DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Uma Avaliação do Cenário da Gestão de Riscos Cibernéticos no Setor Elétrico Brasileiro sob a Ótica da Rotina Operacional do ONS RO-CB.BR.01

Eduardo de Oliveira Lima

Programa de Pós-Graduação Profissional em Engenharia Elétrica

DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

Uma Avaliação do Cenário da Gestão de Riscos Cibernéticos no Setor Elétrico Brasileiro sob a Ótica da Rotina Operacional do ONS RO-CB.BR.01

An Assessment of the Cyber Risk Management Scenario in the Brazilian Power Sector from the ONS Operational Routine RO-CB.BR.01 Perspective

Eduardo de Oliveira Lima

Orientador: Prof. Dr. Rafael Rabelo Nunes, ADM/FACE/UnB

PUBLICAÇÃO: PPEE.MP.025
BRASÍLIA-DF, 25 DE NOVEMBRO DE 2022.

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Uma Avaliação do Cenário da Gestão de Riscos Cibernéticos no Setor Elétrico Brasileiro sob a Ótica da Rotina Operacional do ONS RO-CB.BR.01

Eduardo de Oliveira Lima

Dissertação de Mestrado Profissional submetida ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Mestre em Engenharia Elétrica

Banca Examinadora

Prof. Dr. Rafael Rabelo Nunes, ADM/FACE/UnB _____
Orientador

Prof. Ph.D Robson de Oliveira Albuquerque, ENE-PPEE/UnB _____
Examinador Interno

Prof. Dr. Iony Patriota de Siqueira, UFCG/TECNIX _____
Examinador Externo

FICHA CATALOGRÁFICA

LIMA, EDUARDO DE OLIVEIRA
Uma Avaliação do Cenário da Gestão de Riscos Cibernéticos no Setor Elétrico Brasileiro sob a Ótica da Rotina Operacional do ONS RO-CB.BR.01 [Distrito Federal] 2022.
xvi, 70 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2022).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. ARCiber	2. SCADA
3. Riscos Cibernéticos	4. Setor Elétrico Brasileiro SEB
I. ENE/FT/UnB	II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

LIMA, E.O. (2022). *Uma Avaliação do Cenário da Gestão de Riscos Cibernéticos no Setor Elétrico Brasileiro sob a Ótica da Rotina Operacional do ONS RO-CB.BR.01* . Dissertação de Mestrado Profissional, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 70 p.

CESSÃO DE DIREITOS

AUTOR: Eduardo de Oliveira Lima
TÍTULO: Uma Avaliação do Cenário da Gestão de Riscos Cibernéticos no Setor Elétrico Brasileiro sob a Ótica da Rotina Operacional do ONS RO-CB.BR.01 .
GRAU: Mestre em Engenharia Elétrica ANO: 2022

Eduardo de Oliveira Lima
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

DEDICATÓRIA

Dedico este trabalho à minha esposa, às minhas filhas e aos pesquisadores deste país.

AGRADECIMENTOS

Agradeço primeiramente a Deus, por estar ao meu lado nos momentos difíceis e por me conceder a saúde necessária para enfrentar os desafios e as oportunidades que a vida nos oferece.

A minha esposa, Beatriz, pela motivação, apoio, companheirismo, incentivo e paciência ao longo de toda essa jornada e às minhas filhas, fonte de alegrias e ensinamentos em minha vida.

Aos meus pais (*in memorian*) pela formação e sólida educação que me proporcionaram.

Ao meu orientador Prof. Dr. Rafael Rabelo Nunes, pelo constante apoio, incentivo e dedicação. Estes requisitos foram essenciais para o desenvolvimento deste trabalho e para o meu desenvolvimento como pesquisador.

Aos professores da UNB, pesquisadores brasileiros e estrangeiros, que contribuíram, por meio de vasto material de pesquisa disponibilizado, para a realização deste trabalho.

Aos funcionários do Departamento de Engenharia Elétrica da Faculdade de Tecnologia da Universidade de Brasília – UnB pelo incansável apoio, em especial à Thayna e à Adriana. Aos alunos Jonathan, Fernando, Marcus e Fábio, meus colegas de mestrado, que nos momentos de desânimo me incentivaram, direta e indiretamente, a continuar em frente, rumo ao objetivo traçado desde o início.

À ENBPar – Empresa Brasileira de Participações em Energia Nuclear e Binacional S/A pelo apoio e incentivo, fatores de grande relevância para a realização deste trabalho.

RESUMO

O avanço tecnológico pelo qual o Sistema Elétrico de Potência – SEP vem passando inseriu uma série de novas variáveis e questões importantes nesse ambiente que devem ser consideradas. Uma delas é a segurança dos dados trafegados entre as geradoras, transmissoras e distribuidoras de energia elétrica e seus Sistemas de Proteção, Comando, Aquisição de Dados e Supervisão (SPCS/SCADA). O planejamento e a gestão de riscos cibernéticos passaram a atuar fortemente em prevenção e recuperação. O Operador Nacional do Sistema Elétrico – ONS, visando estabelecer controles mínimos de segurança cibernética a serem implementados pelos agentes e pelo próprio ONS, definiu o Ambiente Regulado Cibernético – ARCiber, inserido no Manual de Procedimentos da Operação - Módulo 5 – Submódulo 5.13, por meio da Rotina Operacional RO-CB.BR.01 R00, de 09/07/2022, o qual estipulou uma série de orientações que deverão ser obrigatoriamente seguidas pelos agentes do Setor Elétrico Brasileiro – SEB. Com base no ambiente de Segurança Cibernética ARCiber, definido pela RO, este trabalho tem por objetivo analisar o cenário da gestão de riscos cibernéticos do SEB. Para tanto, se buscou dois objetivos específicos, quais sejam: em primeiro plano a realização de uma comparação qualitativa entre os controles propostos pelo Framework CIS CSC e os controles mínimos necessários definidos pelo ARCiber e, em segundo plano, a realização de uma análise de conteúdo do Manual SCADA Win CC 7.5 SP2 da Siemens [1] para avaliar a abrangência dos procedimentos de backup e recuperação de dados do sistema SCADA e sua conformidade com os controles definidos no Macrocontrole 11 – Recuperação de Dados do Framework CIS CSC. Os resultados mostram que apenas um dos dezoito grupos de controle que o ONS recomenda excede as exigências desse Framework. Em contraponto, cinco outros grupos de controle não são mencionados pelas recomendações do ONS, dentre eles o Macrocontrole 11 – Recuperação de Dados, e, para os outros grupos, os requisitos do ONS ficam aquém da estrutura do CIS CSC. Apesar de se ter verificado a conformidade entre o Framework CIS CSC e os aspectos funcionais e tecnológicos existentes no processo de recuperação de dados do sistema SCADA, não é possível garantir que empresas do setor elétrico brasileiro executem as rotinas de recuperação de forma sistemática. A relevância desse trabalho está na possibilidade da construção de um debate acerca do tema, diante das recentes ações do ONS para enfrentar os riscos cibernéticos associados à infraestrutura operacional do SEB, que, conforme os resultados, ainda necessitam de melhorias em sua maturidade operacional e de gestão.

ABSTRACT

The technological advance through which the Power Electric System - SEP has been going through has inserted a series of new variables and essential issues in this environment that must consider. One is the security of the data exchanged between power generators, transmitters, and distributors and their Protection, Command, Data Acquisition, and Supervision Systems (SPCS/SCADA). Cyber risk planning and management have moved firmly into prevention. The National Electric System Operator - ONS, aiming to

establish minimum cyber security controls to be implemented by the agents and by ONS itself, has defined the Regulated Cyber Environment - ARCiber, inserted in the Manual of Operating Procedures - Module 5 - Submodule 5.13, through the Operational Routine RO-CB.BR.01 R00, of 07/09/2022, which stipulated a series of guidelines that must be compulsorily followed by the agents of the Brazilian Electric Sector - SEB. Based on the ARCiber CyberSecurity environment, defined by RO, this work aims to analyze the SEB's cyber risk management scenario. For this purpose, two specific objectives were sought: in the first place realization of a qualitative comparison between the controls proposed by the CIS CSC Framework and the minimum necessary controls defined by ARCiber and, in the background, the awareness of a content analysis of the Siemens SCADA Win CC 7.5 SP2 Manual [1] to evaluate the scope of the procedures for backup and recovery of data of the SCADA system and its compliance with the defined controls in Macro Control 11 - Data Recovery of the CIS CSC Framework. The results show that only one of the eighteen control groups that ONS recommends exceeds the requirements of this Framework. In contrast, ONS does not mention five other control group recommendations, including Macro control 11 - Data Recovery. For the other groups, the ONS requirements fall short of the CIS CSC Framework. Despite verifying the conformity between the CIS CSC Framework and the functional and technological aspects of the SCADA system's data recovery process, it is impossible to guarantee that companies in the Brazilian electric power sector systematically execute the recovery routines. The relevance of this work lies in the possibility of building a debate about the theme, given the recent actions of ONS to address the cyber risks associated with the operational infrastructure of the Brazilian Electric System (SEB), which, according to the results, still need improvements in their operating and management maturity.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

Siglas

ABRATE	Associação Brasileira das Empresas de Transmissão de Energia Elétrica
ANEEL	Agência Nacional de Energia Elétrica
ANSI	*American National Standards Institute* (Instituto Nacional Americano de Padrões)
ARCiber	Ambiente Regulado Cibernético
CCS	*Council on Cybersecurity* (Conselho de Segurança Cibernética)
CERT	*Computer Emergency Readiness Team* (Equipe de Prontidão em Emergências de Computador)
CIM	*Common Information Model* (Modelo de Informação Comum)
CIS CSC	*Center for Internet Security - Critical Security Controls* (Centro de Segurança na Internet - Controles críticos de segurança)
CLP	Controlador Lógico Programável
CNPE	Conselho Nacional de Política Energética
COBIT	*Control Objectives for Information and Related Technologies* (Objetivos de controle de informações e tecnologias relacionadas)
CSSP	*Cybersecurity Service Provider* (Provedor de serviços de segurança cibernética)
DER	*Distributed Energy Resource* (Recursos de Energia Distribuía)
DHS	*Department of Homeland Security* (Departamento de Segurança Interna)
DNP3	*Distributed Network Protocol V3* (Protocolo de Rede Distribuída V3)
DOU	Diário Oficial da União
DRTNS	*Dimentional Research and Tenable Network Security* (Pesquisa Dimensional e Segurança de Rede Tenable)
EPE	Empresa de Pesquisa Energética
EU	*European Union* (União Europeia)
FBI	*Federal Bureau of Investigation* (Birô Federal de Investigação)
GE	*General Electric* (Elétrica Geral)
ICCP	*Institute for Certification of Computing Professionals* (Instituto de Certificação de Profissionais da Computação)
ICS	*Industrial Control Systems* (Sistemas de Controle Industrial)
IDS	*Intrusion Detection System* (Sistema de Detecção de Intrusão)
IEA	*International Energy Agency* (Agência Internacional de Energia)
IEC	*International Electrotechnical Commission* (Comissão Eletrotécnica Internacional)

IED	*Inteligent Electronic Device* (Dispositivo Eletrônico Inteligente)
ISA	*The Instrumentation, Systems and Automation Society* (Sociedade de Instrumentação, Sistemas e Automação)
ISACA	*Information Systems Audit and Control Association* (Associação de Auditoria e Controle de Sistemas de Informação)
ISO	*International Organization for Standardization* (Organização Internacional para Padronização)
ISSN	*International Standard Serial Number* (Número de série padrão internacional)
MICRADS	*Multidisciplinary International Conference of Research Applied to Defense and Security* (Conferência Internacional Multidisciplinar de Pesquisa Aplicada à Defesa e Segurança)
MME	Ministério de Minas e Energia
NATO	*North Atlantic Treaty Organization* (Organização do Tratado do Atlântico Norte)
NIST CSF	*National Institute of Standards and Technology Cybersecurity Framework* (Instituto Nacional de Normas e Framework em Tecnologia de Cibersegurança)
NISTR	*National Institute of Standards and Technology Report* (Relatório do Instituto Nacional de Normas e Tecnologia)
ONS	Operador Nacional do Sistema Elétrico
PLC	*Programmable Logic Controller* (Controlador Lógico Programável)
PMU	*Phasor Measurement Unit* (Unidade de Medição de Fasor)
PR	Procedimentos de Rede
QUALIS	Qualis Periódicos para Avaliação de Produção Científica de Pós Graduação
RAT	*Remote Access Trojan* (Trojan de Acesso Remoto)
RIST	Revista Ibérica de Sistemas e Tecnologia da Informação
RO	Rotina Operacional
SCADA	*Supervisory Control and Data Acquisition* (Sistema de Supervisão e Aquisição de Dados)
SEB	Setor Elétrico Brasileiro
SEP	Sistema Elétrico de Potência
SIN	Sistema Interligado Nacional
SPCS	Sistema de Proteção, Comando e Supervisão
UK	*United Kingdown* (Reino Unido)
UN	*The United Nations* (Nações Unidas)
US	*United States* (Estados Unidos)
UTR	Unidade de Terminal Remoto
VPN	*Virtual Private Network* (Rede Privada Virtual)

1 INTRODUÇÃO

Nos últimos anos, sensores avançados, automação inteligente, redes de comunicação e tecnologias da informação (TI) foram integrados à rede elétrica para melhorar seu desempenho e eficiência. A integração dessas novas tecnologias resultou em maiores interdependências entre os componentes físicos e cibernéticos da rede [2].

O intenso uso da tecnologia da informação em todos os segmentos da indústria 4.0, onde se insere o Sistema Elétrico de Potência - SEP, criou um desafio no contexto da gestão de riscos cibernéticos associados às operações de geração, transmissão e distribuição abrangidas pela rede elétrica, o que tem despertado preocupações tanto da indústria quanto da academia [3].

As redes elétricas, muitas vezes, são constituídas de soluções tecnológicas diversas, as quais muitas vezes fogem das recomendações rígidas de segurança que deveriam seguir, mesclando até mesmo sistemas analógicos legados com sistemas digitais automatizados [4] [5].

Tem-se observado para as infraestruturas críticas uma elevação acentuada do número de ocorrências de violações na segurança dos Sistemas de Supervisão e Aquisição de Dados - SCADA, aumentando em 11% entre os anos de 2017 e 2018 e ainda um acréscimo de 67% se for considerado o período entre os anos de 2013 e 2018 [6].

Os ataques cibernéticos às infraestruturas críticas dos SEP procuram explorar normalmente as vulnerabilidades existentes nos Sistemas de Controle Industrial – ICS. Em 2013, o malware Stuxnet causou danos significativos ao Sistema SCADA responsável pelo controle das centrífugas da usina nuclear de Natanz, no Irã [7]. Nos anos seguintes, vários casos também foram relatados: em 2014, a campanha de ataque Havex [8] e a campanha Sandworm usando uma vulnerabilidade de dia zero para atingir o Sistema SCADA da General Electric - GE [9], e nos anos de 2015 a 2017, as ações destrutivas do malware Killdisk [10] e Industroyer [11] causaram o desligamento da rede elétrica ucraniana.

Eventos como este levaram o Departamento de Segurança Nacional dos EUA - DHS e o Federal Bureau of Investigation - FBI a emitir um alerta em 2018 sobre ataques direcionados a energia e outros setores industriais críticos, quase todos eles direcionados aos Sistemas SCADA [12].

A este respeito, o Operador Nacional do Sistema Elétrico - ONS, considerando os riscos cibernéticos a que são submetidas as instalações do SEP, essencialmente aquelas sob influência do Sistema SCADA, publicou em 09 de julho de 2021, uma Rotina Operacional (RO-CB.BR.01 Rev. 00) cujo objetivo é determinar aos agentes do Setor Elétrico Brasileiro - SEB a implantação de controles minimamente necessários, associados ao processo de gestão de riscos cibernéticos, definidos pelo Ambiente Regulado Cibernético, denominado ARCiber [13], até o final de setembro de 2023, cujo escopo abrange o conjunto de redes e equipamentos considerados no domínio da RO.

Até o momento, não existem registros de outras rotinas operacionais do ONS, pertencentes aos Procedimentos de Rede - PR, abordando a gestão da Segurança Cibernética no Setor Elétrico Brasileiro. Este tema era tratado, até então, por meio de iniciativas individualizadas de cada agente do SEB, utilizando-se

as referências de mercado e seus normativos internos, porém sem uma regulação específica [14] [13].

Como órgão regulador do SEB e em consonância com a iniciativa do ONS, a Agência Nacional de Energia Elétrica – ANEEL estabeleceu em 14 de dezembro de 2021 a Resolução Normativa N. 964 [14].

Essa Resolução passou a definir uma maior abrangência para o ambiente de fiscalização da gestão de riscos cibernéticos no Setor Elétrico Brasileiro, considerando agora os limites definidos pelo ARCiber [15] e seus próprios instrumentos regulatórios.

A lista de controles definidos pela Rotina Operacional do ONS para a gestão de riscos cibernéticos no ARCiber não faz menção sobre procedimentos específicos associados à gestão de Recuperação de Dados, Proteção de Dados, Treinamento de Conscientização e Habilidades de Segurança, Gerenciamento de Provedor de Serviços, Segurança de Softwares e Aplicativos, e Testes de Penetração [15].

Além de se protegerem preventivamente de ataques cibernéticos, um elemento fundamental com o qual as empresas do setor elétrico devem se valer para aumentar a sua resiliência é a execução sistemática de um processo de backup e recuperação de dados [16].

No entanto, verifica-se que muitas empresas desse segmento ainda não padronizaram suas métricas associadas ao processo de gestão de riscos cibernéticos, deixando de conhecer e gerenciar adequadamente os seus parâmetros operacionais, tornando ainda mais vital a presença de um processo de gestão de riscos que contemple os procedimentos de recuperação de dados de forma clara e controlada [17].

Neste contexto, este trabalho procurou avaliar se a implantação dos controles mínimos definidos pelo ONS para o ambiente ARCiber seriam suficientes para enfrentar os riscos cibernéticos a que as atividades envolvidas nos processos operacionais estão submetidas [15]. Adicionalmente, a avaliação do Sistema SCADA da Siemens Win CC 7.5 SP2 foi realizada com o objetivo de se verificar a existência de rotinas de recuperação de dados suficientemente abrangentes, de forma que a previsão de controles para essa dimensão pudessem ser prescindíveis no ARCiber [16].

Nesse contexto, este trabalho teve por objetivo analisar o cenário da gestão de riscos cibernéticos do SEB sob a ótica da Rotina Operacional do ONS RO-CB.BR.01.

Para tanto, se valeu de uma análise de conteúdo qualitativa e comparativa entre os controles propostos pelo *framework* CIS CSC e os controles definidos pelo ARCiber, destacando, nesse momento, a subjetividade a que uma análise qualitativa dessa natureza está submetida.

Da mesma forma, foi realizada uma análise de conteúdo do Sistema SCADA da Siemens [1], visando identificar a abrangência dos seus procedimentos de backup e recuperação de dados e sua conformidade com os controles de Recuperação de Dados do *framework* CIS CSC.

A escolha do *framework* CIS CSC V8.0 como parâmetro de comparação com o ARCiber foi baseada no fato de ser ele um *framework* otimizado, construído a partir de uma simplificação da estrutura NIST CSF [18], o qual disponibiliza uma série de controles que apresenta uma relação risco/retorno que facilita a sua implementação, quando comparado com os elevados custos de implantação do *framework* proposto pelo NIST [19].

1.1 MOTIVAÇÃO E JUSTIFICATIVA

- A constatação de um aumento significativo de ataques cibernéticos às redes elétricas de potência ao redor do mundo, na última década [20] [12], com consequências muitas vezes difíceis de se mensurar, tanto para o sistema elétrico como para a sociedade;
- A necessidade de se avaliar o conteúdo e a abrangência da Rotina Operacional RO-CB.BR.01 (AR-Ciber), visando identificar a sua capacidade de gerenciar os riscos cibernéticos, identificando-os, protegendo e recuperando a infraestrutura afetada;
- A necessidade de se analisar a conformidade da RO frente a um Framework Internacional, já testado e avaliado pela comunidade de segurança cibernética mundial, de forma que possa avaliar a capacidade do ARCiber de garantir a continuidade do SEB [21];
- A necessidade de se analisar a existência de controles sistematizados de gestão de riscos cibernéticos, gerados e mantidos pelo processo operacional em tempo real, que possam justificar uma eventual ausência de controles no ARCiber.

1.2 PROBLEMA DE PESQUISA

Este trabalho foca na questão da gestão de riscos cibernéticos no Setor Elétrico Brasileiro, sob a ótica da Rotina Operacional RO-CB.BR.01 Rev. 00. Conforme relatado no capítulo introdutório, até a publicação da RO pelo ONS, a gestão de riscos cibernéticos nesse setor da economia brasileira se baseava em iniciativas individualizadas das empresas de geração, transmissão e distribuição, carecendo de instrumentos regulatórios oficiais, base para a composição de um programa de fiscalização governamental.

No entanto, com a publicação da RO em julho de 2021, o ONS passou a definir os parâmetros que deverão ser obrigatoriamente seguidos pelos agentes do SEB para a composição de um programa de gestão de riscos cibernéticos. O ambiente regulado cibernético, proposto por essa RO e denominado de ARCiber, passou a ser a orientação oficial para a busca de conformidade por esses agentes, preenchendo, até então, uma lacuna existente.

Cabe destacar, nesse momento, que a iniciativa do ONS no sentido de regular a gestão de riscos cibernéticos para os agentes do SEB procurou sanar um vácuo existente na regulação.

Neste ponto, é importante mencionar que sua atuação se restringiu às fronteiras de sua competência e de seu relacionamento com os agentes associados.

A Resolução Normativa ANEEL REN-964/2021 foi publicada em dezembro de 2021, seis meses após a publicação da RO, apresentando, no entanto, características preponderantemente fiscalizatórias, se atendo a apenas alguns aspectos da gestão de riscos cibernéticos.

Com isso, o ONS foi levado a buscar instrumentos que pudessem confrontar esse problema associado aos riscos cibernéticos, de elevada importância para o SEB, cujos reflexos podem afetar diretamente a economia e a segurança nacional. Um aumento significativo de incidentes cibernéticos nesse segmento

produtivo tem sido constatado ao redor do mundo, com ataques cada vez mais sofisticados e eficientes.

A comunidade de segurança cibernética internacional já conta com a disponibilização de importantes *frameworks* de gestão de riscos e segurança cibernética de grande abrangência e reconhecimento dos mais variados setores que lidam com infraestruturas críticas, que é o caso do Setor Elétrico.

Nesse sentido, ao lançar o ARCiber e exigir dos agentes do SEB a sua implantação e conformidade até meados do ano de 2023, o ONS passou a se valer de um instrumento oficial de padronização e avaliação, a ser utilizado para a fiscalização dos agentes quanto ao atendimento aos requisitos de segurança e gestão de riscos cibernéticos definidos para o setor elétrico.

O ARCiber é uma proposta do ONS ainda muito recente, e que se encontra em fase de implantação. A sua validação quanto à efetiva capacidade de gerenciar e mitigar os riscos cibernéticos no SEB deverá ser confirmada ou não ao longo do seu primeiro ciclo de implantação.

O problema de pesquisa passa, portanto, pela avaliação da efetividade da proposta do ONS para a segurança cibernética do SEB sob a ótica da RO e suas influências e consequências para as empresas e demais agentes afetados.

Considerando o **Problema** exposto, formulou-se duas hipóteses;

Hipótese H1: *O processo de gestão dos riscos cibernéticos proposto pelo ONS por meio do ARCiber é capaz de gerenciar e mitigar os riscos cibernéticos a que estão submetidos os seus procedimentos operacionais e aqueles integrados aos agentes do SEB.*

Hipótese H2: *O Sistema SCADA Win CC 7.5 SP2 da Siemens gera e mantém os controles necessários e indicados para a gestão de riscos cibernéticos, associados ao processo de Recuperação de Dados.*

1.3 OBJETIVO GERAL

Este trabalho tem por objetivo geral analisar o cenário da gestão de riscos cibernéticos do SEB sob a ótica da Rotina Operacional do ONS RO-CB.BR.01 (ARCiber).

1.4 OBJETIVOS ESPECÍFICOS

Partindo do objetivo geral deste trabalho definiu-se os seguintes objetivos específicos:

OBJ1: Realizar uma revisão da literatura sobre o Setor Elétrico Brasileiro e sobre os *frameworks* de Gestão de Riscos Cibernéticos voltados para infraestruturas críticas;

OBJ2: Comparar os controles propostos pelo *framework* CIS CSC [22] com os controles definidos pelo ARCiber [13], utilizando-se como subsídio a Rotina Operacional, Normas,

Padrões e Documentos do SEB, com base na metodologia de análise qualitativa definida pelo *framework* CIS CSC;

OBJ3: Avaliar os procedimentos de backup e recuperação de dados apresentados no Manual SCADA da Siemens Win CC 7.5 SP2 [1] para verificar a abrangência dos procedimentos utilizados e suas conformidades com os controles de Recuperação de Dados do *framework* CIS CSC.

1.5 CONTRIBUIÇÕES DESSE TRABALHO

1.5.1 Contribuições Diretas

As publicações abaixo relacionadas apresentam as constatações e resultados obtidos a partir das análises realizadas no arcabouço de gestão de riscos cibernéticos definido pelo ONS que, por meio do ARCiber, procurou suprir uma lacuna existente na regulação.

