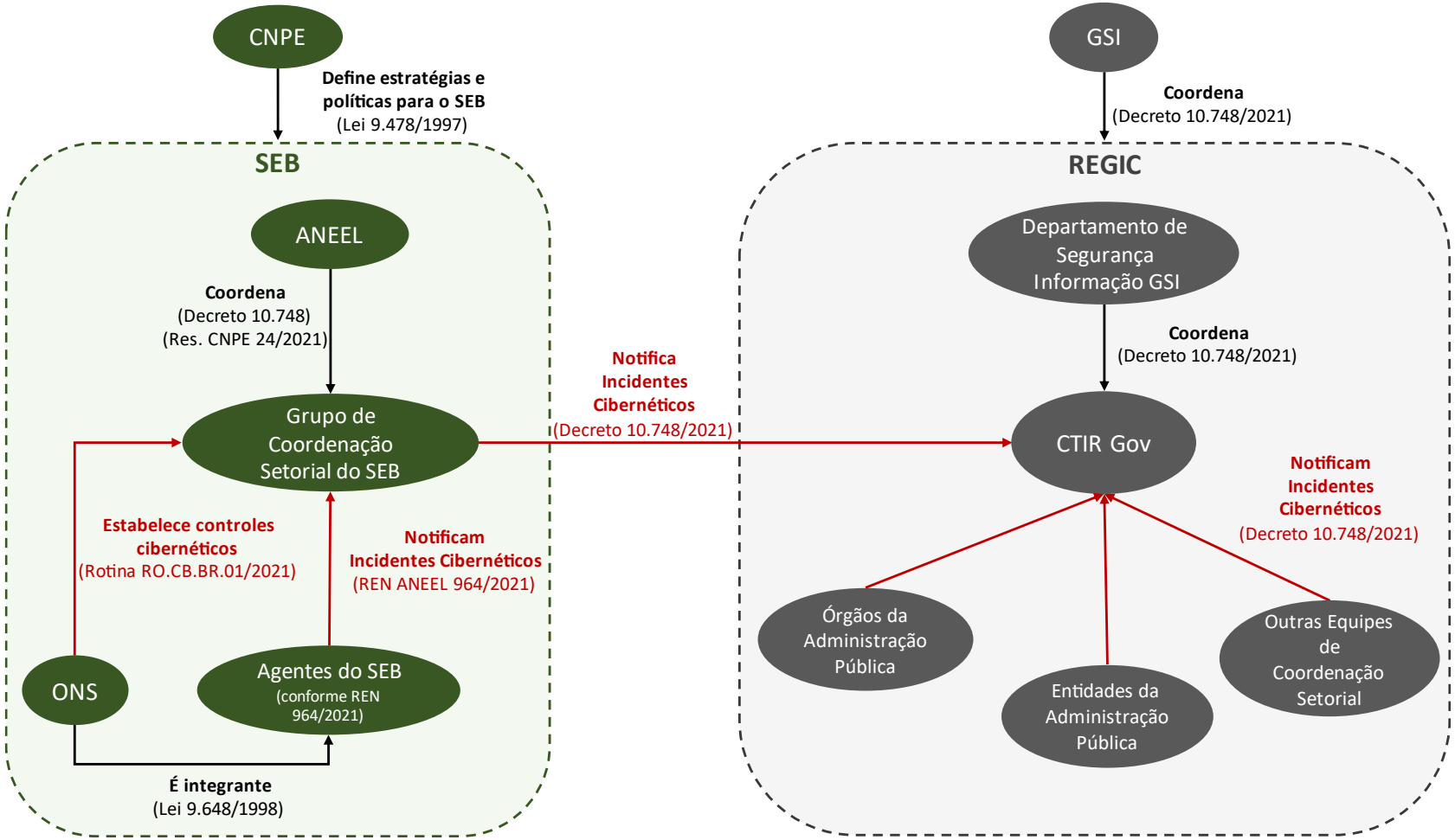


Figura 15 - Notificação de incidentes - REGIC e SEB
Fonte: o autor

O Quadro 25 sintetiza os resultados obtidos em relação ao relacionamento entre os stakeholders no processo de notificação de incidentes cibernéticos.

Quadro 25 - Relacionamento entre os *stakeholders* – REGIC e SEB

Estrutura	Perspectiva de análise	Resultados da análise documental entrevistas
REGIC	Como é o formato da estrutura de relacionamento de stakeholders	É prevista uma estrutura centralizada. O GSI, por meio do CTIR Gov, coordena a REGIC.
	Como é realizada a troca de informações entre os stakeholders?	A troca de informações é realizada pelas equipes de prevenção tratamento e resposta e pelas equipes de coordenação setorial. Informações devem ser enviadas ao CTIR Gov
	Como é abordada a questão da anonimização das informações?	Informações devem observar restrições legais
	Há plataforma para compartilhamento de informações	Não identificado
	Há ou existe previsão de composição de grupos de resposta?	São identificadas as seguintes equipes: 1)Equipes de prevenção, tratamento e resposta a incidentes cibernéticos 2) Equipes de coordenação setorial 3) O CTIR Gov é o CSIRT do governo que coordena a rede e recebe as notificações
	Em caso positivo, qual o papel de cada um desses atores?	1)As equipes de prevenção, tratamento e resposta a incidentes cibernéticos são responsáveis por prestar serviços relacionados à segurança cibernética., no escopo dos órgãos. 2) As equipes de coordenação setorial centralizam informações de seu setor 3)O CTIR Gov é o CSIRT do governo que coordena a rede e recebe as notificações
SEB	Como é o formato da estrutura de relacionamento de stakeholders	É prevista uma estrutura centralizada pelo Grupo de Coordenação Setorial, coordenado pela ANEEL e que prevê a participação de outras organizações relevantes do SEB.
	Como é realizada a troca de informações entre os stakeholders?	Os agentes do SEB devem notificar o grupo de coordenação setorial sobre incidentes de maior impacto.
	Como é abordada a questão da anonimização das informações?	As informações devem ser compartilhadas de forma anônima e não discriminatória.
	Há plataforma para compartilhamento de informações	Há plataforma tecnológica em desenvolvimento para recebimento de informações.
	Há ou existe previsão de composição de grupos de resposta?	Há o grupo de coordenação setorial coordenado pela Aneel e com possibilidade de participação de outros atores
	Em caso positivo, qual o papel de cada um desses atores?	O grupo de coordenação setorial tem o papel de avaliar e classificar os incidentes e direcionar ações.

Avaliação em relação à literatura
Leszczyna *et al.* (2019) apresenta um framework considerando um gestor central para recebimento de informações compartilhadas por outros atores, no setor de energia. Para os autores, o *stakeholder* central deve atuar como um moderador da comunicação e garantidor da distribuição por toda a comunidade de stakeholders Leszczyna e Wróbel (2019) abordam sobre a importância de uma plataforma de compartilhamento de informações, que deve ficar sob gestão central de uma parceria público privada.

Os resultados apresentados no Quadro 25 permitem concluir que tanto na REGIC quanto na estrutura do SEB estão previstas estruturas centrais para recebimento de notificações sobre incidentes cibernéticos. Na REGIC o CTIR Gov é o CSIRT do governo que coordena a rede e recebe as notificações as entidades federais. No SEB o grupo de coordenação setorial tem o papel de tem o papel de avaliar e classificar os incidentes e direcionar ações. A centralização do recebimento de notificações de incidentes é abordada por Leszczyna et al. (2019). Leszczyna e Wróbel (2019) também apontam para a importância de uma plataforma de compartilhamento de informações, que vem sendo endereçado no contexto prático do SEB. Entretanto, Leszczyna et al. (2019) também abordam sobre a possibilidade de troca de informações a partir de uma colaboração lateral, ou *peer-to-peer.* Identifica-se que esse tipo de interação não é previsto ou priorizado no âmbito da REGIC e do SEB. A estruturação de grupos colaborativos foi destacada apenas a partir de grupos de comunicação institucional no SEB, sem previsão de sua existência em normativos ou regulamentos.

5. CONTRIBUIÇÕES E PROPOSTAS DE TRABALHOS FUTUROS

O presente capítulo apresenta as considerações finais da pesquisa. O primeiro subcapítulo discute as contribuições para academia e para profissionais da área e o segundo subcapítulo sugere uma agenda de pesquisa para avanço na discussão do tema na literatura.

