UNIVERSIDADE DA INTEGRAÇÃO INTERNACIONAL DA LUSOFONIA AFRO-BRASILEIRA

INSTITUTO DE ENGENHARIAS E DESENVOLVIMENTO SUSTENTÁVEL

CURSO DE GRADUAÇÃO EM ENGENHARIA DE ENERGIAS

MOISÉS QUINTA ALBERTO IALÁ

ANÁLISE DOS DESAFIOS DE SEGURANÇA CIBERNÉTICA NAS ESTACÕES DE ENERGIA E PERSPECTIVAS

REDENÇÃO

2024

MOISÉS QUINTA ALBERTO IALÁ

ANÁLISE DOS DESAFIOS DE SEGURANÇA CIBERNÉTICA NAS ESTACÕES DE ENERGIA E PERSPECTIVAS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia de Energias do INSTITUTO DE ENGENHARIAS E DESENVOLVIMENTO SUSTENTÁVEL da Universidade da Integração Internacional da Lusofonia Afro-Brasileira, como requisito parcial à obtenção do grau de bacharel em Engenharia de Energias.

Orientador: Prof. Dr. Sabi Yari Moïse BANDIRI

REDENÇÃO

2024

Universidade da Integração Internacional da Lusofonia Afro-Brasileira
Sistema de Bibliotecas da UNILAB
Catalogação de Publicação na Fonte.

Ialá, Moisés Quinta Alberto.

I11a

Análise dos desafios de segurança cibernética nas estacões de energia e perspectivas / Moisés Quinta Alberto Ialá. - Redenção, 2024.
83f: il.

Monografia - Curso de Engenharia De Energias, Instituto De Engenharias E Desenvolvimento Sustentável, Universidade da Integração Internacional da Lusofonia Afro-Brasileira, Redenção, 2024.

Orientador: Prof. Dr. Sabi Yari Moïse Bandiri.

1. Cibersegurança. 2. Ataques. 3. Setor elétrico. 4. Desafios. 5. Diretrizes e regulamentação. I. Título

CE/UF/BSCA CDD 003.5

MOISÉS QUINTA ALBERTO IALÁ

ANÁLISE DOS DESAFIOS DE SEGURANÇA CIBERNÉTICA NAS ESTACÕES DE ENERGIA E PERSPECTIVAS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia de Energias do INSTITUTO DE ENGENHARIAS E DESENVOLVIMENTO SUSTENTÁVEL da Universidade da Integração Internacional da Lusofonia Afro-Brasileira, como requisito parcial à obtenção do grau de bacharel em Engenharia de Energias.

Aprovada em:

BANCA EXAMINADORA

Prof. Dr. Sabi Yari Moïse BANDIRI (Orientador)
Universidade da Integração Internacional da Lusofonia Afro-Brasileira (UNILAB)

Prof. Dr. CÍCERO SARAIVA SOBRINHO
Universidade da Integração Internacional da Lusofonia Afro-Brasileira (UNILAB)

Prof. Dr. ALLBERSON BRUNO DE OLIVEIRA DANTAS
Universidade da Integração Internacional da Lusofonia Afro-Brasileira (UNILAB)

Famílias,

Não há palavras suficientes para expressar o quanto sou grato por todo o amor, apoio e incentivo que me deram ao longo dessa jornada acadêmica. Vocês estiveram ao meu lado em todos os momentos, ajudando-me a superar os desafios e celebrando cada uma das minhas conquistas.

Este trabalho de conclusão de curso representa muito mais do que um simples documento acadêmico. Ele é uma prova do meu comprometimento e dedicação, mas também é uma homenagem ao papel fundamental que cada um de vocês desempenha em minha vida.

Mamae, obrigado por ser minha melhor amiga e me ensinar a importância da perseverança e da paciência. **Pai**, obrigado por me inspirar com seu amor pela educação e pela aprendizagem constante. **Irmãos/as,** obrigado por me fazerem rir e lembrarem-me da importância de manter um equilíbrio saudável entre o trabalho, escola e a diversão. **B. Júnior**, é só questão de tempo, estarás no meu colo, meu rei.

Sei que não teria chegado até aqui sem vocês, e é com muito orgulho e gratidão que dedico este trabalho a cada um de vocês. Espero que ele possa, de alguma forma, retribuir tudo o que vocês fizeram por mim ao longo desses anos.

Com amor e carinho,

Biwotidem Iala na Funghn-na.

AGRADECIMENTOS

Primeiro Agradeço a Deus pela vida que me deu, pela proteção e pela saúde e por estar comigo esse tempo todo;

ABENE NGHALA NI BI MAM BA NA FUNGHN-NA, BA WOT IUNGE GI NBINE KATI KINBODA, WA BA NGA BIN TO TONGH-NA BINHAM KISIF TE MBINI SIFNI.

Titiu GUERRA INDAMI, a gei ge u nkei gana a uil te nguine abdo, u ma ka rasa sate nbe ftinkir a botchi ni Bintoe.

Um agradecimento muito especial para os meus pais, que sempre acreditaram em mim, mesmo passando por dificuldades mas apostaram na minha formação por isso hoje **NHIN-NA IALA NA FUNGHN-NA E BINTOE-AN NA GABE, N gi ba ia ABENE**. Não só por serem meus pais, mas sim por ser melhores pais do mundo.

Aos meus irmãos, irmas e sobrinhos, que nos momentos de minha ausência dedicados ao estudo superior, sempre fizeram entender que o futuro é feito a partir da constante dedicação no presente!

Familia Naualna, abos i nha firkidja, kil ku Deus i da bos pa i multiplikal kada bias mas pabia kil ku bo fasi pa mi i ka tene midida.

Ao Prof. Dr. Sabi Yari Moïse BANDIRI pelo seu tempo, dedicação e orientação valiosa ao longo de todo o processo de pesquisa. Seu feedback e direcionamento foram cruciais para o sucesso deste trabalho.

A Unilab, pela oportunidade de cursar um curso superior numa Universidade Pública Federal do Brasil, pelos recursos e infraestrutura que me foram fornecidos, e pela oportunidade de estudar e me desenvolver academicamente.

Agradeço a todos os elementos de MCI pela força e bons momentos que passamos nessa Universidade, sem vocês essa jornada não seria diferente de um cativeiro.

Agradeço a todos os professores que de qualquer forma me proporcionar o conhecimento não apenas racional, mas a manifestação do caráter e afetividade da educação durante esse processo de formação profissional, por tanto que se dedicaram a mim, não somente por terem me ensinado, mas por terem me feito aprender.

Cybersecurity is embedded in everything we do.
If it's connected, it's a risk.

(Karen Evans)

RESUMO

O artigo aborda a analise dos desafios de segurança cibernética nas estações e subestações de energias e perspectivas para mitigar ataques cibernéticos. Com o objetivo de analisar as principais ameaças cibernéticas que afetam infraestruturas críticas de energia e propor soluções para reduzir a vulnerabilidade. A metodologia utilizada foi a revisão bibliográfica narrativa, que envolve a coleta e análise de informações de livros, artigos científicos, dissertações e teses, tanto nacionais quanto internacionais. O estudo identifica diversos tipos de ataques cibernéticos, como malwares, que podem comprometer a operação segura das estações de energia. Foram analisadas as práticas de segurança adotadas pelas estações, bem como o nível de segurança dos softwares de automação e controle. Além disso, o trabalho examina a adequação das diretrizes e normas de segurança para o setor elétrico brasileiro, comparando-as com as práticas em outros países. Os resultados mostram que, embora várias medidas de segurança tenham sido tomadas, ainda há grandes lacunas que precisam ser corrigidas para garantir uma proteção adequada contra ciberataques. As descobertas mostram que para combater com sucesso as ameaças cibernéticas, são necessárias melhorias contínuas nas práticas de segurança, maior investimento em tecnologias emergentes e cooperação internacional.

Palavras-chave: Cibersegurança. Ataques. Setor Elétrico. Desafios. Diretrizes e Regulamentação.

ABSTRACT

The article addresses the analysis of cybersecurity challenges in energy stations and substations, and perspectives for mitigating cyberattacks. The objective is to analyze the main cyber threats affecting critical energy infrastructures and propose solutions to reduce vulnerabilities. The methodology used was a narrative literature review, involving the collection and analysis of information from books, scientific articles, dissertations, and theses, both national and international. The study identifies various types of cyberattacks, such as malware, that can compromise the safe operation of energy stations. The security practices adopted by the stations, as well as the security level of automation and control software, were analyzed. Additionally, the work examines the adequacy of security guidelines and standards for the Brazilian electric sector, comparing them with practices in other countries. The results show that, although several security measures have been taken, there are still significant gaps that need to be addressed to ensure adequate protection against cyberattacks. The findings indicate that to successfully combat cyber threats, continuous improvements in security practices, greater investment in emerging technologies, and international cooperation are necessary.

Keywords: Cybersecurity. Attacks. Electrical Sector. Challenges. Guidelines and Regulation

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABRADEE	Associação Brasileira de Distribuidores de Energia Elétrica
ABRATE	Associação Brasileira das Empresas de Transmissão de Energia Elétrica
ANEEL	Agência Nacional de Energia Elétrica
ANSSI	Agência Nacional de Segurança dos Sistemas de Informação
APF	Administração Pública Federal
APTs	Ameaças Persistentes Avançadas
AT	Alta Tensão
BES	*Bulk Electric System*
BT	Baixa Tensão
CCEE	Câmara de Comercialização de Energia Elétrica
CEER	*COUNCIL OF EUROPEAN ENERGY REGULATORS*
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CGSI	Comitê Gestor da Segurança da Informação
CIA	*Confidentiality, Integrite and Availability* / Confidencialidade, Integridade e Disponibilidade
CIP	*Critical Infrastructure Protection*
CMSE	Comitê de Monitoramento do Setor Elétrico
CNIIP	Proteção de Infraestrutura Nacional de Informação Crítica /*Critical National Information Infrastructure Protection*
CNPE	Conselho Nacional de Política Energética
COP	Proteção Online de Crianças/ *Children Online Protection*
CS	Cibersegurança
CTIR Gov	Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo
DNS	*Domain Name System* / Sistema de Nomes de Domínio
DoS/DDoS	ataques de Negação de Serviço Distribuídos / *Denial-of-Service or Distributed Denial-of-Service*
DSC	Departamento de Segurança de Cibernética
E-Ciber	Estratégia Nacional de Segurança da Informação
EAT	Extra Alta Tensão
EE	Estação de Energia

ENISA	*European Network and Information Security Agency*
ENSIC	Estratégia Nacional de Segurança de Infraestruturas Críticas
ENTSO-E	The European Network of Transmission System Operators for Electricity
EPE	Empresa de Pesquisa Energética
FERC	*Federal Energy Regulatory Commission*
GESEL	Grupo de Estudos do Setor Elétrico
GOOSE	Generic Object Oriented Substation Event)
GSI	Gabinete de Segurança Institucional
IA	Inteligencia Artificial
ICS	*Industrial Control Systems*
IEC	*International Electrotechnical Commission*
IEDs	*Intelligent Electronic Devices* / Dispositivos Eletrônicos Inteligentes
IoT	*Internet of Things* / Internet das Coisas
ISO	*International Organization for Standardization*
LAN	*Local Area Network* / Rede Local
LGPD	Lei Geral de Proteção de Dados
MME	Ministério de Minas e Energia
MMS	Manufacturing Message Specification)
MT	Média Tensão
NCPF	*National Cybersecurity Policy Framework*
NCSC	Centro Nacional de Segurança Cibernética/*National Cyber Security Centre*
NERC	*North American Electric Reliability Corporation*
NERC	Comissão Reguladora de Eletricidade da Nigéria / *Nigerian Electricity Regulatory Commission*
NIS	*Network and Information Security*
NIST	*National Institute of Standards and Technology*
NITDA	Agência Nacional de Desenvolvimento de Tecnologia da Informação / *National Information Technology Development Agency*
ONS	Operador Nacional do Sistema Elétrico
OT	Tecnologia Operacional/ *Operational Technology*
PERA	*Purdue Enterprise Reference Architecture and Methodology*
PLANSIC	Plano Nacional de Segurança de Infraestruturas Críticas

PLC	*Programmable Logic Controller* / Controladores Lógicos Programáveis
PNSI	Política Nacional de Segurança da Informação
PNSIC	Política Nacional de Segurança de Infraestruturas Críticas
PwC	*PricewaterhouseCoopers*
RGPD	Regulamento Geral sobre a Proteção de Dados / *General Data Protection Regulation*
RTUs	*Remote Terminal Units* / Unidades Terminais Remotas
SCADA	*Supervisory Control and Data Acquisition* / Sistema de Supervisão, Controle e Aquisição de Dados
SE	Subestação de Energia
SEP	Sistema de Elétrico de Potência
SGDSN	Secretário-Geral da Defesa e Segurança Nacional
SI	Segurança de Informação
SIDSIC	Sistema Integrado de Dados de Segurança de Infraestruturas Críticas
SIN	Sistema Interligado Nacional
SSIC	Secretaria de Segurança da Informação e Cibernética
TI	Tecnologia de Informação/*Information Technology*
TIC	Tecnologia de Informação e Comunicação

LISTA DE SÍMBOLOS

kV	kilo volts ou quilo volts

SUMÁRIO

1 INTRODUÇÃO

Este trabalho aborda a Analise dos Desafios de Segurança Cibernética nas Estações e Subestações de Energias e Perspectivas, destacando a importância de uma abordagem integrada para garantir a proteção das redes operacionais e a continuidade dos serviços de energia. A análise será centrada nas práticas de segurança cibernética, na adequação das normas e diretrizes existentes e nas possíveis consequências de ataques bem-sucedidos assim como as perspectivas para o setor até no ano de 2023.

A cibersegurança nas empresas de energia tornou-se uma preocupação crescente nos últimos anos devido ao aumento significativo de ataques cibernéticos direcionados a infraestruturas críticas.

As empresas de energia, devido à natureza de suas operações, são alvos atrativos para cibercriminosos . A análise das práticas de segurança nas estações de energia é essencial para entender o nível de vulnerabilidade e as possíveis melhorias que podem ser implementadas destacando assim a necessidade de um estudo detalhado sobre a segurança das infraestruturas energéticas, focando nas tecnologias utilizadas e nas estratégias de mitigação de riscos.

O setor de energia é um dos pilares da infraestrutura crítica de qualquer nação. A dependência crescente de sistemas digitais para controlar e monitorar operações tornou esses sistemas alvos atraentes para ciberataques. Segundo Glenn *et al.* (2016), a vulnerabilidade do setor elétrico à ameaças cibernéticas é uma questão de segurança nacional devido ao impacto potencial de interrupções no fornecimento de energia e destaca a necessidade de uma análise aprofundada das ameaças e vulnerabilidades específicas do setor elétrico.

Dada a interconexão cada vez maior das redes elétricas com a Internet e a crescente ameaça de ciberataques, os autores como Eric Meyer and Michael Montoya (2022); Campos (2023) assim como Farias (2024) destacam a importância de medidas proativas para proteger infraestruturas críticas contra ameaças cibernéticas, garantindo a confiabilidade e disponibilidade do sistema elétrico. A análise das práticas de segurança das estações de energia revela que há uma necessidade urgente de melhorias. Estudos recentes indicam que muitas dessas estações utilizam *softwares* de automação e controle que não estão adequadamente protegidos contra ciberataques. Essa vulnerabilidade tornou-se maior pela falta de atualização regular dos sistemas e pela ausência de treinamentos específicos para os operadores.

Um dos principais desafios enfrentados pelas empresas de energia é a presença de sistemas legados que não foram projetados com a segurança cibernética em mente. De acordo

com (FREIRE, 2021a), a automação industrial possui equipamentos antigos sem *patches*, com protocolos que não possuem autenticação, autorização ou criptografia. Esses sistemas, essenciais para o funcionamento das redes de energia, são altamente vulneráveis a ataques que exploram essas fraquezas. Os dispositivos críticos, como os Dispositivos Eletrônicos Inteligentes (DEIs), Unidades Terminais Remotas (UTRs) e Controladores Lógicos Programáveis (PLCs), foram desenvolvidos antes da era da cibersegurança e, portanto, carecem de medidas de proteção robustas.

Como mencionado no artigo de (FREIRE, 2021a), esses equipamentos não foram projetados com conceitos de segurança como parte de sua operação isso os torna alvos fáceis para invasores que buscam comprometer a operação das redes de energia. A identificação dessas ameaças é o primeiro passo para a implementação de medidas de segurança eficazes. Além disso, a adequação das normas e diretrizes de segurança é crucial para garantir a proteção das infraestruturas críticas, pois a modernização e a padronização das práticas de segurança são essenciais para criar um ambiente seguro e resiliente contra ciberataques.

Mukherjee (2019) argumenta que a modernização das práticas de segurança não deve ser vista apenas como uma questão técnica, mas também como um processo que envolve a reestruturação de políticas e a ressignificação dos elementos da vida material dos trabalhadores envolvidos. Essa abordagem holística é necessária para garantir que as medidas de segurança sejam efetivamente implementadas e mantidas. Os ataques cibernéticos bem-sucedidos contra infraestruturas de energia podem ter consequências devastadoras. Um exemplo disso é o *malware Double Pulsar*, que foi identificado em subestações e mostrou capacidade de se mover lateralmente entre diferentes subestações sem intervenção humana, aumentando significativamente o risco de comprometer grandes áreas de rede (FREIRE, 2021a).

Para mitigar esses riscos, é essencial que as empresas de energia adotem práticas de segurança cibernética robustas e sigam regulamentações rigorosas. Ações coordenadas entre governo, empresas e órgãos reguladores são fundamentais para mitigar os riscos e garantir a resiliência das redes elétricas. A implementação de criptografia e autenticação nos protocolos de comunicação das subestações, embora desafiadora, é uma medida crucial.

Adicionalmente, a conformidade com normas internacionais de segurança, como as estabelecidas pela *North American Electric Reliability Corporation* (NERC) e o *National Institute of Standards and Technology* (NIST), pode ajudar as empresas de energia a melhorar sua postura de segurança como revela Alexandre Freire (2021) que os controles para reduzir

riscos e aumentar a resiliência cibernética do setor não são pautados por regulamentações.

A comparação das práticas de segurança adotadas no Brasil com aquelas de outros países pode revelar lacunas e oportunidades de melhoria, contribuindo para o desenvolvimento de estratégias mais eficazes.

1.1 JUSTIFICATIVA

A análise dos desafios cibernéticos nas estações de energia é fundamental para garantir a resiliência e a segurança dessas infraestruturas críticas. Este estudo visa identificar as principais ameaças e vulnerabilidades, avaliar as melhores práticas e tecnologias emergentes para a proteção cibernética e propor recomendações para a implementação de estratégias de defesa eficazes. A crescente digitalização das infraestruturas de energia trouxe consigo inúmeros benefícios, como a melhoria da eficiência operacional e a capacidade de gestão em tempo real. Contudo, essa transformação também expôs essas infraestruturas a novos e complexos desafios cibernéticos. Estações de energia, componentes cruciais para a economia e a segurança nacional, estão agora sob constante ameaça de ataques cibernéticos, que podem resultar em interrupções de serviço, danos físicos e impactos econômicos severos (LEWIS, 2006).

A relevância deste estudo é sublinhada pela frequência e sofisticação crescentes dos ataques cibernéticos contra infraestruturas críticas incluindo o setor elétrico. Incidentes notáveis, como o ataque à rede elétrica da Ucrânia em 2015, demonstram a vulnerabilidade dessas infraestruturas e as graves consequências que podem advir de um ataque cibernético bem-sucedido. Esse evento resultou na interrupção do fornecimento de energia para centenas de milhares de pessoas, evidenciando a necessidade urgente de fortalecer a segurança cibernética nas estações de energia (LEE *et al.*, 2016).

Adicionalmente, a crescente dependência de tecnologias digitais como a Internet das Coisas (IoT) e os Sistemas de Controle Industrial nas operações das estações de energia aumenta a superfície de ataque cibernético. Essas tecnologias, embora melhorem a eficiência e a integração das redes de energia, introduzem novas vulnerabilidades que podem ser exploradas por agentes maliciosos como afirma Karnouskos (2011). Portanto, a análise detalhada dessas ameaças e a implementação de estratégias de mitigação são essenciais para proteger as infraestruturas de energia.

A segurança das infraestruturas críticas de energia é uma questão de segurança nacional. Ataques cibernéticos podem causar interrupções significativas nos serviços essenciais,

afetar a economia e comprometer a segurança dos cidadãos. Proteger as estações de energia contra tais ameaças é, portanto, de vital importância para garantir a estabilidade e a segurança nacional (RID; BUCHANAN, 2015).

Além dos riscos operacionais e de segurança, há também implicações econômicas significativas associadas a ataques cibernéticos contra estações de energia. Estudos mostram que ataques bem-sucedidos podem resultar em perdas financeiras substanciais devido a danos físicos, custos de recuperação, perda de dados e interrupções de serviços. A análise e mitigação de riscos cibernéticos não só protegem os ativos financeiros das empresas de energia, mas também ajudam a evitar custos elevados e prejuízos econômicos para a sociedade como um todo (ANDERSON; MOORE, 2009).

Por fim, as regulamentações de segurança cibernética estão se tornando cada vez mais rigorosas em muitas jurisdições. Estar em conformidade com essas regulamentações é não apenas uma exigência legal, mas também uma prática essencial para a segurança geral das operações das estações de energia que para (National Institute of Standards and Technology (NIST), 2018), a conformidade com padrões de segurança cibernética, como o *NIST Cybersecurity Framework*, e outros, ajuda a garantir que as melhores práticas sejam seguidas e que as infraestruturas estejam protegidas contra ameaças emergentes.

A relevância acadêmica deste trabalho é significativa, pois aborda um tema crucial e contemporâneo: a segurança cibernética nas estações de energia. Este estudo não só contribui para o avanço do conhecimento acadêmico na área de segurança de infraestruturas críticas, como também proporciona uma análise detalhada das vulnerabilidades e das soluções necessárias para mitigar riscos em sistemas energéticos, um setor vital para o desenvolvimento sustentável. Além disso, o trabalho serve como uma base sólida para pesquisas futuras, sugerindo a investigação de novas tecnologias de proteção cibernética, a implementação de práticas de segurança mais robustas, e a importância da cooperação internacional para a criação de normas de segurança mais eficazes.