Título 1:	***Avaliação da Rotina Operacional do Operador Nacional do Sistema Elétrico Brasileiro (ONS) em Relação às Ações de Gerenciamento de Riscos Associados à Segurança Cibernética*** [15].
Autores:	Eduardo de O. Lima, Fernando R. Moreira, Flávio E. G. de Deus, Georges D. A. Nze, Rafael T. de S. Júnior e Rafael R. Nunes
RIS:	Qualis A2.
Publicação:	RISTI – Revista Ibérica de Sistemas e Tecnologia da Informação Vol E49 Pag 301-312 - 2022.
url:	<http://www.risti.xyz/issues/ristie49.pdf>
ISSN:	<https://portal.issn.org/resource/ISSN/1646-9895#>

Título 2:	***Gestão de Riscos Cibernéticos no Ambiente Operacional do Sistema Elétrico Brasileiro (ARCiber ONS): uma avaliação do processo de recuperação de dados pelo Sistema SCADA*** [16].
Autores:	Eduardo de O. Lima, Fernando R. Moreira, Carlos A. de M. Alves e Rafael R. Nunes
RIS:	Qualis A2.
Publicação:	RISTI – Revista Ibérica de Sistemas e Tecnologia da Informação Vol E49 Pag 313-325 - 2022.
url:	<http://www.risti.xyz/issues/ristie49.pdf>
ISSN:	<https://portal.issn.org/resource/ISSN/1646-9895#>

1.5.2 Contribuições Indiretas

As publicações a seguir apresentam os resultados de trabalhos de pesquisas bibliométricas realizadas em temas de grande relevância para a gestão de riscos cibernéticos e segurança cibernética, procurando apresentar um panorama mundial sobre o uso e aplicabilidade dos métodos multicritérios para a gestão da

segurança cibernética, e uma avaliação da distribuição e uso do *framework* NIST CSF e das Normas Série NBR ABNT ISO 27.000 no contexto da gestão da segurança da informação.

Título 3:	***Uma análise das aplicabilidades de métodos multicritérios no contexto da segurança da informação*** [23].
Autores:	Fernando R. Moreira, Eduardo de O. Lima, Carlos A. de M. Alves e Rafael R. Nunes
Publicação:	Doity - Anais 32o ENANGRAD - 2021.
url:	<https://doity.com.br/anais/32enangrad/trabalho/194993>
ISSN:	<https://portal.issn.org/resource/ISSN/1983-022X>

Título 4:	***A Utilização dos Frameworks NIST CSF e da Série NBR ABNT ISO 27.000 no Contexto da Gestão da Segurança da Informação*** [24].
Autores:	Paulo H. M. Bueno, Eduardo de O. Lima, Fernando R. Moreira e Rafael R. Nunes
Publicação:	Doity - Anais 32o ENANGRAD - 2021.
url:	<https://doity.com.br/anais/32enangrad/trabalho/194994>
ISSN:	<https://portal.issn.org/resource/ISSN/1983-022X>

1.6 LIMITAÇÕES E RELEVÂNCIA

É importante destacar que uma limitação verificada no processo de avaliação definido pela metodologia disponibilizada pelo CIS CSC, utilizada neste trabalho para a realização da análise comparativa, foi o grau de subjetividade inerente ao processo de escolha de um dos cinco níveis de conformidade: *Equivalent; Superset; Subset; Intersections; None*, ao se fazer a comparação entre os controles previstos no *framework* CIS CSC e os controles definidos pelo ONS no ARCiber.

Adicionalmente, as constatações obtidas a partir da análise de conteúdo do Manual SCADA da Siemens Win CC 7.5 SP2 se limitam a esse fabricante. Outros sistemas poderiam ser avaliados e os resultados obtidos se juntado às conclusões desse trabalho.

A relevância desse trabalho está em suscitar o debate a cerca da RO-CB.BR.01, deixando aberta a discussão sobre segurança cibernética no Setor Elétrico Brasileiro sob a ótica da Rotina Operacional do ONS.

1.7 ESTRUTURA DA DISSERTAÇÃO

Essa dissertação está dividida em 6 capítulos, incluindo este capítulo introdutório.

O Capítulo 2 - Referencial Teórico, é destinado a apresentar os principais trabalhos acadêmicos da área correlata, envolvendo o SEP, o SEB, o MME, o ONS, a Gestão da Segurança Cibernética no SEB, a Rotina Operacional do ONS - ARCiber, o Panorama Mundial e Desafios dos Ataques Cibernéticos para o Setor

Elétrico e as iniciativas da Gestão de Riscos e Segurança Cibernética das Infraestruturas Críticas do SEP.

O Capítulo 3 - Metodologia, aborda os métodos utilizados no trabalho, orientados em duas direções, quais sejam: a comparação entre a RO-CB.BR.01 e os Controles Estruturais do Framework CIS CSC, e, a avaliação dos procedimentos utilizados pelo Sistema SCADA da Siemens frente ao Macrocontrole 11 - Recuperação de Dados do Framework CIS CSC e o ARCiber.

O Capítulo 4 - Resultados, apresenta os resultados coletados e deduzidos a partir das análises realizadas.

O Capítulo 5 - Discussões, mostra uma avaliação dos resultados obtidos frente aos trabalhos correlatos e à situação da Segurança cibernética no Brasil e também de suas influências externas.

Por fim, o Capítulo 6 - Conclusões, no qual são apresentadas as considerações finais sobre o método, as constatações e propostas de trabalhos futuros.

2 REFERENCIAL TEÓRICO

Neste Capítulo serão discutidos tópicos importantes que serão abordados durante o texto dessa dissertação, destacando-se os principais conceitos em gestão de riscos cibernéticos associados às infraestruturas críticas, suas normas de conformidade e os *frameworks* utilizados na segurança cibernética do Setor Elétrico. Adicionalmente, serão apresentados os principais trabalhos relacionados, discutindo-se suas abrangências e limitações, destacando-se os aspectos associados à proposta deste trabalho.

2.1 O SISTEMA ELÉTRICO DE POTÊNCIA - SEP

O SEP consiste em um complexo sistema de engenharia no qual o centro de controle concentra a responsabilidade pelo monitoramento, controle e tomada de decisões operacionais em tempo real [25].

Além disso, os dispositivos eletrônicos de campo, como vistos em redes de comunicação, sistemas de automação de subestações e centros de controle, são incorporados em toda a rede física e envolvem os segmentos de geração, transmissão e distribuição de energia [26].

Assim, esta infraestrutura representa uma tecnologia diversificada com vários graus de conectividade. Além disso, como um desafio clássico, manter o equilíbrio dinâmico entre oferta e demanda de eletricidade é um aspecto fundamental que precisa ser mantido e garantido em tempo real [2].

Os sistemas elétricos de proteção, comando e supervisão das instalações de potência são compostos por uma série de laços responsáveis pela identificação dos sinais de comunicação, protocolos, máquinas/-dispositivos, processamento e ações de controle, associados a cada classificação funcional. Os impactos potenciais dos ataques cibernéticos estão concentrados principalmente nestes processos [27].

A avaliação dos riscos cibernéticos, associados à segurança das redes de energia elétrica, deve ser continuamente refeita, visando garantir uma operação com um nível adequado de segurança. Entretanto, a complexidade do SEP, a longa vida útil de seus componentes e a constante evolução das ameaças cibernéticas começou a apresentar um novo vetor de ataque [28].

A detecção e remoção dos problemas de segurança cibernética passaram a indicar a necessidade de abordagens específicas, tanto para os sistemas e aplicações de energia (SPCS) como também para os sistemas e aplicações associados ao suporte da infraestrutura de Tecnologia da Informação - TI [29].

Nos últimos anos, o uso de Dispositivos Eletrônicos Inteligentes - IED tem sido disseminado para enfrentar estes desafios. Estes dispositivos permitem o gerenciamento do equilíbrio energético, uma vez que operam sistemas de proteção, comando e supervisão do sistema elétrico [27] por meio de um intenso intercâmbio de dados, representando um aumento significativo das vulnerabilidades expostas pela superfície de exploração [26] [2].

Considerando o cenário de riscos cibernéticos apresentado para o SEP, torna-se necessário tratar a questão a partir de uma abordagem de gerenciamento de riscos.

Neste sentido, o apoio às normas e diretrizes de segurança, difundidas e aceitas pela comunidade internacional, torna-se um fator de grande importância e portanto o desafio é definir um bom instrumento para gerenciar os riscos associados às redes de energia elétrica, considerando a melhor relação risco/retorno para o ambiente cibernético [15].

2.2 O SETOR ELÉTRICO BRASILEIRO - SEB

O Sistema Elétrico Brasileiro, após a importante reforma que sofreu a partir de 1996, passou a ser definido pela estrutura de instituições e agentes conforme mostra a Figura 2.1.

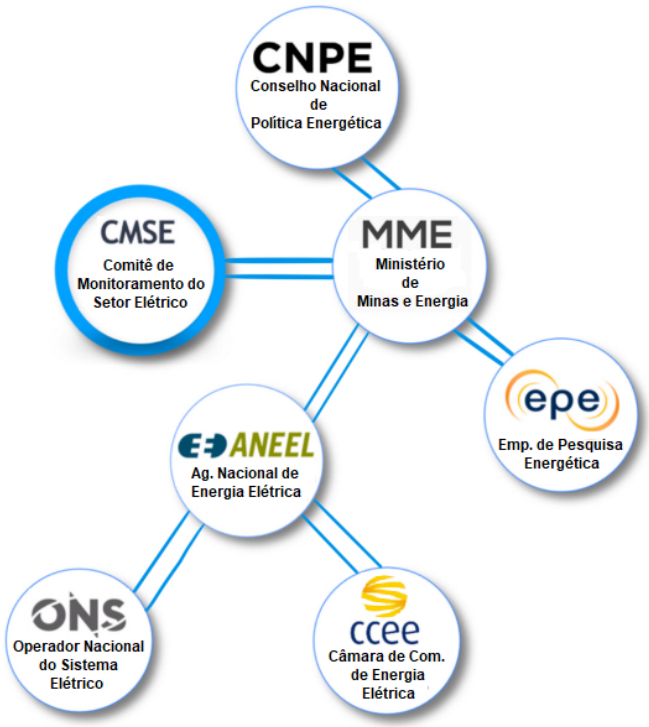

Figura 2.1: Organograma do Setor Elétrico Brasileiro
Fonte: Adaptada de [30].

O Conselho Nacional de Política Energética foi criado pela Lei No. 9.478/97, a qual definiu sua vinculação à Presidência da República, sendo sua presidência exercida pelo Ministro de Estado de Minas e Energia. A sua maior responsabilidade é auxiliar no desenvolvimento da política nacional de energia [31].

Já a tarefa de realizar o monitoramento contínuo do SEB é do Comitê de Monitoramento do Setor Elétrico - CMSE, que também é presidido pelo Ministro de Estado de Minas e Energia. Dentre suas funções principais, destacam-se: continuidade e segurança do suprimento de energia elétrica e a constante avaliação dos fatores que afetam o bom funcionamento do sistema elétrico nacional, definindo as sugestões de soluções [32].

Nesse novo contexto surgiu a Agência Nacional de Energia Elétrica - ANEEL que foi criada pela Lei

No. 9.427/96. Trata-se de uma autarquia de regime especial com vinculação direta ao MME, atuando na regulação e na fiscalização da geração, transmissão, distribuição e comercialização de energia elétrica no Brasil [33].

No ano de 2004, o governo tomou a decisão de criar a Empresa de Pesquisa Energética – EPE por meio da Lei No. 10.847/04, que também possui uma vinculação direta com o MME. Sua responsabilidade é basicamente elaborar o planejamento do setor energético brasileiro [34].

A Câmara de Comercialização de Energia Elétrica – CCEE foi criada no mesmo ano pela Lei No. 10.848/2004 e regulamentada pelo decreto No. 5.177/04. A CCEE é uma pessoa jurídica de direito privado sem fins lucrativos, regulada e fiscalizada pela ANEEL, atuando na contratação de energia no ambiente regulado e no ambiente de contratação livre, nos quais atuam os agentes de geração, de transmissão e de distribuição de energia elétrica [30].

O Brasil se destaca no setor elétrico mundial pela grande disponibilidade de recursos naturais, situação que oferece ao país um cenário bem diferente se comparado ao resto do mundo. Essa característica permite que o sistema brasileiro de produção e transmissão de energia elétrica se apresente como hidro-termo-solar-eólico de grande porte, com predominância de usinas hidrelétricas e com múltiplos proprietários [35].

O aproveitamento desses recursos para geração de energia elétrica ocorre através de diversos tipos de energias renováveis, no entanto, o país depende principalmente da energia hidráulica. O Brasil possui a matriz elétrica mais renovável do mundo [36].

A Figura 2.2 mostra como está distribuída a matriz de energia elétrica no Brasil.

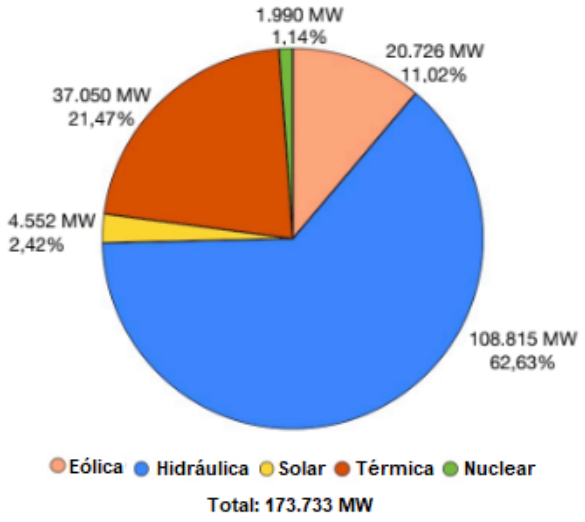

Figura 2.2: Matriz de Energia Elétrica no Brasil
Fonte: Adaptada de [37].

Esse grande potencial de fontes renováveis oferece à matriz energética brasileira um reconhecimento internacional como sendo uma das mais limpas do mundo, onde a usina hidráulica tem um destaque especial no processo de produção de eletricidade [38].

Nos últimos anos verificou-se um crescimento muito grande de novas plantas de geração eólica, em especial nas regiões Nordeste e Sul. Isso levou essa modalidade de geração de energia a um grau de importância muito elevado na matriz de geração, visando o atendimento ao mercado consumidor nacional [37].

O SEB se apoia na estrutura do Sistema Interligado Nacional - SIN que pode ser caracterizado como uma rede elétrica única de abrangência nacional, contando com uma governança técnica centralizada no ONS e regulação/fiscalização da ANEEL, e ainda com a estrutura operacional dos diversos agentes do setor elétrico e as características técnicas das subestações e das usinas de geração [39].

O Sistema Interligado Nacional é constituído por quatro subsistemas: Sul, Sudeste/Centro-Oeste, Nordeste e a maioria da região Norte [37].

A interconexão entre os subsistemas permite a obtenção de ganhos sinérgicos, explorando a diversidade entre os regimes hidrológicos das bacias, permitindo o atendimento ao mercado consumidor com segurança e economicidade [37].

A Figura 2.3 mostra a evolução da capacidade instalada no Sistema Interligado Nacional de agosto de 2022 a dezembro de 2026.

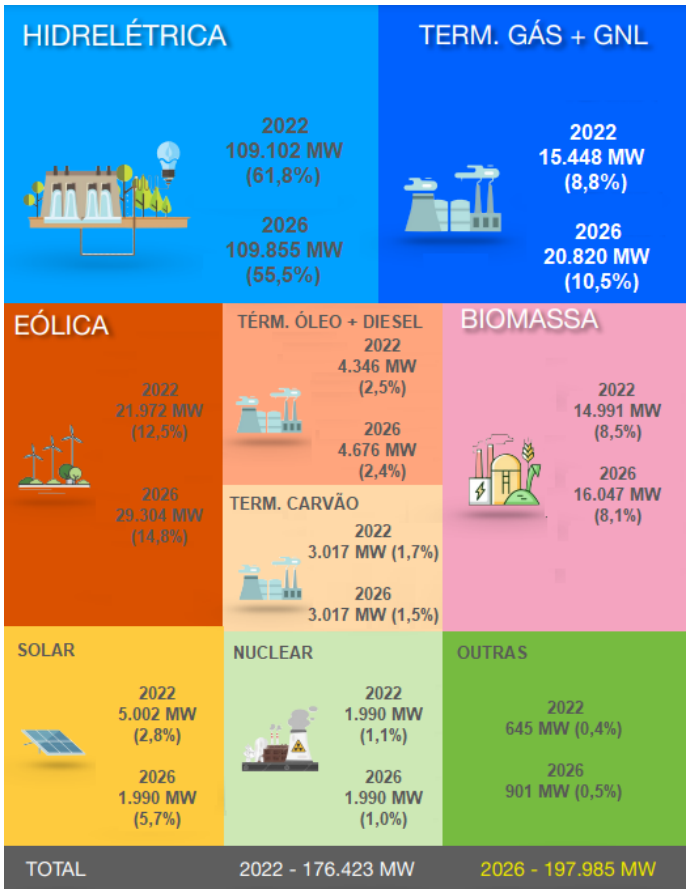

Figura 2.3: Evolução da Capacidade Instalada no SIN de ago/2022 a dez/2026
Fonte: Adaptado de [37].

O complexo Sistema de Transmissão que está inserido no SIN integra essas diferentes fontes de produção de energia e possibilita o suprimento do mercado consumidor por meio do fluxo de energia programado

e despachado pelo ONS [37].

A Figura 2.4 apresenta a extensão da rede básica de transmissão que compõe o SIN.

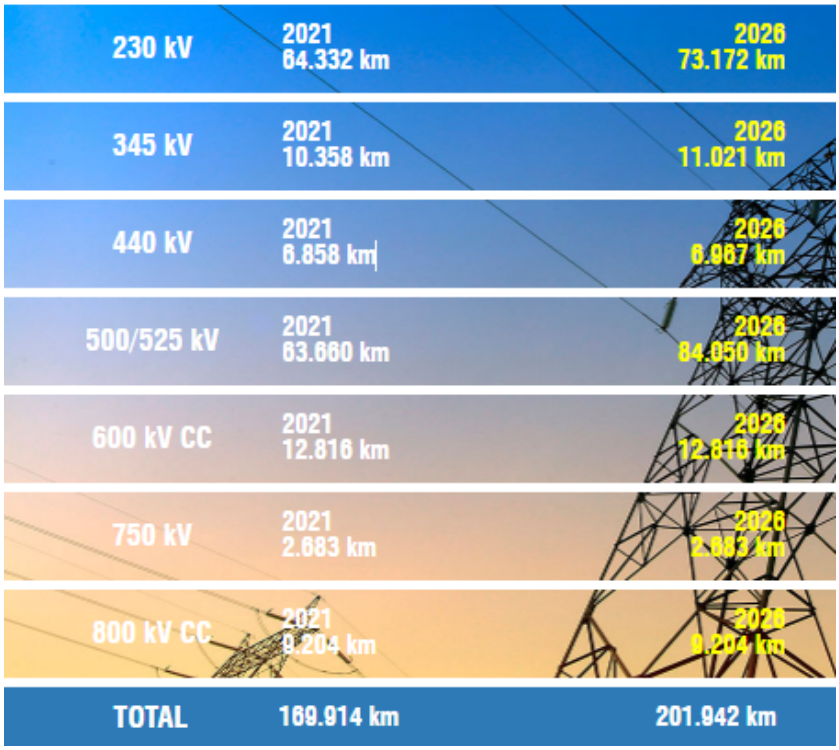

Figura 2.4: Extensão da Rede Básica de Transmissão que compõe o SIN
Fonte: [37].

No entanto, a oferta de energia não está necessariamente próxima do local de maior demanda, representando uma condição desafiadora para se garantir o abastecimento dos pontos consumidores. A transmissão dessa energia elétrica passa a inserir, portanto, fatores inerentemente afetos à segurança energética do Brasil [40].

Esse universo integrado expõe o SIN a um importante cenário de ataques cibernéticos, levando o setor a inserir em seus planos estratégicos programas extensos de medidas protetivas necessárias e adequadas a cada segmento e em todos os seus níveis [39].

Esse aspecto levou o ONS a se preocupar formalmente com o tema a partir de julho de 2021, ocasião em que publicou a RO-CB.BR.01 R00 que passou a regulamentar as ações dos agentes do setor [15].

2.3 O MINISTÉRIO DE MINAS E ENERGIA - MME

O MME é um órgão da Administração Federal cujo objetivo é criar e garantir a prática de políticas públicas relacionadas ao uso sustentável de recursos energéticos e minerais do país [41].

Esse ministério trabalha para que o país se desenvolva socioeconomicamente por meio de políticas que tornam o uso de diferentes tipos de geração de energia mais eficientes [42].

Além disso, o MME atua no Mercado Livre de Energia, regulando a compra e venda de energia de fontes independentes [42].

O trabalho do MME está associado ao do Conselho Nacional de Política Energética - CNPE, um órgão interministerial que cuida da distribuição da energia por todo o país, inclusive, dos lugares mais remotos [42].

O MME, em função do crescimento da transformação digital associada ao serviço de energia elétrica, prestado pelas empresas e entidades públicas, para propiciar à população maior acesso aos serviços prestados, evidenciou a necessidade de se instituir medidas para garantir maior segurança no atendimento dos serviços de energia elétrica [43].

2.4 O CNPE E A SEGURANÇA CIBERNÉTICA NO SETOR ELÉTRICO

Os ataques virtuais já vinham acontecendo com maior frequência em razão da digitalização do serviço de energia elétrica, mas se intensificaram durante a pandemia, quando instituições e empresas adotaram o trabalho remoto. Foram vítimas de ataques cibernéticos, por exemplo, distribuidoras como Light, Energisa, Copel, EPE e a Eletronuclear [44].

Em resposta, foram implantadas ações por órgãos e empresas para prevenir e minimizar efeitos, alinhadas com ações do Comitê de Governança Digital do Ministério de Minas e Energia [43].

O CNPE orientou a criação de um Grupo de Trabalho, visando estabelecer as diretrizes para harmonizar as atividades de segurança cibernética do setor de energia elétrica, utilizando as experiências vivenciadas pelas entidades e empresas, e abordando aspectos relativos à prevenção, tratamento, resposta a incidentes e resiliência sistêmica [31].

Formado por representantes do Gabinete de Segurança Institucional - GSI, do ONS, da ANEEL, da EPE e da CCEE, o grupo foi coordenado pelo MME e contou com apoio de especialistas representantes de órgãos e entidades da sociedade civil [45].

Como resultado, foi aprovado e publicado no Diário Oficial da União - DOU em 20 de outubro de 2021, a Resolução N. 24 do CNPE que definiu as diretrizes sobre segurança cibernética para o setor elétrico, conforme estabelecido na resolução CNPE N. 01, de 10 de fevereiro de 2021, considerando os aspectos de prevenção, tratamento, resposta e resiliência sistêmica [46], definindo as seguintes diretrizes:

- Orientar empresas e instituições do setor elétrico a implantarem ações de gerenciamento de riscos e ameaças cibernéticas com objetivo de garantir a continuidade de negócio, a proteção dos dados e a segurança operacional;
- Estabelecer requisitos e controles mínimos de segurança cibernética para o setor visando reduzir riscos e vulnerabilidades a incidentes cibernéticos;
- Estabelecer políticas que promovam a utilização de recursos tecnológicos e melhorias contínuas que mitiguem riscos de incidentes cibernéticos;

- Estabelecer estrutura de coordenação setorial para atuação em incidentes cibernéticos no setor elétrico, consoante o Decreto no 10.748, de 16 de julho de 2021;
- Promover ambiente de compartilhamento de informações e de apoio ao setor, estabelecendo relacionamentos e ações que contribuam para elevar o nível de maturidade da segurança cibernética das organizações;
- Estabelecer procedimento para identificação continuada de serviços e instalações estratégicas, consideradas estruturas críticas, que requeiram atenção em termos de segurança cibernética, consoante os Decretos no 10.748, de 2021, e no 9.573, de 22 de novembro de 2018, e legislações correlatas; e,
- Orientar os agentes do setor elétrico a implantarem programas de capacitação em segurança cibernética e de conscientização sobre a importância da segurança da informação.

De fato, o Governo Federal do Brasil tem se mobilizado no sentido de disponibilizar uma legislação que possa oferecer os meios necessários para a constituição de um arcabouço legal bem estruturado, que incentive os agentes de um setor crítico como o setor elétrico a se mobilizarem, visando à implantação de ações necessárias para o incremento da segurança cibernética nesse segmento da economia [15].

2.5 O PAPEL DO ONS

O ONS é o órgão responsável pela coordenação e controle da operação das instalações de geração e transmissão de energia elétrica no SIN e pelo planejamento da operação dos sistemas isolados do país, sob a fiscalização e regulação da ANEEL [47].

Instituído como uma pessoa jurídica de direito privado, sob a forma de associação civil sem fins lucrativos, o ONS foi criado em 26 de agosto de 1998, pela Lei nº 9.648, com as alterações introduzidas pela Lei nº 10.848/2004 e regulamentado pelo Decreto nº 5.081/2004 [47].

Para o exercício de suas atribuições legais e o cumprimento de sua missão institucional, o ONS desenvolve uma série de estudos e ações exercidas sobre o sistema e seus agentes proprietários para gerenciar as diferentes fontes de energia e a rede de transmissão, para garantir a segurança do suprimento contínuo em todo o país, com os objetivos de [47]:

- Promover a otimização da operação do sistema eletro energético, visando o menor custo para o sistema, observando-se os padrões técnicos e os critérios de confiabilidade estabelecidos nos Procedimentos de Rede aprovados pela ANEEL;
- Garantir que todos os agentes do setor elétrico tenham acesso à rede de transmissão de forma não discriminatória; e,
- Contribuir, segundo a natureza de suas atividades, para que a expansão do SIN se faça ao menor custo e vise às melhores condições operacionais futuras.