5.1 CONTRIBUIÇÕES ACADÊMICAS E PARA PROFISSIONAIS DA ÁREA

No que tange à contribuição acadêmica e aos profissionais da área, a presente pesquisa fornece referenciais que permitem a compreensão do estado da arte sobre o tema. São selecionados 19 referencias para análise, a partir de um rigoroso processo metodológico adotado na RSL que permitiu a identificação das principais abordagens associadas à segurança cibernética em CPS na literatura. Informações sobre a evolução do tema na literatura, principais setores de aplicação, fases do processo de resposta, formas de representação do processo e relacionamento entre os *stakeholders* são apresentados no Capítulo 3 da presente pesquisa. Desse modo, conforme Torraco (2005), a síntese da revisão da literatura a partir dos resultados identificados e analisados a partir da RSL apresenta uma classificação conceitual contribui para o conhecimento acadêmico.

Profissionais de organizações que atuam em processos de resposta a incidentes cibernéticos, especialmente no contexto dos CPS, podem avaliar a aplicabilidade das medidas de segurança abordadas pela literatura em seu contexto prático. Essa pesquisa apresenta medidas relacionadas a cada uma das fases do processo de resposta a incidentes, alternativas para forma de execução do processo e modelos de relacionamento entre *stakeholders.* As medidas apresentadas podem ser avaliadas como potenciais ferramentas práticas para aprimoramento do processo de resposta a incidentes cibernéticos.

Adicionalmente, além do referencial acadêmico, a pesquisa apresenta um panorama sobre a legislação e regulamentação sobre o tema no Brasil e no SEB, além da visão e interpretação de relevantes instituições do setor, que podem servir de insumo orientativo para outras organizações que se enquadram nos

cenários abordados na pesquisa. No contexto específico da operação de redes elétricas, organizações podem utilizar os resultados do estudo de caso como *benchmarking* para análise comparativa de suas práticas de segurança adotada em relação às práticas adotadas.

No que tange à implicação dos resultados acadêmicos, os resultados da pesquisa situam os pesquisadores sobre os principais avanços em relação ao tema. Considerando os resultados da RSL, acadêmicos podem utilizar a síntese de *frameworks* sobre resposta a incidentes cibernéticos como referência de modelos de processo para resposta a incidentes ou ainda para discussão sobre o relacionamento entre *stakeholders* e suas principais implicações no relacionamento. Adicionalmente, as medidas de segurança abordadas em cada uma das fases de resposta podem ser utilizadas como referência para pesquisas que envolvam estudos associados a tecnologias para monitoramento e detecção de ameaças.

Quanto aos resultados do estudo de caso, foi identificada aderência em relação às abordagens identificadas na literatura e à prática das organizações entrevistadas, especialmente no contexto específico do processo de operação do SEB. Entretanto, os resultados das entrevistas realizadas com as instituições apontam para algumas questões precisam de maior investigação pela literatura. A dificuldade na adoção de modelos ágeis de processo de resposta, a precariedade no compartilhamento de informações, a não adoção de modelos colaborativos multilaterais entre instituições são exemplos de questões que podem ser utilizadas como insumos para futuras investigações.

5.2 PROPOSTAS DE TRABALHOS FUTUROS

Diante o cenário de aumento da preocupação associada à segurança cibernética e surgimento de novas ameaças, além da necessidade de manutenção da segurança da operação de infraestruturas críticas, sugere-se que a agenda de pesquisa avance na investigação teórica e empírica para aumento da segurança da operação dos CPS.

A partir dos potenciais implicações acadêmicas e práticas da presente pesquisa, destacadas no subcapítulo anterior, é proposta a investigação das abordagens identificadas na literatura a partir da realização de outros estudos de

caso no contexto da resposta a incidentes cibernéticos em outros tipos de CPS. Esses estudos são importantes para análise da perspectiva de outros setores que possuem funções diferentes em relação à operação de redes elétricas. Apesar da relevância do avanço de estudos em outros setores, a realização de estudo de casos no contexto da operação de redes elétricas em instituições de outros países também é uma oportunidade para investigação dos diferentes níveis de maturidade e aplicabilidade das abordagens identificadas na presente pesquisa.

Adicionalmente, propõe-se a análise da compreensão da forma de representação ágil do processo de resposta a incidentes e na forma de colaboração multilateral entre *stakeholders*. Quanto à representação de um processo ágil, apesar dos benefícios associados à adaptabilidade, abordados na literatura analisada, a adoção dessa modelo de processo se demonstrou um desafio para aplicação no contexto prático do SEB. Há necessidade de avanço na avaliação da aplicabilidade de adoção desse modelo ou elaboração de alternativas, uma vez que o contexto atual de ameaças e ataques cibernéticos é dinâmico e processos de resposta rígidos e hierárquicos podem ser inefetivos

Quanto ao avanço na análise de modelos de relacionamentos multilaterais entre *stakeholders*, a literatura analisada é focada em modelos centralizados. Adicionalmente, os resultados do estudo de caso indicam a adoção prática de modelos centralizados. Há necessidade na avaliação de modelos de relação multilaterais além da identificação dos desafios de aplicabilidade em um contexto prático de resposta a incidentes cibernéticos na operação de diferentes tipos de CPS.

Por fim, devido a limitação do método de pesquisa adotado na RSL, é sugerida a realização de outras RSL que considerem outros tipos de documento além de artigos acadêmicos revisados por pares. Podem ser incluídos documentos de conferência, teses e dissertações além de literatura não acadêmica relacionada ao tema.

6. CONSIDERAÇÕES FINAIS

Os CPS estão presentes em serviços essenciais e críticos para a sociedade. Os resultados dessa pesquisa evidenciam a diversidade de setores que aplicam os CPS e o aumento da preocupação sobre a segurança cibernética desses sistemas. O objetivo geral da presente pesquisa é a identificação e análise das principais abordagens associadas ao processo de resposta a incidentes cibernéticos em CPS e a investigação desse fenômeno no contexto Setor Elétrico Brasileiro (SEB) e em setores relacionados.

O primeiro objetivo intermediário é a identificação do contexto atual da discussão sobre resposta a incidentes em CPS. Esse objetivo é atendido a partir da realização de uma RSL que resultou na seleção de 19 artigos específicos a partir de uma base inicial de 209 artigos e 90 livros relacionados ao tema. Foram utilizados critérios de inclusão e exclusão específicos para análise de *frameworks* que abordam sobre processo de resposta a incidentes cibernéticos em CPS. Como resultado desse objetivo, identificou-se que a discussão sobre o tema é recente na literatura e que há grande diversidade de periódicos que abordam sobre o tema, reflexo da heterogeneidade das aplicações dos CPS e da atualidade do tema. Adicionalmente, foi identificada a maior tendência de pesquisas relacionadas a infraestruturas críticas, segurança de dado, resposta a incidentes, análise e compartilhamento de informações. A partir de 2021 as pesquisas tendem a focar em crimes computacionais e consciência situacional.

O segundo objetivo intermediário é a identificação das principais abordagens apresentadas pela literatura para o processo de resposta a incidentes cibernéticos no contexto dos CPS. Esse objetivo também é atendido a partir da realização da RSL. Foram identificados os principais setores de aplicação dos CPS e as principais abordagens associadas à segurança cibernética. Em relação aos setores de aplicação, identificou-se o setor o de energia elétrica como o mais abordado pela literatura, o que reforça a aplicabilidade da pesquisa empírica no contexto do SEB. Além do setor elétrico, identificaram-se os setores e indústria, saúde, abastecimento de água, financeiro, petróleo, transporte e atividades associadas ao governo.

Quanto às abordagens identificadas no subcapítulo 3.2, é realizada uma análise crítica e síntese dos principais *frameworks* identificados na literatura,

conforme recomendações de Torraco (2015). Foi possível identificar um padrão nas fases de resposta a incidentes, na forma de representação do processo de resposta e na forma de relacionamento entre os *stakeholders.*

Quanto às fases do processo de resposta a incidentes, identificou-se que a fase mais abordada é a (5) Contenção e Recuperação. É nessa fase que são executadas as principais medidas para mitigação e recuperação do incidente. Quanto à forma de representação dos processos, existe certa divergência entre as abordagens apresentadas pelos autores. Enquanto alguns autores tratam do processo de resposta a incidentes de forma linear e sequencial, outros autores apresentam processos cíclicos. Adicionalmente, há autores que introduzem o conceito de agilidade no processo, com representações de processos que permitem retroalimentação entre as fases. Observa-se que os trabalhos que abordam sobre agilidade são mais recentes, o que pode ser justificado pelo aumento do dinamismo de ameaças cibernéticas.