1.2 OBJETIVO

1.2.1 Objetivo Geral

Analisar os desafios de segurança cibernética nas estações de energia e apresentar perspectivas para redução da possibilidade de ataques cibernéticos.

1.2.2 Objetivos Específicos

- Apresentar os tipos de ataques cibernéticos;
- Analisar as práticas de segurança das estações;
- Analisar nível de segurança de *Softwares* de automação e controle das estações de energia;
- Discutir a adequação das normas e diretrizes de segurança para o setor elétrico brasileiro em comparação com outros países;
- Destacar perspectivas para o setor.

2 METODOLOGIA

Para realização deste trabalho adotou-se como estratégia metodológica, a revisão bibliográfica sobre o tema analise dos desafios de segurança cibernética nas estações e subestações de energia e perspectivas, que de acordo com (BARROS; LEHFELD, 2007), (KÖCHE, 2011), ela se efetua tentando-se resolver um problema ou adquirir conhecimentos a partir do emprego predominante de informações advindas de livros ou obras congêneres. Optou-se por utilizar a revisão narrativa neste trabalho, que é um dos tipos de revisão de literatura, conforme Silva e Trentini (2002), a revisão narrativa não é imparcial porque permite o relato de outros trabalhos, a partir da compreensão do pesquisador sobre como os outros fizeram, permitindo a possibilidade de acesso às experiências de autores que já pesquisaram sobre o assunto. Para Lakatos e Marconi (2007), pesquisa bibliográfica não é apenas uma mera repetição do que já foi dito ou escrito sobre determinado assunto, mas sim, proporciona o exame de um tema sob novo enfoque ou abordagem, chegando a conclusões inovadoras e ainda acrescenta que podemos adicionar a este acervo bases de dados, periódicos e artigos indexados com o objetivo de enriquecer a pesquisa, com finalidade colocar o pesquisador em contato direto com tudo o que foi escrito, dito ou filmado sobre um determinado assunto.

> A pesquisa bibliográfica procura explicar e discutir um tema com base em referências teóricas publicadas em livros, revistas, periódicos e outros. Busca também, conhecer e analisar conteúdos científicos sobre determinado tema ((MARTINS; PINTO, 2001, p. 314).

Na elaboração deste trabalho foi realizado uma revisão narrativa da literatura sobre o tema proposto, visto que esta revisão possibilita dessa forma fazer um analise das pesquisas já concluídas e obter conclusões a partir do tema de interesse. Foi utilizado livros eletrônicos e físicos, artigos científicos nacional e internacional, dissertações e teses. Essas contribuições foram pesquisadas no google acadêmico, no scielo, no *science direct*, no *Multidisciplinary Digital Publishing Institute (MDPI)*, no *Smart Energy International (S de 3 de SSAEI)*, *ResearchGate*,.. em sites de órgãos governamentais brasileiro e em outros sites. A seleção dos materiais de apoio foi realizada a partir de leitura cuidadosa dos artigos, teses, Trabalhos de Conclusão de Curso (TCCs), dissertações e livros encontradas nas plataforma digitais e na biblioteca, sendo selecionada apenas os trabalhos que abordam assunto relacionado com o tema proposto para o estudo. Após a coleta, foi feita a leitura de todo material e realizou-se fichamentos e analise das informações levantadas, procurando a compreensão e a expansão do conhecimento sobre o tema pesquisado com o intuito de elaborar o referencial teórico e o desenvolvimento completo do trabalho.

3 CIBERSEGURANÇA

O conjunto de dados organizados e significativos que fornecem conhecimento ou contexto sobre um determinado assunto ou situação pode ser considerado uma *Informação* que pode ser armazenadas e transmitidas em diversos meios, como papel, discos rígidos, servidores, redes de computadores e dispositivos móveis, em vários formatos, como texto, imagens, áudio, vídeo, entre outros, usadas para comunicar ideias, obter conhecimento e realizar ações específicas. Para Fontes (2017), a informação é muito mais que um conjunto de dados, e transformar esses dados em informação é transformar algo com pouco significado em um recurso de valor para a nossa vida pessoal ou profissional. Ideia essa que segundo (MARCIANO, 2006), o debate acerca dos fundamentos da informação está longe de terminar, partindo duma analise de visto que analisando a literatura, que não é o foco desse trabalho.

Dada a importância das informações para as pessoas e empresas, o seu armazenamento passou a ser muito demandada desde surgimento do homem no mundo ate que em 1968 nos Estados Unidos de *American Documentation Institute*, resolveu mudar o seu nome para *American Society for Information Science,* assim sendo se tornou a primeira instituição de Ciência da Informação do mundo (ARAUJO, 2013).

A partir de uma revisão bibliográfica, doravante como afirma Marciano (2006), como por exemplo no *Journal of Documentation (v. 61, n. 1 - 2005), intitulada Library and Information Science and the philosophy of science* pode-se encontrar diversos artigos acerca das diferentes abordagens pelas quais a ciência da informação pode ser tratada, sob o ponto de vista epistemológico.

Com a criação de ciências de informações e o avanço da Tecnologia de Informação/*Information Technology* (TI) assim como de comunicação, revolucionou-se o processo de processamento, armazenamento e transferência das informações com o uso dos computadores e outros dispositivos conetados à rede fazendo com que houve a necessidade de proteção. Essa proteção que não se trata só de segurança física do local, mas sim, de forma digital dando, assim, o origem da chamada *Segurança de Informação (SI)* que surgiu para garantir de que as elas sejam confidencial, integro e disponível independentemente de forma como está sendo transmitida ou armazenada. A SI de acordo com a (MICROSOFT, 2023), é um conjunto de procedimentos e ferramentas de segurança que protegem amplamente informações corporativas confidenciais contra uso indevido, acesso não autorizado, interrupção ou destruição. Ela abrange segurança física e ambiental que envolve as infraestruturas de segurança, o pessoal responsável

para manutenção de segurança, etc... Controle de acesso ou Sistemas ciberfísica que de acordo com (ASHIBANI; MAHMOUD, 2017) é uma combinação de processos físicos integrados em rede, com os componentes cibernéticos, sensores e atuadores, que interagem em um ciclo de monitoramento dos processos, fornecendo informações para embasar a intervenção humana que pode mudar o funcionamento de determinada máquina ou sistema quando necessário. E por último segurança cibernética.

A cibersegurança e a segurança da informação são conceitos relacionados, mas não são sinônimos, como pode-se ver nas suas definições e atribuições.

3.1 SEGURANÇA DA INFORMAÇÃO

A SI refere-se ao conjunto de medidas tomadas para proteger informações, independentemente do meio em que são armazenadas ou transmitidas. Isso inclui não apenas informações digitais, mas também informações físicas, como documentos em papel.

> A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. (ABNT, 2005, ISO/IEC 27002).

Aqui no Brasil, como consta no *International Organization for Standardization* (ISO) e *International Electrotechnical Commission* (IEC) ABNT, a SI é proteção contra ameaças às informações, de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno de possibilidades e investimentos, (ABNT, 2003). Além disso, a SI também envolve a implementação de controles de acesso físicos e lógicos, a implementação de políticas de segurança, a proteção de dados em trânsito e em repouso e a implementação de medidas de *backup* e recuperação de desastres.

> SI é adotar controles físicos, tecnológicos e humanos personalizados, que viabilizem a redução e administração dos riscos, levando a empresa a atingir o nível de segurança adequado ao seu negócio.(SÊMOLA, 2010, pag.29)

O triângulo *Confidentiality, Integrite and Availability* / Confidencialidade, Integridade e Disponibilidade (CIA) da norma ISO 27001 citado por (COUTO *et al.*, 2022) apud. (HINTZBERGEN *et al.*, 2018), ao especificar os requisitos básicos para estabelecer, implementar, manter e melhorar continuamente qualquer sistema de gerenciamento de segurança da informação, tais princípios são:

1. Confidencialidade ou *Confidentiality*
2. Integridade ou *Integrity*

3. Disponibilidade ou *Availability*

Ainda sobre esses princípios, uma das maiores empresas de América Latina de Big Data e Inteligencia Artificial, a NEOWAY, vem complementando outros princípios e dividindo as em três (03) pilares importantes para a adequação de SI para as pessoas e empresas (NEOWAY, 2020), como demostrado na Figura 1.

Figura 1 – Os Pilares da Segurança de Informação.

Fonte: NEOWAY (2020).

A Figura 1, demostra a divisão dos pilares de SI onde no primeiro pilar temos os mesmos princípios elencados na triangulo CIA acima citado. No segundo Pilar estão listados os princípios como Prevenção, Detecção e Resposta. No terceiro e último são elencados os princípios de Tecnologias, Processos e Pessoas.

Doravante ao ver da NEOWAY (2020) e Saraogi (2004), assim como (WALTERS *et al.*, 2006) e Lucas *et al.* (2016), pode-se definir esses princípios como:

- **Confidencialidade:** é um serviço responsável pela garantia de que as informações serão mantidas em sigilo e acessadas somente por pessoas ou dispositivos autorizadas.
- **Integridade:** é o serviço responsável para garantir que as informações serão mantidas completas e íntegras, sem modificações não autorizadas ou seja se o seu conteúdo de uma mensagem foi alterado após o seu envio.

- **Disponibilidade:** é a garantia de que as informações estarão disponíveis para uso quando necessário, sem interrupções ou falhas.
- **Prevenção:** é adoção de medidas de proteção de ambientes, como sistemas, servidores, programas ou qualquer outro meio.
- **Detecção:** envolve o monitoramento contínuo dos ambientes para identificar ataques, vazamentos e outros problemas o mais rapidamente possível.
- **Resposta:** às ações que são tomadas quando há falhas na prevenção e na detecção.
- **Tecnologia** são as ferramentas que possibilitam colocar em prática a prevenção, detecção e resposta nos sistemas.
- **Processos:** a segurança da informação só é possível por meio de processos bem definidos capazes de dar máxima eficiência às outras medidas.
- **Pessoas:** são o componente mais importante para SI pois são os operadores de todos os princípios e que torne-as possível.

  Por além desses princípios acima citados, segundo autores como (WALTERS *et al.*, 2006) assim como (ULBRICH; VALLE, 2004), ainda temos:
- **Autenticidade:** é a garantia de que as informações são autênticas e originadas de uma fonte confiável, fornecendo condições de identificar se o conteúdo de uma informação foi alterado após o seu envio.
- **Não-repúdio:** que é a garantia de que uma pessoa não poderá negar ter realizado uma determinada ação, como enviar uma mensagem ou assinar um documento digital.
- **Controle de acesso:** que permite controlar quem pode acessar as informações e em que nível de permissão.
- **Auditabilidade:** que é a capacidade de rastrear e registrar as atividades realizadas nas informações, permitindo a identificação de potenciais ameaças e ações indevidas.

3.2 SEGURANÇA CIBERNÉTICA

A Cibersegurança (CS), refere-se especificamente à proteção de sistemas de computador, dispositivos eletrônicos e redes contra ataques cibernéticos. Portanto, a cibersegurança é uma parte importante da segurança da informação, mas não abrange todo o escopo da segurança da informação.

> A segurança cibernética pode ser entendida como a arte de garantir a existência e a continuidade da sociedade da informação de uma nação, assegurando e protegendo, no espaço cibernético, seus ativos de informação e suas infraestru-

> turas críticas. É, portanto, maior que segurança em TI, pois envolve pessoas e processos. (CANONGIA; JUNIOR, 2009, pag. 26)

Por causa da grande quantidade de informações digitais criadas e armazenadas diariamente, é importante ter medidas de segurança eficazes para proteger essas informações contra acesso não autorizado, alterações e perda. Isso inclui a implementação de medidas de CS e políticas de SI que protejam os dados em circulação ou armazenadas, bem como medidas de *backup* e recuperação de desastres para garantir a disponibilidade dessas informações em caso de falhas de sistemas ou desastres naturais.

Além disso, zelar pela privacidade dos dados que também é uma das preocupação importante no mundo digital, através de regulamentações que exigem a proteção adequada de informações pessoais e confidenciais, como por exemplo aqui no Brasil a Lei Geral de Proteção de Dados (LGPD), assim como a Regulamento Geral sobre a Proteção de Dados / *General Data Protection Regulation* (RGPD) para os países da União Europeia.

As principais áreas de CS incluem a prevenção de vírus, proteção de dados, gerenciamento de acesso, monitoramento de redes, detecção de intrusos e outras formas de garantir a segurança do ambiente tecnológico contra os ataques proporcionados por criminosos digitais tais como os *cyberpunks*.

> Esses cyberpunks reais são os Hackers, Crackers, Phreakers,Ravers, Zippies, cypherpunks e Extropians, formando o que podemos chamar de underground da cibercultura. Neste underground,os cyberpunks adotam uma atitude social que é a expressão de um comportamento irreverente em relação às tecnologias eletrônico-digitais... por vezes subversivas como invasões de sites, manipulação de dados, roubo de senhas,criptografia de dados, pirataria de softwares dentre outras atitudes,os cyberpunks burlam e debocham das leis e regras existentes no sistema tecnocrático contemporânea,(LEMOS *et al.*, 2002).

Hackers: Os hackers são indivíduos que usam suas habilidades em computação para acessar sistemas de computadores sem autorização ou para explorar vulnerabilidades de segurança em sistemas de computadores para obter acesso a informações confidenciais ou causar danos aos sistemas. Ao ver do Skoudis e Liston (2005), os hackers divide-se em Hackers do bem, também chamados de *White Hats* (chapéu branco), esses usam suas habilidades para testar a segurança de sistemas de computadores e redes, a fim de identificar vulnerabilidades e fornecer soluções para corrigi-las. Os *Gray hats* (chapéu cinza), geralmente são hackers que usam suas habilidades para fins questionáveis, mas sem intenções maliciosas. Os *Black Hats* (chapéu preto), os chamados de vândalos digitais, estes são verdadeiramente criminosos, sem escrúpulos, que se utilizam de seu conhecimentos apenas para obter lucros sobre qualquer outra pessoa. Tambem existe

os *Crackers, Script Kiddies, Newbie, Lammer, Hacktivist, State-sponsored, Red Teamer, Blue Teamer, Bug Bounty, Hunter* entre outros. (QUISPE, 2018).

A CS sendo uma área complexa e em constante evolução, com uma ampla variedade de termos técnicos. Alguns dos termos mais comuns e importantes usados:

- **Vulnerabilidade:** É uma fraqueza em um sistema de computador ou rede que pode ser explorada por um atacante para comprometer a segurança do sistema.
- **Ameaça:** Refere-se a qualquer tipo de atividade maliciosa que pode causar danos a um sistema de computador ou rede.
- **Ataque:** Refere-se a uma tentativa de explorar uma vulnerabilidade em um sistema de computador ou rede.

3.3 TIPOS DE ATAQUES

Os ataques cibernéticos são um conjunto de técnicas maliciosas usadas por indivíduos ou grupos para invadir, danificar, ou roubar informações de um sistema de computador ou rede. Para GOMES (2015), um ataque cibernético é a execução de uma ação ofensiva, por meio de recursos de Tecnologia de Informação e Comunicação (TIC), com a finalidade de capturar, interromper, penetrar, adulterar, degradar e/ou destruir sistemas e/ou redes de computadores. Existem vários tipos de ataques, de acordo com autores como (SKOUDIS; LISTON, 2005) e da Cartilha de Segurança para Internet, (CERT.BR, 2012), do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) e (DIORIO *et al.*, 2019) temos:

- ***Phishing:*** Um ataque em que um atacante envia e-mails ou mensagens de texto falsas que parecem legítimas para induzir os destinatários a clicarem em links ou fornecerem informações confidenciais, como senhas.
- ***Malware:*** Um tipo de software malicioso usado para comprometer um sistema de computador, roubar informações ou monitorar atividades. Exemplos incluem vírus, worms, Trojans e ransomware, etc...
- ***Ataque de negação de serviço (DoS):*** Um ataque em que um atacante tenta inundar um servidor ou rede com tráfego excessivo para que ele fique inoperável.
- ***Engenharia social:*** Uma técnica usada por atacantes para obter informações confidenciais de usuários por meio de engano, como phishing, pretexting, baiting entre outros.
- ***Man-in-the-middle (MitM):*** Um ataque em que um invasor intercepta comunicações entre dois dispositivos para roubar informações.

- ***Ataque de injeção:*** Um ataque em que um invasor injeta código malicioso em um aplicativo para comprometer o sistema ou roubar informações.
- ***Ataque de força bruta:*** Uma tentativa de quebrar a senha de um sistema ou conta adivinhando repetidamente senhas diferentes.
- ***Spoofing:*** Uma técnica em que um invasor falsifica o endereço IP ou de e-mail para se passar por outra pessoa ou dispositivo.
- ***Smishing:*** Um ataque semelhante ao phishing, mas que usa mensagens de texto em vez de e-mails.
- ***Ataque de buffer overflow***: Um ataque em que um invasor envia mais dados do que o sistema pode manipular, permitindo que o invasor execute código malicioso.
- ***Ataque de DNS spoofing:*** Um ataque em que um invasor falsifica registros *Domain Name System* / Sistema de Nomes de Domínio (DNS) para redirecionar o tráfego de um site para outro.
- ***Ataque de sequestro de sessão:*** Um ataque em que um invasor assume o controle de uma sessão de usuário válida para acessar informações confidenciais.
- ***Ataque de sniffing:*** Um ataque em que um invasor intercepta e captura pacotes de dados transmitidos pela rede.
- ***Ataque de escalonamento de privilégios:*** Um ataque em que um invasor aumenta o nível de acesso em um sistema para obter mais controle.

3.3.1 Malwares

Os ataques cibernéticos por meio de malwares são uma das formas mais comuns de ataques cibernéticos. Os atacantes geralmente usam malwares para roubar informações confidenciais, como senhas, números de cartão de crédito, informações bancárias e outras informações pessoais. Além disso, os malwares também podem ser usados para controlar um sistema remoto, permitindo que o atacante execute ações maliciosas no sistema ou rede comprometida. Existem vários tipos de malwares, incluindo vírus, worms, cavalos de Troia, ransomware, spyware, adware, entre outros, E, entre estes ataques acima citados, segundo (CERT.BR, 2012), o *malware* engloba uma grande variedade tais como:

- *Vírus:* é um programa malicioso que infecta arquivos e se replica para outros programas, podendo causar danos ao sistema.
- *Worms:* são programas maliciosos que se propagam através de redes e se auto-replicam,

causando lentidão na rede e roubo de informações.

- *Trojans:* são programas maliciosos disfarçados de softwares legítimos, que permitem que um invasor tenha acesso remoto ao sistema do usuário.
- *Ransomware:* é um malware que criptografa arquivos do usuário e exige um resgate para desbloqueá-los.
- *Dos/DDoS:* são malwares que sobrecarregam o sistema ou a rede do usuário com tráfego, impedindo que ele seja acessado.
- *Adware:* é um malware que exibe anúncios não solicitados no sistema do usuário.
- *Spyware:* é um malware que coleta informações pessoais do usuário sem o seu conhecimento ou consentimento.
- *Rootkits:* são malwares que se escondem no sistema, permitindo que um invasor obtenha acesso remoto sem ser detectado.
- *Botnets:* são redes de computadores infectados por malware que são controlados por um invasor para realizar ações maliciosas.
- *Keyloggers:* são malwares que registram as teclas digitadas pelo usuário para capturar senhas e outras informações confidenciais.
- *Banking Trojans:* são malwares que visam roubar informações bancárias do usuário.
- *Fileless Malware:* é um malware que não deixa rastros no sistema, tornando mais difícil detectá-lo e removê-lo.
- *Macro Viruses:* são malwares que se propagam através de macros em programas como o Microsoft Office.
- *Backdoors:* são malwares que abrem portas de entrada no sistema, permitindo que um invasor tenha acesso remoto.
- *Adposhel:* é um malware que substitui anúncios legítimos em sites com anúncios maliciosos, redirecionando os usuários para sites falsos.
- *careware:* é um malware que exibe falsos alertas de segurança para enganar os usuários a comprar softwares inúteis.
- *File infectors:* são malwares que infectam arquivos executáveis, tornando-os inoperáveis ou causando danos ao sistema.
- *Browser Hijacker:* é um malware que controla o navegador do usuário, redirecionando-o para sites maliciosos e exibindo anúncios indesejados.
- *Cryptojacking:* é um malware que utiliza o poder de processamento do sistema do usuário

para minerar criptomoedas sem o seu conhecimento ou consentimento.

- *Fake AV:* é um malware que se passa por um programa antivírus legítimo e engana o usuário a pagar por uma licença inútil.
- *Ghostware:* é um malware que apaga seus próprios rastros após comprometer o sistema do usuário, tornando mais difícil detectá-lo e removê-lo.
- *Exploit Kits:* são malwares que exploram vulnerabilidades em softwares desatualizados para invadir o sistema do usuário.

4 ESTAÇÕES DE ENERGIA

4.1 Estação de Energia

Uma Estação de Energia (EE) também conhecido como Usina ou *Power Plant* do Inglês, é uma máquina ou conjunto de equipamentos que gera e entrega um fluxo de energia mecânica ou elétrica, tendo como o principal equipamentos para a geração de energia elétrica, o gerador, que, ao ser acoplado a um motor principal, aciona o gerador e gera a eletricidade, como diz Raja e Srivastava (2006).

Hoje em dia, a eletricidade é uma parte integral de nossas vidas. Nós reconhecemos sua importância para quase todas as nossas necessidades domésticas, comerciais e industriais, e sua demanda só cresce com o tempo. Para chegar até nós passa por etapas desde sua geração , transmissão, distribuição e consumo final saindo de uma Estação, passando por Subestações e ate chegar a usuário final. Neste secção vamos falar de como a energia elétrica é gerada, e quais são as principais formas de geração, transmissão e de distribuição, abordagem sobre as estações, subestações e suas diferenças. É bom lembrar que a energia não é criada ou destruída mas sim transformada.