O ONS é composto por membros associados e membros participantes, que constituem as empresas de geração, transmissão, distribuição, consumidores livres, importadores e exportadores de energia, os quais contribuem para a sua operação empresarial. Também participam do ONS o MME e representantes dos Conselhos de Consumidores [47].

Sua estrutura organizacional estratégica de alto nível é definida pela Figura 2.5.

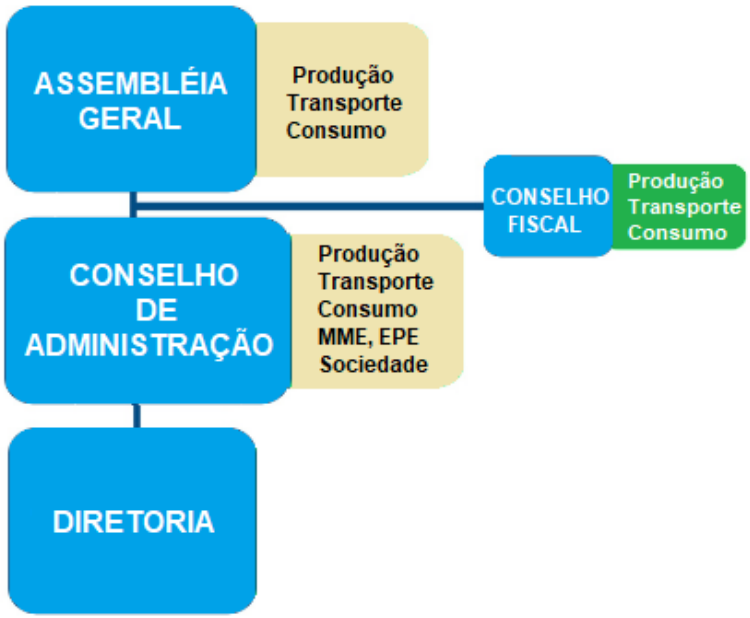

Figura 2.5: Estrutura Organizacional Estratégica de Alto Nível do ONS
Fonte: [48].

A Figura 2.6 mostra a estrutura organizacional do ONS e os órgãos que a compõem:

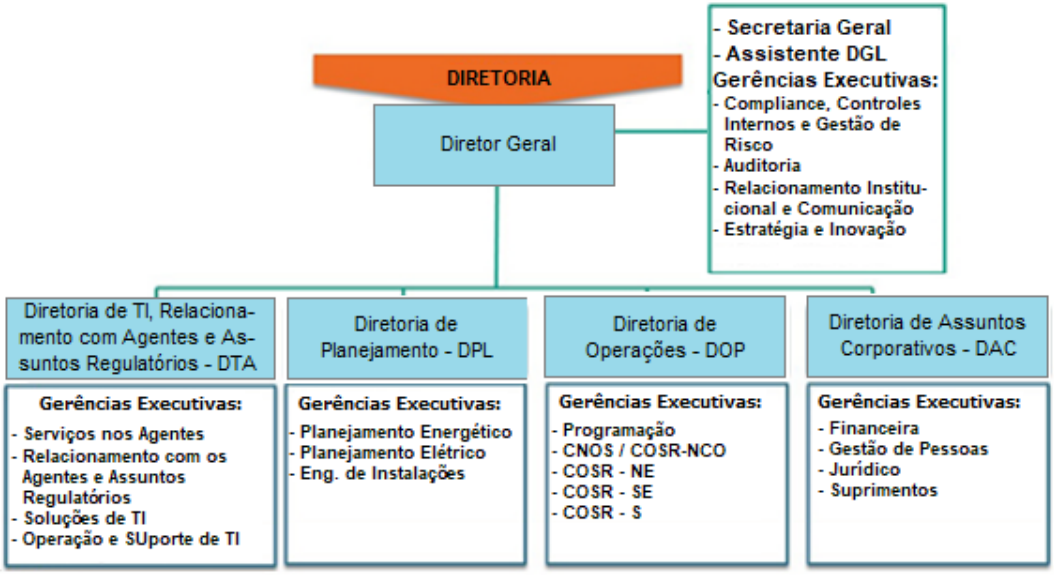

Figura 2.6: Estrutura Organizacional do ONS
Fonte: [49].

2.6 A GESTÃO DA SEGURANÇA CIBERNÉTICA NO SETOR ELÉTRICO BRASILEIRO

O ONS, publicou no Manual de Procedimentos Operacionais – MPO, Módulo 5 - Submódulo 5.13, a Rotina Operacional RO-CB.BR.01 R00, a qual tem por objetivo estabelecer os controles mínimos de segurança cibernética a serem implementados pelos agentes do setor elétrico nacional e pelo próprio ONS no Ambiente Regulado Cibernético [13].

Esta foi a primeira ação efetiva do ONS no sentido de disponibilizar uma rotina operacional tratando do assunto de Segurança Cibernética de forma prática, obrigando a sua completa implantação e operacionalização até o mês de setembro de 2023 [15].

Por meio dessa RO, o ONS definiu o ARCiber - Ambiente Regulado Cibernético como sendo o conjunto de redes e equipamentos considerados no escopo dos Centros de Operação dos Agentes, pelos equipamentos que participam da infraestrutura de envio ou recebimento de dados e voz para ambientes operativos do ONS ou para centros de operação de outros agentes e, também, pelo ambiente operativo do próprio ONS [13].

Seguindo essa direção, a ANEEL publicou em 12 de dezembro de 2021 a Resolução Normativa nº 964, que entrou em vigor no dia 1º de julho de 2022 [14].

Essa Resolução, detalhada na seção 2.6.2, apresenta um campo de visão amplificado para o ARCiber.

Ela estabelece as diretrizes e o conteúdo mínimo das políticas de segurança cibernética dos agentes do setor de energia elétrica no Brasil e os parâmetros para a implantação de processos e procedimentos definidos nesse contexto, base para os programas de auditoria em segurança cibernética do Setor Elétrico Brasileiro [14].

Esse cenário define, atualmente, o domínio da gestão da segurança cibernética no setor elétrico brasileiro, abrangendo a Regulação e Fiscalização no âmbito dos processos de gestão de Riscos Cibernéticos, aplicação de *frameworks* e políticas de segurança cibernética no Setor Elétrico Brasileiro [15].

2.6.1 A Rotina Operacional do ONS e o Ambiente Regulado Cibernético - ARCiber

As orientações contidas na RO passaram a nortear as ações que deverão ser necessariamente desenvolvidas pelos agentes do Setor Elétrico Brasileiro.

O Ambiente Regulado Cibernético - ARCiber apresenta sete dimensões de controles de segurança cibernética: Arquitetura Tecnológica; Governança de Segurança da Informação; Inventários de Ativos; Gestão de Vulnerabilidades; Gestão de Acessos; Monitoramento e Resposta a Incidentes; e trata ainda de possíveis Exceções [13].

Os Agentes do Setor Elétrico Brasileiro devem direcionar seus esforços de controle e gestão, visando o cumprimento da RO em vinte e sete meses, após a publicação da norma, ou seja, em setembro de 2023, como já mencionado anteriormente [15].

Com essa medida, o ONS pretende que os agentes do Setor Elétrico Brasileiro passem a implantar

um processo formal de gestão de riscos cibernéticos para identificar e tratar as possíveis vulnerabilidades, definir um plano de resposta a incidentes e passem a se utilizar de um plano de segurança da informação associado aos ativos, softwares e hardwares conectados ao ARCiber [15].

Importante destacar que após essa data o ONS poderá aplicar sanções aos agentes que não se adequarem às diretrizes definidas pela RO, conforme previsto nos Procedimentos de Rede, Submódulo 19.1 - Identificação, tratamento e penalidades para as não conformidades, com vigência a partir de 05/08/2009 [50].

O Submódulo 19.1 pretende estabelecer o processo de identificação, tratamento e aplicação de penalidades pelo ONS, resultante do não atendimento dos Procedimentos de Rede pelos agentes de operação, mas também de eventuais não conformidades praticadas pelo próprio ONS, o qual também se obriga a atender a RO.

As não conformidades tipificadas por este submódulo sujeitarão os agentes de operação às penalidades de advertência e multa.

Essas multas são classificadas em 02 (dois) grupos:

- Grupo I: corresponderá a 5% (cinco por cento) do valor anual da contribuição associativa paga pelo agente de operação ao ONS, relativa ao exercício em que ocorreu a não conformidade;
- Grupo II: corresponderá a 10% (dez por cento) do valor anual da contribuição associativa paga pelo agente de operação ao ONS, relativa ao exercício em que ocorreu a não conformidade.

Nesse sentido, a não conformidade dos agentes do SEB à RO e, consequentemente, ao ARCiber, os sujeitará a advertências e multas indesejadas.

Essa nova situação remete os agentes do SEB à necessidade de se adaptarem para atender as diretrizes definidas pelo ARCiber no prazo estipulado.

Com isso, as determinações do ONS devem inserir no processo operacional rotinas e melhores práticas de gestão de riscos cibernéticos que sejam cíclicas e com monitoramento contínuo, atendendo aos controles previstos e identificados nos Grupos de Segurança da RO [13].

A Tabela 2.1 mostra as dimensões do ARCiber e seus níveis de proteção.

Tabela 2.1: Processo de Segurança Cibernética para o ARCiber (RO-CB.BR.01)

Grupo de Segurança ARCiber	Macro Controles ARCiber
1- Arquitetura tecnológica para o ambiente do ARCiber	Redes segregadas ARCiber isolado da Internet Existência de soluções anti-malware implantadas e atualizadas no ARCiber
2- Governança de segurança da informação	Existência de processo formal de gestão da segurança cibernética no ARCiber
3- Inventários de ativos	Realização de inventário físico periódico de ativos de hardware, software e dados conectados ao ARCiber Armazenamento seguro do inventário físico
4- Gestão de vulnerabilidades	Gestão da implantação de pacotes de correção de segurança Conexão de novos ativos ao ARCiber
5- Gestão de acessos	Política de gestão de identidade e acesso
6- Monitoramento e resposta a incidentes	Política de monitoramento Plano de resposta a incidentes
7- Exceções	Tratamento de exceções

Fonte: [15]

2.6.2 A Resolução Normativa ANEEL n.º 964, de 14 de dezembro de 2021

A Resolução Normativa n.º 964, de 14 de dezembro de 2021, da ANEEL, que entrou em vigor no dia 1º de julho de 2022, estabelece as diretrizes e o conteúdo mínimo das políticas de segurança cibernética dos agentes do setor de energia elétrica, constituído pelos Concessionários, Permissionários, Autorizados de Serviços ou Instalação e Entidades responsáveis pela Operação do Sistema, Comercialização de Energia e Gestão de Recursos Setoriais [14].

Dentre as suas Diretrizes Gerais, a Resolução da ANEEL estipulou que os agentes do setor elétrico devem adotar normas, padrões e referências de boas práticas em segurança cibernética, não definindo, porém, um *framework* padrão. No entanto, a ANEEL alerta que a segurança das instalações e a continuidade na prestação do serviço é de responsabilidade dos agentes do setor elétrico, cabendo a eles a adoção e a execução da política de segurança cibernética e demais condutas e procedimentos exigidos pela regulação [14].

Essa Resolução vem após a publicação da RO-CB.BR.01 R00, em 9 de julho de 2021 [15].

No entanto, diferentemente da RO publicada pelo ONS, a Resolução da ANEEL se atém às políticas de Segurança Cibernética do Setor Elétrico, não se preocupando diretamente pelos controles que deverão compor as ações efetivas de gestão e mitigação dos riscos cibernéticos a que está submetido. Essa tarefa foi atribuída ao ARCiber, definido pelo ONS [15].

A Resolução estabelece algumas medidas que devem ser implantadas pelos agentes, detalhadas a se-

guir [14]:

- Aplicar anualmente pelo menos um modelo de maturidade em segurança cibernética na companhia;
- Aplicar medidas técnicas que busquem garantir a segurança das informações críticas, incluindo as de rastreabilidade das informações;
- Registrar, analisar a causa e o controle dos efeitos de incidentes de maior impacto, abrangendo informações recebidas de empresas prestadores de serviços a terceiros;
- Estabelecer mecanismos para prevenir, mitigar e recuperar incidentes cibernéticos em sua rede de informação ou na rede das instalações, bem como para impedir que os incidentes afetem a operação;
- Procedimentos para prevenção, tratamento e resposta a incidentes cibernéticos; e,
- Definir um programa de treinamento e conscientização em segurança cibernética no setor elétrico (programas de capacitação e avaliação, medidas de conscientização e educação, evidências de comprometimento da alta administração e simulação de cenários e ameaças).

Como se pode perceber, esta Resolução enseja ações no sentido de se estabelecer ou revisar a Política de Segurança da Informação, Classificar as Informações, definir um Plano de Resposta a Incidentes, um Plano de Recuperação de Desastres e, por fim, um Plano de Continuidade de Negócios [15].

A Resolução da ANEEL, diferentemente da RO publicada pelo ONS, não entra no escopo das salvaguardas constituídas pelos controles específicos de um *framework* de Gestão de Riscos Cibernéticos, complementando, dessa forma, a proposta da RO [15].

2.7 O PANORAMA DOS ATAQUES CIBERNÉTICOS E DESAFIOS DO SETOR ELÉTRICO MUNDIAL

A política mundial estabelece um novo senso de urgência em relação à nova ordem mundial e, por consequência, verifica-se a necessidade de se discutir o que isso significa para a segurança cibernética e o domínio do ciberespaço.

Devido a um número crescente de ataques cibernéticos globais, a cibersegurança tornou-se uma parte crucial da segurança nacional de vários países [51].

Em particular, o Digital Pearl Harbor, ou seja, evento que estatisticamente é improvável de ocorrer, pode realmente ocorrer, tornando-se uma ameaça real e agressiva à segurança.

Esse evento passou a ser considerado como uma questão global que pode inserir grande instabilidade na dinâmica da segurança internacional [51].

A partir dos ataques cibernéticos que tiveram por objetivo atingir o Sistema Político Americano, o Ministério das Relações Exteriores da República Tcheca, o Governo da Croácia e ainda os ataques de 2017 aos

Sistemas da Rede Cibernética do Governo Ucraniano, dentre outros, se passou a ter uma grande preocupação inserida nas agendas internacionais que envolvem diretamente a estabilidade global, a conectividade e o potencial de diminuição de limites globais [52].

A preocupação com a estabilidade global levanta, portanto, a questão de quem controla o ciberespaço e quem é responsável quando as coisas dão erradas [52].

Com aumento da quantidade e da severidade dos ataques cibernéticos, muitos países e organizações internacionais passaram a definir e implantar medidas de segurança cibernética e respostas aos riscos cibernéticos a que passaram a estar submetidos. Ações de cooperação entre essas organizações internacionais passaram a fazer parte das agendas e a se materializarem [51].

A Tabela 2.2 apresentada a seguir mostra uma série de ações de cooperação e ações conjuntas entre os organismos internacionais em resposta aos constantes ataques cibernéticos.

Tabela 2.2: Respostas Recentes dos Organismos Internacionais aos Ataques Cibernéticos

Entidade	**Medidas adotadas**
UN	Adoção de recomendações para a segurança cibernética, apresentadas por especialistas governamentais da ONU (UN-GGE) em 2013.
NATO	Definição de que os ataques cibernéticos se tornaram uma ameças para seus aliados segundo o Lisbon Summit Declaration em 2010.
	Definição de que os ataques cibernéticos em um ou mais membros deveriam ser considerados um ataque a todos os aliados, segundo o Wales Summit Declaration in 2014, e baseado nas provisões para defesa coletiva no Artigo N. 5 da NATO.
EU	Definição de diretiva de rede e segurança da informação de forma a ajudar na implantação dos sistemas de segurança cibernética de seus membros, a partir do Cybersecurity Strategy of the European Union (2013).
EU & NATO	Discussão do potencial de cooperação em resposta à guerra híbrida da Russia, a qual inclui ataques cibernéticos.
U.S.	Desde 2015 que o State of the Union patrocinado pelo presidente Barack Obama definiu que a segurança cibernética é o item de maior importância na agenda, elevando para o nível federal a segurança cibernética nacional.
	Ordem Executiva 13687 definiu sanções à NK em resposta aos ataques cibernéticos atribuídos à NK.
	Ordem Executiva 13691 encorajando e promovendo a segurança cibernética, compartilhando informações sobre ameaças dentro do setor privado e entre o setor privado e governamental.
	Ordem Executiva 13694 definindo o ataque cibernético como uma emergencia nacional, propondo punições severas para hackers e seus cúmplices.
U.K.	Tem fortalecido a segurança cibernética governamental e medidas de contenção contra os ataques cibernéticos de acordo com o UK Cyber Security Strategy (2011).

Fonte: Traduzido de [51]

2.7.1 Os Ataques de Grande Relevância Mundial em Instalações de Infraestruturas Críticas

Os sistemas de controle industrial, em especial os Sistemas SCADA, são utilizados para a operação de infraestruturas críticas e, por esse motivo, são alvos preferenciais dos hackers do mal, representando o cerne das ameaças, das buscas de vulnerabilidades e dos incidentes cibernéticos mais significativos já registrados até hoje [53].

Os ataques procuram se manifestar de forma diferente, podendo ser de forma direcionada, campanhas de cyber-intrusão, malware e grupos de ameaças cibernéticas.

A Tabela 2.3, apesar de não possuir grande abrangência, apresenta em uma linha cronológica o detalhamento das campanhas, ameaças e incidentes cibernéticos mais significativos já registrados em infraestruturas críticas [53].

Tabela 2.3: Detalhamento das Campanhas, Ameaças e Incidentes Cibernéticos mais Significativos em Infraestruturas Críticas em Ordem Cronológica

Ano	Tipo	Nome	Descrição
1903	Attack	Marconi Wireless Hack	A apresentação do telégrafo sem fio da Marconi foi invadida com código Morse.
2000	Attack	Maroochy Water	Um ataque cibernético causou a liberação de mais de 265.000 galões de esgoto não tratado.
2008	Attack	Turkey Pipeline Explosion (not quite cyber)	Os atacantes usaram o software vulnerável de uma câmera de segurança para entrar na rede de controle de uma tubulação.
2010	Malware	Stuxnet	A primeira arma digital publicamente conhecida do mundo.
2010	Malware	Night Dragon	Os atacantes usaram programas maliciosos sofisticados para atingir empresas globais de petróleo, energia e petroquímica.
2011	Malware	Duqu/ Flame/Gauss	Malwares avançados e complexos usados para atingir organizações específicas, incluindo os fabricantes de ICS.
2012	Campaign	Gas Pipeline Cyber Intrusion Campaign	ICS-CERT identificou uma série ativa de cyber-intrusões visando o setor de gasodutos de gás natural.
2012	Malware	Shamoon	Malware usado para atingir grandes empresas de energia no Oriente Médio, incluindo a Saudi Aramco e a RasGas.

Tabela 2.3: Detalhamento das Campanhas, Ameaças e Incidentes Cibernéticos mais Significativos em Infraestruturas Críticas em Ordem Cronológica

Ano	Tipo	Nome	Descrição
2013	Attack	Target Stores	Os hackers inicialmente ganharam acesso aos sistemas financeiros sensíveis da Target através de um terceiro que manteve seus ICSs HVAC, custando à Target $309M.
2013	Attack	New York Dam	O Departamento de Justiça dos Estados Unidos afirma que o Irã conduziu um ataque cibernético na represa Bowman em Rye Brook, NY.
2013	Malware	Havex	Uma campanha malware com foco no ICS.
2014	Attack	German Steel Mill	Uma siderúrgica na Alemanha sofreu um ataque cibernético que resultou em danos maciços ao sistema.
2014	Malware	Black Energy	Malware que visava as interfaces homem-máquina (IHMs) nas ICSs.
2014	Campaign	Dragony/Energetic Bear No. 1	Campanha de espionagem cibernética em andamento, visando principalmente o setor energético.
2015	Attack	Ukraine Power Grid Attack No. 1	O primeiro ataque cibernético de sucesso conhecido na rede elétrica de um país.
2016	Attack	"Kemuri"water company	Os atacantes ganharam acesso a centenas de circuitos lógicos dos Controladores Lógicos Programáveis - CLPs usados para manipular aplicações de controle, e alteraram os produtos químicos de tratamento de água.
2016	Malware	Return of Shamoon	Milhares de computadores na agência de aviação civil da Arábia Saudita e outras organizações do Estado do Golfo limparam em um segundo ataque de malware Shamoon.
2016	Attack	Ukraine Power Grid Attack No. 2	Ataques cibernéticos provocaram o acionamento de disjuntores em 30 subestações, interrompendo o fornecimento de eletricidade para 225.000 clientes em um segundo ataque.
2017	Malware	CRASHOVERRIDE	O malware usado para causar a queda de energia elétrica na Ucrânia foi finalmente identificado.
2017	Group	APT33	Um grupo de espionagem cibernética voltado para os setores de aviação e energia.
2017	Attack	NotPetya	Malwares que visavam a Ucrânia, fazendo-se passar por resgates, mas sem forma de pagar um resgate para descriptografar arquivos alterados.

Tabela 2.3: Detalhamento das Campanhas, Ameaças e Incidentes Cibernéticos mais Significativos em Infraestruturas Críticas em Ordem Cronológica

Ano	Tipo	Nome	Descrição
2017	Campaign	Dragony/Energetic Bear No. 2	Um sofisticado grupo de ataque tem como alvo o setor energético da Symantec R.
2017	Malware	TRITON/Trisis/ HatMan	Sistemas de segurança industrial no Oriente Médio alvo de malware sofisticado.

Fonte: Traduzido de [53]

A seguir serão apresentados, com mais detalhes, alguns dos casos citados na Tabela 2.3 que afetaram de forma significativa e direta o SEP mundial.

2.7.2 O Caso Stuxnet

O ataque Stuxnet, realizado em uma infraestrutura essencial de instalações nucleares iranianas para produção de energia elétrica, foi definido como a primeira arma cibernética já criada a partir de um código de alta complexidade e capacidade de destruição não registrada anteriormente [54].

O worm de computador Stuxnet, nomeação que recebeu após uma combinação dos títulos de arquivos que apareciam constantemente no código "stub" e "MrxNet.sys", é um código malicioso de computador, programado para atacar o Sistema SCADA da empresa Siemens [54].

Em 2010, o Stuxnet já existia e estava entre os malwares mais sofisticados conhecidos na época. Identificado publicamente pela primeira vez em junho de 2010, os pesquisadores acreditavam que o Stuxnet - cujas raízes foram posteriormente rastreadas em junho de 2009 - explorou apenas uma vulnerabilidade não corrigida no Windows e se espalhou por meio de Pen drives nas portas USB dos computadores [55].

O Irã foi o mais atingido pelo Stuxnet, de acordo com pesquisadores da Symantec, que disseram na ocasião que quase 60% de todos os PCs infectados estavam localizados naquele país [55].

O Stuxnet provoca a infecção do Controlador Lógico Programável - CLP, responsável pela automação dos processos eletromecânicos usados para controlar as máquinas e as rotinas industriais. Esse worm de computador foi projetado para explorar falhas dentro do sistema operacional Windows, conhecidas como Zero-Day [54].

Na realidade, esse malware explorou um total de quatro vulnerabilidades não corrigidas da Microsoft, duas que eram vulnerabilidades de autorreplicação e duas que proporcionavam uma escalada de vulnerabilidades de privilégios que eram anteriormente desconhecidas [53].

O Stuxnet também era furtivo, enquanto podia esconder os seus binários através de um rootkit do Windows. Assim, o Stuxnet se tornava uma arma de precisão que procurava um software exato para ser instalado e um equipamento específico para ser ligado a um sistema. Se encontrar a configuração precisa que procura, modifica e sabota o código nos PLCs Siemens injetando diretamente neles o código lógico no Sistema SCADA [53].

Com efeito, uma vez que a usina nuclear de Natanz não possuía nenhuma conexão com a Internet,

sendo a porta de entrada normalmente utilizada pelos vírus para a infecção de computadores, verificou-se que o worm se espalhou por meio de um dispositivo de pen drive infectado, inserido nas máquinas Windows que operavam os Sistemas SCADA da usina, responsáveis pelo controle das centrífugas de enriquecimento de urânio do Irã [56].

Uma vez instaurado no computador, o Stuxnet segue um roteiro de fases que pode ser visualizado a seguir [56]:

- Inicialmente ele executa o código principal;
- Em seguida são geradas cópias que se propagam de forma automática;
- O serviço gerado pelo worm passa a se utilizar de uma certificação digital legítima, obtida por meio de informações internas coletadas previamente na instalação invadida, impedindo que fosse detectado pelo antivírus da instalação e, com isso, contatar um servidor de comando e controle que permitiu aos atacantes descarregar e executar código atualizado [53]; e,
- O rootkit oculta os códigos e processos maliciosos, visando se desviar dos mecanismos de detecção.

Essas características faziam com que os Sistemas SCADA, instalados nos computadores contaminados, não demonstrassem nenhuma alteração nos processos. Mesmo que as velocidades das centrífugas fossem mais altas, os relatórios apresentados aos técnicos não apresentavam nenhuma alteração anormal [56].

Os ataques, apesar de terem sido muito mais significativos em Natanz, também atingiram os CLP da Usina Nuclear de Bushehr, que estava perto de sua inauguração [57].

A Equipe de Emergência dos Sistemas de Controles Industriais Cibernéticos do DHS, já no ano de 2010 emitiu vários pareceres sobre como mitigar o malware Stuxnet, que também infectou sistemas nos Estados Unidos [58].