No que tange ao relacionamento entre *stakeholders*, o modelo centralizado é o mais abordado pela literatura analisada, apesar de também serem apresentados modelos colaborações multilaterais. Entretanto, não foi identificada discussão que relacione a adoção de uma abordagem de relação centralizada ou multilateral entre *stakeholders* e seus impactos na adoção de um modelo de processo cíclico ou ágil. A adoção de um modelo centralizado prevê hierarquias no processo de comunicação de incidentes entre diferentes *stakeholders*, que podem divergir com princípios de processo ágil, conforme abordado por alguns autores na literatura.

O terceiro objetivo intermediário visa avaliar aderência e aplicabilidade das abordagens identificadas na literatura em relação processo de resposta a incidentes cibernéticos no cenário da operação de redes elétricas, a partir de um estudo empírico no SEB. Esse objetivo é alcançado a partir da realização de um estudo de caso que avalia o processo de resposta a incidentes cibernéticos no contexto do processo operação de redes elétricas no SEB, realizado por relevante organização que atua o setor.

Nesse contexto, observou-se aderência às práticas adotadas em relação às abordagens de segurança discutidas na literatura. Em relação ao processo de resposta a incidentes, conclui-se que as fases abordadas no referencial teórico se aplicam ao contexto prático, podendo haver variações que não alteram

a estrutura central do processo. Os resultados dessa análise são apresentados e discutidos no subcapítulo 4.2 da presente pesquisa. Identifica-se como limitação a ausência de registros sobre eventos com potencial situação de crise que permitissem a real avaliação da eficácia do processo em relação às medidas discutidas pela literatura. Quanto à forma de representação do processo, o formato cíclico é o mais adequado à estrutura da organização, devido a necessidade de retroalimentação do processo. O processo ágil é interpretado como um desafio para implementação no contexto prático.

Adicionalmente à análise desse contexto específico, é avaliada a discussão sobre o tema em contexto mais abrangente do SEB e do Brasil, especialmente devido aos impactos da legislação sobre o tema no Brasil que reflete diretamente na regulamentação do SEB e na implementação de ações pelos agentes do setor. No Brasil, especialmente no âmbito da REGIC, percebe-se aderência entre as fases do processo propostas pela PLANGIC. No SEB não há processo estabelecido formalmente, apesar dos entrevistados afirmarem que as fases se aplicam ao contexto do setor. Quanto à representação do processo, novamente o formato cíclico é destacado como o mais aderente ao contexto do processo de resposta a incidentes.

Ainda em atendimento ao terceiro objetivo intermediário, é analisado o relacionamento entre os *stakeholders* no processo de resposta a incidentes cibernéticos. Tanto na literatura analisada quanto na prática avaliada a partir do estudo de caso foi identificada predominância da adoção de modelos centralizados para recebimento de informações e notificações, seja a partir do CTIR Gov no âmbito federal da REGIC, oi pelo grupo coordenação setorial no SEB. O relacionamento multilateral é identificado apenas como uma alternativa, em alguns casos informais para trocas de informações. O compartilhamento de informações é um dos obstáculos mais evidentes identificados na análise do contexto prático, corroborando com as questões apontadas pela literatura.

No que tange às contribuições para academia, são apresentadas a síntese da revisão da literatura e uma classificação conceitual das fases de resposta a incidentes, formas de representação de processo e relacionamento entre *stakeholders*. Adicionalmente, são propostos trabalhos futuros para análise do processo de resposta a incidentes cibernéticos em outros setores de CPS e em outros contextos de operação de redes elétricas. Também são propostas a

análise da adoção do modelo de resposta ágil e de colaboração multilateral entre *stakeholders* e a realização de outras RSL a partir de documentos não revisados por pares.

Em relação às contribuições para profissionais da área, os resultados apresentados podem considerados como potenciais insumos para aprimoramento do processo de resposta a incidentes em instituições que se enquadram no contexto da operação de CPS.

Diante disso, a análise do contexto teórico sobre o processo de resposta a incidentes cibernéticos em CPS fornece insumos conceituais sobre o tema e permitiu avaliar aplicabilidade das abordagens identificadas em um contexto contemporâneo e significante. A pesquisa apresenta uma agenda de pesquisa futura para acadêmicos e potencial aplicação prática para atuantes na área de operação de CPS, contribuindo para a promoção da segurança cibernética desses sistemas.

REFERÊNCIAS BIBLIOGRÁFICAS

AMOROSO, E. G. **Cyber Attacks: Protecting National Infrastructure**. 1. ed. Massachusetts, Butterworth-Heinemann, 2011.

ANEEL. **Nota Técnica nº 84/2021-SFE-SFG/ANEEL**. . Brasilia, Agência Nacional de Energia Elétrica. , 2021a

ANEEL. **Resolução Normativa Aneel nº 964 de 14 de dezembro de 2021. Dispõe sobre a política de segurança cibernética a ser adotada pelos agentes do setor de energia elétrica**. . Brasília, Diário Oficial da União, 2021b

BARTNES LINE, M., ANNE TØNDEL, I., JAATUN, M. G. "Current practices and challenges in industrial control organizations regarding information security incident management - Does size matter? Information security incident management in large and small industrial control organizations", **International Journal of Critical Infrastructure Protection**, v. 12, p. 12–26, 2016..

BOOTH, W. C., COLOMB, G. G., WILLIAMS, J. . **The Craft of Research**. 3. ed. Chicago, EUA, The University of Chicago Press, 2008.

BRASIL. **Decreto 11.200 de 15 de setembro de 2022. Aprova o Plano Nacional de Segurança de Infraestruturas Críticas.** . Brasília, Diário Oficial da União, 2022

BRASIL. **Decreto 9.573 de 22 de novembro de 2018. Aprova a Política Nacional de Segurança de Infraestruturas Críticas.** . Brasília, Diário Oficial da União, 2018a

BRASIL. **Decreto n° 10.748 de 16 de julho de 2021. Institui a Rede Federal de Gestão de Incidentes Cibernéticos.** . Brasília, Diário Oficial da União, 2021

BRASIL. **Decreto nº 10.222 de 05 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética.** . Brasília, Diário Oficial da União, 2020a

BRASIL. **Decreto nº 10.569, de 09 de dezembro de 2020. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas.** . Brasília, Diário Oficial da União, 2020b

BRASIL. **Decreto nº 11.856 de 26 de dezembro de 2023. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança**. . Brasília, Diário Oficial da União, 2023

BRASIL. **Decreto nº 9.637 de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação.** . Brasília, Diário Oficial da União, 2018b

BRASIL. **Lei 9.478 de 06 de agosto de 1997. Dispõe sobre a política energética nacional.** . Brasília, Diário Oficial da União. , 1997

CAUCHIK-MIGUEL, P. A., SOUZA, R., "O Método do Estudo de Caso na Engenharia de Produção". In: CAUCHIK-MIGUEL, P. A., FLEURY, A., MELLO, C. H. P., *et al.* (Org.), **Metodologia de Pesquisa em Engenharia de Produção e Gestão de Operações**, 3. ed. Rio de Janeiro, Elsevier, 2018. .

CELDRÁN, A. H., KARMAKAR, K. K., GÓMEZ MÁRMOL, F., *et al.* "Detecting and mitigating cyberattacks using software defined networks for integrated clinical environments", **Peer-to-Peer Networking and Applications**, v. 14, n. 5, p. 2719–2734, 2021.

CHERDANTSEVA, Y., BURNAP, P., BLYTH, A., *et al.* "A review of cyber security risk assessment methods for SCADA systems", **Computers and Security**, v. 56, p. 1–27, 2016.

CHOI, T. M., CHENG, T. C. E., ZHAO, X. "Multi-Methodological Research in Operations Management", **Production and Operations Management**, v. 25, n. 3, p. 379–389, 2016.

CISA. **About CISA**. 2018. Disponível em: <https://www.cisa.gov/about>.Acesso em novembro de 2023.

CNN-BRASIL. **Eletrobras diz que subsidiária de energia nuclear sofreu ataque cibernético**. 2021. Disponível em: <https://www.cnnbrasil.com.br/economia/eletrobras-diz-que-subsidiaria-de-energia-nuclear-sofreu-ataque-cibernetico/>. Acesso em setembro de 2023.