> A geração de energia elétrica é a transformação de qualquer tipo de energia em energia elétrica. Esse processo ocorre em duas etapas. Na primeira etapa, uma máquina primária transforma qualquer tipo de energia, normalmente hidráulica ou térmica, em energia cinética de rotação. Em uma segunda etapa, um gerador elétrico acoplado à máquina primária transforma a energia cinética de rotação em energia elétrica (MODESTO, 2011, p. 10).

Ainda segundo o mesmo autor, por além de geração temos o termo cogeração que é a forma mais eficiente de gerar calor e energia elétrica a partir de mesma fonte de energia que de acordo com a Agência Nacional de Energia Elétrica (ANEEL) 2005, a Cogeração de energia é o processo de produção combinada de calor e energia elétrica ou mecânica a partir de um mesmo combustível, capaz de produzir benefícios sociais, econômicos e ambientais. Além disso, contribui efetivamente para a racionalização energética, uma vez que possibilita maior produção de energia elétrica e térmica a partir da mesma quantidade de combustível. Esses benefícios sociais e ambientais foram mencionados por outro autor quando tratava de mesmo assunto: "A própria usina deve ser útil econômica e ambientalmente amigável com a sociedade"(RAJA; SRIVASTAVA, 2006, p.01). Dependendo do tipo de usina elétrica, a fonte de energia primária pode variar podendo ser carvão, gás natural, óleo combustível, urânio (em usinas nucleares), vento (em usinas eólicas), luz solar (em usinas solares) ou biomassa, entre outros. Independente da forma de energia, ela é transformada a partir duma outra primaria

já existente. Essa transformação de um tipo de energia já existente em outro, de acordo com Galdino (2011), e Modesto (2011) o sistema de geração de energia é formado pelos seguintes equipamentos: Máquina primária, Geradores, Transformador e Sistema de Controle e Comando e proteção. É importante ressaltar que diferentes tipos de EE, como usinas nucleares, usinas eólicas, usinas solares ou usinas hidrelétricas, terão componentes específicos relacionados à sua tecnologia de geração de energia.

1. *Maquina Primaria:* uma maquina primária, para Modesto (2011), é aquela que faz a transformação de qualquer tipo de energia em energia cinética (movimento) de rotação para ser aproveitada pelo gerador. "As principais máquinas primárias utilizadas hoje são motor diesel, turbina hidráulica, turbina a vapor, turbinas a gás e eólicas"(PERUZZO, 2016, p.67). As principais maquinas primaria são : Hidráulicas, Diesel, Termoelétricas, Termonucleares, Turbinas Eólicas, Fotovoltaicas.
2. *Geradores:* são equipamentos que transformam a energia cinética de rotação das máquinas primárias em energia elétrica segundo Peruzzo (2016).

   Para HELERBROCK (2019), são máquinas capazes de rotacionar em altas velocidades que em seu interior, há grandes ímãs e uma espira que se houver movimento relativo entre o campo magnético dos ímãs e a espira, ocorre o surgimento de uma corrente elétrica."Para explicar o funcionamento dos geradores, pode-se dizer que "quando uma turbina está ligada ao gerador elétrico, a energia cinética (isto é, movimento) do vento, da água que cai, ou do vapor, empurra as pás da turbina, fazendo com que a turbina e, por conseguinte, o rotor ligado ao gerador elétrico, gire e produza eletricidade"(PERUZZO, 2016, p.65).

   Tipo de Maquina primário determina o tipo de usina e com isso temos as formas mais comuns de se geradores de energia elétrica que são: geração hidroelétrica que através da queda da d'água, geração termoelétrica que usa carvão, lenha, bagaço de cana etc. e a geração por reação nuclear elementos químicos radioativos, Eólica a partir da força dos ventos, e Fotovoltaica direto dos raios de Sol.
3. *Transformador:* é o equipamento utilizado para elevar ou rebaixar o nível de tensão gerada pelos geradores numa estação.

4.1.1 Classificação das Estações

Como afirmado antes que quando acoplado a um motor primário que aciona o gerador, a eletricidade é gerada. Raja e Srivastava (2006) ainda afirma que o tipo de motor

primário determina o tipo de usina e com isso pode ser classificado de seguinte forma:

Tabela 1 – Tabela das Classificações das Estações ou Usinas

Usina ou Estações	Convencional	Usinas de Energia de Motores a Vapor Usinas de Turbinas a Vapor Usinas a Diesel Usinas de Turbinas a Gás Usinas Hidrelétricas Usinas Nucleares
	Não Convencional	Geradores Termoelétrico Geradores Termo-Iônico Centrais de Células de Combustíveis Sistema de Energia de Células Solares Fotovoltaicas Usinas MHD (Magneto-Hidrodinâmico) Sistema de Energia do Reator de Fusão Biogás, Sistema de Energia de Biomassas Energia Geotérmica Sistemas de Energia Eólica Conversão de Energia Térmica Oceânica Onda e Maremoto Esquema de Plantação de Energia

Fonte: Adaptado (RAJA; SRIVASTAVA, 2006).

A Tabela 1, apresenta a classificação das usinas quanto as maquinas primárias onde se divide em Convencionais e Não-Convencionais. Os convencionais agrupa EE de motores a vapor, Usinas a diesel,usinas de turbinas a gás, usinas hidroelétricas e as usinas nucleares. Os não-convencionais, por sua vez, englobam todas as que funcionam com maquinas primarias não convencionais como por exemplo sistemas de energias Solar Fotovoltaico, Eólico, Geotérmico, Biomassa, etc.

4.2 Subestação de Energia

Uma Subestação de Energia (SE) também considerado um Sistema de Elétrico de Potência (SEP), é uma instalação do sistema elétrico responsável por modificar as características da energia elétrica, como tensão e corrente, para permitir a sua distribuição aos pontos de consumo de forma adequada. Ela é composta por condutores, aparelhos e equipamentos que realizam a transmissão, distribuição e controle da energia elétrica. Filho e Mamede (2011) determinaram que são conjunto de condutores, aparelhos e equipamentos destinados a modificar as características da energia elétrica (tensão e corrente), permitindo a sua distribuição aos pontos de consumo conectados ao sistema elétrico em níveis adequados de utilização" Ela desempenha

várias funções importantes entre elas da transmissão, distribuição e controle da energia para garantir a confiabilidade e a eficiência do fornecimento de energia, garantir a interligação dos sistemas elétricos, melhorar a qualidade de energia e proteger a integridade física do sistema e das pessoas. Seguindo a mesma linha de pensamento, (CARLETO, 2019) afirma que as subestações são responsáveis pela distribuição da energia elétrica, que antes de chegar às casas, a eletricidade percorre um sistema de transmissão que começa nas usinas e passa por transformadores realizam o aumento ou a diminuição da tensão para se tornar adequada ao consumo

Para garantir o funcionamento de todas essas funções, as subestações contam com uma grande quantidade de componentes interligados. Esses componentes desempenham papéis essenciais no sistema. Conforme a perspectiva de Martins (2011) os principais componentes de uma SEP são:

- Transformadores
- Disjuntores
- Chaves seccionadoras e chaves fusíveis
- Barramentos
- Bancos de capacitores
- Reatores
- Centro de controle
- Relés de proteção
- Pára-raios
- Muflas e buchas de passagem
- Resistor de aterramento
- Reguladores de tensão
- Religadores automáticos

4.2.1 Classificação de Subestações

As subestações de energia podem ser classificadas de diferentes maneiras, dependendo dos critérios utilizados. Na óptica de BARROS e GEDRA (2015) e LEÃO (2018) as subestações podem ser classificado de acordo com o seu tipo, a sua função, as formas de instalação, os níveis de tensão e as formas de comando e operação. Classificações essas que descreveram de seguinte forma:

Tabela 2 – Tabela das Classificações das Subestações

-	Classificação	Sub-Classificação
Tipo	Industrial	-
	Concessionaria	-
Função	SE de Manobra	-
	SE de Transformação	SE Elevadora SE Abaixadora
	SE de Distribuição	-
	SE de Regulação de Tensão	-
	SE Conversoras	CA-CC / CC-CA CA-CA / CC-CC
Nível	Extra Alta Tensão (EAT)	Tensão > 230 kV
	Alta Tensão (AT)	Tensões > 34 kV e < 230 kV
	Média Tensão (MT)	Tensões > 1 kV e < 34 kV
	Baixa Tensão (BT)	Tensões $\leq$ 1 kV
Tipo de Instalação	Subestações Abrigadas	-
	Subastações Desabrigadas;	-
	Subestações Blindadas;	-
	Subestações Móvel	-
Forma de Operação	SE com Operador;	-
	SE Semiautomática;	-
	SE Automática	-
Local de Instalação	Localização;	-
	Facilidade de acesso;	-
	Espaço para expansão;	-
	Regras de uso e ocupação do solo;	-

Fonte: Elaborado pelo autor

4.3 Diferenças entre Estação e Subestação de Energia

Nos subtítulos acima falamos da EE e da SE, suas definições, funções assim como suas classificações. Nesse tópico o foco é comparar-las e trazer as suas diferenças em diversos aspectos. As diferenças entre uma usina e uma subestação reside principalmente em suas funções e nos equipamentos utilizados. Vamos analisá-las a partir de abordagem técnicas, operacionais, financeiro e ambiental.

4.3.1 Diferenças Técnicas:

Estação: A EE é responsável pela geração de energia elétrica a partir de fontes primárias, como água, combustíveis fósseis, energia nuclear, vento ou luz solar. Ela possui equipamentos específicos, como turbinas, geradores e sistemas de controle, que são projetados

para converter a energia primária em eletricidade. As EE têm capacidade de produção e potência instalada, que determinam a quantidade de energia que podem gerar em determinado período de tempo. A operação de uma usina envolve o controle e a manutenção dos equipamentos de geração, além do gerenciamento dos recursos utilizados para a produção de energia.

Subestação: A subestação é responsável pela transformação e distribuição da energia elétrica gerada pela usina ou proveniente de outras subestações. Ela possui equipamentos como transformadores, disjuntores, chaves seccionadoras e capacitores, que são utilizados para alterar a tensão da energia elétrica e direcioná-la para as linhas de distribuição adequadas. As subestações também têm sistemas de controle e proteção, que monitoram o fluxo de energia, protegem os equipamentos contra falhas e garantem o fornecimento estável e seguro para os consumidores. A operação de uma subestação envolve a supervisão dos equipamentos, a manutenção preventiva e corretiva, o monitoramento do fluxo de energia e a realização de testes de proteção e controle. No que diz respeito às diferenças operacionais e financeiras:

4.3.2 Diferenças Operacional:

Estação: A operação de uma EE é mais complexa porque envolve a gestão de múltiplos processos de geração de energia, ela opera na geração contínua de eletricidade, ajustando a produção conforme a demanda e mantendo o funcionamento adequado dos equipamentos. É necessária uma manutenção regular dos equipamentos da usina para garantir sua eficiência e confiabilidade. Isso envolve inspeções, reparos e substituições conforme necessário. As EE podem exigir o gerenciamento de recursos naturais, como água ou combustíveis, para manter a geração de eletricidade.

Subestação: Operação de Transformação e Distribuição, onde a subestação opera no recebimento de eletricidade em alta tensão, transformação para tensões mais baixas e distribuição aos consumidores finais. Monitoramento e Controle, monitorando constantemente o fluxo de energia, a tensão e as condições do sistema elétrico para garantir a distribuição adequada e segura. Manutenção dos Equipamentos, visto que também exigem manutenção regular para garantir seu funcionamento adequado, incluindo inspeções, testes e substituição de componentes, se necessário.

4.3.3 Diferenças Financeiras:

Estação: A construção e operação de uma usina exigem investimentos financeiros significativos. Os custos envolvem a infraestrutura da usina, aquisição e manutenção de equipamentos, além dos custos operacionais e de mão de obra. Os retornos financeiros são obtidos por meio da venda de eletricidade gerada.

Subestação: A construção e manutenção de subestações também requerem investimentos financeiros, mas geralmente em escala menor do que uma usina. O foco principal das subestações é a distribuição eficiente de eletricidade aos consumidores, não gerando receita diretamente.

4.3.4 Diferenças Ambientais

Estação O impacto ambiental de uma EE varia dependendo do tipo de fonte de energia utilizada. Usinas termelétricas queimam combustíveis fósseis e podem contribuir para a emissão de gases de efeito estufa e poluentes atmosféricos. Usinas hidrelétricas têm um impacto ambiental relacionado à construção de barragens e à alteração do curso dos rios. Usinas solares e eólicas são consideradas mais ambientalmente amigáveis, pois geram eletricidade a partir de fontes renováveis.

Subestação As subestações em si têm um impacto ambiental relativamente baixo, pois sua principal função é a distribuição de energia. No entanto, é importante garantir que as subestações sejam projetadas e operadas de maneira segura e ambientalmente responsável, evitando vazamentos de óleo isolante ou outros poluentes. É importante ressaltar que as diferenças mencionadas acima são gerais e podem variar dependendo do tipo específico de usina ou subestação considerada.

5 DESAFIOS DE SEGURANÇA CIBERNÉTICA NO SETOR ELÉTRICO

A segurança cibernética no setor elétrico é uma preocupação crescente à medida que a nossa dependência da energia elétrica e a digitalização das redes elétricas aumentam. Neste contexto, a proteção contra ameaças cibernéticas torna-se crucial, uma vez que qualquer interrupção na geração, transmissão ou distribuição de energia elétrica pode ter impactos significativos na sociedade e na economia. Novas tecnologias, como Inteligencia Artificial (IA), robótica, aprendizado de máquina e *Internet of Things* / Internet das Coisas (IoT), têm impulsionado avanços na automação. Elas possibilitam a operação remota e centralizada de grandes instalações, plantas e subestações. No entanto, também aumentaram significativamente a exposição das empresas a ameaças e riscos de segurança cibernética.

> Um incidente em IT sempre será um incidente. Um incidente em OT pode ser um incidente, ou se tornar um acidente (FREIRE, 2023).

Houve um aumento nos incidentes de segurança cibernética no setor elétrico a partir da aplicação dessas tecnologias , o que pode ter um impacto significativo na sociedade, resultar em multas, problemas regulatórias e prejudicar a reputação das empresas devido a possíveis interrupções nos serviços.

Este setor enfrenta uma série de desafios de segurança, desde ataques sofisticados patrocinados por estados até vulnerabilidades em sistemas de controle e aquisição de dados. A falta de padronização e conscientização de segurança, juntamente com a escassez de pessoal qualificado, também representam obstáculos significativos. Por isso, exploraremos os principais desafios de segurança cibernética que afetam o setor elétrico global e discutiremos como as empresas e as autoridades estão trabalhando juntas para proteger nossa infraestrutura crítica de energia elétrica contra ameaças cibernéticas.

A Segurança Cibernética, desafio do século XXI, vem se destacando como função estratégica de Estado, e essencial à manutenção das infraestruturas críticas de um país, tais como Energia, Defesa, Transporte, Telecomunicações, Finanças, da própria Informação, dentre outras (JUNIOR; CANONGIA, 2010).

O setor elétrico é uma preocupação crítica devido à sua interconexão e impacto nas infraestruturas essenciais. Vários desafios específicos contribuem para a complexidade dessa questão.

Em primeiro lugar, as Ameaças Persistentes Avançadas (APTs) representam um risco significativo. Esses ataques sofisticados são projetados para comprometer sistemas críticos

de energia, como redes de distribuição e sistemas de controle industrial, visando causar danos graves.

Um segundo desafio é a infraestrutura envelhecida. Muitas instalações elétricas ainda dependem de sistemas antigos e não atualizados, que podem conter vulnerabilidades conhecidas e serem alvos fáceis para ataques cibernéticos, como afirma o Alexandre Freire (2021b), que o grande diferencial na comparação do nível de segurança da TIC e Automação é que a automação industrial possui equipamentos antigos sem *patches*, com protocolos que não possuem autenticação, autorização ou criptografia, e que são sistemas utilizados no segmento de energia que não possuem alto poder computacional e que são vulneráveis a diferentes técnicas de ataque e ameaças. Tais sistemas usam os dispositivos como *Intelligent Electronic Devices* / Dispositivos Eletrônicos Inteligentes (IEDs), que são os Reles de Proteção, *Remote Terminal Units* / Unidades Terminais Remotas (RTUs) para acesso remota aos terminais de energia e *Programmable Logic Controller* / Controladores Lógicos Programáveis (PLC)/CLP, para configurar e automatizar os processos, sendo equipamentos que não foram projetados com conceitos de segurança de informação como parte de sua operação, fazendo com que as redes de energia apresentarem muitas superfícies vulneráveis suscetíveis a ataques como a do malware Stuxnet, supostamente usado pelos Estados Unidos e Israel para causar danos ao programa nuclear do Irã, foi projetado para atingir os PLC/CLPs onde subia o código malicioso nos PLCs utilizado na programação dos controladores (CISCOADVISOR, 2022).

A falta de conscientização em segurança cibernética também é um dos desafios para o setor visto que muitos funcionários e prestadores de serviços no setor elétrico podem não estar adequadamente informados sobre as melhores práticas de segurança, o que pode levar a vulnerabilidades adicionais. O uso de Engenharia Social que doravante para (SILVA, 2008) são práticas utilizadas a fim de se obter informações sigilosas e importantes explorando a confiança das pessoas para consegui-las ou seja a arte de manipular pessoas a fim de contornar dispositivos de segurança ou construir métodos e estratégias para enganar as pessoas com palavras caprichosas, utilizando informações cedidas por elas de maneira a ganhar a confiança delas para obter informações .

> Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável. Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança. Esses indivíduos ainda estarão completamente vulneráveis. (MITNICK; SIMON, 2003, p. 03).

De acordo com a pesquisa da DARYUS (2014), mais de 40% das falhas à Segurança da Informação não está ligada diretamente à tecnologia, mas sim em torno de usuários e a maneira na qual os dados, informações e sistemas são utilizados ou guardados nas organizações e que mais de 40% dessas falhas é possível de que boa parte estejam ligados a ataques de engenheiros sociais, e mais especificamente por meio de ações diretas e pessoais.

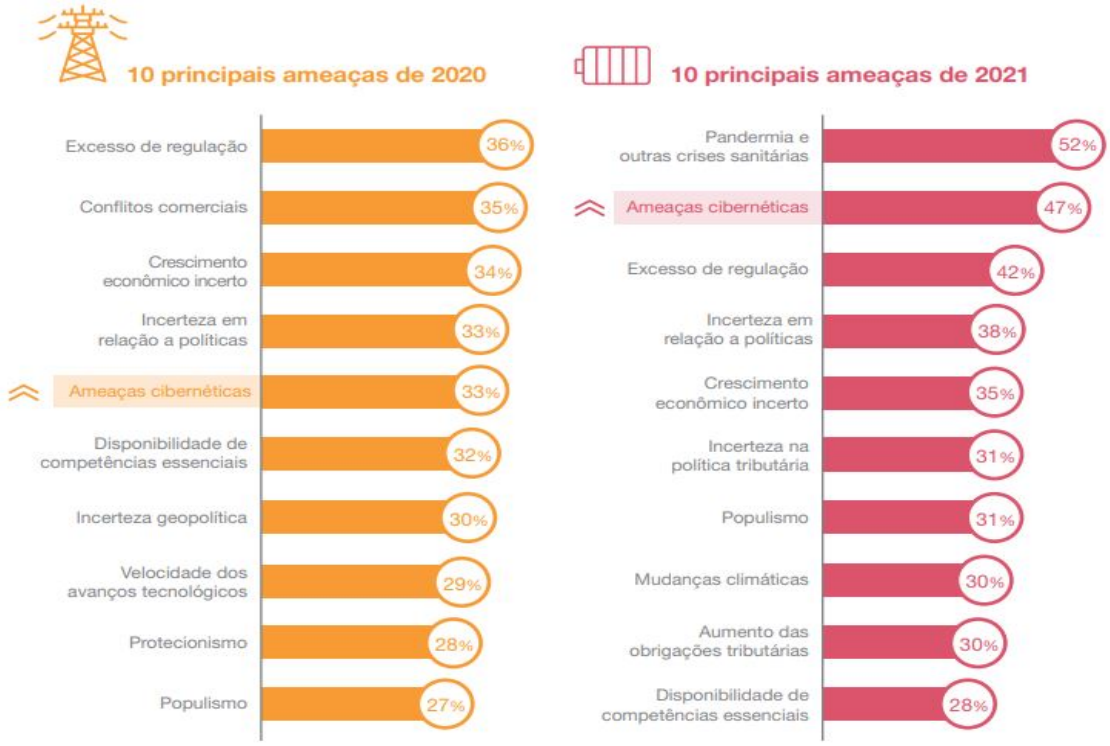
A interconexão crescente entre sistemas de TI e Tecnologia Operacional/ *Operational Technology* (OT) é outro ponto crítico. Embora essa integração possa trazer eficiência operacional, ela também aumenta o risco de ataques cibernéticos, pois os sistemas de OT são frequentemente menos protegidos do que os sistemas de TI, e essa interconectividade aumenta vulnerabilidades nos sistemas abrindo possibilidade para ataques.

Os ataques de Negação de Serviço Distribuídos / *Denial-of-Service or Distributed Denial-of-Service* (DoS/DDoS) são uma preocupação adicional. Interrupções no fornecimento de energia podem ser causadas por ataques DoS/DDoS direcionados aos sistemas de controle industrial, resultando em consequências sérias.

A cadeia de suprimentos do setor elétrico também é uma área de vulnerabilidade. Fornecedores e terceirizados podem não seguir as melhores práticas de segurança cibernética, criando pontos de entrada adicionais para possíveis ataques. Além disso, as empresas do setor elétrico enfrentam o desafio de cumprir as regulamentações de segurança cibernética, que estão em constante evolução devido à natureza dinâmica das ameaças cibernéticas.