As vulnerabilidades encontradas nos computadores dessa usina permitiram que esse complexo código malicioso pudesse interferir diretamente no programa nuclear do Irã, provocando falhas de funcionamento nas centrífugas.

Essas falhas nas centrífugas de enriquecimento de urânio foram inseridas de forma discreta, característica sucinta que permitiu que houvesse uma demora na identificação do problema, parecendo aos técnicos que era apenas um problema de mau funcionamento e não a ação de um ataque cibernético [57].

Um dos primeiros impactos identificados a partir desse ataque, mesmo que não se possa ligá-lo diretamente à segurança internacional, está no fato de que o Stuxnet trouxe uma grande inovação tecnológica para o contexto da segurança cibernética de infraestruturas críticas, uma vez que mostrou na prática a possibilidade de malwares se utilizarem de diferentes recursos de programação para causar estragos ainda não imaginados, como danos físicos reais como os ocorridos em Natanz [59].

Um processo de gestão de riscos cibernéticos, baseado em Frameworks adequados às infraestruturas críticas, certamente poderiam ter evitado esse ataque. Controles associados ao inventário e controle de dispositivos de hardware e também associados ao gerenciamento e controle de acesso, poderiam ter previamente detectado e evitado a contaminação do sistema a partir da conexão de um hardware não autorizado ou estranho à rede interna.

Esse caso mostra que processos de gestão de riscos cibernéticos, quando negligenciados, podem afetar de forma inesperada a segurança cibernética de toda uma instalação, como se pôde verificar no caso da Usina Nuclear de Natanz.

Os casos que serão apresentados a seguir mostrarão a importância de se implantar e efetivamente se utilizar um processo de gestão de riscos cibernéticos bem estruturado nas empresas que atuam com infraestruturas críticas, caso do setor elétrico, podendo evitar, com isso, que os ataques cibernéticos atinjam seus objetivos [15].

2.7.3 O Ataque Havex

Nos anos seguintes, vários casos de ataques às infraestruturas críticas, em especial aquelas associadas ao setor de geração e transmissão de energia elétrica, também foram relatados. Um deles, e não menos importante, foi a campanha de ataque Havex (ou Oldrea) ocorrida em 2014 [8].

O Havex é considerado um malware destinado ao ataque de diferentes setores da indústria, particularmente ao setor de energia [60].

Sua ação foi iniciada por meio da utilização do software disponibilizado para download no site do fabricante do Sistema ICS/SCADA, permitindo que o usuário fosse infectado por um spyware quando fizesse a sua instalação, mostrando um aspecto de segurança muito preocupante do protocolo ICS [61].

O Havex pode também ser espalhado por meio de Spam e Ferramentas de Exploração, além do canal disponibilizado pelo Pacote de Instalação comprometido com o Trojan e fornecido pelo fabricante em seu site oficial citado anteriormente [60].

Com a análise de várias amostras foi possível descobrir que os atacantes se utilizam desses componentes/ferramentas de acesso remoto - RAT para em seguida iniciar o roubo de dados de máquinas utilizadas para o processamento do Sistema ICS/SCADA [62].

Isto significa que os atacantes não só estão interessados na rede da empresa alvo, mas também motivados a controlar os Sistemas ICS/SCADA dessas empresas [60].

O governo dos Estados Unidos da América identificou que o grupo de hackers que estava por trás do Havex era o RIS, especializados em ataques aos servidores responsáveis pelo comando e controle dos sistemas de controles industriais [53].

Este caso mostra, mais uma vez, que falhas associadas ao processo de segurança cibernética de infraestruturas críticas podem levar a situações complexas e muitas vezes catastróficas. A disponibilização de controles importantes de Proteção de e-mails e de Navegadores WEB do Framework CIS CSC, por exemplo, poderiam ter atuado preventivamente e evitado o sucesso desses ataques. Isso mostra que é a partir das falhas muitas vezes pequenas e simples do processo de gestão de riscos cibernéticos que os malwares podem se infiltrar na rede interna, causando grandes transtornos não apenas para as empresas, mas principalmente para a população, quando suas consequências ultrapassam as fronteiras do negócio.

2.7.4 Malware BlackEnergy

Em 2015, dois dias antes do Natal, um ataque cibernético de grandes proporções cortou a energia elétrica de aproximadamente 250 mil pessoas na Ucrânia. Esse foi o primeiro ataque cibernético de sucesso em uma infraestrutura do sistema elétrico de potência de um país [53].

A agência Reuters de notícias informou na ocasião que uma empresa de distribuição de energia elétrica, localizada no oeste da Ucrânia, havia sofrido um blacaute de grandes proporções, impactando uma larga região, incluindo a capital regional Ivano-Frankivsk [63].

O ataque foi responsável pelo desligamento de 30 subestações, deixando a população sem eletricidade por mais de seis horas. Identificou-se que os equipamentos controlados pelos Sistemas SCADA se tornaram inoperantes, obrigando o restabelecimento lento e manual de cada um deles [64].

O malware BlackEnergy foi o grande responsável pelo ataque, o qual se utilizou de vulnerabilidades existentes em macros de documentos no formato MS Excel. Esse malware foi inserido na rede da empresa por meio de phishing instalados em e-mails dos empregados [64].

Com essa ocorrência, houve um entendimento geral de que os ataques cibernéticos são realmente capazes de causarem problemas de grandes proporções nas redes dos sistemas elétricos de potência, servindo de alerta para que medidas fossem imediatamente estudadas e implantadas, visando o aumento da segurança dessas infraestruturas críticas dos países [53].

O ataque à rede de energia elétrica da Ucrânia foi um evento significante na história da segurança cibernética, não apenas pelo pioneirismo do sucesso do ataque nessa infraestrutura, mas também pelo fato de que os ataques foram realizados com a utilização de técnicas simples, pouco sofisticadas, atingindo seu objetivo de forma precisa [53].

Como no Havex, a disponibilidade de controles associados à Proteção de e-mails e de Navegadores WEB que hoje estão disponibilizados no Framework CIS CSC, por exemplo, poderiam ter atuado preventivamente e evitado o sucesso desses ataques

2.7.5 Malware Industroyer (Crashoverride)

Novamente na Ucrânia, o malware Industroyer foi empregado para um ataque cibernético a uma subestação de transmissão de Kiev, que resultou no grande corte de energia verificado no dia 17 de dezembro de 2016 [65] [66].

O Industroyer é tido como a quarta peça de software malicioso utilizada pelos hackers para ataques específicos a alvos de sistemas de controles industriais, sendo o Stuxnet, o BlackEnergy e o Havex os três primeiros. Esse malware, depois do Stuxnet, foi o segundo malware projetado para interromper processos industriais físicos [66], não servindo para espionagem.

Os módulos existentes no Industroyer são ativados para abrir disjuntores em unidades terminais remotas, forçando-os a um loop infinito, visando manter os disjuntores abertos. Mesmo que os operadores da rede intervenham no processo, eles são obrigados a mudar para o modo manual, interrompendo a carga, visando reiniciar o processo de fornecimento de energia [66].

O DHS americano, por meio de seu Sistema Nacional de Conscientização Cibernética (NCAS), emitiu um alerta de análise técnica do malware Industroyer em 12 de junho de 2017, notificando a infraestrutura crítica dos EUA sobre a séria ameaça que o malware representa [67].

As análises desse malware levaram as autoridades americanas do Sistema Nacional de Conscientização Cibernética (NCAS) a elevarem os seus níveis de alerta, uma vez que foi identificado que os criminosos passaram a se utilizar de uma estrutura avançada e reutilizável de malware para realizar os ataques às redes elétricas, demonstrando que eles estão dispostos a causar a interrupção do fornecimento de energia por meio de ataques cibernéticos, elevando significativamente a preocupação com a segurança desse setor vital para a vida dos cidadãos e para a economia dos países [67].

2.8 GESTÃO DE RISCOS CIBERNÉTICOS E A SEGURANÇA DAS INFRAESTRUTURAS CRÍTICAS DO SETOR ELÉTRICO

As redes de transmissão e distribuição de energia elétrica são sistemas de engenharia muito dispersos e de alta complexidade, com diferentes graus de conectividade, onde uma das principais questões a ser perseguida é o equilíbrio dinâmico do fornecimento e da demanda de eletricidade, o qual precisa ser mantido e garantido em tempo real [2].

No entanto, manter esse equilíbrio oferece um grau de dificuldade adicional à tarefa de operar o sistema elétrico com confiabilidade.

Além do aspecto citado acima, desastres naturais, condições climáticas severas e os ataques cibernéticos tornam as tarefas de operar o sistema elétrico com confiabilidade, ainda mais complexas e difíceis [2].

Essas redes, assim como os sistemas cibernéticos inseridos no meio físico, constituem uma combinação de componentes da rede física, que envolvem sensores, dispositivos de comunicação, bancos de dados e softwares, cujos eventos perturbadores em sistemas elétricos de potência podem ser organizados conforme descritos a seguir [2]:

- Eventos nos componentes da rede física, estrutura de grade e sensores;
- Eventos na infraestrutura cibernética, aplicações de software e comunicação de dados; e,
- Eventos correlacionados em componentes do sistema de energia com aspectos cibernéticos e físicos, como sistemas de controle e sistemas de estimativas de estado.

Nesse contexto, verifica-se que os ataques cibernéticos têm aumentado muito nos últimos anos em todo o mundo. À medida que as redes elétricas ficaram mais inteligentes, as habilidades de comunicação de seus componentes e os níveis de sofisticação da tecnologia da informação aumentaram e, por consequência, aumentaram também o número de pontos de acesso à intrusão, cujas invasões cibernéticas têm por objetivo divulgar dados e medidas críticas indesejadas e causar uma interrupção de serviço ou uma negação de serviço (DoS) [2].

O que se pode perceber nesses tipos de invasões é que comandos maliciosos e a injeção de medidas

de variáveis importantes para os processos normalmente associados aos Sistemas SCADA podem levar a danos generalizados ao sistema elétrico associado que, no extremo, podem inclusive provocar um processo de reação em cadeia, com danos elevados para os sistemas elétricos interligados [2].

A partir do Guia de Segurança para os Sistemas ICS, publicado pelo NIST em 2015 [68] e do Programa de Segurança para os Sistemas de Controle [69], pode-se extrair as principais vulnerabilidades em sistemas de controle industriais de forma bem didática e prática.

A lista apresentada na Tabela 2.4 mostra os potenciais ataques cibernéticos a que estão submetidos os sistemas elétricos de potência e as redes inteligentes associadas, assim como as atividades necessárias para mitigá-los [69].

Tabela 2.4: Vulnerabilidades Cibernéticas em Sistemas Elétricos de Potência

Categoria	**Vulnerabilidade Comum**
Vulnerabilidade no domínio do software	Validação de dados de entrada inadequada
	Má qualidade do código
	Permissões e controle de acesso
	Problemas de criptografia
	Configuração inadequada do software
	Problemas de manutenção de software
Vulnerabilidade no domínio do acesso	Controle de permissões, acesso e privilégios
	Autenticação incorreta
	Configuração de segurança inadequada
	Problemas de política de acesso e procedimentos
	Gerenciamento de credenciais
Vulnerabilidade no domínio da rede	Configuração inadequada da rede
	Firewalls fracos
	Configuração inadequada do componente de rede
	Problemas de auditoria e monitoramento de rede

Fonte: [69]

A conexão entre componentes físicos e cibernéticos em sistemas de energia facilita a ocorrência de danos físicos aos componentes da rede causados por invasões cibernéticas [70].

O [69] recomenda que a análise de riscos e vulnerabilidades cibernéticas deve, portanto, começar pelos sistemas de controle, como sugerido em suas diretrizes de segurança de controle industrial. Uma série de estudos de pesquisa sobre interdependências cibernéticas e físicas em sistemas de controle já pode ser observada.

Falhas em cascata seguintes a ataques cibernéticos em sistemas de controle de infraestruturas críticas já foram analisadas. Estudos avaliaram os efeitos das falhas das infraestruturas de informação e elétricas, umas sobre as outras, utilizando, para tanto, modelos qualitativos que permitiram a descrição e a análise dos comportamentos dessas infraestruturas [26].

Esses modelos descrevem, em alto nível, cenários que podem ocorrer quando ocorrem falhas e a re-

lação entre os estados das duas infraestruturas. No entanto, os modelos utilizados foram diferenciados, ao considerar falhas acidentais na infraestrutura de informações e na contabilização de ataques maliciosos [26].

Pode-se perceber por meio desses estudos que independentemente dos motivos das ocorrências, a resiliência para esse tipo de infraestrutura crítica deve considerar ambas as causas de falhas e a análise de riscos cibernéticos deve compor o portfólio das atividades associadas à gestão do ambiente que envolve infraestruturas críticas.

Em [25] observa-se a apresentação de um método de classificação de vulnerabilidades do sistema de controle, visando estabelecer uma avaliação dos riscos cibernéticos em redes elétricas de potência.

Essa metodologia procura fazer uma associação entre as características mais importantes das infraestruturas cibernética e física, provendo subsídios para os processos de revisão e mitigação de riscos envolvendo a dependência entre a infraestrutura crítica de um sistema elétrico de potência e a infraestrutura de suporte associada.

Na Figura 2.7 é apresentada uma visualização da infraestrutura física cibernética de um Sistema Elétrico de Potência e um entendimento sucinto sobre o seu funcionamento integrado.

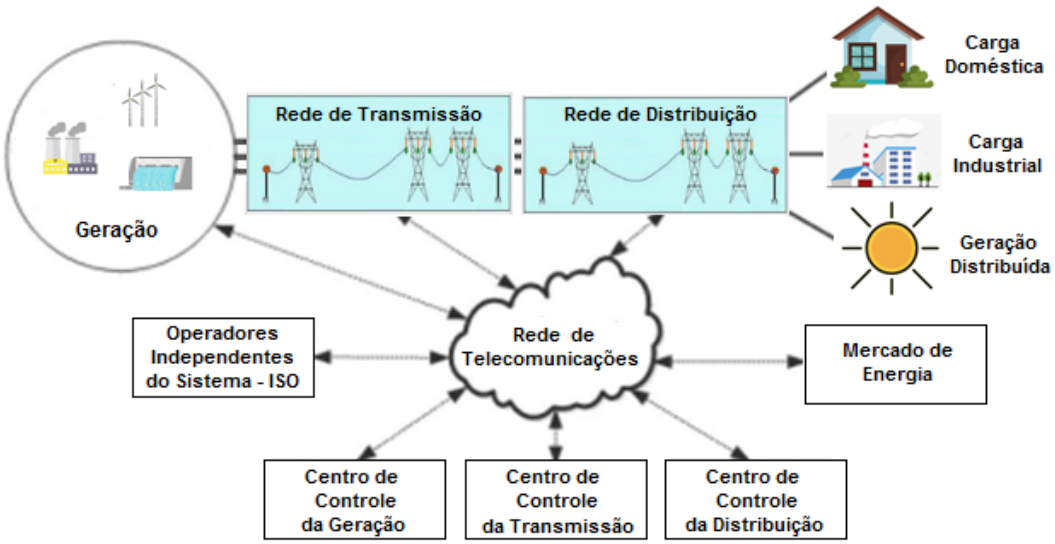

Figura 2.7: Infraestrutura Física Cibernética de um Sistema Elétrico de Potência
Fonte: Adaptado de [25].

Pode-se perceber que os sistemas cibernéticos, constituídos por dispositivos de campo eletrônico, redes de comunicação, sistemas de automação de subestações e centros de controle, estão incorporados em toda a rede física, envolvendo os segmentos de geração, transmissão e distribuição de energia [25].

No centro de controle se concentra a responsabilidade pelo monitoramento, controle e tomada de decisões operacionais em tempo real. Os operadores, independentemente de sistemas, realizam a coordenação entre os utilitários de energia e enviam comandos para seus centros de controle. As concessionárias que participam dos mercados de energia também interagem com os sistemas para apoiar funções de mercado baseadas na geração, transmissão e demanda de energia em tempo real.

Uma visão geral dessa abordagem pode ser verificada na Figura 2.8. O risco é normalmente definido como o impacto multiplicado pela probabilidade de um evento ocorrer [71].

A probabilidade deve ser tratada por meio da etapa de análise de vulnerabilidade da infraestrutura, a qual aborda a capacidade da infraestrutura de limitar o acesso do invasor às funções de controle críticas.

Uma vez descobertas as possíveis vulnerabilidades, a análise de impacto deve ser realizada para determinar as funções de controle efetivas da rede que podem ser afetadas. Essas informações devem então ser utilizadas para se avaliar o impacto no sistema físico [25].

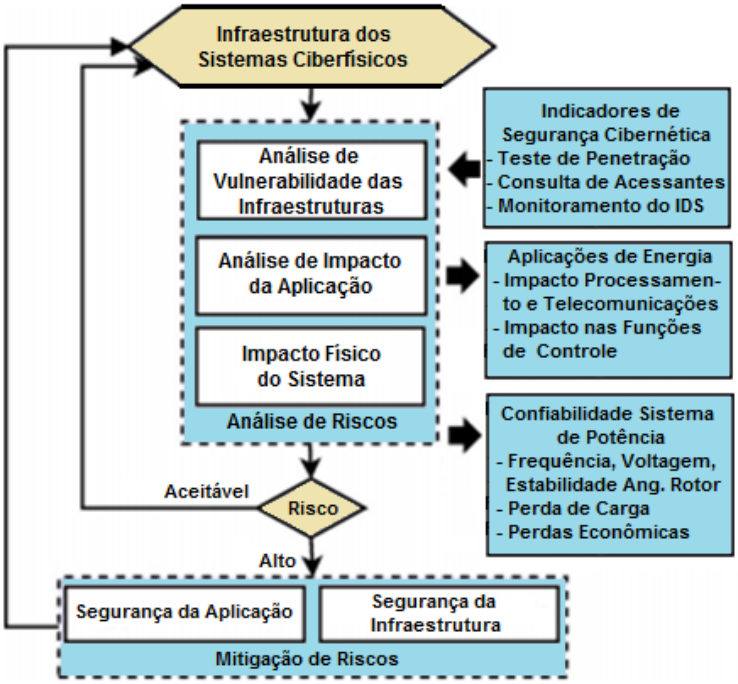

Figura 2.8: Metodologia de Avaliação de Riscos
Fonte: Adaptado de [25].

O desenvolvimento de uma infraestrutura de suporte segura para o sistema elétrico de potência é necessário para que se possa garantir que as informações sejam armazenadas com precisão e transmitidas às aplicações apropriadas com segurança [68].

Embora a infraestrutura de suporte possa compartilhar algumas propriedades comuns com os sistemas tradicionais de TI, a variação é significativa o suficiente para introduzir inúmeras preocupações de segurança únicas e desafiadoras [68].

As propriedades específicas que introduzem tais preocupações associadas à segurança da infraestrutura crítica do sistema elétrico de potência incluem:

- Ciclos de vida longos do sistema (> 10 anos);
- Proteção limitada do ambiente físico;
- Recursos restritos de gerenciamento de atualização/alteração;

- Dependência pesada de sistemas/protocolos legados; e,
- Habilidades limitadas de processamento de informações.

Um sistema de informações seguro, tradicionalmente impõe a confidencialidade de seus dados para proteger contra acesso não autorizado, garantindo que sua integridade permaneça intacta. Além disso, o sistema deve fornecer disponibilidade suficiente de informações aos usuários autorizados [68].

O objetivo principal de qualquer sistema físico-cibernético é fornecer um controle eficiente sobre algum processo físico. Isso naturalmente prioriza a integridade e a disponibilidade das informações para garantir que o estado de controle espelhe de perto o estado do sistema físico.

Mecanismos de segurança como criptografia, controle de acesso e autenticação são necessários para fornecer integridade nos sistemas, no entanto, é importante que se considere ainda que todos os mecanismos de segurança adaptados para este ambiente também devem fornecer alta disponibilidade. Essas restrições muitas vezes limitam a utilização de mecanismos de segurança que podem não ser adequados em um sistema de transmissão, pois podem eventualmente negar o acesso a uma função crítica do sistema [68].

A seguir, serão apresentados alguns itens de segurança cibernética importantes para uma infraestrutura de suporte ao sistema elétrico de potência.

2.8.1 O IED - Intelligent Electronic Device

Uma maior consciência do risco e do gerenciamento de informações relevantes de segurança exerce papel importante no processo de manutenção da confiabilidade de uma infraestrutura crítica.

Os IEDs que, em geral, se caracterizam por serem dispositivos de medição com comunicação embarcada e processamento de dados, são usados para diferentes níveis de controle e proteção em sistemas elétricos de potência, sendo que os sistemas de controle materializam o ponto onde os sistemas cibernéticos e físicos se unem [70].

Esses dispositivos estão presentes em toda a rede elétrica para a realização de funções de monitoramento, controle, proteção, automação e medição, possibilitando a concepção de lógicas de intertravamento e bloqueio [59].

O papel crítico desempenhado pelos IEDs insere, na segurança cibernética, preocupações significativas, uma vez que podem ser fisicamente inseridos em ambientes que eventualmente possam estar desprotegidos [72].

Dessa forma, algumas atividades possuem grande relevância para a composição do processo de segurança que, dentre elas, destacam-se:

- Perícia Digital: Trata-se da capacidade de realizar perícia digital forense dentro da rede elétrica de forma que se possa identificar falhas de segurança e implantar ações de prevenção de futuros incidentes [5];
- O grande número de sistemas embarcados, principalmente nos IEDs e dispositivos legados dentro da rede elétrica, fornecem novos desafios. Dentre eles, destaca-se a implantação de agentes forenses de

segurança cibernética ao longo de toda a cadeia da infraestrutura elétrica de suporte, para permitir e facilitar a coleta de dados sobre potenciais ataques. Portanto, a expansão de recursos forenses em sistemas embarcados é necessária para garantir que esses recursos críticos mantenham a sua integridade [5]; e,

- Segurança de Incidentes e Gerenciamento de Eventos: O desenvolvimento de tecnologias para coletar e analisar fontes de dados representativas, como registros de sistemas, resultados obtidos por meio do Intrusion Detection System – IDS, informações do fluxo de informações na rede (Wireshark, por exemplo), dentre outros, possui grande importância no sentido de se garantir que os dados estejam corretamente organizados e priorizados. A integração dessas várias fontes de dados de segurança cibernética existentes em um processo de comando e controle de sistemas elétricos de potência foi avaliada e se demonstrou uma eficiente capacidade de detecção de ataques [73].

2.8.2 Análise de Vulnerabilidades em Segurança Cibernética

As posturas e metodologias adotadas para a composição do processo de análise de riscos cibernéticos associado a segurança das redes elétricas de potência devem ser continuamente reavaliadas, de forma que se possa ter uma boa margem de garantia de que essas redes operam sob um ambiente com uma segurança adequada [28] e [29].

Características como complexidade do sistema, longa vida útil e ameaças cibernéticas em constante evolução passaram a apresentar um novo vetor de ataque. A detecção e remoção desses problemas de segurança cibernética devem ter abordagens específicas tanto para os sistemas e aplicações de energia, como os SPCS e SCADA, como também para os sistemas e aplicações associados à infraestrutura de suporte e apoio, como os Sistemas de Informação.

As metodologias utilizadas para realizar avaliações de vulnerabilidade e testes de penetração levantaram numerosas preocupações de segurança cibernética dentro das redes elétricas de potência. As tecnologias cibernéticas associadas a essas redes apresentam uma crescente interconectividade, criando um ambiente complexo de grande exposição de sua infraestrutura operacional de missão crítica, assim como uma crescente dependência da confiabilidade de muitos dispositivos diferentes [28] e [29].

O passo inicial no processo de análise de riscos é a análise de vulnerabilidade da infraestrutura. Inúmeras dificuldades são encontradas ao se inserir vulnerabilidades cibernéticas dentro dos ambientes do sistema de controle devido aos altos requisitos de disponibilidade e dependências de sistemas e protocolos legados [68] [4].

Uma análise abrangente de vulnerabilidade deve começar com a identificação de ativos cibernéticos, incluindo software, hardware e protocolos de comunicação. Em seguida, atividades como testes de penetração e varredura de vulnerabilidades podem ser utilizadas para determinar possíveis preocupações de segurança dentro do ambiente.

Além disso, a análise contínua dos avisos de segurança de fornecedores, registros de sistemas e sistemas de detecção de intrusões implantados devem ser utilizados para determinar vulnerabilidades adicionais do sistema.

As vulnerabilidades cibernéticas de um sistema de controle tradicional foram avaliadas pelo Departamento de Segurança Interna dos Estados Unidos da América com base em inúmeras avaliações técnicas e não técnicas [74].

A Tabela 2.5 mostra algumas das vulnerabilidades apresentadas na Tabela 2.3 do Item 2.6.1, fazendo uma categorização em função do local onde foram encontradas, ou seja, em produtos de software do setor (configurações gerais) ou na infraestrutura de rede, fornecendo uma maior visão sobre os prováveis vetores de ataque [74].

Tabela 2.5: Vulnerabilidades/Fraquezas Comuns dos Sistemas de Controle

Vulnerabilidades do SW	**Vulnerabilidades de Configuração**	**Vulnerabilidades de Segurança na Rede**
Attack	Marconi Wireless Hack	A apresentação do telégrafo sem fio de Marconi foi invadida com código Morse.
Attack	Maroochy Water	Um ciberataque causou a liberação de mais de 265.000 galões de esgoto não tratado.
Attack	Turkey Pipeline Explosion (not quite cyber)	Os atacantes usaram o software vulnerável de uma câmera de segurança para entrar na rede de controle de uma tubulação
Malware	Stuxnet	O mundo tem a primeira arma digital conhecida publicamente.
Malware	Night Dragon	Os atacantes usaram malware sofisticado para atingir empresas globais de petróleo, energia e petroquímica.
Malware	Duqu/ Flame/Gauss	Malware avançado e complexo usado para atingir organizações específicas, incluindo os fabricantes de ICS.
Campaign	Gas Pipeline Cyber Intrusion Campaign	ICS-CERT identificou uma série de intrusões cibernéticas ativa, visando o setor de gasodutos de gás natural.
Malware	Shamoon	Malware usado para atingir grandes empresas de energia no Oriente Médio, incluindo a Saudi Aramco e a RasGas.