CNPE. **Resolução CNPE n° 24 de 2021. Aprova Diretrizes sobre Segurança Cibernética para o Setor Elétrico.** . Brasília, Diário Oficial da União. , 2021a

CNPE. **Resolução CNPE n° 01 de 2021. Institui Grupo de Trabalho para estabelecer diretrizes sobre segurança cibernética no Setor Elétrico.** . Brasília, Diário Oficial da União. , 2021b

COOK, A., JANICKE, H., SMITH, R., *et al.* "The industrial control system cyber defence triage process", **Computers and Security**, v. 70, p. 467–481, 2017.

DAWSON, R. "How significant is a boxplot outlier?", **Journal of Statistics Education**, v. 19, n. 2, p. 1–13, 2011.

DENYER, D., TRANFIELD, D. **Producing a Systematic Review**. **The SAGE Handbook of Organizational Research Methods**. [S.l: s.n.]. , 2009

DIOGENES, Y., OZKAYA, E. **Cybersecurity: Attack and Defense Strategies**. 2. ed. [S.l.], Packt Publishing Ltd, UK, 2019.

ECKHART, M., BRENNER, B., EKELHART, A., *et al.* "Quantitative security risk assessment for industrial control systems: Research opportunities and challenges", **Journal of Internet Services and Information Security**, v. 9, n. 3, p. 52–73, 2019.

GONZÁLEZ-GRANADILLO, G., GONZÁLEZ-ZARZOSA, S., DIAZ, R. "Trends , and Usage in Critical Infrastructures", 2021. DOI: 10.3390/s21144759. .

GSI. **CTIR Gov - Histórico**. 2021. 06 de outubro de 2021. Disponível em: <https://www.gov.br/ctir/pt-br/acesso-a-informacao/institucional/historico>. Acesso em: outubro de 2023.

GSI. **Portaria GSI/PR nº 120 - Aprova o Plano de Gestão de Incidentes Cibernéticos para aadministração pública federal.** . Brasília, Diário Oficial da União, 2022

HAN, C. H. "Blockade-detection-response based security operations dashboard design", **Computers in Human Behavior Reports**, v. 4, p. 100143, 2021.

HAN, C. H., PARK, S. T., LEE, S. J. "The Enhanced Security Control model for critical infrastructures with the blocking prioritization process to cyber threats in power system", **International Journal of Critical Infrastructure Protection**, v. 26, p. 100312, 2019.

HE, Y., ZAMANI, E. D., LLOYD, S., *et al.* "Agile incident response (AIR): Improving the incident response process in healthcare", **International Journal of Information Management**, v. 62, n. September 2021, p. 102435, 2022.

HUMAYED, A., LIN, J., LI, F., *et al.* "Cyber-Physical Systems Security - A Survey", **IEEE Internet of Things Journal**, v. 4, n. 6, p. 1802–1831, 2017. DOI: 10.1109/JIOT.2017.2703172.

HUSÁK, M., SADLEK, L., ŠPAČEK, S., *et al.* "CRUSOE: A toolset for cyber situational awareness and decision support in incident handling", **Computers and Security**, v. 115, 2022.

JAATUN, M. G., ALBRECHTSEN, E., LINE, M. B., *et al.* "A framework for incident response management in the petroleum industry", **International Journal of Critical Infrastructure Protection**, v. 2, n. 1–2, p. 26–37, 2009.

KHOLIDY, H. A. "Autonomous mitigation of cyber risks in the Cyber–Physical Systems", **Future Generation Computer Systems**, v. 115, p. 171–187, 2021.KOEN, B. V. **Discussion of the method**. New York, Oxford University Press, 2003.

KURE, H.I., ISLAM, S. "Cyber threat intelligence for improving cybersecurity and risk management in critical infrastructure", **Journal of Universal Computer Science**, v. 25, n. 11, p. 1478–1502, 2019. .

KURE, Halima Ibrahim, ISLAM, S., RAZZAQUE, M. A. "An integrated cyber security risk management approach for a cyber-physical system", **Applied Sciences (Switzerland)**, v. 8, n. 6, 2018.

LESZCZYNA, R., WALLIS, T., WRÓBEL, M. R. "Developing novel solutions to realise the European Energy – Information Sharing & Analysis Centre", **Decision Support Systems**, v. 122, n. January, p. 113067, 2019.

LESZCZYNA, R., WRÓBEL, M. R. "Threat intelligence platform for the energy sector", **Software - Practice and Experience**, v. 49, n. 8, p. 1225–1254, 2019.

LEZZI, M., LAZOI, M., CORALLO, A. "Cybersecurity for Industry 4.0 in the current literature: A reference framework", **Computers in Industry**, v. 103, p. 97–110, 2018.

LIANG, G., ZHAO, J., LUO, F., *et al.* "A Review of False Data Injection Attacks Against Modern Power Systems", **IEEE Transactions on Smart Grid**, v. 8, n. 4, p. 1630–1638, 2017.

MAIMÓ, L. F., CELDRÁN, A. H., PERALES GÓMEZ, Á. L., *et al.* "Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments", **Sensors (Switzerland)**, v. 19, n. 5, p. 1–31, 2019.

MME. **PORTARIA MME nº 662 de 06 de julho de 2022. Institui a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do MME**. . Brasília, Diário Oficial da União, 2022

NATIONAL CYBER SECURITY CENTRE-NCSC. **About the NCSC**. 2023. Disponível em: <https://www.ncsc.gov.uk/section/about-ncsc/what-we-do> Acesso em setembro de 2023.

ONS. **RO-CB.BR.01-Controles mínimos de segurança cibernética para o Ambiente Regulado Cibernético.** . Rio de Janeiro, Operador Nacional do Sistema Elétrico, 2023. Disponível em: <https://www.ons.org.br/paginas/sobre-o-ons/procedimentos-de-rede/mpo> Acesso em novembro de 2023.

ONS. **Submódulo 2.16 - Requisitos operacionais para os centros de operação e instalações da Rede de Operação**. Rio de Janeiro, Operador Nacional do Sistema Elétrico, 2022. Disponível em: <https://www.ons.org.br/paginas/sobre-o-ons/procedimentos-de-rede/vigentes> Acesso em setembro de 2023.

PATIÑO, A. M. S., GIRALDO RAMÍREZ, D. P. "A technological analysis of Colombia's cybersecurity capacity: a systemic perspective from an organizational point of view.", **Ingeniería Solidaria**, v. 15, n. 28, p. 1–30, 2019.

PATTERSON, C. M., NURSE, J. R. C., FRANQUEIRA, V. N. L. "Learning from cyber security incidents: A systematic review and future research agenda " **Computers and Security**, v. 132, 2023.

PROENÇA, D., SILVA, É. R. "Context and process of systematic literature mapping in Brazilian graduate education", **Transinformacao**, v. 28, n. 2, p. 233–240, 2016.

PURCHASE, H. C. "Twelve years of diagrams research", **Journal of Visual Languages and Computing**, v. 25, n. 2, p. 57–75, 2014.

RIEBE, T., KAUFHOLD, M. A., REUTER, C. "The Impact of Organizational Structure and Technology Use on Collaborative Practices in Computer Emergency Response Teams: An Empirical Study", **Proceedings of the ACM on Human-Computer Interaction**, v. 5, n. CSCW2, 2021.

SALVI, A., SPAGNOLETTI, P., NOORI, N. S. "Cyber-resilience of Critical Cyber Infrastructures: Integrating digital twins in the electric power ecosystem", **Computers and Security**, v. 112, p. 102507, 2022.

SHINDE, N., KULKARNI, P. "Cyber incident response and planning: a flexible approach", **Computer Fraud and Security**, v. 2021, n. 1, p. 14–19, 2021.

SILVA, E. L. da, MENEZES, L. da S. E. M. **Metodologia da Pesquisa e Elaboração de Dissertação**. **Portal**. Florianópolis, UFSC. , 2005

SILVA, É. R., PROENÇA JR., D. P., "Não ser não é não ter : Engenharia não é Ciência (nem mesmo ciência aplicada)". In: PROENÇA, A., LACERDA, D. P., ANTUNES JR., J. A. DO V., *et al.* (Org.), **Gestão da Inovação e Competitividade no Brasil: da teoria para a prática**, Porto Alegre, Bookman, 2015.