Segundo o relatório da 24ª CEO Survey 2021, do Centro Avançado para Operações de Segurança Cibernética da *PricewaterhouseCoopers* (PwC) Brasil sobre a evolução do setor elétrico diante das ameaças cibernéticas nos ambientes de missão crítica publicada em março do mesmo ano, demostra que 47% dos executivos entrevistados no mundo de diferentes setores consideram as ameaças cibernéticas como o segundo maior risco ao crescimento das empresas. Esses incidentes têm aumento também no setor elétrico o que pode causar grande impacto para a sociedade devido às características dos serviços prestados, podendo gerar multas regulatórias e prejudicar a reputação das empresas, no caso de possíveis paralisações de prestação dos serviços. A Figura 2, ilustra os dez principais ameaças de 2020 e 2021 onde as ameaças cibernéticas tem um aumento de 14%.

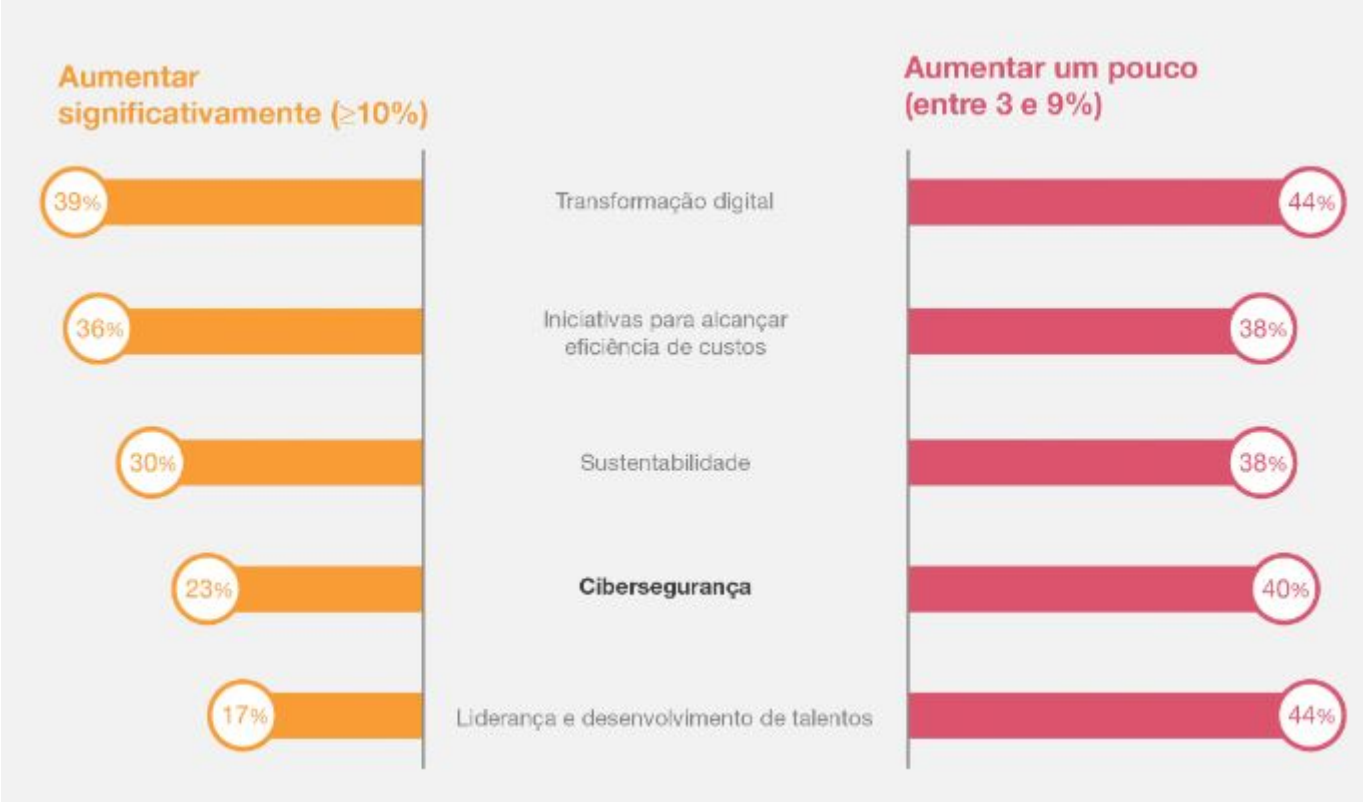
Figura 2 – As dez principais ameaças nos anos 2020 e 2021.



Fonte: 24ª CEO Survey, PwC (2021)

Diante do aumento das ameaças cibernéticas, empresas de energia globalmente têm intensificado seus investimentos em segurança digital. De acordo com dados da pesquisa *Digital Trust Insights*, 58% das empresas desse setor pretendem elevar o montante destinado à cibersegurança em 2021, fazendo com que as empresas do setor aumentarem investimentos do setor de Energia em quase todo mundo nos próximos três(03) anos (PWC, 2021).

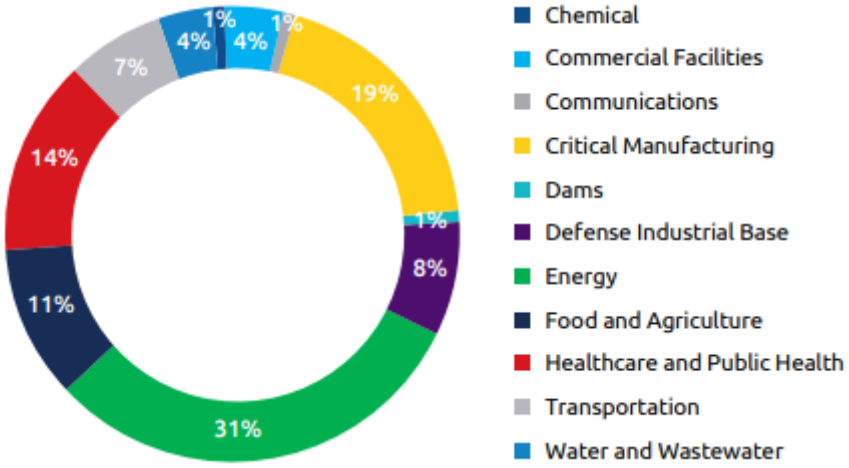
Figura 3 – Projeção de investimentos no setor de energias.



Fonte: 24ª CEO Survey, PwC (2021)

Analizando o *TXOne Annual Report: Insights Into ICS/OT Cybersecurity 2022*, o setor de energia foi o que mais sofreu incidentes nas entre as infraestruturas críticas mundial, o que se deve à crescente conectividade entre a OT e TI.

Figura 4 – Analise dos incidentes a infraestruturas criticas em 2022.



Fonte: TXOne Annual Report: Insights Into ICS/OT Cybersecurity, 2022

5.1 Alguns ataques cibernéticos nas Estações e Subestações de Energias

No que diz respeito à ataques cibernéticos no setor elétrico, não adianta falar somente dos que acontece nas Subestações sem falar dos que acontece nas Usinas, visto que esses ataques podem acontecer tanto nas estações assim como nas subestações de energias. A nível das Estações foram registados ataques em vários países como por exemplo, *STUXNET*, no ano 2010, que é um malware altamente sofisticado que foi descoberto em 2010 e é considerado um dos primeiros ataques cibernéticos conhecidos direcionados especificamente a *Supervisory Control and Data Acquisition* / Sistema de Supervisão, Controle e Aquisição de Dados (SCADA), causando graves danos no complexo nuclear de Natanz, no Irã.

Em 2003, Florianópolis viveu o maior apagão da sua história, mais de 50 horas sem energia, que supostamente foi causado por ataque cibernético, embora, o caso foi atribuído a incêndio em uma das galerias da Ponte Colombo Salles.

> De fato, em 2007, o especialista da CIA Tom Donahue foi autorizado a dizer em uma audiência pública para especialistas que a Agência estava ciente de ocorrências dessa natureza feita por hackers. Embora Tom não tenha mencionado onde os hackers causaram o apagão com um esquema criminoso, mais tarde foi revelado que o incidente ocorrera no Brasil. O apagão de 2003 durou para a maioria das pessoas algumas longas horas.(...), (CONDE, 2022)

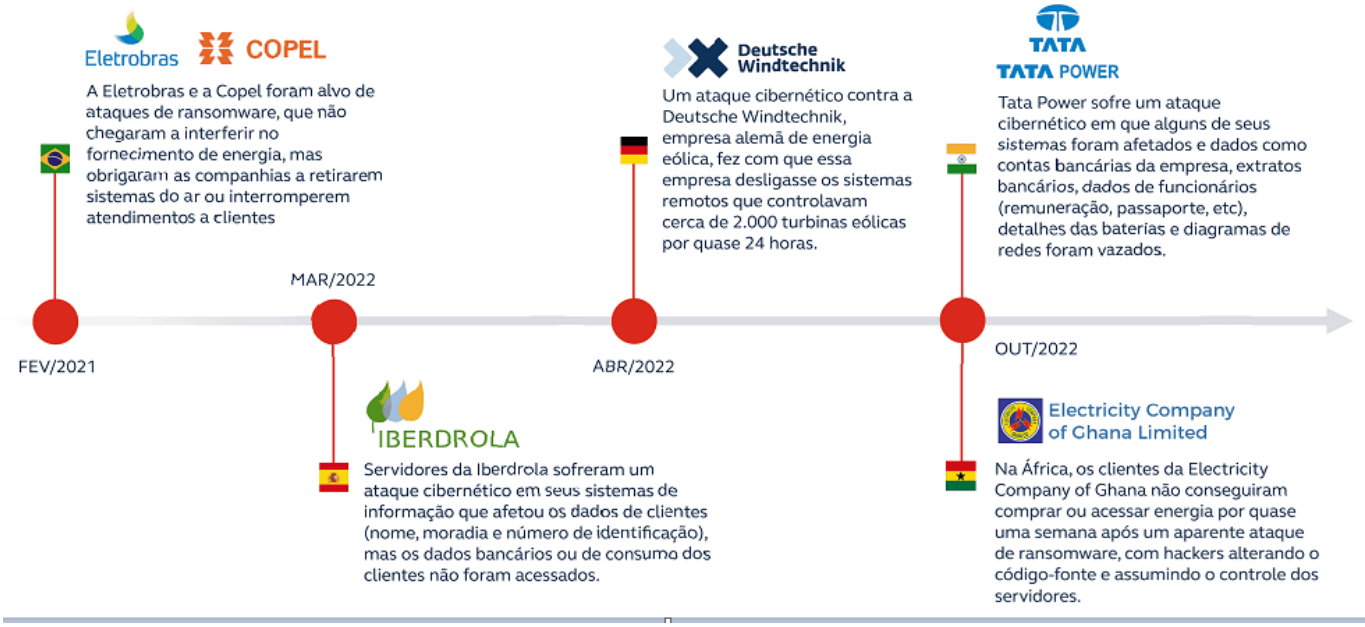
Nos anos 2015 e 2016, ocorreu o *BLACKENERGY*, que é uma família de malware que tem sido associada às várias campanhas cibernéticas, incluindo ataques a infraestruturas críticas, como sistemas de energia, na Ucrânia, e outros países e organizações incluindo organizações nos Estados Unidos e na Europa. Nas Subestações de Energias foram também registados ataques em vários países inclusive no Brasil que em 2020 mais de 5 companhias relataram ataques incluindo Sistema Interligado Nacional (SIN) que também foi alvo de ataques. O Blackenergy, é usado tanto para ataques nas Estações assim como nas Subestações. A Ucrânia sofreu ataques de *Blackenergy e KillDisk* que causaram apagão no país, enquanto que nos Estados Unidos em 2014, empresa de segurança cibernética *Symantec* relatou que um grupo de hackers, tinha como alvo várias empresas de energia nos Estados Unidos.

Segundo a Empresa de Tecnologia Brasilene (2022), e CiscoAdvisor (2022) a Nordex uma empresa Alemã de turbinas eólicas sofreu ataque em Março de 2022, onde um ciberataque a empresa de comunicações via satélite Viasat causou o mau funcionamento de 5.800 turbinas eólicas Enercon na Alemanha. Do mesmo modo, a fabricante de turbinas eólicas Vestas foi atingida por um ataque de ransomware em novembro de 2021, e o grupo por trás do tanto Vestas assim como a Nordex, tiveram que desligar seus sistemas para impedir que o problema se

espalhasse. A outra empresa alemã Enercon também sofreu um ataque no início da invasão da Rússia à Ucrânia, afetando sistemas de monitoramento e controle remoto de quase 6 mil turbinas Enercon, totalizando 11 GW. Ainda acrescenta que no ano de 2021, um relatório da Agência Internacional de Energia disse que os ataques cibernéticos são uma grande ameaça à energia eólica e outras fontes de energia renovável, enquanto em 2020 a seguradora GCube alertou que as ameaças cibernéticas se tornariam mais predominantes durante a pandemia de covid-19.

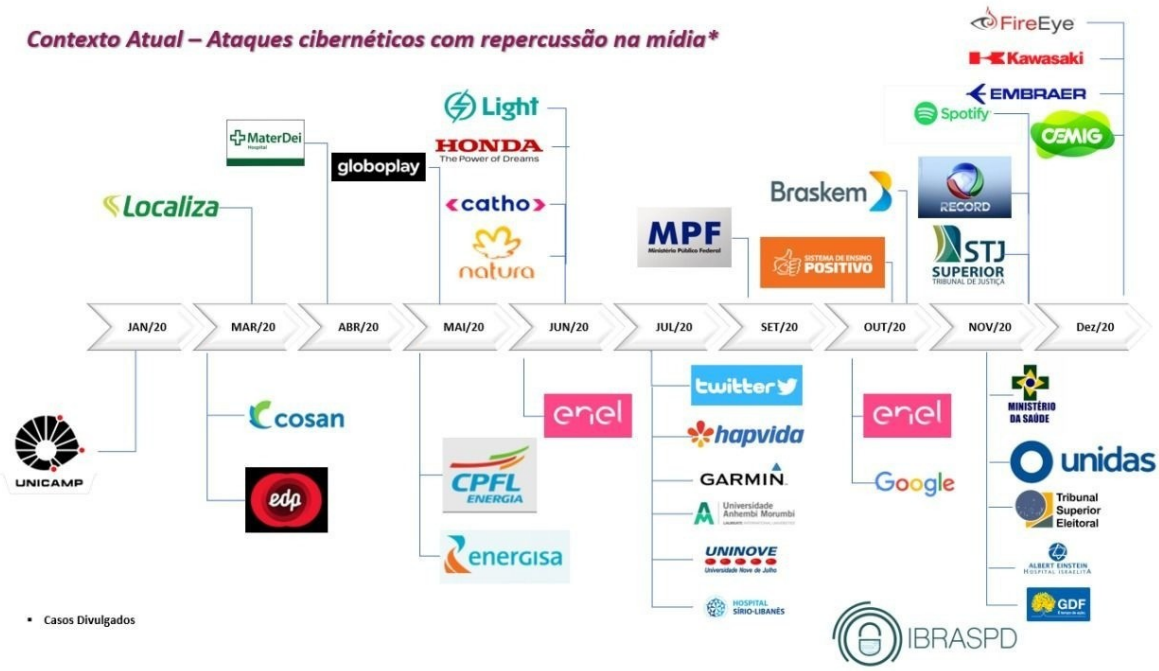
Empresas do setor elétrico brasileiro nomeadamente a Copel, Eletrobras, Enel, Light, Energisa e outros foram alvo de ataques de 2020 e 2021. A Figura 5, mostra alguns dos ataques repercutidos no mundo entre 2021 à 2022.

Figura 5 – Ataques repercutidos no mundo entre 2021 a 2022



Fonte: (JIMENEZ; COSTA, 2024)

Figura 6 – Alguns Ataques cibernéticos registados no Brasil no ano 2020



Fonte: Oliveira (2021)

A Figura 6, apresenta ordem cronologia dos ataques divulgados que aconteceram no Brasil no ano 2020, onde as empresas do setor de energia nomeadamente, EDP, COSAN, ENERGISA, ENEL, LIGHT, CPFL ENERGIA, CEMIG, foram alvos de ataques.

5.2 Cibersegurança no Setor Elétrico Brasileiro

Ao longo de muitas décadas, o setor elétrico brasileiro sofreu muitas transformações e enfrentou vários desafios para chegar na fase que hoje se encontra. Atualmente, de acordo com a Associação Brasileira de Distribuidores de Energia Elétrica (ABRADEE), o setor elétrico brasileiro está dividido em quatro segmentos principais: Geração, Transmissão, Distribuição e Comercialização.

Geração: responsável pela gerência das fontes geradoras que abastecem a energia no país;

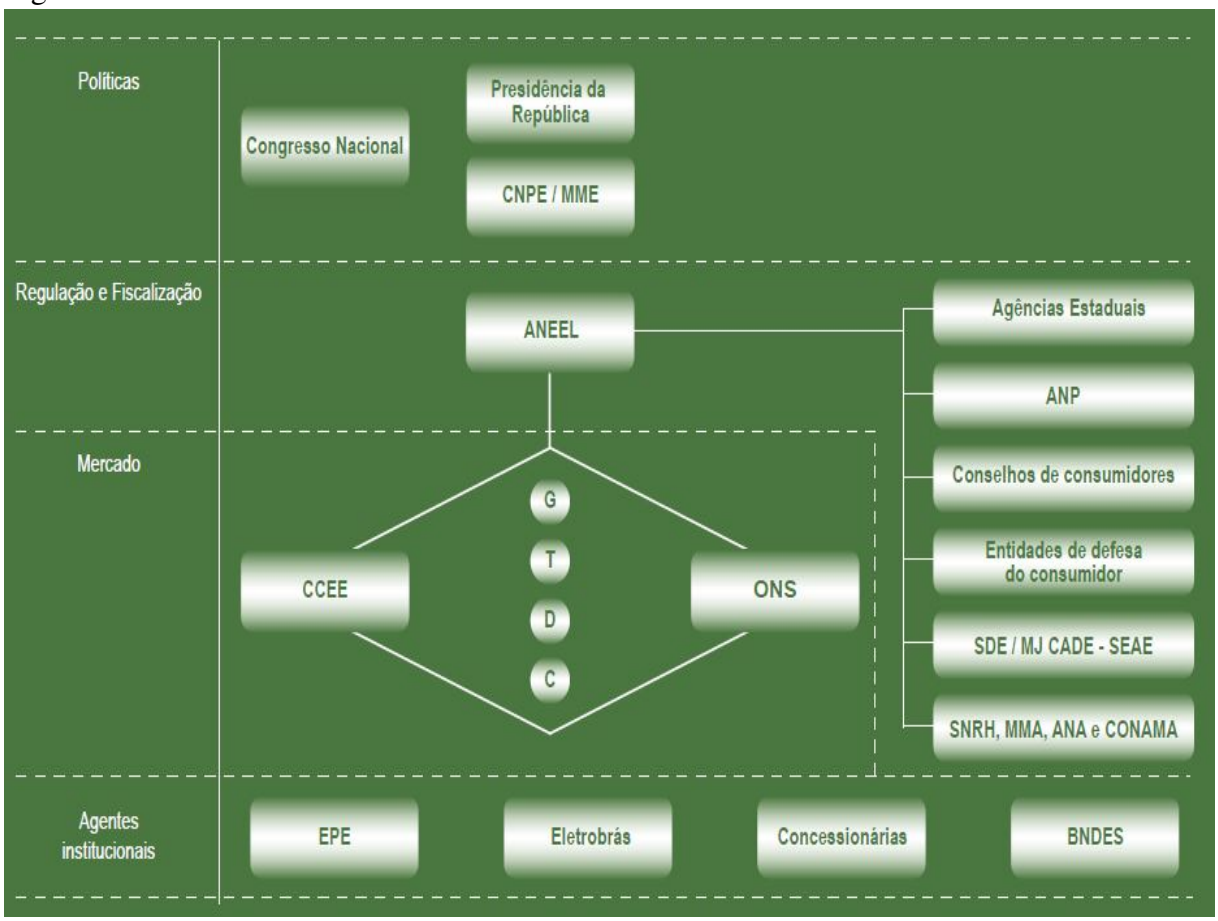
Transmissão: responsável pelas estrutura que leva energia dos pontos de geração aos pontos de distribuição;

Distribuição: são as estações que têm função de convertem a energia para uma tensão menor ou maior e levar até o consumidor final;

Comercialização: são os mecanismos de compra e venda de energia no ambiente de contratação livre.

Todos esses segmentos são gerenciados por uma rede de órgãos governamentais que regulamentam e acompanham todas as atividades que envolvem o setor elétrico. Com a implementação da Lei 10.847/2004 e da Lei 10.848/2004b, o novo modelo de estrutura de setor elétrico, segundo Atlas de Energia Elétrica do Brasil 2008, o Governo Federal, manteve a formulação de políticas para o setor de energia elétrica como atribuição do Poder Executivo Federal, por meio do Ministério de Minas e Energia (MME) e tendo como assessores o Conselho Nacional de Política Energética (CNPE) e o Congresso Nacional. Esses por sua vez criaram a Empresa de Pesquisa Energética (EPE), vinculada ao MME e que é responsável para realizar os estudos necessários ao planejamento da expansão do sistema elétrico, assim como criaram a Câmara de Comercialização de Energia Elétrica (CCEE), que cuida da negociação da energia no mercado livre. O outro criado foi o Comitê de Monitoramento do Setor Elétrico (CMSE) para acompanhar e avaliar permanentemente a continuidade e a segurança do suprimento eletro-energético nacional, além de sugerir das ações necessárias. A Aneel, e o Operador Nacional do Sistema Elétrico (ONS), são responsáveis por coordenar e supervisionar a operação centralizada do SIN. Existe ainda outros institutos e departamentos que foram criadas por além dos acima citados tai como: Conselhos de Consumidores, Agencias Estaduais, Entidades de defesa de consumidores, entre outros.

Figura 7 – Estrutura Institucional do Setor Elétrico Brasileiro



Fonte: (ANEEL, ANDEE, 2008)

A Figura 7, demonstra a estruturação do setor elétrico brasileiro de acordo com as suas divisões hierárquicos desde políticas, regulação e fiscalização, mercado e agentes institucionais, bem como as suas ramificações. A Figura 8 apresenta as sete (07) instituições do Sistema Elétrico Brasileiro e as competências desses órgãos.