Fonte: Traduzido de [74]

Após a identificação de vulnerabilidades e riscos cibernéticos, a etapa de análise de impacto deve ser realizada para determinar possíveis impactos nos aplicativos suportados pela infraestrutura elétrica. Em seguida, a análise de impacto físico deve ser realizada visando quantificar a dimensão do impacto no sistema elétrico envolvido [25].

As atividades subsequentes têm por objetivo mitigar e minimizar os níveis de risco inaceitáveis. Isso pode ser realizado através da implantação de uma infraestrutura de suporte mais robusta ou soluções elétricas que ofereçam um nível de resiliência capaz de suportar as eventuais ocorrências ou mesmo soluções

físicas que mitiguem esses riscos, bloqueando os impactos indesejados [26].

Estudos de ataque também ajudarão a desenvolver contramedidas que podem prevenir ataques ou mitigar o impacto de ataques. Dentre as contramedidas possíveis, podem ser incluídas técnicas de detecção de dados e algoritmos de controle resilientes ao ataque [25].

O Guia de Diretrizes para a Segurança Cibernética das Redes Elétricas Inteligentes [18] do NIST propôs um conjunto robusto de requisitos de segurança cibernética, visando garantir a adequação do mecanismo de proteção cibernética. Tais requisitos identificam interfaces lógicas entre os sistemas e suas partes, atribuindo um nível de criticidade (por exemplo: alto, médio, baixo) para os requisitos de confidencialidade, integridade e disponibilidade de cada interface.

O documento final gerado pela metodologia apresenta, portanto, uma lista de controles que são necessários serem gerenciados para ser possível se garantir um nível de segurança adequado para as interfaces identificadas.

2.8.3 O Processo de Gestão de Riscos Cibernéticos em Sistemas Elétricos de Potência

Conforme citado no item anterior, o processo de gestão de riscos cibernéticos passa, inicialmente, pela análise de vulnerabilidades que a infraestrutura de um sistema elétrico, em geral, está submetida.

Nesses ambientes, as principais vulnerabilidades podem ser identificadas nos produtos de terceiros e softwares embarcados, assim como aquelas encontradas em configurações e fragilidades associadas à rede de comunicação [74].

Após a identificação de vulnerabilidades e riscos cibernéticos, destaca-se mais uma vez que a etapa de análise de impacto deve ser realizada para determinar as possíveis consequências nos aplicativos suportados pela infraestrutura elétrica [25].

As atividades subsequentes têm por objetivo mitigar e minimizar os níveis de risco inaceitáveis [26].

O processo de gestão de riscos cibernéticos exige, portanto, a definição de procedimentos e controles que irão permitir não apenas o monitoramento da execução das ações de segurança e de mitigação de riscos, como também o acompanhamento sistemático da rotina e dos respectivos controles associados.

A manutenção da disponibilidade, da confidencialidade e da integridade das informações associadas aos controles só é possível caso eles sejam suportados sob três dimensões: tecnologia, processos e pessoas, considerando o contexto de um processo de gestão de riscos cibernéticos [75].

As redes industriais são compostas por componentes e aplicações especializadas, como controladores lógicos programáveis (PLCs), Sistemas SCADA e sistemas de controle distribuídos (DCS) [76].

No entanto, existem outros componentes, como Unidade de Terminal Remoto - UTR, IED e Unidades de Medição de Phasor - PMU, os quais se comunicam com a interface homem-máquina localizada na rede de controle e, com isso, alerta que o risco de ataque cibernético passa a ser real quando a rede corporativa e de controle passam a ter comunicações para operações comerciais regulares, uma vez que parte do sistema de rede corporativa está aberta à Internet para se comunicar com stakeholders e entidades empresariais fora da rede operativa [76].

Recursos robustos podem ser investidos na capacidade do sistema de supervisão e controle e, também, na infraestrutura associada. Com isso, busca-se desviar o evento de ataque, usar recursos redundantes, responder e recuperar dentro do prazo definido com um mínimo impacto e continuar aprendendo as vulnerabilidades e vetores de ataque [76].

Não menos importante, deve-se avaliar/atualizar continuamente as políticas de segurança e privacidade, destacando-se a análise periódica dos riscos cibernéticos por meio de controles adequados e abrangentes, apresentados pelos principais Frameworks disponíveis no mercado [77].

Esses controles devem conseguir garantir a execução de uma análise abrangente de vulnerabilidades, partindo-se desde a identificação de ativos cibernéticos, incluindo software, hardware e protocolos de comunicação até a execução de testes de penetração. Além disso, a análise contínua dos avisos de segurança de fornecedores, registros de sistemas e sistemas de detecção de intrusões implantados devem ser utilizados para determinar vulnerabilidades adicionais do sistema [68].

As atividades subsequentes têm por objetivo mitigar e minimizar os níveis de risco inaceitáveis. Isso pode ser realizado através da implantação de uma infraestrutura de suporte mais robusta ou soluções elétricas que ofereçam um nível de resiliência capaz de suportar as eventuais ocorrências ou mesmo soluções físicas que mitiguem esses riscos, bloqueando os impactos indesejados [26].

Nesse sentido, o espectro de ataques cibernéticos e tentativas de intrusões cada vez mais sofisticadas têm revisitado um dilema importante para o setor de energia elétrica: como tornar a infraestrutura de eletricidade mais segura sem, no entanto, comprometer a produtividade? Essa é efetivamente uma pergunta crucial [15].

Esse dilema vai exigir continuamente o desenvolvimento e a implantação de tecnologias de curto e longo prazo, assim como de processos de gestão de riscos, os quais irão certamente afetar as características fundamentais do sistema elétrico de potência [78].

2.8.4 Gerenciamento de Riscos, Normas, Diretrizes e Frameworks

A abordagem de gerenciamento de riscos se apoia em uma série de normas e diretrizes de segurança necessárias para uma adequada composição do processo de segurança da informação das redes elétricas de potência.

A Organização Internacional para a Padronização - ISO e a Comissão Eletrotécnica Internacional - IEC [79] disponibilizaram normas para a gestão de riscos e segurança da informação, dentre as quais podem ser destacadas, para efeito de gerenciamento de riscos cibernéticos em sistemas elétricos de potência, as seguintes:

- ISO/IEC 31000 - Gerenciamento de Riscos – Princípios e Diretrizes;
- ISO/IEC 31010 - Gestão de Riscos – Técnicas de Avaliação de Riscos;
- ISO/IEC 27001 - Tecnologia da Informação - Gerenciamento de Segurança da Informação;
- ISO/IEC 27002 - Tecnologia da Informação - Técnicas de Segurança – Código de Práticas para

Controles de Segurança da Informação;

- ISO/IEC 27005 - Tecnologia da Informação - Técnicas de Segurança – Gerenciamento de Riscos de Segurança da Informação;
- ISO/IEC 27019 - Tecnologia da Informação - Técnicas de Segurança – Diretrizes de Gerenciamento de Segurança da Informação com base na ISO/IEC 27002 para sistemas de controle de processo específicos da indústria de serviços de energia;
- ISO/IEC 27701 - Extensão ISO 27001/2 para Privacidade de Dados;
- ISO/IEC 62351 - 1 a 11 - Série Segurança Cibernética para Redes Inteligentes (Protocolos da Série TC 57: IEC 60870-5, IEEE 1815 DNP3, IEC 60870-6 ICCP, IEC 61850 Client-Server, IEC 61970/61968 Common Information Model - CIM); e,
- ISO/IEC 62443 - Sistemas de Segurança para Redes Industriais.

Além das normas ISO/IEC citadas acima, outra importante instituição que se dedicou ao tema foi o NIST.

O NIST procurou harmonizar as normas internacionais e americanas, viabilizando um sistema de gestão de segurança da informação e um processo de gestão de riscos semelhante aos descritos nas normas ISO/IEC, o que proporcionou uma forma de facilitar a conformidade baseada nessas normas, assim como com as normas e orientações do próprio NIST.

Para o NIST, as organizações podem examinar quais recursos implementarão nas cinco funções de alto nível identificadas no *framework*: Identificar, Proteger, Detectar, Responder e Recuperar [71].

É importante que se tenham pelo menos os recursos básicos implementados em cada uma dessas áreas, de forma que se possam começar a revisar quais categorias e subcategorias particulares usam atualmente para ajudar a alcançar esses resultados [71].

Embora não substitua um processo de gerenciamento de riscos, as funções fornecerão uma forma concisa para se extrair os conceitos fundamentais de risco de segurança cibernética, visando avaliar como os riscos identificados são gerenciados e avaliar se a organização se posiciona em um nível elevado de contrapartidas, diretrizes e práticas de segurança cibernética existentes [71].

A Norma NISTR-7628 tem uma abordagem direcionada aos sistemas de missão crítica, em especial os sistemas elétricos de potência, disponibilizando um prático, porém abrangente, *framework* para a implantação do processo de análise de segurança cibernética em redes elétricas inteligentes [18].

Devido a sua evolução, impulsionada principalmente pela ordem executiva emitida em 12 de fevereiro de 2013 pelo presidente dos EUA, Barack Obama, o NIST publicou a estrutura NIST-CSF, que apresenta uma vasta lista de controles que precisam ser gerenciados para garantir um nível adequado de segurança cibernética para as interfaces identificadas nas infraestruturas críticas, em especial no SEP [80].

Além da estrutura publicada pelo NIST, a ISO disponibilizou normas para a segurança da informação e gerenciamento de riscos, entre as quais a série ISO/IEC 27000 (Segurança da Informação) e a série

ISO/IEC 31000 (Gerenciamento de Riscos) podem ser destacadas na relação de normas ISO/IEC listadas anteriormente.

O Council on Cybersecurity (CIS) Top 18 Critical Security Controls [22], ANSI/ISA-62443-2-1 [81] e ANSI/ISA-62443-3-3 [82] fornecem uma forma de facilitar a conformidade com base nas normas internacionais, bem como nas normas e diretrizes do NIST.

2.8.5 O *Framework* CIS CSC

A grande robustês e o consequente custo de implantação do *framework* proposto pelo NIST CSF, mencionado no item anterior, motivou o CIS - Center for Internet Security a construir uma estrutura mais leve e otimizada, consistindo em 18 (dezoito) grupos de controles, definidos como Macrocontroles, obtidos a partir do NIST CSF [15].

Os controles propostos para o *framework* CIS CSC foram projetados no sentido de se fornecer às organizações um número menor de controles que, no entanto, pudessem oferecer os recursos básicos para se atingir resultados de segurança eficazes, imediatos e de alto impacto [83].

A definição desses Macrocontroles pelo CIS foi realizada tendo como premissa básica atender às exigências das infraestruturas críticas com a melhor relação risco/retorno, utilizando como orientação metodológica o Princípio de Pareto [84].

Com isso, o *framework* CIS CSC se utilizou do princípio de que 20% das causas ou riscos são responsáveis por cerca de 80% dos efeitos, ou impactos, portanto, cerca de 20% dos controles definidos pelo NIST CSF podem representar 80% de melhoria no nível de segurança cibernética [84].

Os Controles apresentados no *framework* CIS CSC constituem um conjunto prioritário de ações (salvaguardas) recomendadas para a defesa cibernética, que oferecem formas específicas e acionáveis de se impedir e mitigar os ataques cibernéticos mais usuais contra sistemas e redes, no entanto, com custos escaláveis e não tão intensos como os envolvidos em todas as Subcategorias do NIST CSF [15].

Esse *framework* é gerenciado pelo Center for Internet Security – CIS, e seus controles foram aprimorados para acompanhar os sistemas e softwares modernos, envolvendo nuvem, virtualização, mobilidade, terceirização, trabalho remoto, evolução das táticas de ataque, etc [22].

Além disso, O CIS CSC estrutura a implementação dos seus controles em Grupos de Implementação-IGs, que consideram os recursos e o perfil de risco de cada organização.

Os IGs apresentam, portanto, uma orientação de priorização recomendada pelo CIS CSC, de tal forma que se possa atender as empresas de todos os portes, considerando as suas disponibilidades orçamentárias e apetite ao risco de cada uma [22].

Assim, a implementação dos controles do *framework* CIS CSC começa com o grupo IG1, obrigatório para todas as organizações, incluindo aquelas com recursos limitados, seguido pelo grupo IG2, que considera organizações com recursos moderados, e finalmente, o grupo IG3, para organizações que lidam com infraestruturas críticas e com alta exposição ao risco [85].

O Grupo de Implementação IG1, que contempla os 56 controles críticos considerados básicos, é de-

finido como "higiene cibernética essencial" [85]. Trata-se do conjunto fundamental de salvaguardas de defesa cibernética que toda empresa deve aplicar para se proteger contra os ataques mais comuns.

O IG2 contempla 74 novos controles que, adicionalmente aos 56 controles do Grupo IG1, vão ajudar as equipes de segurança e gestão de riscos cibernéticos a lidar com o aumento da complexidade operacional [22].

No IG2 verifica-se a existência de controles que dependerão de tecnologias de nível empresarial e experiências mais especializadas de técnicos para ser possível sua instalação e configuração adequadas. Empresas desse Grupo podem suportar apenas pequenas interrupções de serviço [22].

As empresas que constituem o Grupo de Implementação - IG3 são aquelas que normalmente já possuem em seu quadro de colaboradores técnicos especializados em diferentes facetas da segurança cibernética, dentre elas gerenciamento de riscos, gerenciamento de vulnerabilidades, segurança de hardware e software, etc [22].

Para essas empresas, os ativos e dados contém informações ou funções, que estão sujeitas à supervisão regulatória e de conformidade. Ataques bem sucedidos às empresas IG3 podem causar danos significativos ao bem-estar público [22].

Dessa forma, as 23 novas salvaguardas selecionadas para o IG3, em conjunto com os 130 controles já definidos para os Grupos IG1 e IG2, devem diminuir os ataques direcionados de um adversário sofisticado e reduzir o impacto dos ataques de dia zero [22].

A Figura 2.9 ilustra a abrangência dos Grupos de Implementação do *framework* CIS CSC.

Figura 2.9: Abrangência dos Grupos de Implementação Propostos pelo CIS CSC
Fonte: Adaptado de [22].

Portanto, o número de controles do IG3 é maior que o do IG2, e o do IG2 é maior que o número de controles do IG1, como mostra a Tabela 2.6 [15].

O Center for Internet Security disponibiliza o livre acesso ao seu *framework* CIS CSC (Controls V8) onde é possível a identificação de todas as salvaguardas propostas para cada Macrocontrole apresentado

nesta mesma Tabela [22].

Tabela 2.6: Grupos de Controle do CIS CSC e o Número de Subcontroles (Salvaguardas) em cada Grupo de Implementação

Grupos de Controles CIS CSC	**IG1**	**IG2**	**IG3**
1- Inventário e Controle de Dispositivos de Hardware	2	4	5
2- Inventário e Controle de Ativos de Software	3	6	7
3- Proteção de Dados	6	12	14
4- Configuração Segura dos Softwares e Ativos Empresariais	7	11	12
5- Gerenciamento de Contas	4	6	6
6- Gerenciamento do Controle de Acesso	5	7	8
7- Gerenciamento Contínuo de Vulnerabilidades	4	7	7
8- Gerenciamento dos Logs de Auditoria	3	11	12
9- Proteção de e-mails e Navegadores WEB	2	6	7
10- Proteção Contra Aplicações Maliciosas	3	7	7
11- Recuperação de Dados	4	5	5
12- Gerenciamento da Infraestrutura de Rede	1	7	8
13- Defesa e Monitoramento da Rede	0	6	11
14- Treinamento de Conscientização e Habilidades de Segurança	8	9	9
15- Gerenciamento de Provedor de Serviços	1	4	7
16- Segurança de Softwares e Aplicativos	0	11	14
17- Gerenciamento de Resposta a Incidentes	3	8	9
18- Teste de Penetração	0	3	5

Fonte: [22]

Observa-se nesta Tabela 2.6 que os grupos 13, 16 e 18 não têm controles IG1, mas IG2 e IG3. Portanto, estes controles são implementados em organizações com maior disponibilidade de recursos [15].

A Figura 2.10 mostra de forma mais clara a proporcionalidade da composição dos controles CIS CSC aplicáveis em cada Grupo de Implementação. Verifica-se que o segmento IG1 contempla 56 controles, o IG2 contempla 130 controles (56 do IG1 e mais 74 controles exclusivos do IG2) e o IG3 que contempla 153 controles (130 do IG2, que já contempla os controles do IG1, e mais 23 controles exclusivos do IG3).

Com base no exposto, o *framework* CIS CSC foi escolhido para este trabalho por ser um *framework* otimizado, constituído de dezoito Macrocontroles obtidos a partir do NIST-CSF [22].

Um destaque especial será direcionado ao Macrocontrole 11 que trata especificamente dos aspectos sobre Recuperação de Dados do *framework* CIS CSC, cujo objetivo é disponibilizar condições para se estabelecer e manter práticas de recuperação de dados que sejam suficientes para garantir a recuperação dos ativos empresariais para uma situação igual àquela identificada antes do incidente, de forma confiável e segura [16].

Esse Macrocontrole 11 é composto de cinco subcontroles, cuja abrangência atende às funções de segurança associadas à recuperação e proteção dos dados. São eles:

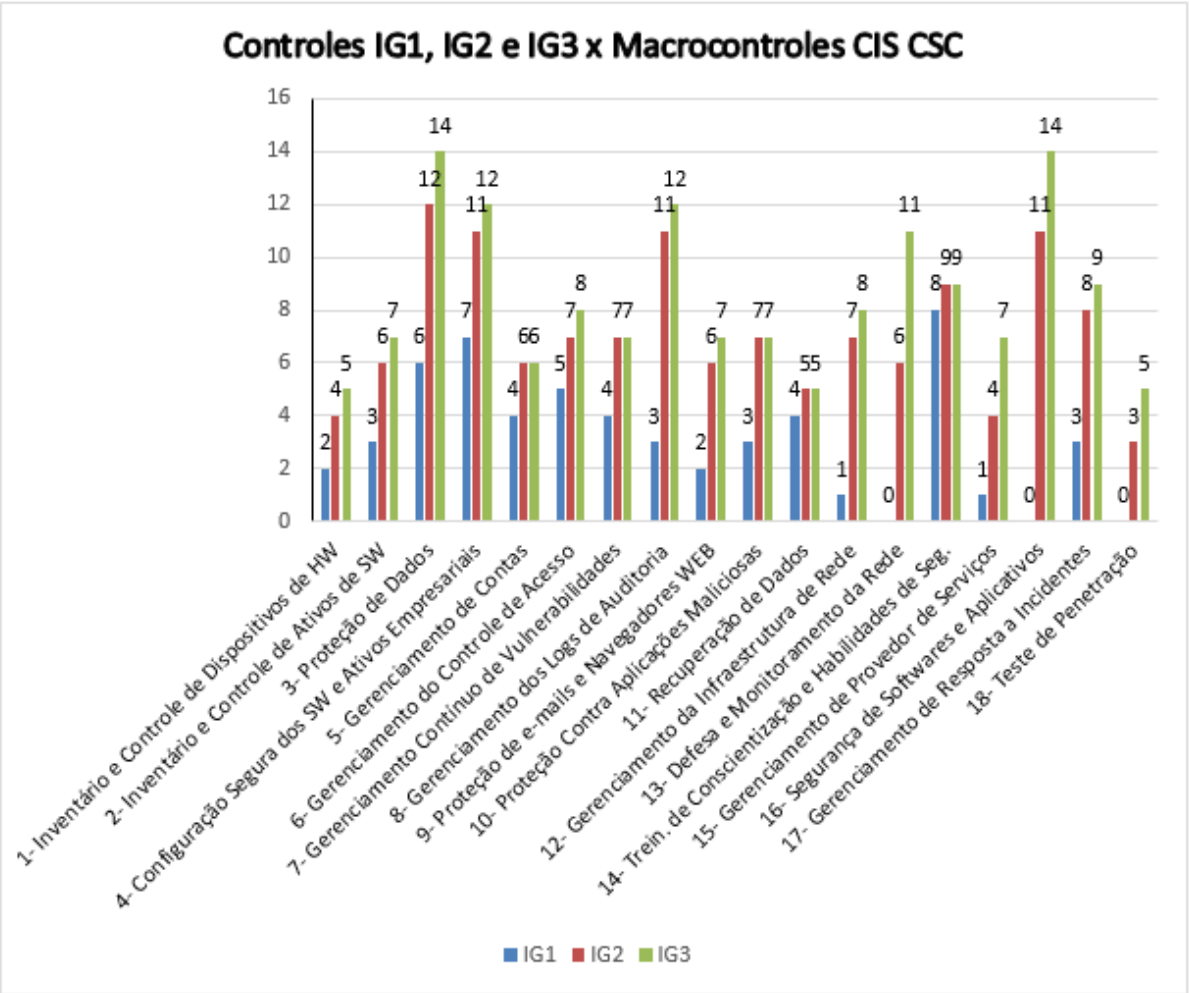

Figura 2.10: Composição dos Controles de cada Grupo de Implementação - IG para os dezoito Macrocontroles do CIS CSC

Fonte: [22].

- Subcontrole 11.1 – Visa estabelecer e manter um processo de recuperação de dados. No processo, deve ser abordado o escopo das atividades de recuperação de dados, a priorização da recuperação e a segurança dos dados de backup. Revisar e atualizar a documentação anualmente, ou quando ocorrerem mudanças significativas na empresa que possam impactar este Subcontrole (Salvaguarda);
- Subcontrole 11.2 – Realizar backups automatizados de ativos empresariais no escopo. Executar backups semanalmente, ou com maior frequência, com base na importância dos dados;
- Subcontrole 11.3 – Proteger os dados de recuperação com controles equivalentes aos dados originais. Dependendo dos requisitos, pode ser utilizada criptografia ou separação de dados;
- Subcontrole 11.4 – Estabelecer e manter uma instância isolada de dados de recuperação. Exemplos de implantações incluem versão controlando destinos de backup através de sistemas ou serviços off-line, em nuvem ou fora do local; e,
- Subcontrole 11.5 – Testar a recuperação do backup trimestralmente, ou mais frequentemente, para

uma amostragem dos ativos da empresa no escopo.

Esses subcontroles atingem as três categorias de IGs, independentemente dos recursos e do perfil de risco de cada organização, exceto o Subcontrole 11.5, para o qual o *framework* CIS CSC dispensa a sua adoção para o Grupo de Implantação IG1 [15].

No entanto, para as empresas de geração, transmissão e distribuição de energia elétrica, todos os subcontroles (salvaguardas), são importantes: “Para essas empresas, os processos são dotados de uma elevada criticidade, em especial aqueles monitorados pelo Sistema SCADA. As avaliações de segurança devem ser incluídas como parte da governança de um sistema crítico e seu gerenciamento de segurança” [86].

2.9 SISTEMAS SCADA E OS SEUS PROCESSOS DE RECUPERAÇÃO DE DADOS - UMA ANÁLISE DO SCADA SIEMENS WIN CC 7.5 SP2

O Sistema SCADA tem uma função crucial para os processos industriais. É ele que assume a responsabilidade pelo acompanhamento e supervisão dos processos produtivos, cujo principal objetivo é garantir a sua correta execução, de conformidade com os padrões de projeto. Ele ainda oferece os subsídios para a atuação de sistemas auxiliares de proteção, comando e controle [16], por exemplo.

As vulnerabilidades associadas aos Sistemas SCADA são umas das mais importantes a serem avaliadas em um processo de gestão de riscos cibernéticos [68].

A Figura 2.11 mostra como ocorre o loop típico de controle dos sistemas elétricos de potência, se utilizando normalmente de sistemas de controle tradicionais, constituídos pelos Sistemas SCADA, os controles locais e os novos controles associados aos serviços oferecidos pela rede inteligente.

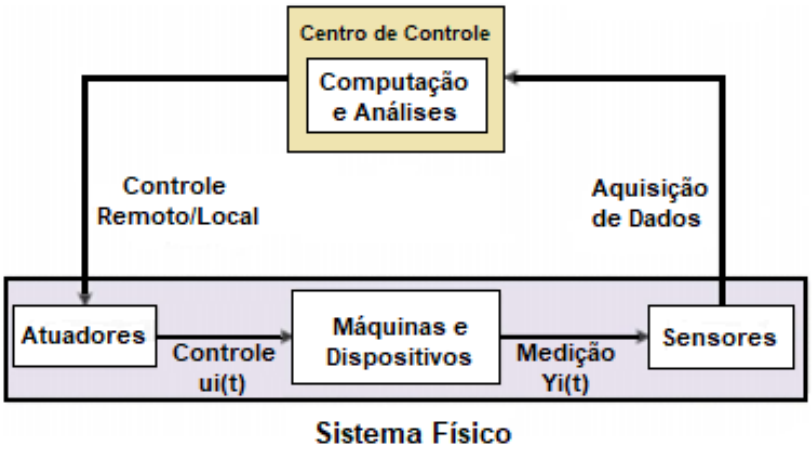

Figura 2.11: Loop Típico de Controle do Sistema Elétrico de Potência
Fonte: Adaptado de [25].