SMITH, R., JANICKE, H., HE, Y., *et al.* "The Agile Incident Response for Industrial Control Systems (AIR4ICS) framework", **Computers and Security**, v. 109, p. 102398, 2021. DOI: 10.1016/j.cose.2021.102398.

SNYDER, H. "Literature review as a research methodology: An overview and guidelines", **Journal of Business Research**, v. 104, n. August, p. 333–339, 2019. DOI: 10.1016/j.jbusres.2019.07.039.

STAVES, A., ANDERSON, T., BALDERSTONE, H., *et al.* "A Cyber Incident Response and Recovery Framework to Support Operators of Industrial Control Systems", **International Journal of Critical Infrastructure Protection**, v. 37, n. March 2021, p. 100505, 2022.

SUN, C. C.., HAHN, A., LIU, C.-C. "Cyber security of a power grid: State-of-the-art", **International Journal of Electrical Power and Energy Systems**, v. 99, n. January, p. 45–56, 2018.

THOMÉ, A. M. T., SCAVARDA, L. F., SCAVARDA, A. J. "Conducting systematic literature review in operations management", **Production Planning and Control**, v. 27, n. 5, p. 408–420, 2016.

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

VAN ECK, N. J., WALTMAN, L. "Citation-based clustering of publications using CitNetExplorer and VOSviewer", **Scientometrics**, v. 111, n. 2, p. 1053–1070, 2017.

VIELBERTH, M., BOHM, F., FICHTINGER, I., *et al.* "Security Operations Center: A Systematic Study and Open Challenges", **IEEE Access**, OK - Cita CPS, v. 8, 2020.

WALLIS, T., LESZCZYNA, R. "EE-ISAC—Practical Cybersecurity Solution for the Energy Sector", **Energies**, v. 15, n. 6, p. 1–23, 2022.

YIN, R. **Estudo de Caso: planejamento e métodos**. 5. ed. Porto Alegre, Bookman, 2015.

APÊNDICE 1 - PROTOCOLO DE PESQUISA

O presente protocolo de pesquisa apresenta os principais procedimentos e regras gerais a serem adotados durante a realização do estudo de caso, conforme indicado por Yin (20115). É composto por quatro seções que cobrem a visão geral do estudo de caso, onde constam as definições iniciais de pesquisa, a definição dos procedimentos de coleta de dados, as questões de estudo de caso e o processo de análise e consolidação dos dados.

A. Visão geral do Estudo de Caso

Conforme estabelecido nos objetivos de pesquisa, este trabalho tem como objetivo identificar e discutir as principais abordagens associadas ao processo de resposta a incidentes cibernéticos em CPS, além de investigar esse fenômeno no contexto da operação de redes elétricas. A partir da investigação teórica das medidas para resposta a incidentes cibernéticos apresentadas no Capítulo 3, são avaliadas a aderência e aplicabilidade das abordagens identificadas a partir de um estudo de caso no SEB.

B. Procedimentos para coleta de dados

Os procedimentos de coleta de dados se referem à indicação das fontes e métodos para coleta dos dados. A Figura 16 apresenta a relação entre as principais instituições que compõem, ou se relacionam com o SEB, onde há potencial relevância para coleta de dados.

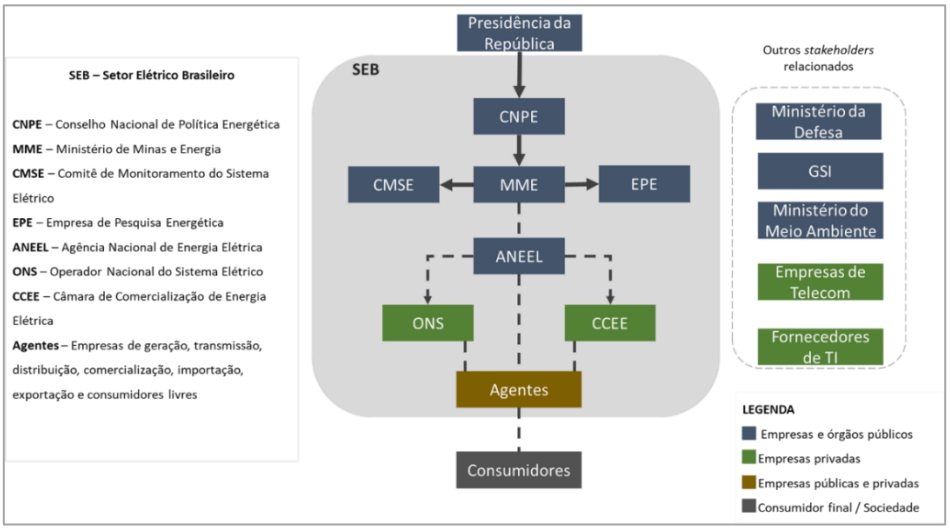


Figura 16 - Instituições que compõem ou se relacionam com o SEB
fonte: adaptado de ONS (2011)

No que tange à realização das entrevistas, é previsto o contato com analistas, engenheiros e servidores das instituições, de áreas específicas ou relacionadas às áreas de segurança da informação ou cibernética.

O agendamento das entrevistas é realizado no intervalo entre maio de 2023 e setembro de 2023, com tempo médio de 1h de duração de forma virtual. As informações são registradas a partir das notas tomadas pelo autor ao longo das reuniões.

C. Questões de estudo de caso

As questões que orientam a coleta de dados têm como base os resultados teóricos apresentados no Capítulo 3 desta pesquisa. Como as entrevistas são realizadas com grupos de diferentes atuações técnicas as perguntas têm caráter aberto e cada entrevistado tem a oportunidade de conduzir a discussão de acordo com sua perspectiva em relação ao tema. As questões têm como enfoque a segurança cibernética no processo de operação das instalações de geração e transmissão de energia elétrica do SIN.

O Quadro 26 apresenta as principais questões direcionadas aos entrevistados. Ressalta-se que algumas perguntas podem não se aplicar ao contexto de determinadas equipes e essa validação é realizada durante as entrevistas.

Quadro 26 - Questões do Estudo de Caso

Tópico da Questão	Questão
1. Em relação ao processo de resposta a incidentes, de forma ampla	Há um processo para resposta a incidentes cibernéticos no contexto do SEB ou em sua instituição?
	As etapas do processo de resposta do referencial teórico se aplicam ao contexto do SEB ou em sua instituição?
	Como as etapas estão dispostas nesse processo? O formato do processo se assemelha ou difere das representações identificadas na literatura? Em que grau? Há variação de formatos de processo durante as diferentes etapas do processo de resposta a incidentes?

Tópico da Questão		Questão
		Quais são os principais atores desse processo?
2. Em relação às atividades do processo de resposta a incidentes (etapas do referencial teórico)	2.1 Etapa preparação	São estabelecidos planos, políticas, normas e regulamentos no SEB e/ou no contexto específico de sua instituição? São constituídas equipes de segurança entre os agentes do setor ou dentro de sua instituição? Em caso positivo, há programas de treinamento para essas equipes? Há processo de gestão de risco que inclua avaliação dos ativos das organizações do setor, incluindo o da sua instituição? São avaliados dados históricos e lições aprendidas? Há avaliação em relação a outras instituições, setores/países e instituições?
	2.2 Etapa Monitoramento	É realizada a coleta de dados da operação de sistemas por sua instituição e/ou outras instituições do setor? Há uso de tecnologias de coleta de dados (Ex.: SIEM, SCADA, ou outros sistemas)? Há compartilhamento de dados monitorados entre as instituições?
	2.3 Detecção	Como são detectados os incidentes cibernéticos? Há uso de tecnologias para detecção (ex.: *intrusion deteccion*)? Há histórico sobre evolução de incidentes detectados no SEB ou em sua instituição? Qual sua avaliação em relação ao histórico?
	2.4 Avaliação/Análise e Decisão	Como as informações sobre incidentes detectados o SEB ou em sua instituição são analisadas? É realizada alguma priorização? Se sim, como? Há uso de tecnologias para apoio à decisão? Se não, há previsão/estudos? Quais são os atores (internos e/ou externos) envolvidos nessa fase?
	2.5 Contenção/recuperação	Existem procedimentos definidos para contenção/recuperação? Como os procedimentos estão estruturados? São utilizados ou recomendadas tecnologias para apoio? Como é realizada a comunicação com *stakeholders* do setor? Há hierarquia para coordenação dessas atividades?