De acordo com o Texto de Discussão do Setor Elétrico Nº 103/2021 do Grupo de Estudos do Setor Elétrico (GESEL), da Universidade Federal do Rio de Janeiro, entre as infraestruturas críticas no Brasil, o sistema elétrico desempenha um papel catalizador ao transmitir e distribuir um insumo essencial aos demais setores de infraestrutura.

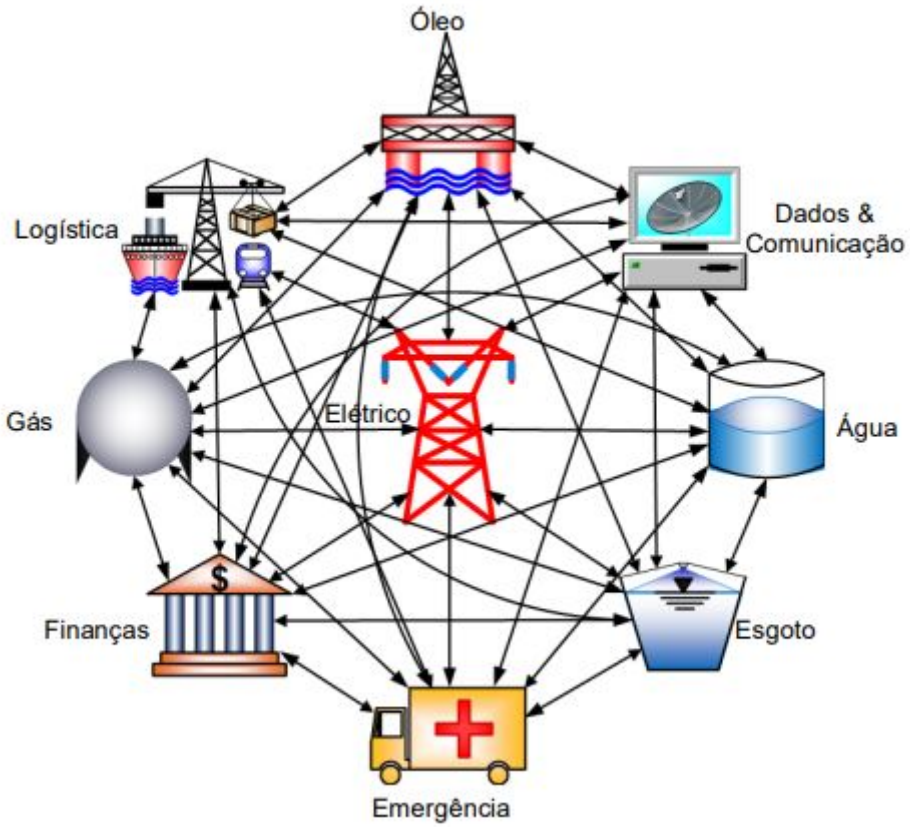
> A interdependência entre as infraestruturas críticas é um fator determinante para a segurança cibernética nacional, principalmente pela relação de dependência ou interferência de uma em outra ou de uma área prioritária de infraestruturas críticas em outra, em particular quando provocadas por ataques cibernéticos. Destaca-se que esta interdependência possui um efeito catalizador e amplificador das consequências de um incidente ou ataque em qualquer rede de infraestruturas críticas(GESEL, 2021, p.13).

Figura 8 – Instituições do Setor Elétrico Brasileiro e suas Competências

Fonte: Ministério de Minas e Energia, 2021

Ao mesmo tempo o setor elétrico depende de outros setores para o fornecimento de insumos energéticos como: água, óleo, gás, diesel, carvão, informações e meios de comunicação, finanças e outros. Portanto, SI no setor elétrico depende não apenas de sua exposição própria aos ataques, mas de sua extensão e integração com os demais, bem como interdependência com os demais setores críticos, como ilustrado na Figura 9.

Figura 9 – Interdependência entre as infraestruturas críticas.



Fonte: GESEL (2021) apud. Siqueira (2013)

Ainda acrescenta que para uma boa análise de sua segurança, será importante caracterizar a estrutura do SIN como uma rede elétrica única de abrangência nacional, com governança técnica centralizada no ONS, a estrutura operacional dos diversos agentes do setor elétrico e as características técnicas das subestações e das usinas de geração.

5.2.1 Normas e Diretrizes de Segurança para setor Elétrico Brasileiro

O Brasil ao longo da sua história teve um crescimento em todas as áreas e o setor elétrico também acompanhou esse crescimento. Enfrentando enumero problemas regulatório que vão surgindo com o passar dos tempos fazendo com que haja necessidade de criação de leis, decretos, resoluções, portarias, regras e procedimentos a serem seguidas para melhorar o setor. O governo criou vários diretrizes, resoluções, normas, etc. destinadas ao setor de segurança de informação, e dentre as iniciativas pode-se mencionar algumas regras e diretrizes voltadas para segurança cibernética e proteção de dados :

Em 1998 foi criado a ONS, pela Lei nº 9.648, com as alterações introduzidas pela

Lei nº 10.848/2004c e que depois foi regulamentado pelo Decreto nº 5.081/2004a para coordenar e controlar da operação das instalações de geração e transmissão de energia elétrica no Sistema Interligado Nacional (SIN) e pelo planejamento da operação dos sistemas isolados do país, sob a fiscalização e regulação da Agência Nacional de Energia Elétrica (Aneel) (BRASIL, 2023a).

A Lei nº 13.709/2018c, que é a LGPD ou seja Lei Geral de Proteção de Dados Pessoais, que rege sobre proteção de dados pessoais no país.

Decreto nº 9.573/ publicado no ano 2018a, aprovou a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC) e que ainda define três instrumentos para a implementação da PNSIC: a Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC), o Plano Nacional de Segurança de Infraestruturas Críticas (PLANSIC), e o Sistema Integrado de Dados de Segurança de Infraestruturas Críticas (SIDSIC).

Decreto nº 9.637/2018b, que aprova Política Nacional de Segurança da Informação (PNSI), que abrange segurança cibernética, defesa cibernética, segurança física e a proteção de dados organizacionais;

Decreto nº 10.222/2020a que estabelece a Estratégia Nacional de Segurança da Informação (E-Ciber);

Decreto nº 10.569/2020b, que aprova a ENSIC.

A Resolução Nº 1, de 11 de setembro de 2021b, aprova o Regimento Interno do Comitê Gestor da Segurança da Informação (CGSI) .

Apesar de tanto esforço e tantas normas e diretrizes, ainda se tem um problema regulatório que é o risco de ocorrência de incidentes de segurança cibernética no setor elétrico. Para mitigar esse flagelo, a ANEEL promoveu consulta pública sobre segurança cibernética no setor elétrico brasileiro, criando assim a Resolução Normativa (RN) nº 964/2021a que dispõe sobre a política de segurança cibernética que deverá ser adotada pelos agentes do setor elétrico a vigorar a partir de 1º de julho de 2022.

Também de acordo com as informações que disponíveis em (BRASIL, 2023b), destaca-se a criação do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) que faz parte do Departamento de Segurança de Cibernética (DSC), e essa por sua vez faz parte da Secretaria de Segurança da Informação e Cibernética (SSIC) do Gabinete de Segurança Institucional (GSI) da Presidência da República.

O CTIR Gov tem por objetivo coordenar e integrar as ações destinadas à gestão de incidentes computacionais em órgãos ou entidades da Administração Pública Federal (APF),

bem como: prevenir, monitorar, analisar e mitigar os incidentes de segurança da informação; promover o intercâmbio científico-tecnológico; participar da articulação para o estabelecimento de diretrizes sobre gestão de incidentes computacionais; e criar processo de inteligência de ameaças cibernéticas para subsidiar criação de políticas públicas e tomada de decisão.

De acordo com o relatório de Análise de Impacto Regulatório nº 3/20212021, sobre segurança cibernética no Setor Elétrico Brasileiro, tendo em conta o crescente risco de ataques cibernéticos no setor elétrico foi uma das motivações para estudar esse problema no âmbito regulatório. Para enfrentar esses riscos, Governo por além dos Decretos nº 9.637/2018, nº 10.222/2020 e nº 10.748/2021, que abrangem todas as infraestruturas críticas do Brasil, incluindo o setor elétrico, utilizou as técnicas de *Design Thinking* que para (WOEBCKEN, 2019) é uma abordagem centrada no ser humano para a inovação, que utiliza ferramentas de design para integrar as necessidades das pessoas, as possibilidades da tecnologia e os requisitos para o sucesso empresarial, onde todo o processo envolve etapas iterativas de empatia, definição, ideação, prototipagem e teste para resolver problemas complexos de forma criativa e eficaz. ou seja, não traz uma fórmula específica para sua implantação, mas sim, ele cria as condições necessárias para maximizar a geração de *insights* e a aplicação prática deles. Isso ajudou a identificar quatro causas principais para esse problema regulatório:

- **Atuação de agentes maliciosos e cibercriminosos:** Estes agentes realizam ataques cibernéticos que resultam em incidentes;
- **Falta de segurança adequada:** A vulnerabilidade dos sistemas no setor elétrico pode facilitar a ação de hackers ou crackers. Apesar de existirem agentes com políticas de segurança cibernética bem desenvolvidas, nem todos alcançaram o mesmo nível de maturidade, expondo parte ou todo o sistema a incidentes.
- **Conectividade dos sistemas:** Com a crescente conexão dos sistemas, há um aumento na eficiência, monitoramento, integração e análise de dados, mas isso também amplia o potencial de alcance de um ataque.
- **Carência de recursos humanos especializados:** A importância crescente do problema destacou a falta de especialização na área e a ausência de uma cultura de segurança cibernética nas empresas do setor, embora o interesse tenha crescido nos últimos anos.

Entretanto, as consequências dos incidentes de segurança cibernética no setor elétrico são diversas, incluindo:

- Interrupção no suprimento que é uma das consequências mais imediatas, afetando

tanto consumidores quanto geradores, transmissoras e distribuidoras.

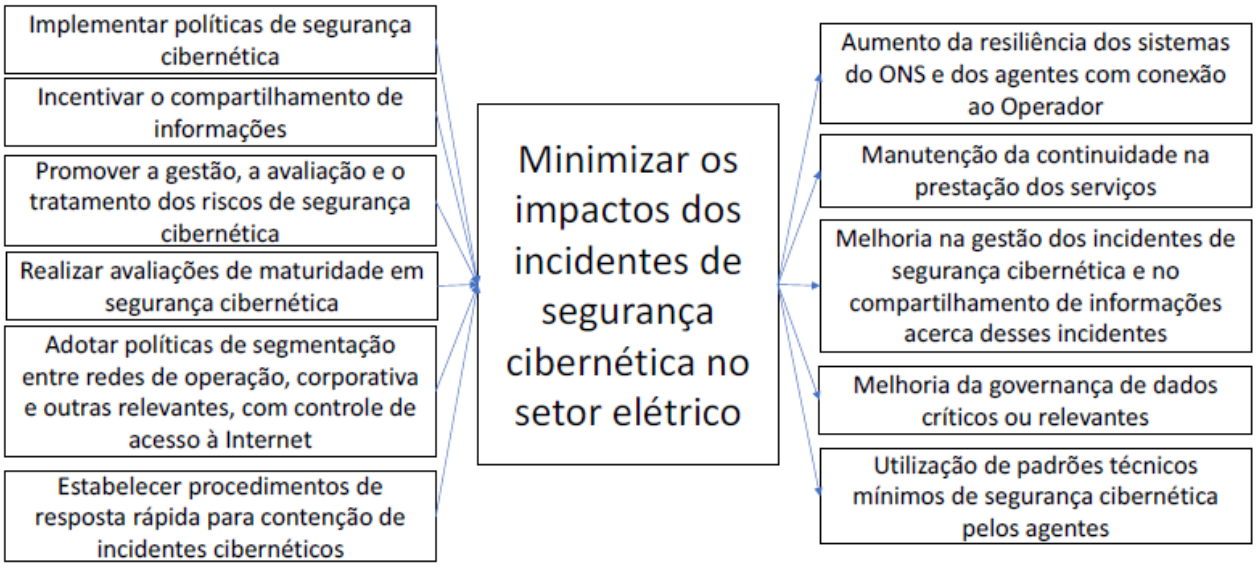
- Impossibilidade de realizar operações técnicas, comerciais ou de faturamento podendo, assim, resultar na interrupção do serviço e na operação ineficiente do Sistema Interligado Nacional.

- Extravio de dados levando ao acessos indevidos, furtos de propriedade intelectual, uso e venda de dados.

Figura 10 – Diagrama do Problema Regulatório, as suas causas e consequências.

Fonte: Relatório de Análise de Impacto Regulatório nº 3/2021

Figura 11 – Objetivos que se pretende alcançar com a regularização.



Fonte: Relatório de Análise de Impacto Regulatório nº 3/2021

A Figura 10, é uma representação das causas principais para esse problema regulatório e das sua consequências para o setor elétrico mostrando assim o desafio que a regulamentação,

enquanto que, a Figura 11 aparenta os objetivos que se pretende alcançar com a regularização.

5.2.2 Práticas de Segurança Cibernética nas Estações

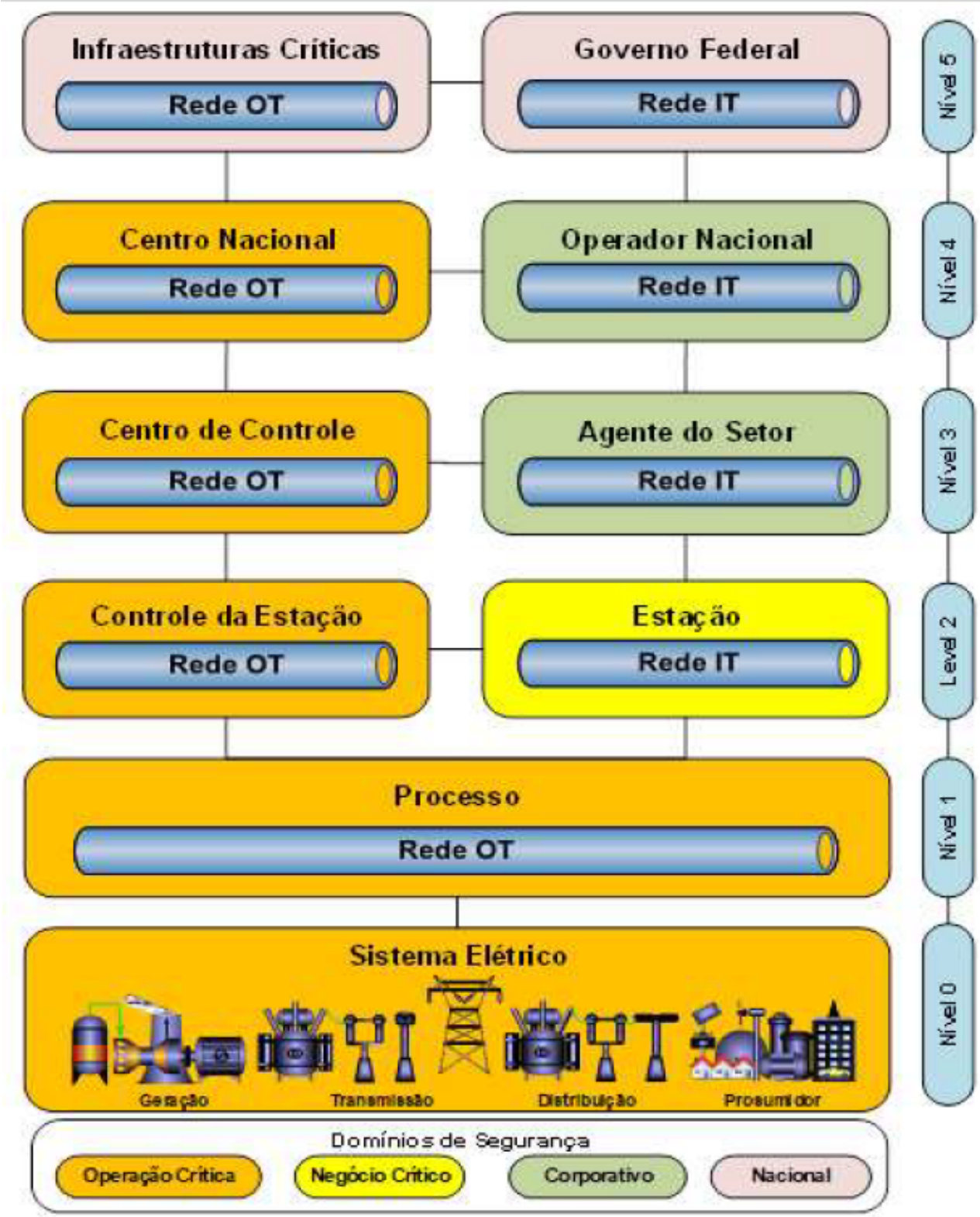
O Brasil por além de cumprir com as diretrizes por ele criadas, também aplica outros protocolos internacionais voltados ao setor de energias. A segurança cibernética de cada instalação do SIN por si, precisa estar de acordo às diretrizes da Política Nacional de Segurança, às normas nacionais e aos procedimentos exigidos pelo ONS e aos padrões de segurança, propostos pela ABNT, e outros instituições nacionais ou internacionais aplicáveis ao setor, como por exemplo da IEC, IEEE e NIST, DNP3, etc.

> No Brasil, os controles para reduzir riscos e aumentar a resiliência cibernética do setor não são pautados por regulamentações, mas sim pelos melhores esforços da comunidade em boas práticas utilizando-se frameworks como NIST e ISA99/IEC 62443 (FREIRE, 2021a).

A norma IEC 61850 é a principal referência para a automação de subestações. Seu propósito é estabelecer diretrizes para a modelagem virtual dessas instalações, padronizar os métodos de comunicação entre os dispositivos e definir os requisitos de desempenho do sistema. Ela engloba um conjunto de protocolos como *Generic Object Oriented Substation Event) (GOOSE)* responsável pelas comunicações entres os IEDs de forma horizontal ou seja mantém as informações no mesmo nível, assim como *Manufacturing Message Specification) (MMS)* que fica responsável de comunicações entre os níveis de forma vertical. Também definindo em três níveis dentro de um sistema de automação de subestação: Nível de Estação, Nível de Bay e Nível Processo (FERRARI; LIMA, 2020).

A Segurança Cibernética do Setor Elétrico pode ser avaliada considerando uma arquitetura em camadas, modelada segundo o padrão original *Purdue Enterprise Reference Architecture and Methodology* (PERA) (...) e adaptada para o contexto nacional brasileiro (GESEL, 2021, p. 65). Segundo o mesmo, para cada domínio de segurança, são aplicáveis medidas e controles específicos, seguindo as recomendações do padrão IEC 62351 para sistemas de automação, conforme a política selecionada.

Figura 12 – Modelo PERA da Purdue.



Fonte: (GESEL, 2021).

A Figura 12 apresenta uma arquitetura de ativos de TI/OT que esta dividida em seis camadas hierárquicas ou níveis e três domínios de Segurança nomeadamente Operação Critica,

Negócio Crítico e Corporativo ou Nacional. Para isso podemos ver na Tabela 3 a composição e descrição desses níveis.

Tabela 3 – Arquitetura em camadas, modelada segundo o padrão original PERA da Purdue

Nível	Camada	Descrição
0	Rede de Campo	Todos os itens físicos de alta e baixa tensão das instalações elétricas do SIN, tais como disjuntores, transformadores, reatores, geradores, etc.
1	Rede de Processo	Todos os ativos de hardware e *software* que monitoram, medem ou controlam diretamente todos os equipamentos do sistema elétrico.
2	Rede de Estação	Todos os itens de hardware e *software* que supervisionam, monitoram e controlam centralizadamente uma subestação ou usina.
3	Rede de Centro de Controle	Todos os itens de *hardware* e *software* e os protocolos de comunicação que supervisionam, monitoram e controlam, a nível corporativo
4	Rede de Corporativa ou Nacional	Todos os itens de *hardware* e *software* e os protocolos de TI, TL e TO do ONS que interagem com os Centros de Controle dos agentes no Nível 3, para processar tarefas operacionais, comerciais, de engenharia e administrativas, e com os demais agentes e entidades setoriais, de mercado e governamentais.
5	Rede de Externa	Todos os centros de controle binacionais, internacionais e de monitoramento setorial, os centros de controle de outros setores críticos e todos os itens de entidades externas que se comunicam com o ONS

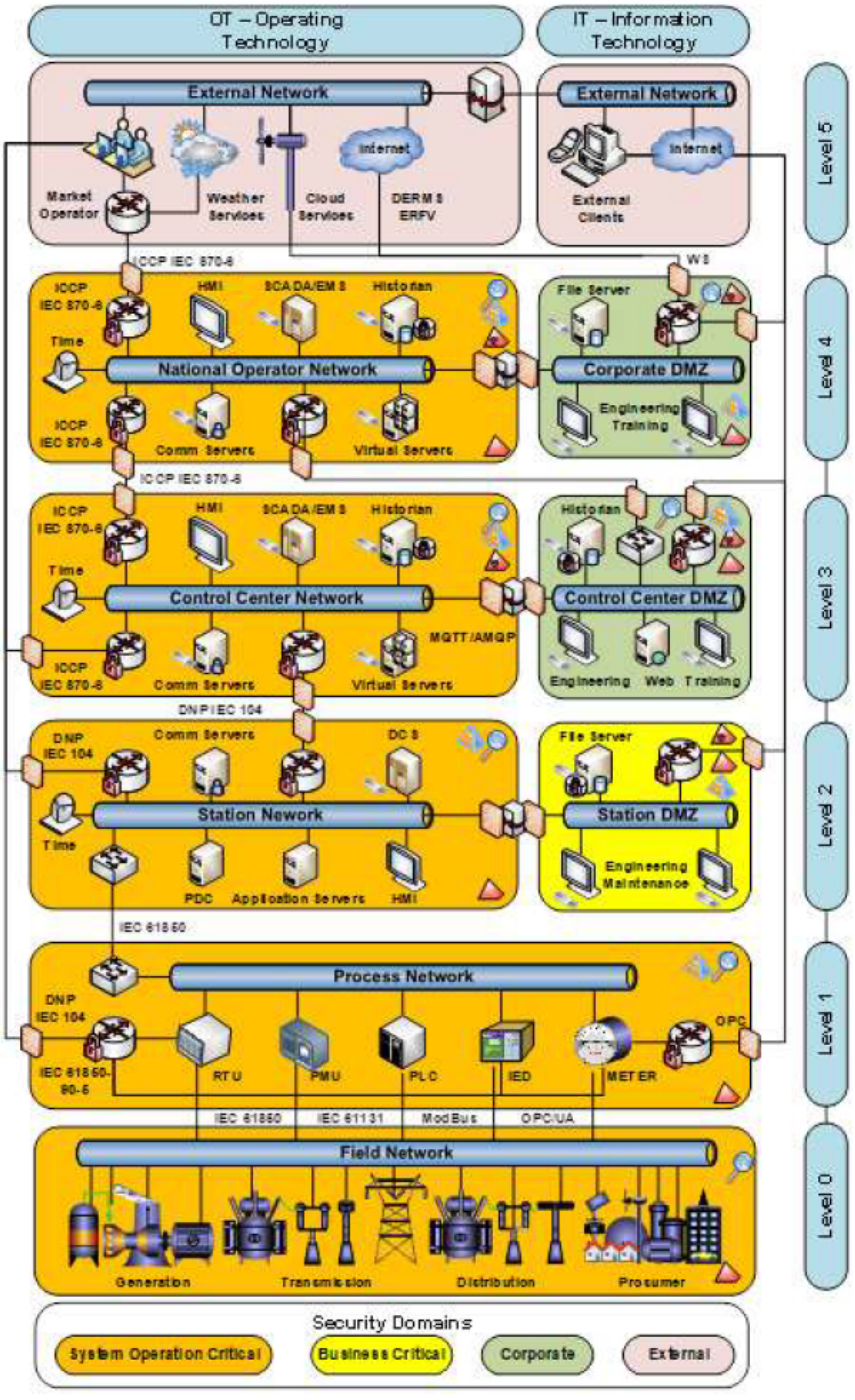
Fonte: Elaboração Propria, Adaptado (GESEL, 2021).