As questões de segurança cibernética para os Sistemas SCADA têm sido bem exploradas, uma vez que os Sistemas SCADA e DER desempenham um papel importante nos serviços de confiabilidade do sistema elétrico de potência [87] e [88].

A Figura 2.12 mostra como a arquitetura do Sistema SCADA é estruturada:

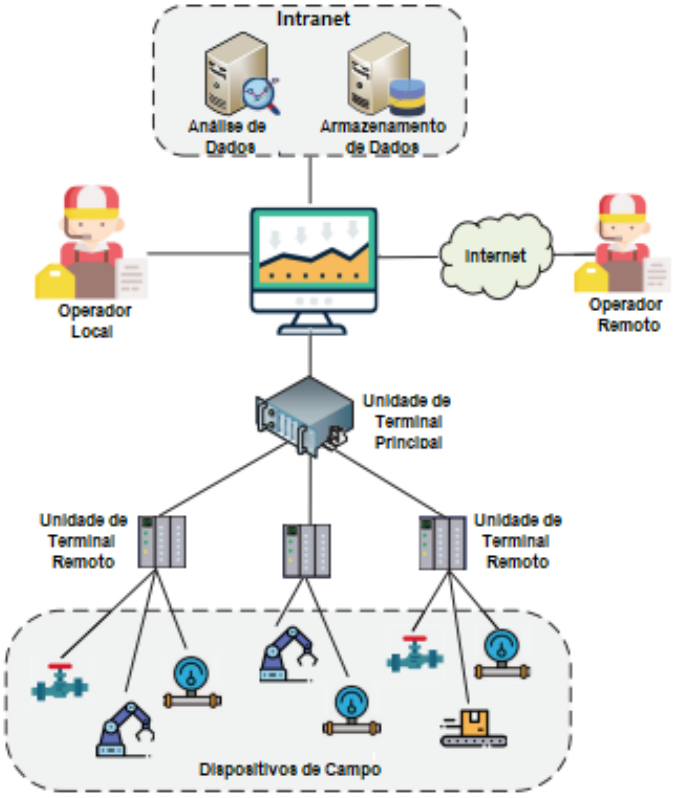

Figura 2.12: Arquitetura do Sistema SCADA
Fonte: Adaptado de [89].

A infraestrutura associada aos Sistemas SCADA é constituída de servidores, drivers de comunicação, sensores e atuadores conectados ao processo. Com isso, torna-se possível a sua atuação em tempo real [90].

Ele é projetado para ser possível a implantação de configurações específicas para cada tipo de processo, armazenar dados e disponibilizar recursos para intervir manual ou automaticamente no processo, quando necessário. Apesar de atuar preponderantemente em processos industriais, o Sistema SCADA também tem sido muito utilizado em processos experimentais [90].

Além de coletar os dados, o Sistema SCADA, também chamado de sistema supervisório, permite ainda a visualização e supervisão dessas informações. Essa visualização é normalmente apresentada de forma amigável em telas sinópticas, se valendo de gráficos de tendências, evolução histórica e sinalização de alarmes e falhas [90].

Os sistemas elétricos de potência se utilizam dos Sistemas SCADA, dos controles locais e dos novos controles associados aos serviços oferecidos pela rede inteligente, para os quais os estudos de ataque ajudam a desenvolver contramedidas que podem prevenir ataques ou mitigar seus impactos [25].

Os links de telecomunicações utilizados pelas empresas do setor elétrico em seus processos operacionais com a utilização dos Sistemas SCADA, e que estejam parcialmente fora do controle da organização, representa um caminho potencialmente inseguro para as operações empresariais, bem como uma ameaça à própria rede elétrica, caracterizando um excelente ponto de referência para uma análise de vulnerabilidade

cibernética [78].

Para que se obtenha uma proteção abrangente, há a necessidade de se contar com um controle inteligente, seguro e distribuído, de forma que partes da rede possam permanecer operacionais e até mesmo se reconfigurarem automaticamente, caso haja a necessidade de lidar com falhas locais ou com ameaças de falha, provocadas por ataques cibernéticos [78].

2.9.1 O Sistema SCADA Siemens Win CC 7.5 SP2

Vários Sistemas SCADA estão em operação nas subestações transformadoras de energia elétrica ao redor do mundo, os quais são providos por diferentes fabricantes [16].

O Sistema SCADA da Siemens, WinCC V7.5 SP2 possui um grande número de funcionalidades associadas aos procedimentos de arquivamento de dados do processo, assim como de arquivos de usuários [1].

A versão atual do Sistema SCADA da Siemens possui um escopo de funcionalidades abrangentes, em especial aquelas associadas aos processos de Backup/Recovery (Recuperação de Dados). Buscou-se utilizar um Sistema SCADA neste trabalho que apresentasse um bom nível de automação e com alta tecnologia embarcada [16].

Este Sistema SCADA apresenta os principais grupos de funcionalidades associadas ao Backup/Recovery, sendo esse segmento de fundamental importância para o processo de gestão de riscos cibernéticos e objeto de várias salvaguardas/controles importantes apresentados pelo Framework CIS CSC, quais sejam [1]:

- Arquivamento Rápido (Fast) e lento (Slow): armazenam em arquivos do sistema *runtime* os dados sensoriais em tempo real, divididos por categoria das *tags*, ou seja, com ciclos de menos de 1 minuto e ciclos de mais de 1 minuto, respectivamente;

- Backup de Arquivos de Processo: configurado para ser iniciado após 15 min da primeira mudança de segmento relacionada no tempo e realizado de forma sincronizada com o início do *runtime*. Para sistemas redundantes, o backup é realizado a partir do servidor mestre com assinatura de modificação após a realização do backup, sendo a ativação do processo de backup e a definição dos arquivos a serem inseridos no backup realizadas por meio de configuração;

- Configurações Gerais de Origem e Destino de Arquivos de Processo e de Usuários: os arquivos de usuários, da mesma forma que os arquivos de processo, também podem ser configurados em redundância paralela e seu backup é realizado a partir do servidor mestre, que passa o controle para o servidor secundário em caso de falha. O backup dos arquivos de usuário também pode ser realizado por meio de processos manuais, offline, utilizando-se os métodos EXPORT e IMPORT;

- Configurações de Infraestrutura de Rede e Servidores de Backup/Recovery: o servidor de backup, seja onde estiver, é acessado por OLE_DB ou pelo editor WEB Data Monitor, possuindo links de conexão direta com o *runtime*, viabilizando o acesso direto do processo em tempo real para a realização de backup. Esse vínculo pode ser realizado por meio de script, utilizando-se o objeto VBS Datalogs, sendo que a restauração de segmentos de arquivos é realizada por meio do método

VBS.METHOD.RESTORE, permitindo sua recuperação para o diretório COMMON ARCHIVING do projeto *runtime*;

- Links de Conexão com Servidores de *Backup/Recovery*: o Sistema permite a utilização de caminhos da rede de comunicação e armazenamento de dados em nuvem. Caminhos redundantes podem ser utilizados, o segundo assumindo, caso o primeiro tenha falha na conexão;
- LOG de Monitoramento: todas as operações de gravação e recuperação de dados são gravadas em LOG específico. Em caso de uma desconexão, os arquivos do backup modificados e desconectados não são automaticamente vinculados e uma mensagem é emitida no Log de eventos para que o Windows alerte o gestor de segurança do sistema SCADA; e,
- Criptografia: a integridade dos dados de usuário e de processo é garantida por meio de algoritmos de criptografia.

A partir desses grupos de funcionalidades é de se esperar que os subsídios necessários para a construção, alimentação e monitoramento dos subcontroles definidos no Macrocontrole 11 do Framework CIS CSC estejam disponíveis, independentemente dos Grupos de Implantação (IG1, IG2 e IG3) a que pertencem [16].

3 METODOLOGIA ADOTADA

3.1 TIPOLOGIA DA PESQUISA

O presente trabalho se utilizou de uma pesquisa aplicada com objetivos descritivos exploratórios que teve como principal característica a captação de informações, visando o entendimento de uma realidade e suas aplicações práticas [91] [92].

Para esse fim, foram utilizadas investigações documentais, levantamentos bibliográficos e análise de exemplos para o estímulo da compreensão, realizados no contexto da pesquisa [91] [92].

A pesquisa realizada foi do tipo qualitativa secundária [93], uma vez que foi baseada na análise e interpretação de material documental como um dos principais métodos adotados, destacando-se: *frameworks* para Gestão de Riscos Cibernéticos, Livros, Artigos, Journals, Manual do Sistema SCADA da Siemens, Regulação do Setor Elétrico Brasileiro, Manual dos Procedimentos de Rede do ONS, Normas e Padrões [94].

O processo utilizado para a realização da interpretação e inferências associadas às informações e dados coletados, se baseou na análise comparativa e na análise de conteúdo para os focos principais da abordagem [92].

Essa tipologia de pesquisa apresentada foi aplicada aos seguintes cenários de estudo:

1. Análise comparativa entre a Rotina Operacional do ONS e os controles estruturais do *framework* CIS CSC, visando confirmar à Hipótese 1 formulada;
2. Análise de conteúdo do Sistema SCADA da Siemens, com o foco no processo descrito pelo Macrocontrole 11 - Recuperação de Dados do CIS CSC *framework*, visando confirmar à Hipótese 2 formulada.

3.2 A ANÁLISE DE CONTEÚDO DE LAURENCE BARDIN

A análise de conteúdo é entendida como um conjunto de técnicas de análise das comunicações, que visa obter, por procedimentos sistemáticos e objetivos de descrição do conteúdo das mensagens, indicadores (quantitativos ou não) que permitem as inferências de conhecimentos relativos de condições de produção/recepção (variáveis inferidas) destas mensagens [95].

Nesse sentido, destacam-se as dimensões da codificação e categorização, as quais oferecem a possibilidade e a facilitação das interpretações e inferências que serão feitas a partir da análise de conteúdo [95].

Em relação ao tipo de pesquisa realizada, o referido estudo se deu por meio da análise e interpretação de publicações, destacando-se o Manual SCADA da Siemens, o *framework* CIS CSC, a RO do ONS, dentre outras publicações secundárias, visando a obtenção de informações e conhecimentos sobre o problema para o qual se busca uma resposta [95].

A partir das constatações verificadas ao longo do processo de análise de conteúdo sistemática, os dados correspondentes foram então tabulados em três fases evolutivas:

- Pré-análise;
- Exploração do material, categorização ou codificação; e,
- Tratamento dos resultados, inferências e interpretação.

A Figura 3.1 apresentada a seguir, mostra a sequência da técnica de análise de conteúdo proposta por Bardin e utilizada no trabalho.

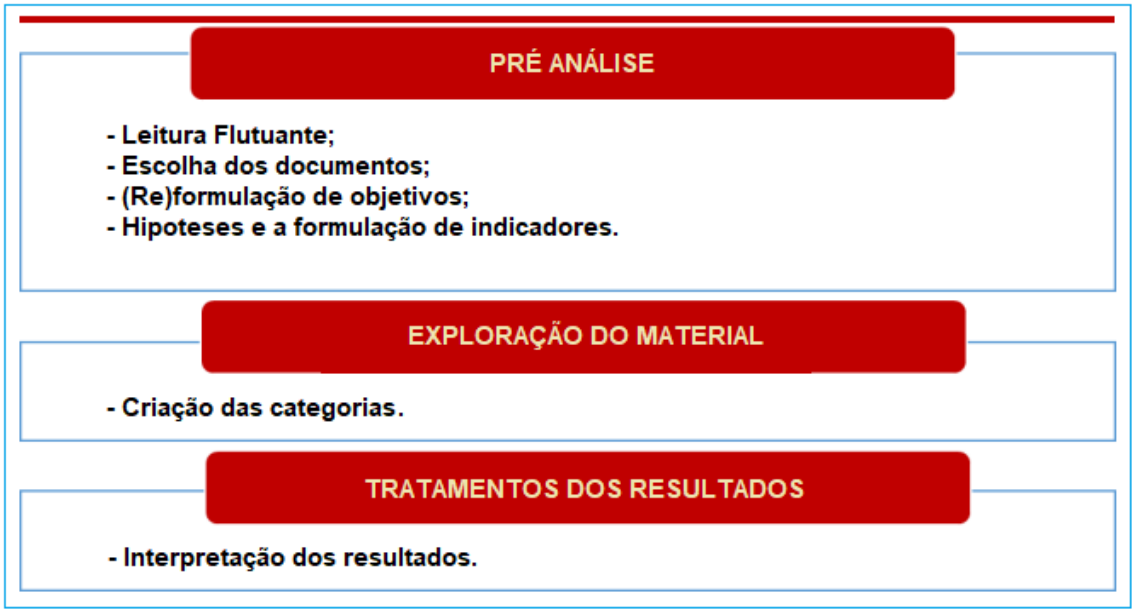

Figura 3.1: Sequência da Técnica da Análise de Conteúdo
Fonte: Adaptado de [95].

3.2.1 A Fase da Pré-Análise

Segundo [95], a pré-análise é a fase em que devem ser realizadas a leitura flutuante, a escolha dos documentos, as reformulações de objetivos e hipóteses e a formulação de indicadores.

De acordo com essas diretrizes, verifica-se que a fase de Pré-Análise deve ser responsável pelo contato com os dados apresentados pelos documentos e buscar uma primeira percepção das mensagens neles contidas. Nesta fase é definida a importância de se apresentar as impressões, representações, estados emotivos, a abrangência dos conhecimentos e as expectativas do analista [96].

Este é o momento em que a organização do material identificado se mostra importante para a pesquisa e, em seguida, ele é explorado até o ponto de ser possível a categorização ou codificação do estudo desejado, tabulando-se as descrições analíticas elaboradas [97].

3.2.2 A Fase da Exploração do Material

Realizada a Pré-Análise, o foco passa a ser a fase de Exploração do Material, na qual o material deverá ser estudado mais profundamente, visando o estabelecimento das unidades de registro e das unidades de contexto. Nesta fase deve-se tratar os dados brutos da maneira mais significativa e válida possível, viabilizando-se a construção das categorias de interesse [95].

Para a realização da Categorização, uma boa descrição analítica contribui de forma significativa para o estudo detalhado e consistente. Esse processo deve basear-se nas hipóteses e nos referenciais teóricos adotados. É no momento da criação das categorias que se realiza a classificação, ocasião em que se deve fazer o desmembramento e o posterior agrupamento ou reagrupamento das unidades de registro do texto [97].

3.2.3 A Fase do Tratamento dos Resultados

Em seguida, é realizada a fase de Tratamento dos Resultados, momento em que as inferências e interpretações do analista passam a ter um papel importante. É nesta fase que as reflexões e críticas exercem grande influência na viabilização dos conteúdos de interesse existentes no material identificado. Trata-se de uma fase lógica, cujos resultados são obtidos a partir das conexões existentes entre proposições inferidas e outras já tidas como verdadeiras [98].

Nesta fase final, os dados coletados são tratados de maneira que possam ser significativos. No caso do trabalho que foi realizado, optou-se por fazer o uso de palavras significativas para o tema da pesquisa, estabelecendo-se a partir dos eixos temáticos das recorrências e das diferenças, as categorias de análise da pesquisa, identificadas por meio de uma operação de classificação de elementos integrantes de um conjunto, classificação essa realizada por diferenciação e, logo em seguida, por reagrupamento a partir de um processo de analogia com os critérios que foram previamente definidos [95].

Com este direcionamento, a repetição de palavras e/ou termos significativos, assim como a equivalência de níveis de comparação, foram estratégias adotadas no processo de codificação da análise de conteúdo, cujos resultados serão apresentados a seguir, definindo-se, conforme a metodologia orienta e de forma integral ou parcial, as unidades de registro e, posteriormente, as categorias da análise de conteúdo que permitirão o tratamento, as interpretações e as inferências associadas [99].

3.3 ANÁLISE DE CONTEÚDO COMPARATIVA ENTRE A RO-CB.BR.01 E OS CONTROLES ESTRUTURAIS DO *FRAMEWORK* CIS CSC

Para a avaliação da Hipótese 1, os controles da Rotina Operacional RO-CB.BR.0 foram comparados com os controles estruturais do *framework* CIS CSC.

A avaliação da relação entre os pares de controle *framework* CIS CSC e ARCiber considerou a intensidade da semelhança ou da diferença entre os controles existentes em ambos, avaliando a relação dos controles da estrutura CIS CSC para os itens de segurança propostos pelo ONS para o ARCiber [15].

Esta comparação utilizou os mesmos critérios de classificação que a estrutura do *framework* CIS CSC

utiliza para se comparar com outras estruturas existentes no mercado.

Os controles do *framework* CIS CSC já foram comparados com diversos outros controles previstos em outros *frameworks* voltados para a segurança cibernética, como a que já foi realizada entre ele e o NIST SP 800-53 (NIST SP 800-53, 2020), o qual é uma importante referência em segurança cibernética [100].

A partir da metodologia que o Center for Internet Security - CIS utiliza para a realização dessas comparações, e da análise de conteúdo realizada na documentação identificada e selecionada, quando se verifica que um determinado controle do CIS CSC está implementado na organização, pode-se inferir que diversos requisitos de vários outros *frameworks* também estão totalmente atendidos, parcialmente atendidos ou não atendidos. Deste modo, estar conforme com os controles do *framework* CIS CSC é estar conforme com diversos outros modelos de referência padrão do mercado, total ou parcialmente [100].

De outra forma, caso se constate que o padrão utilizado por uma determinada empresa está em desconformidade com este ou aquele controle proposto pelo *framework* CIS CSC, então a dedução lógica é a de que a partir das comparações realizadas, a empresa também está em desconformidade, total ou parcialmente, com outros padrões de referência ou *frameworks* conhecidos [100].

A Tabela 3.1 mostrada a seguir apresenta os critérios utilizados pela metodologia proposta pelo *framework* CIS CSC para a realização das comparações entre ele próprio e outros *frameworks* existentes no mercado, destacando as avaliações qualitativas graduadas em cinco níveis de percepção: *Equivalent; Superset; Subset; Intersection; None* [22].

Tabela 3.1: Metodologia de Relação Qualitativa entre os Controles do *framework* CIS CSC e os Controles de Outros *frameworks* (Ex.: ONS ARCiber)

Relação CIS x ARCiber Nível de Percepção	**Atenuação Defensiva**
Equivalent	O controle CIS contém o mesmo conceito de Segurança Cibernética do controle ARCiber.
Superset	O Controle CIS possui um conceito mais amplo de Segurança Cibernética e contém o controle ARCiber.
Subset	O Controle CIS possui um conceito mais restrito de Segurança Cibernética e está contido no controle ARCiber.
Intersections	Há muitas semelhanças entre os dois, porém nenhum dos dois está contido dentro do outro. Não pode ser usado para atender aos requisitos do outro.
None	Não há nenhum controle ARCiber que se relacione com o Controle do *framework* CIS CSC.

Fonte: Traduzido de [22]

Assim, considerando o nível de percepção definido para cada um dos Grupos de Implementação – IG do CIS CSC, correspondentes aos dezoito macrocontroles do *framework* CIS CSC, e seus respectivos subcontroles (salvaguardas), foram realizadas a análise de conteúdo e as comparações com os controles definidos no ambiente regulado ARCiber [15].

Esta análise permitiu a construção de um mapeamento que mostra os 18 grupos de controle do *fra-*

mework CIS CSC e como o ambiente regulado ARCiber, definido pelo ONS, se relaciona com cada Grupo de Implementação IG1, IG2 e IG3, segundo a classificação qualitativa exposta acima [15].

3.4 ANÁLISE DE CONTEÚDO DO SISTEMA SCADA WIN CC 7.5 SP2 DA SIEMENS FRENTE AOS *FRAMEWORKS* CIS CSC E ARCIBER

Como consequência dos resultados encontrados na comparação entre os controles do *framework* CIS CSC e do ARCiber, uma análise de conteúdo de Bardin foi realizada nos Capítulos 7 e 8 do Manual do Sistema SCADA Siemens WinCC V7.5 SP2, visando obter informações que pudessem confirmar a Hipótese 2 e justificar os achados encontrados na comparação realizada entre os controles associados ao processo de Recuperação de Dados desses *frameworks*.

Desse modo, esta análise de conteúdo teve como direcionamento a sua capacidade de gerar as informações necessárias (insumos) para o suprimento de informações para a operacionalização dos subcontroles (salvaguardas) previstos no Macrocontrole No. 11 – Recuperação de Dados do *framework* CIS CSC [16].

Assim, a metodologia de Bardin foi utilizada para averiguar se o próprio Sistema SCADA da Siemens conseguiria disponibilizar, automaticamente, não apenas os insumos, mas também os subcontroles formalmente previstos no *framework* CIS CSC, Macrocontrole 11, buscando uma identificação dos motivos pelos quais o ONS não se preocupou em considerar esse segmento de controles no ARCiber, haja vista a importância dos controles associados à Recuperação de Dados (*Backup/Recovery*) para a Gestão de Riscos Cibernéticos no SEP [16].

4 RESULTADOS E DISCUSSÕES

Nesta seção serão apresentados e discutidos os principais resultados encontrados com a realização desta pesquisa.

4.1 RESULTADOS OBTIDOS A PARTIR DA ANÁLISE COMPARATIVA QUALITATIVA ENTRE O ARCIBER E O *FRAMEWORK* CIS CSC

O ONS definiu para o SEB um ambiente de segurança cibernética regulado, ARCiber, o qual deverá ser adotado obrigatoriamente por todos os agentes do setor elétrico nacional até o segundo semestre de 2023.

Em busca da veracidade ou não da Hipótese 1 formulada no item 1.2, esse trabalho se propôs a realizar uma análise comparativa qualitativa exploratória entre o ARCiber e outro *framework* de segurança cibernética que fosse mundialmente reconhecido e aplicado a infraestruturas críticas.

Nessa direção foi inicialmente avaliada a adoção do *framework* definido pelo NIST CSF para a realização dessa análise comparativa, no entanto, a abrangência desse *framework* se mostrou muito grande, onde se verifica a existência de 5 (cinco) grandes funções, englobando 23 (vinte e três) categorias e, por fim, 108 (cento e oito) controles ou subcategorias.

Visando a realização de uma análise qualitativa a partir de um domínio mais restrito, porém com um alcance adequado, optou-se pela adoção do CIS CSC, o qual apresenta uma abrangência significativa de grupos de controles capazes de atuar na gestão de cerca de 80% dos riscos cibernéticos contemplados pelo NIST CSF, se mostrando adequado para ser utilizado em infraestruturas críticas, característica inerente ao SEP [84].

O CIS CSC, adotado para a realização desse trabalho e cujas características estão descritas no item 2.7.5, se utiliza de 18 (dezoito) Grupos de Controle, denominados macrocontroles, cujos controles estão classificados por Grupos de Implantação (IGs). Esses IGs inserem os controles de forma acumulativa a partir dos recursos e do perfil de risco de cada organização.

Considerando que o SEB se caracteriza por ser um setor constituído por empresas que atuam com uma infraestrutura de alta criticidade, remuneradas por tarifas reguladas e associadas à geração, transmissão e distribuição de energia elétrica, utilizou-se como base de comparação para essa análise, o grupo de implantação IG3, uma vez que ele engloba os controles previstos para os grupos de implantação IG1, IG2 e aqueles específicos ao IG3.

A utilização do CIS CSC para a definição de um programa de gestão de riscos cibernéticos para o SEB deve contemplar para os 18 (dezoito) Grupos de Macrocontroles, todos os 147 (cento e quarenta e sete) controles previstos nos Grupos de Implantação IG3, como mostra a Tabela 2.6 apresentada no item 2.7.5.

A RO publicada pelo ONS no MPO do SEB procurou definir os níveis de segurança cibernética mínimos necessários que devem ser alcançados pelos seus agentes, direcionando os esforços de gestão e

controle que deverão ser adotados por cada um deles até meados do segundo semestre de 2023, como informado anteriormente.

A partir de uma análise de conteúdo da RO, verificou-se que o denominado ARCiber apresenta a definição de 7 (sete) grandes grupos de segurança cibernética, mostrados na Tabela 2.1 do item 2.5.1.

Para o Grupo de Arquitetura Tecnológica, a análise mostrou a necessidade da implantação de controles que contemplem a garantia de redes operacionais segregadas, ambiente operacional isolado da Internet e implantação de soluções anti-malware. Para o Grupo de Governança de Segurança da Informação, identificou-se que o ARCiber exige a existência de processo formal de gestão de segurança cibernética implantado no agente. O Grupo identificado como de Gestão de Ativos exige que o agente mantenha um processo ativo de inventário físico periódico dos ativos de hardware, software e de dados que estejam sob a guarda do ARCiber.

Outro Grupo identificado no ARCiber foi o de Gestão de Vulnerabilidades, que envolve a implantação de controles associados à Gestão de Atualizações, que contempla a implantação de pacotes de correção da segurança e também a Gestão da Conexão de Novos Ativos nesse ambiente regulado.

A Gestão de Acesso ao ARCiber também foi identificado como um Grupo de Segurança Cibernética considerado, o qual deverá prezar pela gestão de identidade e acesso de usuários e aplicações a esse ambiente, isoladamente da rede corporativa.

Por fim, o Grupo de Monitoramento e Resposta a Incidentes definido pelo ARCiber deverá aferir a existência e a efetividade de uma Política implantada pelos agentes que permita a manutenção de um processo ativo e contínuo de monitoramento do ambiente regulado. O objetivo é a emissão de respostas rápidas aos incidentes identificados que possam afetar a segurança e a continuidade dos processos de negócio, em especial aqueles associados à geração, transmissão e distribuição de energia elétrica.