Tópico da Questão		Questão
	2.6 Atividades pós-incidente	Há processos e ferramentas para documentação dos incidentes? São analisadas as causas dos incidentes? Como são discutidas as lições aprendidas? Como é o envolvimento dos *stakeholders* nessa etapa? São realizadas auditorias / fiscalizações em sua instituição ou em outras instituições do SEB?
3. Em relação ao relacionamento entre os stakeholders		O formato da estrutura de relacionamento de *stakeholders* se assemelha ou difere das estruturas identificadas na literatura? Em que grau? Como é realizada a troca de informações entre os *stakeholders* do setor? Há variação de modos de relacionamento durante as diferentes etapas do processo de resposta a incidentes? Há plataforma para compartilhamento de informações no setor? Como é abordada a questão da anonimização das informações? Há ou existe previsão de composição de grupos de resposta (Ex.: SOC, CERT, CSIRT, outros) no SEB? Em caso positivo, qual o papel de cada um desses atores?

Fonte: o autor

D. Análise e consolidação dos dados

Os relatos de todos os entrevistados são consolidados individualmente de acordo as abordagens identificadas na literatura e conforme questões elaboradas. Posteriormente, os relatos são consolidados para construção de uma síntese que representa percepção das organizações entrevistadas. Essa síntese é consolidada em conjunto com o resultado da análise documental, para posteriormente ser avaliada com as abordagens identificadas no referencial teórico. No que tange à comparação da prática executada pelas organizações analisadas e ao referencial teórico, são apontados os pontos que convergem,

complementam ou divergem, a partir do registro e consolidação em tabelas que são apresentadas no Capítulo 4 desta pesquisa.

APÊNDICE 2 – REGISTRO DAS ENTREVISTAS – ESTUDO DE CASO

I. Organização integrante do SEB e membro definitivo do grupo de coordenação setorial do SEB. Data entrevista: 24/07/2023.

Questões gerais

Grupo de coordenação setorial tem como principal objetivo classificar os eventos e comunicar ao GSI incidentes graves. Atualmente o Grupo tem caráter rotativo e multidisciplinar. Cultura de Segurança Cibernética está em desenvolvimento no Brasil e empresas têm receito de disponibilizar dados de incidentes.

Forma de representação do processo de resposta a incidentes cibernéticos

O processo de resposta a incidente cibernético varia de “linear” a “cíclico” no SEB. Alguns agentes do SEB “importam” a cultura de segurança de suas matrizes multinacionais e organizações mais avançadas já discutem conceitos de agilidade. Em relação ao arcabouço regulatório, o processo de resposta a incidentes é predominantemente discutido de forma linear.

Etapas processo de resposta a incidentes cibernéticos

Atualmente, o grupo de coordenação setorial deveria receber notificação ode incidentes de todo o SEB, após a fase de Detecção do incidente. A partir do registro de um evento, deve ser feita a avaliação e classificação. Dependendo no nível de criticidade, a notificação deve ser encaminhada ao GSI. Eventos não críticos devem ser registrados e acompanhados estatisticamente. Está sendo desenvolvido um sistema de informação para recebimento de informações de todos os agentes do SEB. Em nível nacional, há discussão sobre a criação de uma agência reguladora, para tratamento de assuntos relacionados à segurança cibernética no Brasil

Relacionamento entre Stakeholders

Atualmente existem diversos grupos constituídos que precisam entrar em convergência. Na eventual ocorrência de um incidente cibernético, o grupo de coordenação setorial do SEB deve avaliar o envio de alerta geral a outros órgãos e instituições, após análise de criticidade pela equipe de tratamento do grupo.

Atualmente, entende que o órgão regulador do SEB A ANEEL tem papel educativo, com foco no aprendizado e aplicação de boas práticas. Está fomentando o desenvolvimento no setor a partir do estímulo à colaboração. A atuação fiscalizatória deve ser adotada apenas em médio ou longo prazo. Em relação à forma de representação, entende que há uma centralização devido à regulação setorial, mas que a tendência é o estímulo à colaboração multilateral.

II. Organização integrante do SEB. Membro do grupo de coordenação setorial do SEB. Data entrevista: 13/07/2023

Forma de representação do processo de resposta a incidentes cibernéticos

Em relação às representações de processos, entende que o cíclico ou ágil são mais aplicáveis, evoluindo inicialmente do cíclico para o ágil. A velocidade é uma métrica importante a ser considerada no processo. Hoje há processo para autoavaliação para entendimento do nível de maturidades e posterior estabelecimento de metas

Etapas processo

As fases destacadas pela literatura se aplicam ao contexto da organização. Algumas etapas podem ser condensadas e outras detalhadas, mas de forma geral se aplicam. Há maior enfoque nas fases de prevenção, monitoramento de vulnerabilidades e detecção. Não há desenho claro para processo de resposta a incidentes cibernéticos.

Atualmente a organização utiliza ferramenta de gestão de riscos para monitoramento de vulnerabilidades. O entrevistado informou que entende que há possibilidade de avanços na normatização interna, especialmente em relação às fases 4-Avaliação/Análise e decisão, 5- Contenção e Recuperação e 6-Atividades pós incidentes. A organização está analisando frameworks potencialmente aplicáveis e deseja criar indicadores para segurança da informação.

A organização está investindo no monitoramento e está colaborando com outros atores e participando de fóruns, inclusive para acompanhamento na evolução da regulamentação.

Relacionamento entre Stakeholders

A agência reguladora, ANEEL, estabeleceu estrutura de Comitê (grupo de coordenação setorial do SEB), com participação de entidades do setor e está estruturando um sistema para coleta de informações sobre incidentes cibernéticos. A proposta é que o comitê tenha ciência do que está acontecendo no setor.

De acordo com o entrevistado, o comitê está desenvolvendo uma matriz de criticidade para classificação do incidente e tomada de ações. O comitê deseja que o reporte pelos agentes do setor seja realizado mesmo que não se tenha ainda todas as informações (reporte ágil). A ideia é que o comitê não seja fiscalizador, mas que tenha uma visão do todo no mercado de energia. Ressalta-se que o comitê atua de modo vinculado à REGIC.

III. Organização integrante do SEB e REGIC. Data entrevista: 19/07/2023

Forma de representação do processo de resposta a incidentes cibernéticos

Os incidentes são avaliados individualmente de forma “linear”. Entretanto, quanto ao processo como o todo, entende que é tratado de forma cíclica na organização, com avaliação e implementação de melhorias. Em relação a adoção de um modelo ágil, entende que a adoção não seria um avanço significativo. Um modelo cíclico bem implementado seria suficiente.

Etapas processo de resposta a incidentes cibernéticos

Os entrevistados entendem que as etapas do processo de resposta a incidentes, consolidadas na literatura, se aplicam ao contexto prático da organização.

Em relação ao planejamento, entende que a preocupação das instituições deve avançar além da discussão tecnológica e entende que há dificuldades para aplicação dos normativos e regulamentos existentes atualmente. Entende que a Estratégia Nacional de Segurança Cibernética precisa ser desdobrada no âmbito regulatório. Os entrevistados entendem que atualmente a discussão normativa não acompanha a evolução natural prática sobre o tema e que há grande diversidade/ dispersão de atos normativos, que dificultam a adoção.

Em relação ao monitoramento, atualmente a organização deve enviar informações ao CTIR Gov e entende que há possibilidade de melhoria no processo de envio de informações que podem aumentar a agilidade de envio, análise e resposta entre as instituições. Incidentes históricos já foram registrados e enviados para análise do órgão.

Relacionamento entre Stakeholders

A organização está em processo de adesão à REGIC, que é coordenado de forma centralizada pelo GSI. Entendem que a interação lateral é importante, para promover maior agilidade. Essa interação lateral existe, entretanto, é informal e ocorre a partir de iniciativas próprias das instituições. Os entrevistados informaram que a criação de uma agência em âmbito nacional para centralização da discussão sobre o tema seria interessante

IV. Organização objeto do estudo – Área Segurança Cibernética.

1ª entrevista - Data entrevista: 26/05/2023

Questões gerais

O entrevistado entende que atualmente não há processo de resposta a incidentes no contexto do SEB. Entretanto, entende que a agência reguladora, ANEEL, está estruturando um processo para recebimento de notificações de incidentes. O entrevistado informou que foi criado um grupo com foco na centralização do recebimento de informações de incidentes entre agentes e entidades governamentais (CERTbr e outros)

Forma de representação do processo de resposta a incidentes cibernéticos

Existem etapas prévias a resposta ao incidente que são cadenciadas. Durante o incidente, vai depender da dinâmica do incidente e podem ocorrer variações. As etapas praticadas se assemelham às etapas abordadas na literatura, mas existe uma atividade m paralelo que desde a detecção até pós incidentes que é a etapa de “coleta e retenção de evidências”. O monitoramento é ininterrupto. Desde a detecção, as evidências precisam ser coletadas. Em muitos casos é necessário realizar atividades “pós mortem”, para submissão a processos legais associados. A documentação é muito importante durante o processo

Etapas processo de resposta a incidentes cibernéticos

PREPARAÇÃO

Existem políticas e normas na organização.