Pode se notar que esse modelo usa IEC 61850 como base, o que apresenta uma vulnerabilidade visto que as comunicações estão sendo feita de forma horizontal e vertical ao mesmo tempo entre os níveis. Um ataque bem sucedido a qualquer nível poderá causar estragos imensurável aos demais.

Como opção tecnológica para atender aos controles e às políticas regulamentados, para (SIQUEIRA *et al.*, 2021) os agentes do SEB podem optar por soluções disponíveis comercialmente ou desenvolvidas sob medida para cada ativo, domínio ou camada da arquitetura do SIN e ainda apresentaram uma sugestão das tecnologias de segurança aplicáveis a cada camada e domínio da hierarquia funcional do SIN, devendo ser selecionada pelos agentes para atender ao conjunto de contramedidas e políticas estabelecidas para o SEB, conforme as arquiteturas apresentadas da Figura 13 onde foram acrescentados mais proteções internas entre as camadas como por exemplo as Restrições de tráfego para comunicação proibida (Firewalls) com entidades

internas, como centros de controle de backup, subestações, usinas e usuários corporativos, bem como com entidades externas, implementação de Zonas Desmilitarizadas - DMZ, para separar *Local Area Network* / Rede Local (LAN) de redes não confiáveis principalmente para trocar dados com usuários corporativos e clientes externos; Segregação de tráfego (VPN) para proteger a comunicação com entidades internas; entre outras medidas (SIQUEIRA *et al.*, 2021).

Figura 13 – Modelo sugerido pela GESEL



Fonte: (SIQUEIRA *et al.*, 2021).

A ONS, em parceria com a NAZOMI NETWORKS, pretende criar sistemas e protocolos que permite minimizar os desafios cibernéticos e operacionais para implementação de controles em centros de operação e subestações. Desafios esses mostradas na Figura 14, que para (FREIRE, 2021b), no primeiro ponto permitir que sejam posições de supervisão, estações de engenharia, dispositivos eletrônicos inteligentes - IEDs, as Remotas - RTUs ou PLCs, e compreender seus papeis no ambiente que podem variar de acordo com suas funções na supervisão e aquisição de dados. O segundo ponto é compreender as vulnerabilidades do sistema com falta de atualização, patches ou versões de sistemas operacionais que não são mais suportados, vulnerabilidades em serviços, protocolos, aplicações e riscos gerais de uso do ambiente como comunicações com a Internet. O terceiro desafio trata-se do monitoramento para detecção de mudança nos processos, procurar as origem e causas de uma mudança no funcionamento dos elementos, e mudanças que possam ocasionar algum evento de indisponibilidade do ambiente. O ultimo trata-se de ataques cibernéticos ou seja ameaças já estão presentes nas redes operativas de empresas de energia em países da América Latina incluindo o Brasil) em ambientes de subestações e usinas monitorados pela Nozomi Networks na região, foi possível observar pontos que merecem atenção e que foram identificados em ambientes de produção.

Figura 14 – Desafios Cibernéticas e Operacionais

Fonte: (FREIRE, 2021b).

A Associação Brasileira das Empresas de Transmissão de Energia Elétrica (ABRATE) elaborou um framework com o intuito de mitigar os riscos. Foi indicada a ferramenta C2M2 (Cybersecurity Capability Maturity Model) para gerenciamento de segurança cibernética. Assim, o *framework* foi projetado para auxiliar as organizações do setor elétrico a identificarem o nível de segurança cibernética atual, o nível desejado, lacunas nos programas de gerenciamento de

risco, prioridades para implementação das práticas relativas aos níveis de maturidade, entre outras atribuições (ANEEL, 2021) tendo como um dos principais motivadores desse estudo é a proposta do ONS de submódulo para os Procedimentos de Rede. A conformidade com várias regulamentações, juntamente com a implementação de práticas avançadas de monitoramento contínuo de OT, é essencial para garantir a segurança, eficiência e resiliência do sistema elétrico. Essa escolha deve estar alinhada com as diretrizes da RO-CB.BR.01 segundo a ONS, ANEEL (2021),que abordou os temas sobre arquitetura tecnológica para o ambiente, governança de segurança da informação; inventário de ativos; gestão de vulnerabilidades; gestão de acessos; monitoramento e resposta a incidentes; e orientações técnicas complementares, para mitigar os diversos desafios técnicos de segurança que sistemas elétricos enfrenta tais como a Escalabilidade, Largura de Banda, Sincronização de Tempo, Complexidade e Riscos de Cibersegurança. Para tal, o país deve adotar outras praticas descritas em normas estrangeiras como esta sendo feito a fim de auxiliar a enfrentar esses desafios.

6 DESAFIOS DE CIBERSEGURANÇA NO SETOR ELÉTRICO MUNDIAL

A Segurança Cibernética, desafio do século XXI, vem se destacando como função estratégica de Estado, e essencial à manutenção das infraestruturas críticas de um país, tais como Energia, Defesa, Transporte, Telecomunicações, Finanças, da própria Informação, dentre outras.(JUNIOR; CANONGIA, 2010) sera apresentado de forma panorâmico .....

6.1 ÁFRICA

A cibersegurança é uma preocupação crescente globalmente, e as estações de energia são alvos particularmente vulneráveis devido à sua importância crítica para a infraestrutura nacional. No continente africano, essa preocupação se torna ainda mais acentuada devido aos desafios únicos enfrentados na região, como sistemas tradicionais em fase de modernização das redes de energia e a crescente dependência de tecnologias digitais para a gestão e operação dessas infraestruturas.

As estações de energia no continente africano têm visto um aumento significativo na adoção de tecnologias avançadas para melhorar a eficiência e a confiabilidade da produção e distribuição de energia. No entanto, essa modernização também trouxe à tona novas vulnerabilidades, tornando a cibersegurança uma prioridade para governos e operadores de redes de energia.

6.1.1 África do Sul

A África do Sul é líder no continente em termos de avanços tecnológicos no setor de energia. O país tem investido em smart grids e tecnologias de automação para melhorar a eficiência da distribuição de energia. Além disso, a Eskom, empresa estatal de eletricidade, tem implementado sistemas SCADA para monitorar e controlar suas operações. A África do Sul tem um quadro regulamentar robusto para a cibersegurança no setor de energia, diretrizes baseado no *National Institute of Standards and Technology* (NIST), no que diz respeito às obrigações legais, as entidades do setor energético deverão familiarizar-se com a Lei de Proteção de Infraestruturas Críticas n.º 8 de 2019 (CIPA), em vigor desde 1 de abril de 2022 como afirma (Herbert Smith Freehills, 2023).

A Africa do Sul criou em 2015 a *National Cybersecurity Policy Framework* (NCPF) segundo (Government of South Africa, 2023), que define as diretrizes e as melhores práticas para

proteger as infraestruturas críticas, incluindo as estações de energia de questões cibernéticas.

Segundo (KANALI, 2023) da Africa Business Communities, grupos cibernéticos patrocinados pelo Estado têm como alvo ativo o governo sul-africano, relatório Trellix, onde as organizações governamentais continuam a ser os principais alvos dos agentes de ameaças que procuram infiltrar-se nos sistemas de TI sul-africanos, que acordo com o último relatório sobre ameaças, apresentado no *Trellix Cyberthreat Intelligence Briefing* para a África do Sul, 26% de todas as atividades de ameaças detectadas foram direcionadas a sistemas governamentais que inclui o setor energético. A África do Sul sofreu vários ataques cibernéticos, segundo (Herbert Smith Freehills, 2023), um ataque em 2019 a fornecedor de serviços de eletricidade da cidade de Joanesburgo, City Power, que resultou na interrupção dos serviços de energia, o ataque desativou o site da concessionária e impediu que seus clientes pudessem comprar eletricidade da concessionária. Em 2022, a empresa estatal de eletricidade da África do Sul, Eskom, que gera e distribui a maior parte da eletricidade da África do Sul, sofreu um ataque de ransomware que criptografou os dados dos servidores da empresa. Esses ataques e outros revelou vulnerabilidades críticas na infraestrutura digital do país mesmo com as diretrizes adotadas..

Com contínuos investimentos em cibersegurança e a implementação de tecnologias avançadas, a África do Sul está bem posicionada para mitigar futuros riscos cibernéticos. No entanto, a necessidade de treinamento contínuo e atualização das políticas de segurança é essencial para manter a resiliência.

6.1.2 Quênia

Assim como a Africa do Sul, Quênia tem investido em energia renovável e na modernização de sua infraestrutura de energia. A *Kenya Electricity Generating Company* (KenGen) que é a principal empresa de geração de energia elétrica na África Oriental, tem adotado tecnologias avançadas para a geração e distribuição de energia, incluindo a integração de sistemas inteligentes para monitoramento e controle.

A Autoridade de Comunicações do Quênia (CA) lançou diretrizes específicas para a cibersegurança das infraestruturas críticas, incluindo o setor de energia. Essas diretrizes enfatizam a necessidade de proteger as redes contra ameaças cibernéticas. A Lei de Informação e Comunicações do Quénia de 1998, mandata a Autoridade de Comunicações do Quénia (CA) para desenvolver um quadro nacional de gestão da segurança cibernética e a fim de mitigar as ameaças cibernéticas e promover um ciberespaço queniano mais seguro. (Communications

Authority of Kenya, 2023) indica que que o governo criou a Equipa Nacional de Resposta a Incidentes Informáticos do Quénia – Centro de Coordenação (National KE-CIRT/CC), um quadro de colaboração multi-agências que é responsável pela coordenação nacional da segurança cibernética como ponto de contacto nacional do Quénia em questões de segurança cibernética. Em A promulgação da Lei do Uso Indevido de Computadores e Crimes Cibernéticos de 2018 percorreu um longo caminho no fortalecimento desta estrutura de colaboração multi-agências, entre outras facetas importantes que apoiam a resiliência da segurança cibernética nacional.

Em 2017, o Quênia sofreu um ataque cibernético que afetou a infraestrutura de energia, levando a cortes de energia em algumas áreas. Segundo (JACKSON, 2023), esse ataque destacou a necessidade de melhorar as defesas cibernéticas no setor mesmo assim em 2023, a Autoridade Nacional de Transporte e Segurança do Quénia (NTSA), a Kenya Power and Lighting Company (KPLC) uma das principais companhias elétricas do país e a Kenya Railways também sofreram interrupções nos serviços .

O Quênia está focado em fortalecer suas capacidades de cibersegurança através de parcerias internacionais e investimentos em tecnologia. A criação de centros de resposta a incidentes cibernéticos é uma das iniciativas para melhorar a resiliência contra ataques investindo na criação e implimentação de *Kenya Cybersecurity Strategy 2022*, assim como em inovação, pesquisa e Estrutura de desenvolvimento para promover a segurança cibernética de soluções seguras, segurança cibernética competitiva, econômica e personalizada soluções (Ministry of ICT, Innovation and Youth Affairs, 2022). A Quénia está provavelmente tão bem preparado como qualquer governo em África para responder a ataques, diz (BBC News, 2023), que afirma ainda que o país tem uma infra-estrutura de resposta emergente de segurança cibernética e informática bem desenvolvida. Está classificado em 51º lugar entre 182 países no ranking da Índice de Compromisso com a Cibersegurança da ONU. No entanto, ressalta que o país foi gravemente afetado de tantas maneiras diferentes que mostra “os perigos de se tornar dependente da tecnologia digital para funções econômicas críticas sem levar a sério a segurança cibernética”.

6.1.3 Nigéria

A Nigéria tem feito progressos na modernização de sua infraestrutura de energia, especialmente com a introdução de tecnologias de medição inteligente e a automação da rede para transformar modernizar sua infraestrutura que é um sistema de rede tradicional e convencional, com as consequentes limitações nas operações. A rede é um sistema centralizado com

comunicação unidirecional e onde a energia flui numa direção – desde os sistemas de geração, passando pela infraestrutura de transmissão e distribuição, até ao consumidor (OGUNDARI *et al.*, 2021). Os setores da eletricidade, petróleo e gás estão sujeitos a ataques cibernéticos, diz Babagana Monguno num workshop organizado pelo Gabinete do Conselheiro de Segurança Nacional (NSA) sobre a implementação da Política e Estratégia Nacional de Segurança Cibernética (NCPS) 2021, onde afirma que o crescimento digital nestes setores pode trazer riscos cibernéticos, a transformação digital destes setores é um desenvolvimento bem-vindo; no entanto, a adoção de tecnologias digitais e as vantagens financeiras que acompanham as tecnologias aumentam os riscos de ataques de ransomware (The Electricity Hub, 2021).

Segundo (NITDA, 2007) a Agência Nacional de Desenvolvimento de Tecnologia da Informação / *National Information Technology Development Agency* (NITDA) foi criada em abril de 2001 para implementar a Política Nigeriana de Tecnologia da Informação e coordenar o desenvolvimento geral de TI no país .E que a Lei Nacional de Desenvolvimento de Tecnologia da Informação de 2007 nos trata-se da criação de uma estrutura para o planejamento, pesquisa, desenvolvimento, padronização, aplicação, coordenação, monitoramento, avaliação e regulamentação de práticas, atividades e sistemas de Tecnologia da Informação na Nigéria. Comissão Reguladora de Eletricidade da Nigéria / *Nigerian Electricity Regulatory Commission* (NERC)) 2023 é um órgão regulador independente com autoridade para a regulamentação da indústria de energia elétrica na Nigéria, formado em 2005 através da Lei de Reforma do Sector de Energia Eléctrica de 2005 que agora é a Lei da Electricidade de 2023 para a formação e revisão das tarifas de eletricidade, políticas transparentes em matéria de subsídios, promoção de políticas que sejam eficientes e amigo do ambiente, incluindo também a formação e aplicação de normas na criação e utilização da energia, politicas de segurança ciberfisica, entre outros.

Apesar das regulações, a implementação e dos diretrizes não parece ser uma pratica como afirma o Caleb Adebayo quando disse:

> Numa pesquisa recente realizada pelo Sophos Group, uma empresa britânica de software e hardware de segurança, foi revelado que a Nigéria tem a maior percentagem de fugas de dados em todo o mundo e está classificada entre as cinco primeiras em questões como ransomware, malware e cryptojacking. Não é de admirar que no final do ano passado, durante os protestos do ENDSARS, vários websites de agências governamentais nigerianas, incluindo o website do Banco Central da Nigéria, tenham sido pirateados.(...) Apesar desta porosidade flagrante dos nossos sistemas de cibersegurança, nenhuma medida especial foi tomada para proteger infra-estruturas críticas como os nossos gasodutos, que são a base da nossa segurança energética e, inevitavelmente, da nossa segurança nacional. Parece haver a crença errada de que "*a Nigéria ainda não chegou lá"* e não é susceptível a estes ataques da elite (ADEBAYO, 2021).

A Nigéria tem sido alvo de vários ataques cibernéticos, incluindo tentativas de invasão em sistemas de controle de energia. Esses ataques sublinham a vulnerabilidade das infra-estruturas críticas do país. Com o aumento da digitalização, a Nigéria precisa continuar a investir em tecnologias de cibersegurança e fortalecer suas políticas para proteger as infraestruturas de energia. A cooperação internacional e o desenvolvimento de capacidades locais são cruciais para enfrentar esses desafios.

6.1.4 Ghana

O Gana fez progressos significativos no reforço da sua infra-estrutura de segurança cibernética, particularmente no sector eléctrico. O Centro Nacional de Segurança Cibernética/*National Cyber Security Centre* (NCSC) é uma agência nacional criada em 2018 sob o Ministério das Comunicações. O NCSC de acordo com Ghana National Cyber Security Center (), é responsável pelo desenvolvimento da segurança cibernética, coordenação da resposta a incidentes de segurança cibernética dentro do governo e com o setor privado, criação de Conscientização e Capacitação, Coordenação e Resposta a Incidentes de Segurança Cibernética (CERT), Proteção de Infraestrutura Nacional de Informação Crítica /*Critical National Information Infrastructure Protection* (CNIIP), Proteção Online de Crianças/ *Children Online Protection* (COP) e Cooperação Internacional, é responsável pelo desenvolvimento e implementação da Política e Estratégia Nacional de Segurança Cibernética do Gana, entre outros. Esta iniciativa centra-se na proteção de infraestruturas críticas de informação nacional, incluindo o setor elétrico, através de respostas coordenadas a incidentes de segurança cibernética e atividades de capacitação

A *CYBERSECURITY ACT, 2020* é uma pedra angular do quadro de segurança cibernética do Gana e foi criada pela Lei de Segurança Cibernética - Lei 1038 de 2020, para regular as atividades de segurança cibernética no país; promover o desenvolvimento da segurança cibernética no país e providenciar assuntos relacionados. Esta lei descreve medidas abrangentes para proteger infraestruturas críticas e estabelecer supervisão regulatória para práticas de segurança cibernética em vários setores, incluindo energia. O NCSC realiza extensos programas de formação e campanhas de sensibilização pública para reforçar as competências de segurança cibernética nos sectores governamental e privado. Isto é crucial para manter defesas robustas contra ameaças cibernéticas.

O país colabora com organismos internacionais como o Banco Mundial e o Fórum Económico Mundial para melhorar as suas capacidades de segurança cibernética. Essas parcerias

fornecem acesso às melhores práticas e recursos globais. Estas medidas destacam a abordagem proativa do Gana para proteger a sua infra-estrutura eléctrica contra a ameaça crescente de ataques cibernéticos.

A cibersegurança nas estações de energia é uma questão crítica para o continente africano já que maior parte do continente ainda tem sistemas convencionais tradicional com infraestruturas antigas e sem um sistema SCADA para monitoramento completo dos seus ativos. Embora haja avanços significativos em tecnologias e regulamentações, os desafios persistem devido ao aumento das ameaças cibernéticas. A colaboração internacional, o desenvolvimento de capacidades locais e investimentos contínuos em cibersegurança são essenciais para garantir a resiliência das infraestruturas de energia na África.

6.2 AMÉRICA

A cibersegurança no setor elétrico americano é uma área dinâmica e de crescente importância. Com a adoção de normas rigorosas, a superação de desafios técnicos e operacionais e a implementação de estratégias avançadas de resiliência, o setor elétrico está se tornando mais preparado para enfrentar ameaças cibernéticas. No entanto, a colaboração contínua entre o setor público e privado, juntamente com investimentos em tecnologias e talentos, será essencial para garantir a segurança e a confiabilidade da rede elétrica no futuro. A capacidade de adaptação e a inovação serão cruciais para proteger esta infraestrutura crítica contra as crescentes ameaças cibernéticas. O setor elétrico dos Estados Unidos é uma das infraestruturas críticas mais importantes do país, fornecendo energia essencial para residências, indústrias e serviços públicos. No entanto, à medida que a digitalização e a conectividade aumentam, o setor elétrico se torna cada vez mais vulnerável a ataques cibernéticos. Estes ataques podem ter consequências devastadoras, como interrupções no fornecimento de energia, danos a equipamentos críticos e impactos econômicos significativos.

A segurança cibernética no setor elétrico é regida por um conjunto abrangente de normas e diretrizes, estabelecidas por várias entidades reguladoras e de padronização.

> No cenário internacional, as principais referências em segurança cibernética para o setor elétrico são as regras *Critical Infrastructure Protection* (CIP) da *North American Electric Reliability Corporation* (NERC) e o *framework* do NIST. Há um sombreamento das atividades entre os dois órgãos dos Estados Unidos, mas em geral o framework do NIST serve como recomendação para os agentes. Além disso, o NIST emite diretrizes para as agências dos Estados Unidos da América, como a *Federal Energy Regulatory Commission* (FERC), a qual está vinculado a NERC. Essa, portanto, é uma regulação obrigatória para os agentes do sistema elétrico dos EUA. 56. Além disso, a jurisdição da

> FERC/NERC, consequentemente as regras do CIP, abrange o *Bulk Electric System* (BES) dos EUA, ou seja, os grandes geradores e transmissores de energia. O que tem uma certa equivalência à Rede Básica do Sistema Elétrico Brasileiro (ANEEL, 2021, p. 18).