Uma vez identificados os grupos de controles do ARCiber e os seus respectivos controles básicos, a pesquisa se utilizou do método analítico qualitativo disponibilizado pelo *framework* CIS CSC para realizar a comparação entre a abrangência dos controles apresentados pelo ARCiber e aqueles definidos pelo CIS CSC para infraestruturas críticas.

A Tabela 4.1 apresentada a seguir mostra os resultados da comparação realizada entre o *framework* CIS CSC e os controles apresentados pelo ARCiber, utilizando-se a metodologia de análise qualitativa descrita no item 3.1 deste trabalho.

Tabela 4.1: Comparação entre os Controles do *framework* CIS CSC e os Controles ARCiber (RO-CB.BR.01)

CIS CSC x ARCiber				
Macrocontrole CIS CSC	**Grupo de Implementação IG1**	**Grupo de Implementação IG2**	**Grupo de Implementação IG3**	**Grupos de Segurança ARCiber**
1	Equivalent	Superset / None	None	ARCiber
2	Equivalent	Superset / None	None	Grupos3 e 6
3	None	None	None	-
4	Equivalent / None	None	None	Grupos 1, 3, 4, 5 e 6
5	Equivalent / Superset	None	None	Grupos 3 e 5
6	Equivalent / Superset	None	None	Grupos 3 e 5
7	Equivalent / Superset	None	None	Grupos 3, 4 e 6
8	Equivalent	Equivalent / None	None	Grupo 6
9	Subset	Subset	Equivalent	Grupo 1
10	Equivalent	Equivalent / Superset	Equivalent / Superset	Grupo 1
11	None	None	None	-
12	Equivalent	Equivalent / None	None	Grupos 1, 3, 4 e 5
13	-	Equivalent	Equivalent	-
14	None	None	None	-
15	None	None	None	-
16	-	None	None	-
17	Equivalent	Equivalent	None	Grupos 2 e 6
18	-	None	None	-

Fonte: [15]

4.1.1 Tratamento dos Resultados

A partir dos resultados, é possível observar que dos 18 grupos de controle do *framework* CIS CSC, apenas o grupo 9 do *framework* CIS CSC é um subset dos controles ARCiber (Tabela 2.1), ou seja, o *framework* ARCiber é mais restritivo nesse grupo de controles.

Isso é explicado por dois motivos: alguns dos controles não se aplicam ao cenário do ARCiber, e em

outros, há superação das exigências do *framework* CIS CSC visto que o ARCiber determina a segregação absoluta da arquitetura da rede de operação e a corporativa, vedando acesso à internet pelos dispositivos IEDs.

No outro extremo, tem-se que 6 dos 18 grupos de controles do CIS não tem nenhuma menção no ARCiber em nenhum dos níveis de implementação IG1, IG2 e IG3. Para esses 6 (seis) grupos verifica-se a identificação de "None" nos resultados da Tabela 4.1. São eles:

- 3 - Proteção de dados;
- 11 - Recuperação de Dados;
- 14 - Treinamento de Conscientização e Habilidades de Segurança);
- 15 - Gerenciamento de Provedor de Serviços;
- 16 - Segurança de Softwares e Aplicativos; e,
- 18 - Testes de penetração.

Isso significa que a aplicação desses controles por agentes do setor elétrico pode ser considerada opcional.

Apesar de se poder justificar a ausência da aplicação de controles do Grupo 3, já que os agentes não tratarão dados pessoais em sua maioria, a não previsão de controles dos grupos 11, 14, 15, 16 e 18 demonstra um baixo nível de maturidade na segurança cibernética do setor elétrico brasileiro. Nesse quesito é importante registrar dois pontos:

- A falta desses controles pode dificultar no sucesso na implantação de programas de segurança cibernética [101], [102], [103], [104]; e,
- Podem potencializar o impacto de riscos que porventura comprometam os discos rígidos dos equipamentos, pois não se menciona em nenhum momento para o ARCiber, a obrigatoriedade de rotinas de backup e recuperação de dados, como se prevê no Grupo de Controles 11 do *framework* CIS CSC.

Conforme define o CIS CSC, o Macrocontrole 11, associado à recuperação de dados, deve ser necessariamente considerado por todas as empresas que tenham por objetivo implantar um processo de gestão de riscos cibernéticos, independentemente do tamanho e capacidade financeira (IG1, IG2 e IG2) [15] [16].

4.1.2 Discussões Consequentes

Considerando apenas a relação de casos de ataques cibernéticos bem sucedidos apresentados na Tabela 2.3, verifica-se o grau de importância que um programa de gestão de riscos cibernéticos tem para a gestão das infraestruturas críticas [53].

Os resultados mostram que um programa de gestão de riscos cibernéticos que não abrange parte dos principais itens de controle considerados críticos, mesmo que esteja apoiado em uma infraestrutura considerada segura, deixa características de fragilidades que a qualquer momento podem ser exploradas, com consequências sérias, como as que foram verificadas na Usina Nuclear de Natanz, no Irã [55].

Lá, um simples controle de acesso à rede local foi negligenciado. Apesar da inexistência de conexões da rede interna com a Internet, a ausência de controles de acesso em portas externas dos computadores (USB) utilizados pelos técnicos da usina, submeteu toda a rede a uma contaminação muito séria pelo malware Stuxnet que se disseminou por entre os Controladores Lógicos Programáveis (CLPs) que equipavam os computadores hospedeiros do Sistema SCADA, responsáveis pela supervisão e controle das centrífugas utilizadas no processo de enriquecimento de urânio do Programa Nuclear Iraniano [55].

A existência de um criterioso programa de gestão de riscos poderia ter atuado no sentido de avaliar a sua abrangência e sua conformidade com os aspectos de segurança cibernética previstos nos padrões e *frameworks* já existentes na época.

Situações como a citada acima levaram à identificação da necessidade de se realizar a análise do ARCiber proposto pelo ONS de forma que ele pudesse ser comparado com o *framework* CIS CSC, utilizando-se da mesma metodologia que o próprio CIS utiliza para se comparar com outros *frameworks* [15].

Apesar de ser uma simplificação do *framework* NIST CSF, o *framework* CIS CSC é suficientemente abrangente [22], apesar de menos intenso em custo e esforço, para garantir a disponibilidade das salvaguardas necessárias para uma gestão de riscos cibernéticos eficiente [84].

A definição de uma regulação que obrigue um setor de infraestrutura crítica, como o setor elétrico brasileiro, a implantar e utilizar um *framework* de gestão de riscos cibernéticos é louvável [13], e assim se antecipou o ONS por meio do ARCiber, porém a sua abrangência não pode se abster de considerar as dimensões de segurança que são necessárias, mesmo que isso signifique investimentos mais robustos e a adoção de processos mais complexos por parte das empresas filiadas e dos agentes participantes desse segmento da indústria.

As fronteiras apresentadas pelo ARCiber às vezes se confundem entre a Segurança da Informação e a Segurança Cibernética. Esse aspecto pode ser um fator de múltiplas interpretações que, eventualmente, podem levar a justificar ou não a existência de importantes controles de gestão de riscos cibernéticos, situação que, a princípio, deve ser evitada. Ambos os aspectos são importantes, no entando, a gestão de riscos cibernéticos deve atuar no limite da segurança cibernética, sendo esta uma visão mais ampla do que apenas a visão da segurança da informação (integridade, confidencialidade e disponibilidade).

Os resultados mostram a identificação da categoria “None” nos resultados da Tabela 4.1 para os seguintes Macrocontroles: 3 (Proteção de dados), 11 (Recuperação de Dados), 14 (Treinamento de Conscientização e Habilidades de Segurança), 15 (Gerenciamento de Provedor de Serviços), 16 (Segurança de Softwares e Aplicativos) e 18 (Testes de penetração).

Isso nos leva ao entendimento de que a aplicação desses seis controles não identificados no ARCiber pode ser considerada opcional pelos agentes do SEB para as interfaces existentes com o ONS [15].

Apesar de a não aplicação de controles do Grupo 3 ser justificável, já que os agentes não tratarão dados pessoais em sua maioria [105], não se justifica a ausência de controles dos grupos 11, 14, 15, 16 e 18,

demonstrando um baixo nível de maturidade na segurança cibernética a que estão submetidos os aspectos operacionais de responsabilidade do ONS.

Nesse quesito, é importante registrar dois pontos: a falta desses controles pode dificultar o sucesso da implantação de programas de segurança cibernética, como já citado anteriormente, e ainda potencializar o impacto de riscos que porventura comprometam os discos rígidos dos equipamentos, pois não se menciona em nenhum momento da RO, a obrigatoriedade de rotinas de backup e recuperação de dados (Grupo 11 do *framework* CIS CSC) [106].

Quando se considera o grupo de implementação IG2, os grupos de controle 1, 2, 8, 10, 12, 13 e 17 possuem equivalência relativa, sendo que em alguns casos, os controles do CIS CSC são mais abrangentes do que o do ARCiber. Além disso, registra-se que os grupos de controle 3, 4, 5, 6, 7, 11, 14, 15, 16 e 18 não tem correspondência com o ARCiber nesse segmento do grupo de implementação.

Considerando o grupo de implementação IG3, o ARCiber não possui equivalência com a maioria dos controles, tendo alguma relação apenas nos controles dos grupos 9, 10 e 13, expondo muitas lacunas quando se consideram os controles que deveriam ser aplicados em ambientes com alto risco e criticidade [22], como o SEB.

Esses resultados demostram que o nível de controle que será exigido para o ARCiber se aproxima mais ao do grupo de implantação IG1, que conforme descrito, se aplicaria às organizações com restrições de recursos, o que não deveria ser o caso, uma vez que o ARCiber abrange empresas de médio e grande porte e atuando em um processo produtivo de alta criticidade.

4.2 AVALIAÇÃO QUALITATIVA DO SCADA DA SIEMENS WIN CC 7.5 SP2 FRENTE AO MACROCONTROLE 11 DO CIS CSC

Esta pesquisa mostra que eventuais riscos cibernéticos, caso venham a se realizar, podem de alguma forma comprometer os discos rígidos dos equipamentos do sistema SCADA, por exemplo, uma vez que não se menciona, em nenhum momento, a obrigatoriedade da existência de rotinas de backup e recuperação de dados (Grupo 11 do CIS CSC) para o ARCiber, como mostrado no item 4.1 [16].

Nesse contexto, o foco do presente trabalho se voltou à busca de informações que pudessem responder quanto a validade ou não da Hipótese 2 formulada inicialmente.

Como consequência, o esforço foi direcionado no sentido de analisar a abrangência dos procedimentos de backup e recuperação de dados do sistema SCADA da Siemens - WinCC V7.5 SP, uma vez ser ele um sistema de grande penetração no mercado de energia elétrica [107].

O objetivo dessa análise foi, portanto, avaliar se o Sistema SCADA apresenta conformidade com os controles de Recuperação de Dados definidos pelo *framework* CIS CSC e verificar, a partir dos resultados dessa avaliação, se é possível afirmar que a ausência de controles específicos para essa finalidade no ARCiber pode ser suprida por contrapartidas existentes no sistema SCADA que, de forma automática, justifique essa ausência.

Para a execução dessa análise, utilizou-se a metodologia de análise de conteúdo definida por Bar-

din [95], descrita no item 3.2, cujos resultados são apresentados a seguir.

4.2.1 A Pré-Análise das Seções de Geração e Recuperação de Dados do Manual SCADA

A Tabela 4.2 apresenta o número de ocorrências de palavras/termos de interesse, ou seja, as unidades de registro identificadas nos Capítulos 7 e 8 do Manual do Sistema SCADA da Siemens, *"Archiving Process Values"* e *"User Archive"*, respectivamente, os quais representam os capítulos que tratam dos temas da análise, unidades estas obtidas por meio do software *Word Counter* [108].

Essa estratégia foi adotada no processo de codificação da Pré-Análise para criar as unidades de registro [95]. Com isso, foram obtidas as unidades de registro mais representativas para a análise de conteúdo.

Pelo resultado, verifica-se que o Sistema SCADA apresenta, em ordem decrescente, os termos 'Configuração', 'Arquivamento', 'Backup', 'Exportar dados', 'Importar', 'Gravar', 'Redundância', 'Restaurar', 'Recuperar'. Isso permite inferir que o foco principal do processo de Recuperação de Dados para o Sistema SCADA baseia-se em primeiro lugar na Configuração do Sistema, já que o número de ocorrências desse termo é quase o dobro do segundo, como pode ser observado na Tabela 4.2.

Em seguida, aparecem aspectos associados ao 'Backup', 'Exportação' e 'Importação' de Dados.

Tabela 4.2: Unidades de Registro da Documentação

Unidades de Registro	**Número de ocorrências das Palavras**
Configuração	641
Arquivamento	315
Backup	57
Exportar dados	34
Importar	22
Gravar	13
Redundância	13
Restaurar	10
Recuperar	1

Fonte: [16]

Por meio das Unidades de Registro apresentadas na Tabela 4.2, foi possível a definição das categorias iniciais, descritas na seção a seguir.

4.2.2 Categorias Identificadas por meio da Exploração do Material

A Tabela 4.3 a seguir mostra a distribuição dessas categorias, baseando-se na significância das palavras e termos oriundos da leitura dos documentos.

Tabela 4.3: Categorias Iniciais

Número	Categorias iniciais
1	Exportar registro de dados para backup de segurança
2	Arquivamento de valores de processo
3	Arquivamento de registros de usuários e configurações
4	Backup de valores de processo
5	Backup de registros de usuário
6	Recuperar e importar dados de processo para base de produção
7	Recuperar dados de configuração do Sistema SCADA
8	Recuperar dados do usuário
9	Ciclo de arquivamento em *runtime*
10	Configurações de arquivamento de valores de processo *archiving*
11	Arquivamento sob demanda
12	Arquivamento em Inicialização e desligamento do sistema
13	Ciclo de arquivamento processo cíclico e acíclico
14	Armazenamento de dados em memória

Fonte: [16]

As categorias iniciais, apresentadas na Tabela 4.3, foram definidas a partir das unidades de registro identificadas na Tabela 4.2.

Tanto o Sistema SCADA, como a RO do ONS, sugeriram segmentos de atividades classificados pela sua importância no processo.

A partir das categorias iniciais, descritas na mesma Tabela 4.3, foram definidas três categorias finais, todas associadas ao objeto do Macrocontrole No. 11 do *framework* CIS CSC.

A Tabela 4.4 a seguir ilustra as categorias finais identificadas a partir das categorias iniciais e seus respectivos conceitos norteadores.

Tabela 4.4: Categorias Finais/Intermediárias

Categoria Final	**Conceito Norteador**	**Categoria Inicial**
Geração de Backup Externo ao Sistema SCADA Atende: CIS CSC 11.1 e 11.4	O Sistema SCADA é dotado de ferramentas responsáveis pela geração de cópias de arquivos de segurança externos ao runtime, os quais são armazenados em diretórios específicos informados por caminho a ser utilizado, podendo ser em Servidores da Rede de Comunicação de Dados ou armazenamento externo. Além da possibilidade de alta disponibilidade oferecida por um sistema com redundância (Cluster), o sistema também oferece outra via de recuperação de dados de processos e geração de backup, os quais são configurados no runtime ou gerados a partir de procedimentos manuais de exportação para arquivos externos.	(1)(2)(3)
Geração de arquivos internos ao Sistema SCADA com dados de processo e de usuários Atende: CIS CSC 11.2	Para a geração de backups de segurança, o Sistema SCADA é configurado para a geração de arquivos em tempo real de informações do processo supervisionado ou arquivos de usuários utilizados para interfaces com sistemas de proteção, comando e controle, assim como informações de interface com plataformas externas. A geração das informações de processos obedecem configurações específicas que definem os ciclos a serem utilizados automaticamente ou arquivamento por demanda operacional e local de armazenamento.	(4)(5)(9)(10) (11)(12)(13) (14)
Recuperação de arquivos do Backup Externo ao Sistema SCADA Atende: CIS CSC 11.3 e 11.5	A recuperação de dados armazenados em arquivos externos (backups) também é uma função customizável do Sistema SCADA, sendo realizada por comando interno manual configurável. Essa operação pode ser realizada por meio do método de recuperação do WinCC ou ação de importação, de forma segura e integra, utilizando arquivos gerados pelos métodos de backups internos (*runtime* em arquivos de processo e arquivos de usuário) ou externos (exportação), respectivamente.	(6)(7)(8)

Fonte: [16]

4.2.3 Tratamento dos Resultados

Essas categorias finais representam, respectivamente, um processo interno e externo de geração de backups, a geração dos arquivos internos de *runtime*, a partir dos quais os backups são gerados e, por último, o processo de recuperação de dados de processo e de usuários existentes em backup.

Pelo exposto, é possível verificar que para os Subcontroles do Macrocontrole 11 do *framework* CIS CSC, os subsídios para a sua efetiva construção e gerenciamento de recuperação de dados podem ser identificados no Sistema SCADA, independentemente de o agente definir e operar um processo formal e estruturado de backup e restauração de dados, que esteja vinculado ao processo de gestão de riscos.

Apesar da existência desses subsídios, não foi possível identificar nas funcionalidades associadas ao Backup e Recuperação de Dados do Sistema SCADA, alguma que permitisse a customização, ativação e disponibilização automática dos controles de gestão de riscos cibernéticos definidos pelo CIS CSC, com atualização automática e possibilidade de monitoramento periódico dos operadores e gestores de segurança cibernética, o que poderia justificar a ausência desses controles no ARCiber e responder afirmativamente à Hipótese 2 formulada.

4.2.4 Discussões Consequentes

Neste ponto, cabe uma importante reflexão à cerca das lacunas identificadas no ARCiber a partir da análise qualitativa realizada, utilizando-se a metodologia comparativa definida e adotada pelo CIS CSC: não haveria alguma explicação que fosse capaz de justificar as ausências de salvaguardas tão importantes para a gestão de riscos cibernéticos do SEB?

Direcionando o foco para o Macrocontrole 11 do *framework* CIS CSC, esse trabalho avaliou os motivos que eventualmente pudessem ser utilizados para justificar a sua ausência no ARCiber e, consequentemente, de seus respectivos subcontroles ou salvaguardas.

Essa avaliação procurou constatar se o Sistema SCADA conseguiria gerar os controles previstos pelo ARCiber [13], automaticamente, inserindo-os e atualizando-os no processo de recuperação de forma natural e disponibilizando-os para análises e auditorias inerentes ao processo de gestão de riscos cibernéticos de conformidade com os critérios de avaliação para cada salvaguarda específica.

A partir das informações obtidas e organizadas nas Tabelas 4.2, 4.3 e 4.4 pôde-se verificar que os subsídios necessários para a geração dos controles previstos no Macrocontrole 11 do *framework* CIS CSC estão disponíveis no Sistema SCADA, independentemente do Grupo de Implantação (IG1, IG2 e IG3).

Contudo, a construção dos respectivos controles deve ser considerada e formalizada pelo processo de gestão de riscos associado, tendo como suporte os pilares definidos pelas três dimensões básicas: tecnologia, processos e pessoas. Com isso, será possível manter a disponibilidade, a confidencialidade e a integridade das informações que serão tratadas por esses controles [75] .

As salvaguardas ou subcontroles previstos no Macrocontrole 11 do *framework* CIS CSC, ou mesmo aqueles previstos no ARCiber, não são automaticamente gerados pelo Sistema SCADA a pondo de se poder afirmar que eles não são necessários constar da relação de controles obrigatórios definidos pelo ONS [16].

A análise realizada permitiu verificar que, de fato, os aspectos sobre backup e recuperação de dados relacionados à dimensão “tecnologia” estão cobertos pelo manual do Sistema SCADA da Siemens, porém demandam necessariamente de ações adicionais no campo da gestão de riscos cibernéticos.

Nesse sentido, a implantação de um processo de backup e recuperação de dados que utilize e valide essas funcionalidades depende do planejamento e operação de cada organização. Isso inclui garantir que as pessoas consigam executar o processo conforme o que foi definido e que estejam preparadas para operar as funcionalidades de restauração de dados em caso de materialização de algum risco [16].

Para que se possa garantir a existência desse preparo, um processo de controle e verificação periódica, inerente à gestão de riscos cibernéticos, é necessário que exista e seja efetivamente testado a partir de controles específicos do processo de recuperação de dados operacionais e de usuários implantados nas instalações dos agentes operacionais do SEB.

O Setor Elétrico Brasileiro possui uma infraestrutura vital para o país, não apenas para o seu desenvolvimento econômico, mas também para a sua segurança em todos os aspectos. Nesse sentido, não se justificaria a inexistência de controles para o ARCiber definidos como críticos pelos principais Frameworks mundiais de segurança cibernética como, por exemplo, controles associados à recuperação de dados tratados no processo de supervisão, aquisição e controle operacional [16].

A perda definitiva das informações de usuários e de processos do Sistema SCADA, em tempo real, podem provocar interrupções no fornecimento de energia elétrica e um tempo de recomposição demasiadamente grande, causando grandes prejuízos aos consumidores e às empresas concessionárias.

A constatação de que 6 dos 18 grupos de controles do CIS CSC (Macrocontroles) não estão sendo considerados e sequer mencionados no ARCiber, em qualquer um dos três níveis de implementação IG1, IG2 e IG3, é preocupante [15].

5 CONCLUSÕES

A comparação realizada, utilizando avaliações qualitativas graduadas nos 18 grupos de controle do *framework* CIS CSC, constatou que apenas um grupo de controle do ARCiber superou as exigências do *framework* CIS CSC, se posicionando além nos demais.

Por outro lado, verificou-se que 6 dos 18 Macrocontroles do CIS CSC não são sequer mencionados no ARCiber (None), nem mesmo para o nível de implementação IG1, o mais básico dos três níveis previstos pelo CIS CSC.

Com base nessa constatação, pôde-se concluir que a RO oferece aos agentes do setor elétrico a opção facultativa de inserir ou não, em seus processos de gestão de riscos cibernéticos, os controles associados à Proteção de Dados, Recuperação de Dados, Treinamento de Conscientização e Habilidades de Segurança, Gerenciamento de Provedor de Serviços, Segurança de Softwares e Aplicativos e, por último, Testes de Penetração, sendo estes os Macrocontroles 3, 11, 14, 15, 16 e 18 do *framework* CIS CSC, respectivamente.

Isto nos permite concluir pela existência de uma importante lacuna no processo de gestão de riscos cibernéticos, definido pela RO proposta pelo ONS.

Essa situação se agrava quando se considera o grupo de implementação IG2, que contempla empresas de médio porte e restrição de recursos financeiros. Nesse IG2, observa-se que cerca de 40% dos Macrocontroles do CIS CSC possue equivalência relativa, e os outros 60% restantes não possuem nenhuma correspondência com o ARCiber.

Para o grupo de implementação IG3, caso do SEB, o ARCiber se mostrou ainda mais vulnerável, pois não apresentou nenhuma equivalência com a maioria dos controles, expondo muitas lacunas quando se consideram os controles que deveriam ser aplicados em ambientes com alto risco.

Os resultados obtidos nos permitem concluir que o nível de controle que será exigido para o ARCiber se aproxima mais ao nível do grupo de implantação CIS CSC - IG1, que conforme descrito, se aplicaria às organizações em geral e com restrições de recursos.

Por meio das constatações acima, conclui-se que apesar de já ser um avanço, o ARCiber elenca um conjunto de controles significativamente menor do que os mínimos necessários às infraestruturas críticas, de forma que os principais aspectos da segurança cibernética possam ser monitorados, gerenciados e tratados pelos Agentes do Setor Elétrico.

Partindo-se da análise de conteúdo realizada no manual do Sistema SCADA WinCC 7.5 SP2 da Siemens é possível concluir que, apesar de se ter verificado a existência de abrangentes funcionalidades associadas ao processo de Recuperação de Dados, que dariam ao Sistema SCADA a capacidade de subsidiar as informações necessárias às salvaguardas previstas no Macrocontrole 11 do CIS CSC, não se identificou a disponibilidade efetiva dos controles definidos por este Macrocontrole que pudessem ser automaticamente alimentados pelo SCADA, testados, arquivados e monitorados, aliviando as responsabilidades do ARCiber nesse quesito.

É importante registrar ainda que a falta de controles específicos associados ao processo de Recuperação de Dados pode dificultar sobremaneira o sucesso da implantação de programas de segurança cibernética e, ainda, potencializar o impacto de riscos que porventura comprometam os dispositivos de armazenamento de dados dos equipamentos.

Isto posto, a ausência de controles de backup e recuperação de dados no ARCiber sugere uma lacuna que deve ser enfrentada pelos agentes do SEB, esperando-se que em uma próxima versão do ARCiber o ONS possa reavaliar esse aspecto da RO.

Neste ponto, cabe destacar o papel operacional do ONS. A publicação da RO nos Procedimentos de Rede mostra a louvável preocupação do ONS com o tema da segurança cibernética e da gestão de riscos cibernéticos.

A importante iniciativa do Operador Nacional de disponibilizar um novo instrumento de gestão a ser adotado pelos agentes do SEB no segmento de segurança cibernética, que na realidade desempenha um papel regulatório que teoricamente não seria de sua responsabilidade, mas sim da ANEEL, não deve ser motivo suficiente que impeça sugestões de melhorias no ARCiber, independentemente de já ser um grande avanço.

O fato do ARCiber determinar a segregação das Redes Operativas e Corporativas, não pode e não deve ser utilizado para se justificar a implantação de um processo de gestão de riscos cibernéticos mais brando para os agentes do SEB. Inúmeros ataques bem suscedidos ao SEP foram realizados a partir da própria rede operativa, como mostrou este trabalho.