No SEB ainda está sendo preparado normativo para fase de comunicação

Equipes de segurança: Não há equipes de segurança entre os agentes de forma conjunta. Mas há equipes dentro da organização Equipes são formadas durante a decretação do incidente. Dependendo tipo e nível do incidente, diferentes tipos de equipes podem ser acionados, internamente ou externamente à TI

Gestão de Risco: há processo de gestão de risco, com avaliação de maturidade, gestão de risco organizacional e gestão de risco da TI que está sendo evoluído de um processo de gestão de vulnerabilidades. É um processo complementar ao de gestão de riscos organizacional. No setor, a REN 964 da ANEEL determina que os agentes façam uma avaliação ode maturidade, que é uma das etapas de um processo de Gestão de riscos. No setor é feito parcialmente.

Dados Históricos: Não há avaliação de dados históricos, pois não há dados históricos de incidentes, pois nunca foi detectado incidente grave, apesar de tentativas terem sido realizadas. Como não há dados históricos relevantes, são realizas análises em comparação com o ambiente externo

MONITORAMENTO

Existe uma empresa de SOC terceirizada contratada para monitoramento. Existe ferramenta de SIEM para detectar e correlacionar os eventos detectados. O SOC monitora incidentes na TI corporativa e operativa

Não há compartilhamento de dados monitorados com instituições do setor

DETECÇÃO

O SIEM utilizado possui tecnologia de Machine Learning embarcada para melhorar capacidade de correlação de dados. Ferramentas de gestão de credenciais também possuem tecnologias de ML. Existem camadas de *intrusion detection* nas redes.

Sobre o histórico de evolução de incidentes, existem poucos incidentes registrados internamente e no SEB os incidentes são conhecidos de modo informal. Não há processo instituído formalmente (institucional) para comunicação e compartilhamento e incidentes ainda. Um sistema está sendo desenvolvido pela ANEEL e de acordo com REN 964/2021, a comunicação dos agentes do setor passará a ser obrigatória

AVALIAÇÃO

Ocorre priorização na avaliação dos incidentes pelo SOC de forma estruturada e largamente automatizada. São incidentes pontuais, com comportamento suspeito de uso de credenciais. Incidentes identificados pelo SOC são automatizados.

Para incidentes que podem se tornar crise (grande porte) não há processo pré-definido, pois há necessidade de análise subjetiva dos atores envolvidos na organização. Existe um processo de comunicação e criação da sala de guerra, para avaliação, tratamento e comunicação do incidente.

Os atores envolvidos na situação de crise são os stakeholders da área de TI, Riscos, DPO e área de comunicação à sociedade e agentes. Dependendo do incidente, área jurídica pode ser envolvida.

CONTENÇÃO

Para incidentes cotidianos e de menor complexidade, tratados pelo SOC, há procedimentos e tecnologias para contenção. Exemplo: EDR (tecnologia embarcada, solução *endpoint*). São criados *playbook* em conjunto com o SOC

Para incidentes de crise, não há procedimentos prontos/estruturados, devido à diversidade de incidentes.

Hierarquia: Existe um comitê que é formado na detecção de crise.

PÓS INCIDENTE

Existe um serviço contratado de acordo que é utilizado de acordo com o nível de necessidade para avaliação dos incidentes. Causas e razões dos incidentes são analisadas de forma geral pela equipe de TI.

Sobre auditoria/fiscalização: nunca ocorreu fiscalização pela ANEEL. A REN 964 não explicita processo fiscalizatório. Há a percepção de que não há intenção fiscalizatória nesse momento.

Sobre a aplicação da Rotina Operacional RO-CB.BR.01: Os agentes do SEB devem declarar se estão ou não em conformidade com a Rotina e devem listar os motivos. No momento, tem-se o resultado de uma autoavaliação dos agentes, a partir da declaração, apresentada em maio/2023. Foi possível ter uma avaliação ode maturidade do setor como um todo.

Relacionamento entre Stakeholders

Formalmente, haverá uma equipe coordenada pela ANEEL. O objetivo da equipe é receber as comunicações dos agentes e informar para as entidades federais.

Está sendo constituído um sistema de informação para comunicação dos agentes ao grupo. O sistema permitirá o compartilhamento de informações sobre ameaças.

Entende-se que o grupo é relevante para tomada de decisão e para proteção sistêmica e para defesa nacional pelo governo.

2ª entrevista - Data entrevista: 28/07/2023

Etapas processo de resposta a incidentes cibernéticos

PREPARAÇÃO

Em relação à fase de preparação, existe um processo de gestão de vulnerabilidades que ocorrem em paralelo à fase de preparação. O processo tem como objetivo minimizar e mitigar riscos cibernéticos.

Em relação à aplicação da REN ANEEL 964/2021, o entrevistado entende que a REN é orientativa e que é um considerável avanço na discussão sobre o tema no SEB.

Relacionamento entre Stakeholders

No que tange à comunicação de incidentes a outros órgãos, não há relação direta com o CETIR GOV. Quanto ao CERT BR, existe uma relação consultiva e de troca de experiências. O foco de reporte de incidentes no SEB é o grupo de coordenação setorial liderado pela ANEEL.

V. **Organização objeto do estudo – Área de Gestão de Assuntos Regulatórios:**
Data da Entrevista: 12/05/2023

Questões gerais

Entende-se que a organização possui um processo gestão de vulnerabilidades em implantação, associada às fases de planejamento e monitoramento do processo de resposta a incidente. Esse processo é executado de acordo com o escopo da Rotina Operacional RO-CB.BR.01. Faz parte do escopo desse processo as seguintes etapas: inventário, avaliação da vulnerabilidade e remediação.

Forma de representação do processo de resposta a incidentes cibernéticos

De acordo com o entrevistado, a Gestão de vulnerabilidades é naturalmente cíclica e o processo é periodicamente é revisado. Entretanto, quando alguma questão inesperada se manifesta, o processo precisa ser atualizado de forma ágil. Não é possível aguardar um novo ciclo.

Etapas processo de resposta a incidentes cibernéticos

PREPARAÇÃO

A Organização realiza treinamentos internos com seus colaboradores para áreas, para aumentar a conscientização. Os ativos são avaliados na fase de inventário e avaliação das vulnerabilidades, no âmbito do processo de Gestão de Riscos.

Não há conhecimento de dados históricos de incidentes para aprendizado / lições aprendidas.

O processo de comunicação externa sobre incidentes registrado está sendo estruturado com o grupo de coordenação setorial o grupo de gestão de incidentes que está sendo constituído.

MONITORAMENTO E DETECÇÃO

A organização utiliza tecnologias (estimador de estados) que permitem monitoramento da rede elétrica e entendimento do comportamento da rede.

Invasões aos sistemas de supervisão, provavelmente não afetariam as instalações

Não há conhecimento sobre incidentes que tenham afetado a operação, mas há tecnologias para identificação de anomalias e do comportamento da rede.

CONTENÇÃO/RECUPERAÇÃO

Atualmente, há redundância entre centros de operação, para caso de perda completa de um centro

Relacionamento entre Stakeholders

Está sendo desenvolvido sistema, base *open source*, para informe e divulgação de incidentes no âmbito do grupo de coordenação setorial, do SEB. Foi criado um grupo

multidisciplinar com participação de relevantes órgãos do setor e a ANEEL é responsável pela coordenação.

Quanto ao formato centralizado ou descentralizado, entende que há um mix. Os agentes compartilham informações com grupo de coordenação setorial do SEB. Entretanto, dentro do grupo há uma colaboração entre os órgãos.