Os padrões NERC, CIP são obrigatórios para todas as empresas de serviços elétricos na América do Norte e incluem requisitos rigorosos para a proteção de *Industrial Control Systems* (ICS) e Tecnologias Operacionais. Estes padrões abrangem desde a segurança física e cibernética até o controle de acesso e a resposta a incidentes.

A FERC aprova e faz cumprir os padrões de cibersegurança no setor elétrico. Em colaboração com a NERC, a FERC supervisiona a implementação dos padrões CIP, garantindo que as empresas de serviços públicos estejam em conformidade. O NIST oferece diretrizes através do Framework que é amplamente adotado para gerenciar riscos de cibersegurança. Este framework é reconhecido por sua abordagem flexível e abrangente, adaptável às necessidades específicas das organizações.

Segundo ANEEL (2021), vale ressaltar que os EUA, por terem uma grande infraestrutura de energia elétrica, por serem uns dos países mais avançados em tecnologia, são naturalmente os maiores alvos de ataques cibernéticos. Sendo assim, os regulamentos relativos à segurança cibernética desenvolvidos pelos EUA estão entre os mais completos. Dessa forma, outros países desenvolvidos em regulação, como Austrália e Canadá, seguem as mesmas regras do NIST e NERC. O México está sujeito à regulamentação do NIST e NERC nas interligações com os EUA. Mas, mesmo assim, O setor elétrico enfrenta vários desafios técnicos e operacionais em relação à cibersegurança tais como:

Complexidade dos Sistemas: A infraestrutura elétrica é composta por uma rede complexa de sistemas ICS e OT, que precisam ser integrados de forma segura com sistemas de TI.

Escassez de Profissionais Qualificados: Existe uma significativa escassez de profissionais qualificados em cibersegurança (GLENN *et al.*, 2016).

Recursos Limitados: Muitas empresas do setor elétrico enfrentam restrições orçamentárias que dificultam a implementação de medidas de cibersegurança robustas.

Vale ressaltar que os sistemas de distribuição e transmissão local são regulados pelos Estados.Portanto, não há uma uniformidade nas obrigações quanto à segurança cibernética. Mesmo sendo uma das principais referências em segurança cibernética para o setor elétrico, isso não faz com que seja seguro ao ponto de não sofrer ataques cibernéticos. Alguns dos ataques

reportados são:

Colonial Pipeline (2021): Este ataque de ransomware interrompeu o fornecimento de combustível na costa leste dos EUA.

SolarWinds (2020): em meados de dezembro, ocorreu uma grande violação da segurança cibernética da cadeia de abastecimento que afetou tanto o governo federal como as empresas do setor privado, incluindo empresas do setor energético (Center for Security Policy, 2024). *Ataques à Rede Elétrica dos EUA (2019):* Hackers militares dos EUA lançaram ataques cibernéticos contra a rede elétrica russa em resposta a tentativas de hacking durante as eleições de 2018 e campanhas de desinformação. Estes ataques destacaram a necessidade de proteção robusta contra ameaças estrangeiras.

Campanha de Intrusão (2014-2019): Diversos incidentes documentados pelo Departamento de Energia dos EUA envolvem ataques que visavam sistemas de informação sobre redes elétricas. Estes ataques resultaram em compromissos significativos e demonstraram a necessidade de uma vigilância constante.

> A região da América Latina e o Caribe sofreu 200 bilhões de tentativas de ataques em 2023, o que corresponde a 14,5% do total reportado globalmente no ano passado. Os países latino-americanos com maior atividade de ataques cibernéticos em 2023 foram, pela ordem, México, Brasil e Colômbia.

BHI Energy (2023): conta como foi o hackeado por ransomware a seus sistemas. A Empresa de serviços de engenharia de energia dos EUA detalha como a operação de ransomware Akira violou suas redes e roubou os dados durante o ataque CISO Advisor (2023).

Glenn *et al.* (2016) afirma que o impacto de um ataque cibernético pode ser grave para empresas de serviços públicos, fornecedores e o público, no entanto, não existe nenhum esforço de mitigação que possa ser 100% eficaz.

> Um mecanismo de defesa que funciona hoje pode não ser eficaz amanhã – as formas e os meios dos ataques cibernéticos mudam constantemente. É fundamental que todos os participantes do sector energético permaneçam conscientes das mudanças na segurança cibernética e continuem a trabalhar para prevenir potenciais vulnerabilidades nos sistemas que gerem (GLENN *et al.*, 2016)

Reconhecendo a crescente importância da segurança cibernética, muitas empresas de serviços públicos nos EUA adotaram iniciativas para prevenir e mitigar ameaças cibernéticas. Elas desenvolveram e implementaram um conjunto robusto de melhores práticas para proteger suas infraestruturas. No entanto, mesmo com essas práticas, as empresas de serviços públicos continuarão a necessitar de apoio do governo federal. Esse suporte é crucial para manter a prontidão cibernética, acessar informações sobre ameaças e combater as ameaças cibernéticas conforme elas surgem.

6.3 EUROPA

A União Europeia está intensificando as regras de cibersegurança, não apenas para dispositivos conectados à Internet, mas também para o setor elétrico. de Acordo com as informações da *European Comission* 2024, as novas diretrizes visam garantir a segurança cibernética em todos os produtos ligados direta ou indiretamente a outros dispositivos ou redes, incluindo dispositivos inteligentes como notebooks, smartphones e até geladeiras tecnológicas.

O setor elétrico europeu é uma das infraestruturas críticas mais importantes do continente, fornecendo energia essencial para a vida diária, economia e serviços públicos. Na União Europeia, o órgão que propõe a regulamentação para a segurança cibernética é a *European Network and Information Security Agency* (ENISA), que em 2016, publicou a Diretiva *Network and Information Security* (NIS), que foi, em seguida, incorporada pelos países membros (ANEEL, 2021). Embora tenha havido certa flexibilidade durante a incorporação, pois alguns países, como a França, já possuíam regulação para segurança cibernética.

Na França foi criada em 2009, a Agência Nacional de Segurança dos Sistemas de Informação (ANSSI), a autoridade nacional em matéria de cibersegurança. Sua missão é compreender, prevenir e responder ao risco cibernético. Segundo (França, 2023) a ANSSI está colocado sob a autoridade do Primeiro-Ministro, reportando ao Secretário-Geral da Defesa e Segurança Nacional (SGDSN), beneficia de uma posição que lhe permite implementar uma política global de cibersegurança e assegurar a sua coordenação à escala interministerial. Esta política visa defender as infraestruturas digitais públicas e privadas mais críticas. A ANSSI dirige-se também a todos os intervenientes na transformação digital do país e promove as condições para um diálogo de confiança com os seus congéneres a nível europeu e internacional.

No Reino Unido, criou-se a NCSC, A Defesa Cibernética Ativa (ACD) busca reduzir os danos causados e o *Cyber Incident Response* CIR. A França assim com o Reino Unido e os demais países da União Europeia, além de aplicar as Diretivas NIS, também tem suas próprias normas de acordo com o relatório de Aneel:

> Assim, embora a Diretiva NIS não seja específica para o setor elétrico, ela fornece princípios orientativos e estratégia de alto nível de segurança de redes e sistemas de informação para os países membros seguirem, como, por exemplo, a exigência de que os operadores relatem incidentes que afetem segurança, fornecimento, confidencialidade e integridade do serviço (ANEEL, 2021).

Na mesma senda, a União Europeia possui também a RGPD, não específica para o setor elétrico, pois para setor elétrico utiliza como base padrões internacionais de segurança de dados e de rede, além das regulações do NIST e NERC. Um dos objetivos principais da RGPD é

atualizar e melhorar a cultura de proteção de dados assim como LGPD no Brasil. As diretrizes do *COUNCIL OF EUROPEAN ENERGY REGULATORS* (CEER) focam na melhoria da segurança cibernética em sistemas de controle industrial e redes de distribuição de energia e promove a harmonização das práticas de cibersegurança entre os países membros.

Apesar dos esforços para manter uma boa segurança cibernética nesses países da união Europeia, ainda assim foram atingidos com ataques nos diferentes setores incluindo o setor elétrico como na Ucrânia, explorando as vulnerabilidades existentes nos sistemas, por exemplo:

Ataques de *ransomware* em fevereiro de 2020 a Grupo INA aleijou algumas operações comerciais da maior companhia petrolífera da Croácia e a maior cadeia de publicações de abastecimento (KASPERSKY, 2020).

Kaspersky citou que em abril de 2020, foi noticiado que a gigante energética portuguesa Energias de Portugal (EDP) tinha sido vítima de um ataque. Os criminosos cibernéticos que usavam o Ragnar Locker criptografaram os sistemas da empresa e exigiram um ransomware de quase 10 milhões de dólares.

A Schneider Electric é uma empresa multinacional francesa que fabrica produtos de energia e automação que vão desde componentes elétricos domésticos encontrados em grandes lojas até produtos de controle industrial e automação predial de nível empresarial, segundo a (CISO Advisor, 2024), em Janeiro deste ano, sofreu um ataque de ransomware realizado pelo grupo autodenominado Cactus, que levou ao roubo de dados corporativos, de acordo com pessoas familiarizadas com o assunto e confirmou ao BleepingComputer que a sua divisão de Negócios de Sustentabilidade sofreu um ataque cibernético e que os dados foram ex filtrados pelos operadores do ransomware.

De acordo com Power Technology (2020), a The European Network of Transmission System Operators for Electricity (ENTSO-E) que representa 42 operadores europeus de redes de transmissão em 35 países, afirmou em 2020 que tinha recentemente encontrado provas de uma intrusão cibernética bem-sucedida na sua rede de escritórios e estava a introduzir planos de contingência para evitar novos ataques.

A cibersegurança no setor elétrico europeu está evoluindo para enfrentar novos desafios e ameaças com a Adoção de Tecnologias Avançadas como inteligência artificial e *machine learning* que estão sendo utilizadas para detectar e responder a ameaças cibernéticas em tempo real, Colaboração Internacional entre os Estados-Membros da União Europeia, através de iniciativas como a ENISA, Desenvolvimento de Resiliência Cibernética se tornando um foco

central, com esforços direcionados para garantir que as infraestruturas críticas possam resistir e se recuperar rapidamente de ataques cibernéticos, assim como na Educação e Treinamento que são os investimentos em programas de educação e treinamento é crucial para preparar a próxima geração de profissionais de cibersegurança. Com a adoção de normas rigorosas, a superação de desafios técnicos e operacionais e a implementação de estratégias avançadas de resiliência, o setor elétrico está se tornando mais preparado para enfrentar ameaças cibernéticas. No entanto, a colaboração contínua entre os Estados-Membros da UE e o setor privado, juntamente com investimentos em tecnologias e talentos, será essencial para garantir a segurança e a confiabilidade da rede elétrica no futuro. A capacidade de adaptação e a inovação serão cruciais para proteger esta infraestrutura crítica contra as crescentes ameaças cibernéticas.

7 PERSPECTIVAS E POSSÍVEIS SOLUÇÕES

O setor elétrico enfrenta desafios significativos em matéria de cibersegurança, mas as perspetivas são positivas devido à adoção de tecnologias avançadas, à implementação de novas arquiteturas de segurança e ao aumento da cooperação internacional. Investir em novas tecnologias, formar especialistas e reforçar a cooperação internacional é uma forma importante de garantir a resiliência das infraestruturas elétricas contra ameaças cibernéticas. A adaptação e a inovação contínua são fundamentais para proteger o sector energético global das crescentes ameaças cibernéticas.

Governos, empresas e organizações em todo o mundo estão a tomar consciência das ameaças cibernéticas e a investir em medidas de segurança e resiliência. Este capitulo trata-se da perspectiva internacional sobre questões de segurança cibernética no sector eléctrico, centrando-se nas novas tendências emergentes, nas novas tecnologias e na necessidade de cooperação internacional.

7.1 Tendências Emergentes

- Adoção de tecnologias avançadas: O uso de tecnologias como inteligência artificial (IA) e aprendizado de máquina é cada vez mais utilizado para monitorar e responder a ameaças cibernéticas no momento. Essas tecnologias permitem analisar grandes quantidades de dados e identificar padrões estranhos que indicam um ataque cibernético iminente (CARLSON *et al.*, 2019).
- Segurança da Internet das Coisas (IoT): Com o uso crescente de dispositivos IoT na indústria eletrônica, a segurança desses dispositivos tornou-se uma prioridade máxima. Estão sendo desenvolvidas medidas para proteger os dispositivos IoT contra ataques, incluindo autenticação forte e criptografia de dados.
- Arquitetura Trustless: A implementação de arquiteturas de segurança "trustless", nas quais nenhuma entidade dentro ou fora da rede é automaticamente confiável, está ganhando popularidade. Este modelo exige que todas as tentativas de acesso aos recursos da rede sejam verificadas, reduzindo o risco de ataques internos e externos.(Iniciativa de Transparência Marítima da Ásia).

7.2 Inovações Tecnológicas

- Tecnologia Blockchain: A tecnologia Blockchain está sendo pesquisada para melhorar a segurança das transações eletrônicas e proteger dados confidenciais em redes inteligentes. A natureza distribuída e imutável do blockchain pode fornecer outra camada de segurança contra a manipulação de dados.
- Sistemas Avançados de Detecção de Intrusão (IDS): Estão sendo desenvolvidos novos sistemas de detecção de intrusão baseados em IA que identificam comportamentos suspeitos em tempo real, permitindo uma resposta rápida.Segurança na nuvem: à medida que aumenta a migração para serviços em nuvem, medidas de segurança estão sendo implementadas para proteger dados e aplicativos baseados em nuvem. Isso inclui o uso de criptografia avançada e políticas de acesso
- Segurança em Nuvem: Com a migração crescente para serviços em nuvem, medidas de segurança robustas estão sendo implementadas para proteger dados e aplicativos baseados em nuvem. Isso inclui o uso de criptografia avançada e políticas de acesso restritas .

7.3 Cooperação internacional

A cooperação internacional é essencial para combater as ameaças cibernéticas no setor eletrónico. Organizações como a Agência Internacional de Energia (AIE) e a Agência Europeia para a Segurança das Redes e da Informação (ENISA) estão a promover a cooperação entre países para partilhar informações sobre ameaças à segurança e melhores práticas. Segundo (PAULA, 2016), da mesma forma que hackers compartilham, entre si, novas técnicas de invasão, os Estados também terão que compartilhar, entre si, dados e sistemas de informações para coordenarem a defesa das diversas infraestruturas críticas cada vez mais interligadas. Afirma ainda que o Brasil já realizou acordos bilaterais com os seguintes países: África do Sul, Alemanha, Argentina, Bolívia, Canadá, Chile, China, Colômbia, Coreia do Sul, Equador, Espanha, EUA, França, Holanda, Índia, Israel, Itália, Japão, México, Paraguai, Peru, Portugal, Reino Unido, Rússia, Sri Lanka, Suécia, Suriname, Turquia e Polônia.

Partilha de informações: A criação de uma plataforma para a troca de informações sobre ameaças cibernéticas permite que os países aprendam com as experiências uns dos outros e adotem contramedidas.

Formação em cibersegurança: A formação em cibersegurança, como a Cyber

Europe da ENISA, ajuda os países a testar e melhorar a sua capacidade de responder aos problemas. **Desenvolvimento de padrões internacionais:** O desenvolvimento de padrões e diretrizes internacionais, como os da ISO/IEC, ajudará a unificar os esforços de segurança cibernética em todo o mundo para continuar a proteger infraestruturas críticas.

Em termo de soluções, podemos destacar o desenvolvimento da tecnologias para detectar ataques cibernéticos à rede elétrica, como C3D criado pelo Departamento de Energia dos EUA (DOE), que é uma tecnologia de monitoramento de sensores que pode ajudar fornecendo autenticação dos sensores de processo para ajudar a minimizar o impacto dos backdoors de hardware e dos ataques cibernéticos man-in-the-middle.Ajudando assim a mitigar os problemas dos padrões NERC de Proteção de Infraestrutura Crítica (CIP) e os requisitos da Cadeia de Fornecimento NERC que excluem o monitoramento dos sensores de processo (WEISS, 2021).

A Nozomi Networks desde 2015, participa do grupo de trabalho do IEC TC57 WG15, formado para realizar o desenvolvimento de padrões de segurança cibernética para comunicações do sistema de energia, tendo como seu escopo e propósito são focados no desenvolvimento de padrões de segurança dos protocolos de comunicação definidos pelo IEC TC57, entre eles as série IEC 60870-5, IEC 60870-6 e a série IEC 61850. (FREIRE, 2021a), e será responsável por sugerir mudanças na base de operação dos protocolos de energia como DNP3, MMS e Goose para fazer com que os protocolos que antes era inseguros por padrão, comecem a evoluir com novas versões agregando a autenticação, autorização e integridade.

8 CONCLUSÃO

Os desafios operacionais e cibernéticos crescentes com que se deparam as empresas da indústria energética são assuntos complexos, que estão a tornar-se mais agudos devido ao rápido desenvolvimento da digitalização e interconexão de sistemas. A crescente dependência de tecnologias digitais, nomeadamente sistemas de controlo industrial e a Internet das Coisas , permitiu melhorar significativamente a eficiência e a gestão, mas também expandiu o número de pontos vulneráveis à invasão de *hackers*.

No entanto, em termos de operações, as empresas de energia estão enfrentando a necessidade não apenas de assegurar a continuidade do abastecimento, mas também de gerir o aumento da procura. Tal situação implica a implementação de infraestrutura robusta e altamente resiliente que pode se adaptar a falhas e outras interrupções rapidamente a qualquer momento. O processo de modernização das redes elétricas, também conhecido como *Smart Grids*, envolve o uso de tecnologias avançadas que podem aumentar a eficiência, mas requerem investimentos substanciais e a eliminação de desafios regulatórios e financeiros.

Em paralelo, os riscos cibernéticos também se tornaram uma questão primária. Os ataques à infraestrutura crítica podem ser devastadores, pois não só param a energia, mas também prejudicam a ordem pública e a economia. As empresas de energia estão em risco constante do ataque de Malwares, Ransomwares, e ataque de negação de serviço distribuído que põem em causa a integridade, disponibilidade e confidencialidade dos sistemas. Para garantir a proteção dos sistemas, é necessária uma abordagem integrada que combine tecnologias de segurança avançadas, incluindo detecção e resposta a incidentes, uma forte governança e políticas de conformidade.

Para enfrentar tais desafios, a resposta exige um esforço comum de várias partes interessadas – governos, reguladores, tecnólogos fornecedores e as empresas de energia em si. A colaboração internacional também é importante, já que a ciber-ameaça não conhece fronteiras e muitas vezes é promovida por estados-nação e grupos criminosos fortemente organizados. Desenvolvimento de padrões globais de segurança cibernética e compartilhamento de informações sobre ameaças emergentes sãos os passos necessários para aumentar a resiliência do setor.

REFERÊNCIAS

ABNT, N. Iec 17799-tecnologia da informação: código de prática para a gestão da segurança da informação. **Rio de Janeiro: ABNT**, 2001.

ABNT, N. Iec 17799-tecnologia da informação: código de prática para a gestão da segurança da informação. **Rio de Janeiro: ABNT**, 2003.

ABNT, N. **NBR ISSO/IEC 27002**. [S.l.: s.n.], 2005.

ADEBAYO, C. **Cybersecurity in Nigeria's Energy Sector: Lessons from the "DarkSide"**. 2021. Disponível em: <https://nairametrics.com/2021/05/12/cybersecurity-in-nigerias-energy-sector-lessons-from-the-darkside/>. Acessado: 2024-06-12.

AGêNCIA Nacional de Energia Elétrica ANEEL. Rio de Janeiro, 2005.

ANDERSON, R.; MOORE, T. The economics of information security. **Science**, v. 314, n. 5799, p. 610–613, 2009.

ANEEL. **Análise de Impacto Regulatório (AIR) sobre segurança cibernética no Setor Elétrico Brasileiro: Relatório de Análise de Impacto Regulatório nº 3/2021-SRT-SGI-SRD-SRG-SFE-SFG/ANEEL**. 2021.

ANEEL, ANDEE. Atlas de energia elétrica do brasil. **Brasília**, 2008.

ARAUJO, C. A. **O que é Ciência da Informação? Informação amp; Informação**, v. 19, n. 1, dez. 2013. Disponível em: <https://doi.org/10.5433/1981-8920.2014v19n1p01>.

ASHIBANI, Y.; MAHMOUD, Q. H. **Cyber physical systems security: Analysis, challenges and solutions**. **Computers Security**, v. 68, 2017. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404817300809>.

BARROS, A. J. d. S.; LEHFELD, N. A. d. S. Fundamentos de metodologia científica. 3ª edição. **São Paulo**, 2007.

BARROS, B. D.; GEDRA, R. **Cabine Primária - Subestação de Alta Tensão de Consumidor**. Saraiva Educação S.A., 2015. ISBN 9788536528779. Disponível em: <https://books.google.com.br/books?id=m4uwDwAAQBAJ>.

BBC News. **Kenya Hit by Major Cyberattack**. 2023. Disponível em: <https://www.bbc.com/news/world-africa-66337573>. Acessado em: 2024-06-12.

BRASIL. **LEI Nº 9.648, DE 27 DE MAIO DE 1998. Altera dispositivos das Leis no 3.890-A, de 25 de abril de 1961, no 8.666, de 21 de junho de 1993, no 8.987, de 13 de fevereiro de 1995, no 9.074, de 7 de julho de 1995, no 9.427, de 26 de dezembro de 1996, e autoriza o Poder Executivo a promover a reestruturação da Centrais Elétricas Brasileiras - ELETROBRÁS e de suas subsidiárias e dá outras providências.** 1998. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/L9648cons.htm>. Acessado em: 09 de Maio de 2024.