Considerando a criticidade do setor elétrico para o país e o volume de recursos destinado a ele, pode-se concluir que o nível de maturidade exigido para os controles do ARCiber, quando se verifica apenas a RO, ainda é baixo, o que demonstra que a situação não estará confortável mesmo se todos os controles previstos para os agentes do setor elétrico sejam implantados até o final de setembro de 2023.

Verifica-se, portanto, a necessidade de se ampliar o debate sobre a necessidade de revisão da RO-CB.BR.01, uma vez que foram constatadas lacunas importantes no ARCiber, quando comparado com o CIS CSC, como, por exemplo, a ausência de controles de Recuperação de Dados, dentre outros.

Por fim, esse trabalho oferece uma contribuição ao processo de avaliação dos riscos cibernéticos a que está submetida a infraestrutura crítica operacional do SEB, considerando as fronteiras de atuação do ONS e diante de suas recentes ações regulatórias.

5.1 TRABALHOS FUTUROS

Sugere-se como trabalhos futuros, as seguintes linhas de pesquisa:

- Realização de pesquisa e trabalhos acadêmicos futuros, com vistas a acompanhar e validar a implantação dos controles propostos pelo ARCiber, comparando-os com outros *frameworks* utilizados para a gestão de riscos cibernéticos em infraestruturas críticas;
- Realização de pesquisa qualitativa, visando avaliar eventuais compensações no âmbito do ARCiber,

com vistas à ausência de previsão em seu escopo de controles definidos pelos Macrocontroles 14 (Treinamento de Conscientização e Habilidades de Segurança), 15 (Gerenciamento de Provedor de Serviços), 16 (Segurança de Softwares e Aplicativos) e 18 (Testes de penetração) do CIS CSC; e,

- Estudos exploratórios futuros, baseados em entrevistas com profissionais experientes e atuantes no segmento de segurança cibernética do Setor Elétrico Brasileiro, que tratem sobre a maturidade dos agentes do SEB quanto ao uso do ARCiber, sua evolução e efetividade na mitigação de riscos cibernéticos.

REFERÊNCIAS BIBLIOGRÁFICAS

1 SIEMENS, A. G. *WinCC V7.5 SP2 WinCC/Connectivity Pack System Manual*. 2020. <https://cache.industry.siemens.com/dl/files/612/109792612/att_1051890/v1/WinCC_ConnectivityPack_en-US_en-US.pdf>. Accessed: 2022-10-11.

2 ARGHANDEH, R.; MEIER, A. von; MEHRMANESH, L.; MILI, L. On the definition of cyber-physical resilience in power systems. *Renew. Sustain. Energy Rev.*, v. 58, p. 1060–1069, 2016.

3 PARDINI, D. J.; Universidade Fumec, FACE, Belo Horizonte, MG, Brasil; HEINISCH, A. M. C.; PARREIRAS, F. S.; Universidade Fumec, FACE, Belo Horizonte, MG, Brasil; Universidade Fumec, FACE, Belo Horizonte, MG, Brasil. Cyber security governance and management for smart grids in brazilian energy utilities. *J. Inf. Syst. Technol. Manag.*, v. 14, n. 3, p. 385–400, 2017.

4 PINHEL, A.; RICERCA, G.; PATRIOTA, I. Como conciliar as ameaças cibernéticas ao setor elétrico com a realidade operacional da indústrica 4.0. *Eletroevolução - Cigre Brasil*, dez. 2018.

5 CHANDIA, R.; GONZALEZ, J.; KILPATRICK, T.; PAPA, M.; SHENOI, S. Security strategies for SCADA networks. In: *IFIP International Federation for Information Processing*. Boston, MA: Springer US, 2007. p. 117–131.

6 BISSEL, K.; PONEMON, L.; Accenture. *The Cost of Cybercrime - Ninth Annual Cost of Cybercrime Study Unloking Value of Improved Cybersecurity Protection*. 2019. <https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf>. Accessed: 2022-10-5.

7 BAEZNER, M.; ROBIN, P. *Stuxnet*. 2018. <https://www.researchgate.net/publication/323199431_Stuxnet>. Accessed: 2022-10-11.

8 PICHEL, A. *HAVEX targets industrial control systems*. 2014.

9 MUNCASTER, P. *Microsoft Zero Day Traced to Russian 'Sandworm' Hackers*. 2014. <https://www.infosecurity-magazine.com/news/microsoft-zero-day-traced-russian/>. Accessed: 2022-10-11.

10 ZETTER, K. Inside the cunning, unprecedented hack of ukraine's power grid. *Wired*, mar. 2016.

11 GREENBERG, A. 'crash override': The malware that took down a power grid. *Wired*, jun. 2017.

12 CERT-CISA. *Russian government cyber activity targeting energy and other critical infrastructure sectors*. [S.l.], 2018.

13 ONS. *Manual de Procedimentos da Operação - Módulo 5 - Submódulo 5.13, Controles mínimos de segurança cibernética para o Ambiente Regulado Cibernético, Revisao 00*. 2021. <http://www.ons.org.br/AcervoDigitalDocumentosEPublicacoes/RO-CB.BR.01_Rev.00.pdf>. Accessed: 2022-10-9.

14 ANEEL – Agência Nacional de Energia Elétrica. *Resolução Normativa ANEEL N. 964, Dispõe sobre a Política de Segurança Cibernética a ser Adotada pelos Agentes do Setor de Energia Elétrica,*. 2021. <https://www2.aneel.gov.br/cedoc/ren2021964.html>. Accessed: 2022-10-5.

15 LIMA, E.; MOREIRA, F.; DEUS, F.; NZE, G. D. A.; JUNIOR, R. T. de S.; NUNES, R. R. Avaliação da rotina operacional do operador nacional do sistema elétrico brasileiro (ONS) em relação às ações de gerenciamento de riscos associados à segurança cibernética. *RIST*, E49, p. 301–312, 2022.

16 LIMA, E.; MOREIRA, F.; ALVES, C.; NUNES, R. Gestão de riscos cibernéticos no ambiente operacional do sistema elétrico brasileiro (ARCiber ONS): uma avaliação do processo de recuperação de dados pelo sistema SCADA. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, E49, p. 313–325, 2022.

17 PLĖTA, T.; TVARONAVIČIENĖ, M.; CASA, S. D.; AGAFONOV, K. Cyber-attacks to critical energy infrastructure and management issues: overview of selected cases. *Insights into Regional Development*, v. 2, n. 3, p. 703–715, 2020.

18 NIST-CSF. *Roadmap for Improving Critical Infrastructure Cybersecurity*. 2014. <https://www.nist.gov/system/files/roadmap-021214.pdf>. Accessed: 2022-10-9.

19 Dimentional-Research. *Trends in Security Framework Adoption - A Survey of it and Security Professionals*. 2016. <https://lookbook.tenable.com/nist_csf/survey_report>. Accessed: 2022-10-9.

20 LIANG, G.; WELLER, S. R.; ZHAO, J.; LUO, F.; DONG, Z. Y. The 2015 ukraine blackout: Implications for false data injection attacks. *IEEE Trans. Power Syst.*, v. 32, n. 4, p. 3317–3318, 2017.

21 Nist-Sp; 800-39. *Managing information security risk: Organization, mission, and information system view*. Gaithersburg, MD, 2011.

22 CIS. *The 18 CIS Critical Security Controls*. 2022. <https://www.cisecurity.org/controls/cis-controls-list>. Accessed: 2022-10-8.

23 MOREIRA, F. R.; LIMA, E. D. O.; NUNES, R. R.; GIOZZA, W. F.; NZE, G. D. A. Uma análise das aplicabilidades de métodos multicritérios no contexto da segurança da informação. In: Doity (Ed.). Fortaleza CE Brasil: [s.n.], 2021.

24 BUENO, P. H. M.; MOREIRA, F. R.; LIMA, E. D. O.; NUNES, R. R. A utilização dos frameworks NIST CSF e da série NBR ABNT ISO 27.000 no contexto da gestão da segurança da informação. In: Doity (Ed.). Fortaleza CE Brasil: Doity, 2021.

25 SRIDHAR, S.; HAHN, A.; GOVINDARASU, M. Cyber–physical system security for the electric power grid. *Proc. IEEE Inst. Electr. Electron. Eng.*, v. 100, n. 1, p. 210–224, 2012.

26 LAPRIE, J.-C.; KANOUN, K.; KAANICHE, M. Modelling interdependencies between the electricity and information infrastructures. 2008.

27 HUANG, Y.-L.; CÁRDENAS, A. A.; AMIN, S.; LIN, Z.-S.; TSAI, H.-Y.; SASTRY, S. Understanding the physical and economic consequences of attacks on control systems. *Int. J. Crit. Infrastruct. Prot.*, v. 2, n. 3, p. 73–83, 2009.

28 PARKS, C. *BSAND2007-7328: Guide to critical infrastructure protection cyber vulnerability assessment*. [S.l.], 2007.

29 PERMANN, M. R.; ROHDE, K. Cyber assessment methods for SCADA security. In: OSTI (Ed.). USA: [s.n.], 2005.

30 CCEE. *Estrutura do SEB*. 2022. <https://www.ccee.org.br/governanca>. Accessed: 2022-10-12.

31 CNPE. *Conselhos e Comitês - Ministério de Minas e Energia*. 2022. <https://www.gov.br/mme/pt-br/assuntos/conselhos-e-comites/cnpe>. Accessed: 2022-10-9.

32 CMSE. *Conselhos e Comitês - Ministério de Minas e Energia*. 2022. <http://antigo.mme.gov.br/web/guest/conselhos-e-comites/cmse>. Accessed: 2022-10-9.

33 SANTOS, F. M. *Sistema elétrico brasileiro: Histórico, estrutura e análise de investimentos no setor*. Brasil: UFSC, 2015.

34 EPE. *Quem somos*. 2022. <https://www.epe.gov.br/pt/a-epe/quem-somos>. Accessed: 2022-10-9.

35 INTERNATIONAL ENERGY AGENCY. *World Energy Balances 2019*. [S.l.], 2019.

36 TOLMASQUIM, M. T. Perspectivas e planejamento do setor energético no brasil. *Estud. Av.*, v. 26, n. 74, p. 247–260, 2012.

37 ONS. *Matriz de Energia Elétrica no Brasil*. 2022. <http://www.ons.org.br/paginas/sobre-o-sin/o-sistema-em-numeros>. Accessed: 2022-10-12.

38 REIS, L. B. d. *Energia, recursos naturais e a prática do desenvolvimento sustentável*. Barueri: Ed. Manole, 2012.

39 SIQUEIRA, I. P.; CASTRO, N.; MOSZKOWICZ, M.; CÂMARA, L. *Segurança Cibernética do Setor Elétrico Brasileiro: Desafios Regulatórios e Tecnológicos*. [S.l.], 2021.

40 PAIVA, I.; CASTRO, N.; LIMA, A. P. *Aspectos Teóricos e Analíticos da Segurança Energética e os Desafios do Setor Elétrico Brasileiro*. 2017. <https://www.gesel.ie.ufrj.br/app/webroot/files/publications/26_tdse_71.pdf>. Accessed: 2022-10-9.

41 GOV, B. *Atribuições do Ministério de Minas e Energia - MME*. 2022. <https://dados.gov.br/organization/about/ministerio-de-minas-e-energia-mme>. Accessed: 2022-10-13.

42 EsferaEnergia. *Entenda o papel do Ministério de Minas e Energia (MME)*. 2021. <https://esferaenergia.com.br/blog/mercado-livre-de-energia/ministerio-minas-energia/>. Accessed: 2022-10-13.

43 MME-CGD. *Comitê de Governança Digital - Ministério de Minas e Energia*. 2019. <http://antigo.mme.gov.br/web/guest/todas-as-noticias/-/asset_publisher/pdAS9IcdBICN/content/ministerio-de-minas-e-energia-institui-comite-de-governanca-digit-1>. Accessed: 2022-10-13.

44 ABRATE. *Diretrizes de cibersegurança no setor elétrico - Ações CNPE*. [S.l.]: ABRATE - Associação Brasileira das Empresas de Transmissão de Energia Elétrica, 2021. <https://abrate.org.br/cnpe-cria-gt-para-discutir-diretrizes-de-ciberseguranca-no-setor-eletrico/>. Accessed: 2022-10-13.

45 CNPE-CGDMME. *Diretrizes sobre segurança cibernética no setor elétrico*. 2021. <https://www.gov.br/mme/pt-br/assuntos/noticias/cnpe-destaca-licitacao-dos-volumes-excedentes-ao-contrato-de-cessao-onerosa-e-diretrizes-sobre-seguranca-cibernetica Accessed: 2022-10-13.

46 CNPE-RES. *Diretrizes sobre Segurança Cibernética para o Setor Elétrico*. 2021. <http://www.gov.br/mme/pt-br/assuntos/conselhos-e-comites/cnpe/resolucoes-do-cnpe/resolucoes-2021/ResoluoCNPE24_2021.pdf>. Accessed: 2022-10-13.

47 ONS-Institucional. *O que é ONS*. 2022. <http://www.ons.org.br/paginas/sobre-o-ons/o-que-e-ons>. Accessed: 2022-10-13.

48 ONS-Governança. *Governança do ONS - Visão Geral*. 2022. <http://www.ons.org.br/paginas/sobre-o-ons/governanca/visao-geral>. Accessed: 2022-10-13.

49 ONS-Organograma. *Estrutura Organizacional do ONS*. 2022. <http://www.ons.org.br/Paginas/Noticias/20171108-reestruturacaoorganizacional.aspx>. Accessed: 2022-10-13.

50 ONS - Procedimentos de Rede - Submódulo 19.1 - Identificação, tratamento e penalidades para as não conformidades. [S.l.], 2009.

51 LEE, K.-B.; LIM, J.-I. Lightweight acknowledgement-based method to detect misbehavior in MANETs. *KSII Trans. Internet Inf. Syst.*, v. 10, n. 2, p. 857–880, 2016.

52 GREIMAN, V. The winds of change in world politics and the impact on cyber stability. *Int. j. cyber warf. terror.*, v. 9, n. 4, p. 27–43, 2019.

53 HEMSLEY, K. E.; FISHER, D. R. E. *History of industrial control system cyber incidents*. [S.l.], 2018.

54 ZETTER, K. *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. [S.l.]: The Crown Publishing Group, 2014.

55 KEIZER, G. *Is Stuxnet the 'best' malware ever?* 2010. <https://www.computerworld.com/article/2515757/is-stuxnet-the--best--malware-ever-.html>. Accessed: 2022-10-9.

56 PATIL, A.; SHINDE, S.; BANERJEE, S. Stuxnet-tool for zero-day attack. In: *Handbook of Research on Cyber Crime and Information Privacy*. Hershey, PA: IGI Global, 2020. p. 652–675.

57 LOPES, G. V.; OLIVEIRA, C. F. J. d. STUXNET E DEFESA CIBERNÉTICA ESTADUNIDENSE à LUZ DA ANÁLISE DE POLÍTICA EXTERNA. *Rev. Bras. Estud. Def.*, v. 1, n. 1, 2014.

58 ICS-CERT. *Advisory (ICSA-10-238-01B): Stuxnet malware mitigation (update B)*. 2014. <https://www.cisa.gov/uscert/ics/advisories/ICSA-10-238-01B>. Accessed: 2022-10-9.

59 SANTOS, F.; PEREIRA, M. Uma abordagem prática do iec61850 para automação, proteção e controle de subestações. In: Simpase (Ed.). [S.l.]: VII SIMPASE, 2007.

60 ZHOU, X.; XU, Z.; WANG, L.; CHEN, K.; CHEN, C.; ZHANG, W. APT attack analysis in SCADA systems. *MATEC Web Conf.*, v. 173, p. 01010, 2018.

61 WANYING, Q.; WEIMIN, W.; SURONG, Z.; YAN, Z. The study of security issues for the industrial control systems communication protocols. In: *Proceedings of the 2015 Joint International Mechanical, Electronic and Information Technology Conference*. Paris, France: Atlantis Press, 2015. p. 693–698.

62 Protocol 46. *HAVEX Malware is on the Hunt for ICS & SCADA Systems*. [S.l.]: Protocol 46, 2014. <https://protocol46.com/havex-malware-is-on-the-hunt-for-ics-scada-systems/>. Accessed: 2022-10-9.

63 POLITYUK, P. Ukraine to probe suspected russian cyber attack on grid. *Reuters*, Reuters, dez. 2015.

64 ZETTER, K. Everything we know about ukraine's power plant hack. *Wired*, jan. 2016.

65 CHEREPANOV, A. *WIN32/INDUSTROYER: A new threat for industrial control systems*. 2017. <https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf>. Accessed: 2022-10-8.

66 Dragos. *Analysis of the threat to electric grid operations*. 2017. <http://www.dragos.com/blog/crashovdrride/CrashOverride-01.pdf>. Accessed: 2022-10-9.

67 DHS-US-SEDRT. *Alert (TA17-163): CRASHOVERRIDE malware*. 2017. <http://www.us-cert.gov/ncast/alerts/TA17-163A>. Accessed: 2022-10-8.

68 STOUFFER, K.; PILLITTERI, V.; LIGHTMAN, S.; ABRAMS, M.; HAHN, A. *SP 800-82 Guide to industrial control systems (ICS) security*. [S.l.], 2015.

69 DHS-NCCIC. *Industrial Control Systems Cyber Emergency Response Team*. 2014. <https://www.cisa.gov/uscert/sites/default/files/Annual_Reports/Year_in_Review_FY2014_Final.pdf>. Accessed: 2022-10-8.

70 SRIVASTAVA, A.; MORRIS, T.; ERNSTER, T.; VELLAITHURAI, C.; PAN, S.; ADHIKARI, U. Modeling cyber-physical vulnerability of the smart grid with incomplete information. *IEEE Trans. Smart Grid*, v. 4, n. 1, p. 235–244, 2013.

71 NIST. *A tool for improving privacy through enterprise risk management, version 1.0*. Gaithersburg, MD, 2020.

72 SUN, C.-C.; HAHN, A.; LIU, C.-C. Cyber security of a power grid: State-of-the-art. *Int. j. electr. power energy syst.*, v. 99, p. 45–56, 2018.

73 BRIESEMEISTER, L.; CHEUNG, S.; LINDQVIST, U.; VALDES, A. Detection, correlation, and visualization of attacks against critical infrastructure systems. In: *2010 Eighth International Conference on Privacy, Security and Trust*. [S.l.]: IEEE, 2010. p. 15–22.

74 DHS-CISA. *Common cybersecurity vulnerabilities in industrial control systems*. 2011. <https://www.cisa.gov/uscert/sites/default/files/recommended_practices/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf>. Accessed: 2022-10-8.

75 NAKAMURA, E. T.; GEUS, P. L. de. *Segurança de Redes em Ambientes Cooperativos*. [S.l.]: Novatec Editora, 2007.

76 CARDENAS, A. A.; AMIN, S.; SINOPOLI, B.; GIANI, A.; PERRIG, A.; SASTRY, S. *Challenges for Securing Cyber Physical Systems*. 2009. <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.152.5198&rep=rep1&type=pdf>. Accessed: 2022-10-8.

77 HUMAYED, A.; LIN, J.; LI, F.; LUO, B. Cyber-physical systems security—a survey. *IEEE Internet Things J.*, v. 4, n. 6, p. 1802–1831, 2017.

78 AMIN, S. M. Electricity infrastructure security: Toward reliable, resilient and secure cyber-physical power and energy systems. In: *IEEE PES General Meeting*. [S.l.]: IEEE, 2010.

79 ISO/IEC. *ISO/IEC 27001:2005*. [S.l.], 2013.

80 GANZER, M. *What is the NIST Cybersecurity Framework?* [S.l.]: Verve Industrial Protection, 2022. <https://verveindustrial.com/resources/what-is-the-nist-cybersecurity-framework-thank-you/?submissionGuid=7b93f84a-e311-4a9d-9226-f5b996402814>. Accessed: 2022-10-9.

81 ISA. *ISA-62443-2-1-2009, Security for industrial automation and control systems part 2-1: Establishing an industrial automation and control systems security program*. 2009. <https://www.isa.org/products/isa-62443-2-1-2009-security-for-industrial-automat>. Accessed: 2022-10-9.

82 ISA. *ANSI/ISA-62443-3-3 (99.03.03)-2013 Security for industrial automation and control systems Part 3-3: System security requirements and security levels*. 2013. <https://www.isa.org/products/ansi-isa-62443-3-3-99-03-03-2013-security-for-indu>. Accessed: 2022-10-15.

83 SHAMMA, B. *Implementing CIS Critical Security Controls for Organizations on a Low-Budget*. Dissertação (Mestrado) — University of Houston, USA, 2018.

84 MCCLAIN, S. *Auditing, assessing, analyzing: A prioritized approach using the Pareto principle*. 2018. <https://www.cisecurity.org/wp-content/uploads/2018/01/Pareto-Principle.pdf>. Accessed: 2022-10-15.

85 IBRAHIM, A.; VALLI, C.; MCATEER, I.; CHAUDHRY, J. A security review of local government using NIST CSF: a case study. *J. Supercomput.*, v. 74, n. 10, p. 5171–5186, 2018.

86 ALCARAZ, C.; ZEADALLY, S. Critical infrastructure protection: Requirements and challenges for the 21st century. *Int. J. Crit. Infrastruct. Prot.*, v. 8, p. 53–66, 2015.

87 CLEVELAND, F. M. Cyber security issues for advanced metering infrasttructure (AMI). In: *2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*. [S.l.]: IEEE, 2008. p. 1–5.

88 CARDENAS, A. A.; AMIN, S.; SASTRY, S. Secure control: Towards survivable cyber-physical systems. In: *2008 The 28th International Conference on Distributed Computing Systems Workshops*. [S.l.]: IEEE, 2008. p. 495–500.

89 PLIATSIOS, D.; SARIGIANNIDIS, P.; LAGKAS, T.; SARIGIANNIDIS, A. G. A survey on SCADA systems: Secure protocols, incidents, threats and tactics. *IEEE Commun. Surv. Tutor.*, v. 22, n. 3, p. 1942–1976, 2020.

90 DANEELS, A.; SALTER, W. What is SCADA. In: . Trieste, Italy: International Conference on Accelerator and Large Experimental Physics Control Systems, 1999.

91 VERGARA, S. C. *Projetos e Relatorios de Pesquisa em Administração*. 1998. <https://www.passeidireto.com/arquivo/38301433/vergara-sylvia-constant-projetos-e-relatorios-de-pesquisa-em-administracao>. Accessed: 2022-10-12.

92 SILVA, E.; MENEZES, E. *Metodologia de pesquisa e elaboração de teses e dissertações*. 2005. <https://tccbiblio.paginas.ufsc.br/files/2010/09/024_Metodologia_de_pesquisa_e_elaboracao_de_teses_e_dissertacoes1.pdf>. Accessed: 2022-10-30.

93 MARCONI, M.; LAKATOS, E. *Fundamentos de Metodologia Científica*. São Paulo: Editora Atlas, 2003.

94 PRODANOV, C. C.; FREITAS, E. C. de. *Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico*. Rio Grande do Sul: Universidade FEEVALE, 2013.

95 BARDIN, L. *Análise de Conteúdo*. São Paulo: Edições 70, 2011.

96 FRANCO, M. *Análise de conteúdo*. [S.l.]: Brasília Liber Livro, 4a Ed., 2021.

97 MOZZATO, A. R. *Análise de Conteúdo como Técnica de Análise de Dados Qualitativos no Campo da Administração: Potencial e Desafios*. 2011. <https://www.scielo.br/j/rac/a/YDnWhSkP3tzfXdb9YRLCPjn/?lang=pt&format=pdf>. Accessed: 2022-10-16.

98 SILVA, A.; FOSSÁ, M. *ANÁLISE DE CONTEÚDO: EXEMPLO DE APLICA*

CÃO DA TÉCNICA PARA ANÁLISE DE DADOS QUALITATIVOS. 2015. <http://www.fei.am.gov.br/wp-content/uploads/2020/06/2113-7552-1-PB.pdf>. Accessed: 2022-10-16.

99 MENDES, R. M.; MISKULIN, R. G. S. A análise de conteúdo como uma metodologia. *Cad. Pesqui.*, v. 47, n. 165, p. 1044–1066, 2017.

100 GALVÃO, M. *Segurança Cibernética com o CIS Critical Security Controls - versão 8*. [S.l.], 2021.

101 MUFLIHAH, Y.; SUBRIADI, A. P. A basic element of IT business continuity plan: Systematic review. *JURNAL INFORMATIKA*, v. 12, p. 17–23, 2018.

102 AL-DAEEF, M. M.; BASIR, N.; MOHD, M. Security awareness training : A review. In: . [S.l.: s.n.], 2016.

103 THOMAS, T. W.; TABASSUM, M.; CHU, B.; LIPFORD, H. Security during application development: An application security expert perspective. In: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: ACM, 2018.

104 KHERA, Y.; KUMAR, D.; Sujay; GARG, N. Analysis and impact of vulnerability assessment and penetration testing. In: *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*. [S.l.]: IEEE, 2019. p. 525–530.

105 LEI 13709/18 - LGPD. 2018. <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Accessed: 2022-10-31.

106 FENG, N.; WANG, M.; LI, M.; LI, D. Effect of security investment strategy on the business value of managed security service providers. *Electron. Commer. Res. Appl.*, v. 35, n. 100843, p. 100843, 2019.

107 Siemens, Inc. *SIMATIC SCADA WINCC Software*. 2021. <https://new.siemens.com/br/pt/produtos/software/industria/automacao/scada.html>. Accessed: 2022-10-31.

108 Countwordsfree. *Text Processing Tools - Words and characters counter*. 2022. <https://countwordsfree.com/>. Accessed: 2022-10-8.