VI. Organização objeto do estudo - Área de Gestão de Riscos:

Data entrevista: 26/05/2023

Forma de representação do processo de resposta a incidentes cibernéticos

Em relação ao formato das fases o ideal seria com retroalimentação. Idealmente, as lições aprendidas devem retroalimentar o ciclo, mas as fases do PGI estão apresentadas de forma mais linear do que cíclica. Há recomendação de que as lições aprendidas sejam observadas no processo.

Etapas processo de resposta a incidentes cibernéticos

PREPARAÇÃO

Existe um PGI que descreve atividades para gestão de incidentes cibernéticos.

Fases PGI: identificação o incidente (o que são sinais), notificação do incidente (com rótulos), documentação do incidente, resposta ao incidente coleta e manipulação de evidências, erradicação e recuperação). Também possui instruções para resposta a vazamento de dados pessoais, em atendimento às recomendações da Autoridade Nacional de Proteção de dados. O PGI também destaca fases pós incidente. Não há critério para priorização dos incidentes detectados. Existe explicitação dos atores envolvidos, restrito ao contexto interno da organização.

Ao longo do processo de gestão de incidentes, contatos externos devem ser registrados, no momento da documentação do incidente. O PGI rata da importância de se reter evidências para análise futura.

Na TI operativa existe o PPSP, para cenário de perda da conexão das salas de controle, mas não há procedimento específico para casos de incidentes cibernéticos, uma vez que os planos são abrangentes.

Sobre políticas, existe uma política de segurança da informação e gestão de riscos, mais genéricas. Quanto ao processo de gestão de riscos., o ataque cibernético é um dos eventos priorizados pela organização e são mapeadas as causas e avaliados controles. O monitoramento de eventos cibernéticos é uma ação que vem sendo desdobrada pela equipe de TI.

Em reação à evolução do processo, existe um processo de avaliação contínua do índice de maturidade de segurança da informação.

MONITORAMENTO E DETECÇÃO

O PGI foca muito na documentação sobre tudo que ocorre durante a gestão do incidente. Coleta de evidências, de decisões que foram tomadas, contatos efetuados devem ser documentados.

CONTENÇÃO/RECUPERAÇÃO

No PGI há recomendações de que dano deve ser potencialmente contido, mas não há detalhamento operacional.

VII. <u>Organização objeto do estudo – Árae de Normatização da Operação:</u>
<u>Data entrevista: 17/06/2023</u>

Forma de representação do processo de resposta a incidentes cibernéticos

Entende-se que o processo de gestão de incidentes (que inclui o tipo ciberbético) é linear e gerido de forma cíclica. Periodicamente existem reuniões para avaliação do processo

Etapas processo de resposta a incidentes cibernéticos

As fases abordadas na literatura são aplicáveis à uma crise no centro de operação.

Na operação são tratados os cenários prováveis de incidente (ex. problemas na rede corporativa)

PREPARAÇÃO

São feitos testes e atualizações periódicas (semanalmente no caso da operação). Aplicativos e instruções sensíveis são disponibilizados de forma redundante, para fácil acesso em caso de crise. São criados cenários nos testes com um centro assumindo outro. Testa telefonia, rede ações.

Existe um sistema de Gestão da Qualidade com todos os procedimentos, que inclui o PPSP, certificado ISO 9001. São feitas avaliações periódicas, análise críticas e propostas melhorias com avaliação de lições aprendidas e nesse contexto, não há relacionamento direto entre outras instituições.

Anualmente é feito exercício simulado para testes de ferramentas no planejamento.

No escopo de Gestão de Riscos. São avaliados cenários de riscos para caso da ocorrência de incidentes. Há linhas de ação para avaliação.

MONITORAMENTO E DETECÇÃO

TI monitora rede operativa e corporativa 24, que são segregadas. Operadores podem identificar incidentes no dia a dia, durante 24h contínuas.

Existem medidas adotadas na segurança da TI operativa que não permitem acesso ao ambiente interno da operação a partir de um ambiente externos.

Caso haja problemas no envio de informações por determinado agente, existe a tecnologia de estimador de estado, que pode ser utilizado em caso de problemas no recebimento de operações. Caso a área afetada seja muito grande, e o estimador seja afetado, a operação poderia contingenciada.

Reforça-se que todos os canais de comunicação são contingenciados e que fornecedores de tecnologia são avaliados de forma que requisitos de alta disponibilidade sejam atendidos.

Quanto à detecção, eventuais incidentes/problemas podem ser detectados na sala de controle para serem reportados às equipes de tecnologia.

AVALIAÇÃO, ANÁLISE, CONTENÇAO E RECUPERACAO

A decisão é tomada pelo próprio Tempo Real. Há backup/redundância das salas de controle. No caso da substituição de um centro de controle por outro, agentes são comunicados e o centro afetado se recupera e passa a assessorar o centro que assumiu até o retorno à normalidade.

POS INCIDENTE

No pós incidente, são analisadas causas, áreas envolvidas, lições aprendidas e o que pode ser realizado para que o incidente/falha aconteça. Existem auditorias internas do Sistema de Gestão da Qualidade e externa da ISO 9001 e ainda não ocorreram fiscalizações técnicas de órgãos reguladores nesse processo.

Relacionamento entre Stakeholders

PPSP está restrito ao contexto interno e existe uma interação múltipla entre os centros, quando novas práticas, ações e melhorias são identificadas.

VIII. Organização objeto do estudo – Área de Telecomunicações

Data entrevista: 29/06/2023

Forma de representação do processo de resposta a incidentes cibernéticos

As fases se aplicam ao contexto de resposta a incidentes cibernéticos.
A representação cíclica é a que mais se aplicaria ao contexto da organização, com a possibilidade de retroalimentação uma vez que a todo tempo são necessários ajustes no processo.

Etapas processo de resposta a incidentes cibernéticos

PREPARAÇÃO

Existem vários níveis de segurança para tolerância a falha. São definidas rotas alternativas com as operadoras de telefonia. A segurança está associada à disponibilidade dos recursos.

MONITORAMENTO

Há alta necessidade de disponibilidade de recursos e estão sendo cada vez mais a robustez das redes, visando disponibilidade. Requisitos definidos para os para os agentes estão dispostos no Submódulo 2.15 dos Procedimentos de Rede.

-Sem comentários sobre outras fases e relacionamento entre *stakeholders*-

IX. Organização objeto do estudo – Comunicação Institucional

Data entrevista: 29/06/2023

Forma de representação do processo de resposta a incidentes cibernéticos

Formato de representação que mais se assemelha ao que é executado é o cíclico. A comunicação é cíclica. Conforme assuntos avançam e há interação constante com as áreas, até o encerramento do processo de gestão do incidente.

Forma de representação do processo se aplicaria ao contexto da organização. O Plano de comunicação em situação de crise se aplica a qualquer evento que aconteça.

Questões gerais

O Plano de comunicação em situação de crise se aplica a qualquer evento que aconteça.

São dois cenários:

1) Preparação com possibilidade de antecipação à crise, com preparação antecipada (exemplo crise hídrica). Quando há previsibilidade da crise. Definição de ações pré-crise, com preocupação de proteção à imagem e reputação da organização e tem como objetivo a antecipação à crise. Nesse contexto, as etapas da literatura se aplicam a esse contexto. A avaliação é feita de acordo com a imagem da organização.
2) Incidente de curto prazo, sem possibilidade de ampla preparação. As ações devem ser tomadas de forma rápida. É importante que também. A proteção da imagem da organização é um dos pontos de destaque. Deve ser analisada a profundidade da crise e é importante a transparência à sociedade.

Etapas do processo de resposta a incidentes cibernéticos

CONTENÇÃO

A área de comunicação fornece orientações e comunica público geral e empregados. Outros atores da organização fazem a comunicação. O presidente comunica outros representantes institucionais. A comunicação faz um papel de assessoria da presidência.

Empregados também são comunicados.

Dependendo do incidente, há alinhamento entre as áreas de comunicação dos órgãos do setor.

Não há histórico de comunicação sobre incidentes cibernéticos

Relacionamento entre *stakeholders*

A comunicação já participou de exercício com outras instituições, com simulações de como agir e responder a incidentes cibernéticos.

É importante que os atores saibam o papel durante a resposta a incidentes.

Além do grupo de coordenação setorial, existe um canal de comunicação entre líderes de instituições do setor. Não há centralização. O grupo formado é utilizado para discussão de questões gerais do setor. É um grupo colaborativo e a interação é múltipla.