BRASIL. **DECRETO Nº 5.081, DE 14 DE MAIO DE 2004. Regulamenta os arts. 13 e 14 da Lei no 9.648, de 27 de maio de 1998, e o art. 23 da Lei no 10.848, de 15 de março de 2004, que tratam do Operador Nacional do Sistema Elétrico - ONS.** 2004. Disponível em:

<https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/decreto/d5081.htm>. Acessado em: 05 de Maio de 2024.

BRASIL. **LEI Nº 10.848, DE 15 DE MARÇO DE 2004. Dispõe sobre a comercialização de energia elétrica, altera as Leis nºs 5.655, de 20 de maio de 1971, 8.631, de 4 de março de 1993, 9.074, de 7 de julho de 1995, 9.427, de 26 de dezembro de 1996, 9.478, de 6 de agosto de 1997, 9.648, de 27 de maio de 1998, 9.991, de 24 de julho de 2000, 10.438, de 26 de abril de 2002, e dá outras providências.** 2004. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/lei/l10.847.htm#:~:text=LEI%20N%C2%BA%2010.847%2C%20DE%2015%20DE%20MAR%C3%87O%20DE%202004.&text=Autoriza%20a%20cria%C3%A7%C3%A3o%20da%20Empresa,Art.>. Acessado em: 28 de Março de 2023.

BRASIL. **LEI Nº 10.848, DE 15 DE MARÇO DE 2004. Dispõe sobre a comercialização de energia elétrica, altera as Leis nºs 5.655, de 20 de maio de 1971, 8.631, de 4 de março de 1993, 9.074, de 7 de julho de 1995, 9.427, de 26 de dezembro de 1996, 9.478, de 6 de agosto de 1997, 9.648, de 27 de maio de 1998, 9.991, de 24 de julho de 2000, 10.438, de 26 de abril de 2002, e dá outras providências.** 2004. Disponível em: <hhttps://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/lei/l10.848.htm>. Acessado em: 09 de Maio de 2024.

BRASIL. **DECRETO Nº 9.573, DE 22 DE NOVEMBRO DE 2018. Aprova a Política Nacional de Segurança de Infraestruturas Críticas.** [S.l.]: D.O.U. DE 23/11/2018, P. 40., 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm>. Acessado em: 02 de Maio de 2024.

BRASIL. **DECRETO Nº 9.637, DE 26 DE DEZEMBRO DE 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput , inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.** [S.l.]: DD.O.U de 27/12/2018, pág. nº 23, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9637.htm>. Acessado em: 02 de Maio de 2024.

BRASIL. **LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).** [S.l.]: Diário Oficial da União: de 15/08/2018, pág. nº 59, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acessado em: 02 de Maio de 2024.

BRASIL. **DECRETO Nº 10.222, DE 5 DE FEVEREIRO DE 2020. Aprova a Estratégia Nacional de Segurança Cibernética**. [S.l.]: D.O.U. DE 06/02/2020, P. 6, 2020. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm>. Acessado em: 02 de Maio de 2024.

BRASIL. **DECRETO Nº 10.569, DE 9 DE DEZEMBRO DE 2020. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas**. [S.l.]: D.O.U de 10/12/2020, pág. nº 8, 2020. Disponível em: <https://www.planalto.gov.br/cCivil_03/_Ato2019-2022/2020/Decreto/D10569.htm>. Acessado em: 03 de Maio de 2024.

BRASIL. **Ministério de Minas e Energia: Conheça as instituições do setor elétrico brasileiro e as competências de cada uma**. 2021. Disponível em: <https://www.gov.br/mme/pt-br/assuntos/noticias/conheca-as-instituicoes-do-setor-eletrico-brasileiro-e-as-competencias-de-cada-uma>. Acessado em: 4 de Maio de 2024.

BRASIL. **RESOLUÇÃO NORMATIVA ANEEL Nº 964, DE 14 DE DEZEMBRO DE 2021. Dispõe sobre a política de segurança cibernética a ser adotada pelos agentes do setor de energia elétrica.** [S.l.]: AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA – ANEEL, 2021. Disponível em: <https://www2.aneel.gov.br/cedoc/ren2021964.html>. Acessado em: 03 de Maio de 2024.

BRASIL. **RESOLUÇÃO Nº 1, DE 11 DE SETEMBRO DE 2019. Aprova o Regimento Interno do Comitê Gestor da Segurança da Informação**. [S.l.]: DIÁRIO OFICIAL DA UNIÃO Publicado em: 19/09/2019 | Edição: 182 | Seção: 1 | Página: 1, 2021. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-n-1-de-11-de-setembro-de-2019-217042776>. Acessado em: 03 de Maio de 2024.

BRASIL. **O Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo**. 2023. Disponível em: <https://www.gov.br/ctir/pt-br/acesso-a-informacao/institucional/apresentacao>. Acessado em: 03 de Maio de 2024.

BRASIL. **O Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo**. 2023. Disponível em: <https://www.gov.br/ctir/pt-br/acesso-a-informacao/institucional/apresentacao>. Acessado em: 03 de Maio de 2024.

BRASILENE. **Fabricante de turbinas eólicas é fechada após ataque cibernético**. 2022. Disponível em: <https://brasiline.com.br/blog/fabricante-de-turbinas-eolicas-e-fechada-apos-ataque-cibernetico/>. Acesso em: 28 de Março de 2023.

CAMPOS, A. Como proteger infraestruturas críticas contra ameaças digitais. **CISO Advisor**, 2023. Disponível em: <https://www.cisoadvisor.com.br/security-room-posts/como-proteger-infraestruturas-criticas-contra-ameacas-digitais/>.

CANONGIA, C.; JUNIOR, R. M. **Segurança cibernética: o desafio da nova Sociedade da Informação. Parcerias Estratégicas**, v. 14, n. 29, 2009.

CARLETO, N. **Subestações elétricas**. [S.l.]: Brasília: NT Editora, 2019.

CARLSON, W.; EAGLE, S.; FERNANDEZ, M.; GOLDEN, V.; HALEY, A.; HANNIGAN, J.; LYNCH, T.; MAZZELLA, M.; MEHORTER, R.; SPADY, A. **Power Struggle: Anticipating Cyberattacks on the Electric Grid**. 2019. Disponível em: <https://journalism.csis.org/power-struggle-anticipating-cyberattacks-on-the-electric-grid/>. Acesso em: 18 maio 2024.

Center for Security Policy. **Recent Critical Infrastructure Attacks Expose Our Vulnerability and the Need for Change**. 2024. Disponível em: <https://centerforsecuritypolicy.org/recent-critical-infrastructure-attacks-expose-our-vulnerability-and-the-need-for-change/>. Acessado em: 10 de Maio de 2024.

CERT.BR. Cartilha de segurança para internet, versão 4.0. **São Paulo: Comitê**, 2012.

CISCOADVISOR. **Ataque derruba rede da fabricante de turbinas eólicas Nordex**. 2022. Disponível em: <https://www.cisoadvisor.com.br/ataque-derruba-rede-da-fabricante-de-turbinas-eolicas-nordex/>. Acesso em: 01 de Abril de 2023.

CISO Advisor. **BHI Energy conta como foi o hack por ransomware a seus sistemas**. 2023. Disponível em: <https://www.cisoadvisor.com.br/bhi-energy-conta-como-ransomware-hackeou-seus-sistemas/> Acessado em: 18 maio 2024.

CISO Advisor. **Gigante de energia Schneider Electric atingida por ransomware**. 2024. Disponível em: <https://www.cisoadvisor.com.br/gigante-de-energia-schneider-electric-atingida-por-ransomware/>. Acessado em: 17 maio 2024.

Communications Authority of Kenya. **Cyber Security**. 2023. Disponível em: <https://www.ca.go.ke/cyber-security>. Acessado: 2024-06-12.

CONDE, A. Simpósio acadêmico de segurança e defesa cibernética. **Escola Superior de Guerra**, 2022.

COUTO, K. S.; AMORIM, Y. R.; LIMA, K. M.; JÚNIOR, I. G. Os três pilares da segurança da informação na internet chinesa. **Journal of Technology & Information (JTnI)**, v. 2, n. 2, 2022.

DARYUS, C. E. e. T. Pesquisa nacional de seguranÇa da informaÇÃo 2014. 2014.

DIORIO, R. F.; SERAFIM, E.; ALVES, K. R.; MEIRA, M. C. Ataques de força bruta: Um estudo prático. **Departamento de Informática. Instituto Federal de Educação, Ciência e Tecnologia de São Paulo (IFSP). Capivari–SP**, 2019.

Eric Meyer and Michael Montoya. Como proteger a infraestrutura crítica contra ataques cibernéticos. **InfraFM**, 2022. Disponível em: <https://infrafm.com.br/Textos/5/22240/Como-proteger-a-infraestrutura-critica-contra-ataques-ciberneticos>.

European Commission. **The Digital Services Act: ensuring a safe and accountable online environment**. 2024. <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en>. Acessado em: 10 de Maio de 2024.

FARIAS, H. A cibersegurança em ambientes industriais: Desafios e estratégias para gestão de vulnerabilidades. **RESH Blog**, 2024. Disponível em: <https://resh.com.br/blog/a-ciberseguranca-em-ambientes-industriais-desafios-e-estrategias-para-gestao-de-vulnerabilidades/>.

FERRARI, V.; LIMA, P. Integração entre redes do sistema elétrico e da automação industrial. In: **Congresso Brasileiro de Automática-CBA**. [S.l.: s.n.], 2020. v. 2, n. 1.

FILHO, J.; MAMEDE, D. **Proteção de sistemas elétricos de potência**. Grupo Gen - LTC, 2011. ISBN 9788521618843. Disponível em: <https://books.google.com.br/books?id=8w3SygAACAAJ>.

FONTES, E. L. G. **Segurança da informação**. [S.l.]: Saraiva Educação SA, 2017.

França. **Découvrir l'ANSSI**. 2023. Disponível em: <https://cyber.gouv.fr/decouvrir-lanssi>. Acessado em: 16 de Maio de 2024.

FREIRE, A. **Desafios Operacionais e Cibernéticos das Empresas de Energia**. 2021. Disponível em: <https://www.linkedin.com/pulse/desafios-operacionais-e-cibern%25C3%25A9ticos-das-empresas-de-energia-freire/?trackingId=Ln3UtshERX2tcDkXi5ED3w%3D%3D>. Publicado no LinkedIn.

FREIRE, A. Desafios operacionais e cibernéticos das empresas de energia. 2021.

FREIRE, A. **O rápido desenvolvimento dos profissionais na de OT**. 2023. Disponível em: <https://www.linkedin.com/pulse/o-r%25C3%25A1pido-desenvolvimento-dos-profissionais-na-de-ot-am%25C3%25A9rica-freire/?trackingId=bRAH5f2JSQuKQKxK%2F9V9Wg%3D%3D>. Acessado em: 07 de Maio 2024.

GALDINO, J. C. da S. **Curso: Manutenção de ferrovia – Eletrotécnica II**. Instituto Federal do Rio Grande do Norte, 2011.

GESEL. Segurança cibernética do setor elétrico brasileiro: Desafios regulatórios e tecnológicos. 2021.

Ghana National Cyber Security Center. **About Ghana National Cyber Security Center**. Disponível em: <https://cybersecurity.gov.gh/about.html>. Acessado em: 8 de junho de 2024.

GLENN, C.; STERBENTZ, D.; WRIGHT, A. **Cyber threat and vulnerability analysis of the US electric sector**. [S.l.], 2016.

GOMES, L. A. O uso de malwares em guerras cibernéticas. Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte, 2015.

Government of South Africa. **Green Paper on National Health Insurance for South Africa**. 2023. Disponível em: <https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf>. Acessado em: 8 de junho de 2024.

HELERBROCK, R. **Usinas de Eletricidade**. [S.l.]: Brasil Escola, 2019. Disponível em: <https://brasilescola.uol.com.br/fisica/usinas-eletricidade.html>. Acesso em 18 de abril de 2023.

Herbert Smith Freehills. **High-profile cyberattacks increase emphasis upon cyber resilience in South Africa's energy sector**. 2023. Disponível em: <https://www.herbertsmithfreehills.com/notes/africa/2023-08/high-profile-cyberattacks-increase-emphasis-upon-cyber-resilience-in-south-africas-energy-sector/>.

HINTZBERGEN, J.; HINTZBERGEN, K.; BAARS, H. **Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002**. [S.l.]: Brasport, 2018.

JACKSON, A. **Cyberattack in Kenya Impacts Online Government Platforms**. 2023. Disponível em: <https://cybermagazine.com/application-security/cyberattack-in-kenya-impacts-online-government-platforms>. Acessado: 2024-06-12.

JIMENEZ, T.; COSTA, L. **A cibersegurança no setor energético**. 2024. Disponível em: <https://media.txone.com/prod/uploads/2023/02/TXOne-Annual-Report-Insights-Into-ICSOT-Cybersecurity-2022-202302.pdf>. Acessado em: 20 de Abril de 2024.

JUNIOR, R. M.; CANONGIA, C. Livro verde segurança cibernética no brasil. 2010.

KANALI, N. **State-sponsored cyber groups are actively targeting South African government - Trellix report**. 2023. Disponível em: <https://africabusinesscommunities.com/tech/tech-news/state-sponsored-cyber-groups-are-actively-targeting-south-african-government-trellix-report/>.

KARNOUSKOS, S. Stuxnet worm impact on industrial cyber-physical system security. In: **Proceedings of the IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society**. [S.l.: s.n.], 2011. p. 4490–4494.

KASPERSKY. **Top Ransomware de 2020**. 2020. Disponível em: <https://www.kaspersky.com.br/resource-center/threats/top-ransomware-2020>. Acessado em: 18 de Maio de 2024.

KÖCHE, J. C. **Fundamentos de metodologia científica**. EDITORA VOZES | Petrópolis, 2011. Disponível em: <http://www.adm.ufrpe.br/sites/ww4.deinfo.ufrpe.br/files/Fundamentos_de_Metodologia_Cienti%CC%81fica.pdf>.

LAKATOS, E. M.; MARCONI, M. d. A. Fundamentos de metodologia científica. 5. reimp. **São Paulo: Atlas**, v. 310, 2007.

LEÃO, R. Distribuição de energia elétrica. **Ceará**, v. 31, 2018.

LEE, R. M.; ASSANTE, M. J.; CONWAY, T. **Analysis of the cyber attack on the Ukrainian power grid**. [S.l.], 2016.

LEMOS, A.; SEARA, S.; PÉRSIO, W. Hackers no brasil. **Revista Contracampo**, n. 06, 2002.

LEWIS, J. A. **Cybersecurity and critical infrastructure protection**. [S.l.], 2006.

LUCAS, T. J.; TOJEIRO, C. C.; DIANA, A.; CARDOSO, T.; MORAES, E. A. de. Computação em nuvem–disponibilidade: Pesquisa aplicada na faculdade de tecnologia de ourinhos. **RETEC-Revista de Tecnologias**, v. 9, n. 2, 2016.

MARCIANO, J. L. P. Segurança da informação: uma abordagem social. 2006.

MARTINS, B. G. **Sistemas de Energia (SIE)**. 2011.

MARTINS, G. d. A.; PINTO, R. L. **Manual para elaboração de trabalhos acadêmicos**. [S.l.]: Atlas, 2001.

MICROSOFT, B. **O que é InfoSec (segurança da informação)?** 2023. Disponível em: <https://www.microsoft.com/pt-br/security/business/security-101/what-is-information-security-infosec>. Acesso em: 15 de Março 2023.

Ministry of ICT, Innovation and Youth Affairs. **Kenya Cybersecurity Strategy 2022**. [S.l.], 2022.

MITNICK, K. D.; SIMON, W. L. **The art of deception: Controlling the human element of security**. [S.l.]: John Wiley & Sons, 2003.

MODESTO, A. M. **Geração Transmissão e Distribuição de Energia Elétrica. APOSTILA REFERENTE A GERAÇÃO TRANSMISSÃO E DISTRIBUIÇÃO DE ENERGIA ELÉTRICA SEUS EQUIPAMENTOS E TECNOLOGIAS APLICADAS.** [s.n.], 2011. Disponível em: <https://silo.tips/queue/geraao-transmissao-e-distribuiao-de-energia-eletrica?&queue_id=-1&v=1683311468&u=MjAwLjEyOS4xOS4xMTE=>.

MUKHERJEE, S. Modernization and its impact on society. **Journal of Social Studies**, 2019.

National Institute of Standards and Technology (NIST). **Framework for improving critical infrastructure cybersecurity**. [S.l.], 2018.

NEOWAY. **Segurança da informação: O que é, e seus impactos e soluções nas empresas**. 2020. Disponível em: <https://blog.neoway.com.br/seguranca-da-informacao/>. Acesso em: 23 de Abril 2023.

Nigerian Electricity Regulatory Commission. **History and Role of the Nigerian Electricity Regulatory Commission**. 2023. Disponível em: <https://nerc.gov.ng/history-and-role/>. Acessed: 2024-06-12.

NITDA, N. I. T. D. A. **Official Website of the National Information Technology Development Agency (NITDA)**. 2007. Disponível em: <https://nitda.gov.ng/>. Acessado: 2024-06-12.

OGUNDARI, I.; OTUYEMI, F.; MOMODU, A.; SALU, L. Cyber security assessment of nigeria's electric power infrastructure. **African Journal of Science Policy and Innovation Management**, v. 1, n. 2, p. 87 – 104, Apr. 2021. Disponível em: <https://ajspim.oauife.edu.ng/index.php/ajspim/article/view/79>.

OLIVEIRA, E. **Relembre os piores ataques cibernéticos de 2020. Elétricas no alvo**. 2021. Disponível em: <https://pt.linkedin.com/pulse/relembre-os-piores-ataques-cibernÃl'ticos-de-2020-alvo-erich-oliveira>. Acesso em: 29 de Setembro 2023.

Parliament of Ghana. **Cybersecurity Act, 2020 (ACT 1038)**. 2020. Disponível em: <https://ir.parliament.gh/bitstream/handle/123456789/1800/CYBERSECURITY%20ACT,%202020%20(ACT%201038).pdf?sequence=1>. Acessado em: 8 de junho de 2024.

PAULA, E. R. de. Monografia, **Guerra Cibernética: Perspectivas para a Consolidação de uma Estratégia Cibernética para o Estado Brasileiro**. Rio de Janeiro: [s.n.], 2016.

PERUZZO, L. C. **Eletricidade**. [S.l.]: Centro Universitário Leonardo da Vinci, UNIASSELVI, 2016. ISBN 978-85-7830-970-1.

Power Technology. **The Five Worst Cyberattacks Against the Power Industry Since 2014**. 2020. Disponível em: <https://www.power-technology.com/features/the-five-worst-cyberattacks-against-the-power-industry-since2014/?cf-view>. Acessado em: 18 maio 2024.

PWC, C. S. A evolução do setor elétrico diante das ameaças cibernéticas nos ambientes de missão crítica. 2021.

QUISPE, C. A. F. **Tipos de Hackers**. [S.l.]: Disponivel em: <http://www.revistasbolivianas.org.bo>, 2018.

RAJA, A.; SRIVASTAVA, A. P. **Power plant engineering**. [S.l.]: New Age International, 2006.

RID, T.; BUCHANAN, B. Attributing cyber attacks. **Journal of Strategic Studies**, v. 38, n. 1-2, p. 4–37, 2015.

SARAOGI, M. **Security in wireless sensor networks**. In: CITESEER. **ACM SenSys**. [S.l.], 2004.

SÊMOLA, M. A importância da gestão da segurança da informação. Slides, 2010.

SILVA, D. G. V. d.; TRENTINI, M. Narrativas como técnica de pesquisa em enfermagem. **Revista Latino-Americana de Enfermagem**, Escola de Enfermagem de Ribeirão Preto / Universidade de São Paulo, v. 10, n. 3, p. 423–432, May 2002. ISSN 0104-1169. Disponível em: <https://doi.org/10.1590/S0104-11692002000300017>.

SILVA, E. M. da. **Cuidado com a engenharia social**. 2008. Disponível em: <https://www.tecmundo.com.br/msn-messenger/1078-cuidado-com-a-engenharia-social.htm>. Acessado em: 04 de Abril de 2024.

SIQUEIRA, I. **Redes de Infraestruturas Críticas - Análise de Desempenho e Riscos dos Setores de Energia, Petróleo, Gás, Água, Finanças, Logística e Comunicações**. [S.l.: s.n.], 2013. ISBN 9788571933156.

SIQUEIRA, I. P. de; CASTRO, N. de; MOSZKOWICZ, M.; CâMARA, L. Segurança cibernética do setor elétrico brasileiro: Desafios regulatórios e tecnológicos. Grupo de Estudo do Setor Eletrico- UFRJ, 2021.

SKOUDIS, E.; LISTON, T. **Counter hack reloaded: a step-by-step guide to computer attacks and effective defenses**. [S.l.]: Prentice Hall PTR, 2005.

The Electricity Hub. **Nigeria: Energy Sector Prone to Cyber Attacks - Monguno**. 2021. Disponível em: <https://theelectricityhub.com/nigeria-energy-sector-prone-to-cyber-attacks-monguno/>. Acessado em: 2024-06-12.

TXONE. **ANNUAL REPORT: Insights Into ICS/OT Cybersecurity 2022**. 2022. Disponível em: <https://media.txone.com/prod/uploads/2023/02/TXOne-Annual-Report-Insights-Into-ICSOT-Cybersecurity-2022-202302.pdf>. Acessado em: 20 de Abril de 2024.

ULBRICH, H. C.; VALLE, J. D. **Universidade Hacker: Desvendando todos os segredos do submundo dos hackers**. 4. ed. [S.l.]: Digerati, 2004.

WALTERS, J. P.; LIANG, Z.; SHI, W.; CHAUDHARY, V. Security in distributed, grid, and pervasive computing. **Wireless sensor network security: A survey**, 2006.

WEISS, J. **Information Technology**. 2021. Disponível em:<https://www.controlglobal.com/home/blog/11290637/information-technology>. Acessado em: 16 mai 2024.

WOEBCKEN, C. **Design Thinking: uma forma inovadora de pensar e resolver problemas**. 2019. Disponível em: <https://rockcontent.com/br/blog/design-thinking/>. Acessado em: 03 de Maio de 2024.