# CLASSIFICAÇÃO E ANÁLISE DOS IMPACTOS DE ATAQUES CIBERNÉTICOS EM MERCADOS LOCAIS DE ENERGIA

Rafael Alves Porte


Departamento de Engenharia Eletrotécnica

Mestrado em Engenharia Eletrotécnica – Sistemas Elétricos de Energia

**2020**

Relatório elaborado para satisfação parcial dos requisitos da Unidade Curricular de DSEE - Dissertação do Mestrado em Engenharia Eletrotécnica - Sistemas Elétricos de Energia do Instituto Superior de Engenharia do Porto (ISEP/IPP) e do Trabalho de Conclusão de Curso do Curso de graduação em Engenharia Elétrica do Instituto Federal de educação, Ciência e Tecnologia de Santa Catarina (IFSC – Câmpus Florianópolis). Este trabalho foi elaborado no âmbito do acordo internacional de Dupla Titulação entre o Instituto Superior de Engenharia do Porto (Portugal) e o Instituto Federal de educação, Ciência e Tecnologia de Santa Catarina (Brasil) como parte dos requisitos para obtenção do título de Mestre em Engenharia Eletrotécnica - Sistemas Elétricos de Energia pelo ISEP/IPP e de Engenheiro Eletricista pelo IFSC.

Candidato: Rafael Alves Porte, Nº 1182177, 1182177@isep.ipp.pt

Orientação científica: Professora Doutora Isabel Cecília Correia da Silva Praça Gomes Pereira, icp@isep.ipp.pt , e Professor Doutor Rubipiara Cavalcante Fernandes, piara@ifsc.edu.br

Coorientação: Professor Doutor Sérgio Filipe Carvalho Ramos, scr@isep.ipp.pt

Este trabalho foi realizado no âmbito do Projeto SPET com PTDe/EEI-EEE/ 29165/2017


Departamento de Engenharia Eletrotécnica

Mestrado em Engenharia Eletrotécnica – Sistemas Elétricos de Energia

**2020**

Ficha de identificação da obra elaborada pelo autor.

Porte, Rafael
**CLASSIFICAÇÃO E ANÁLISE DOS IMPACTOS DE ATAQUES** CIBERNÉTICOS **EM MERCADOS LOCAIS DE ENERGIA / Rafael Porte** ; orientação **de Rubipiara Cavalcante Fernandes.** - Florianópolis, **SC,** 2020.
82 p.

**Trabalho de Conclusão de Curso (TCC)** - **Instituto** Federal **de Santa Catarina, Câmpus** Florianópolis. Bacharelado **em Engenharia Elétrica. Departamento** Acadêmico **de** Eletrotécnica.
Inclui Referências.

**1. Mercados Locais de Energia.** 2. **Segurança** Cibernética. **3. Smart Grid. 4. Smart Home. I. Cavalcante** Fernandes, **Rubipiara. II. Instituto Federal de** Santa Catarina. **Departamento Acadêmico de** Eletrotécnica. III. Título.

Instituto Superior de Engenharia do Porto

# ATA DE PROVAS DE MESTRADO

Nº: MEESEE / 3 / 2020

Data: 2020 - 07 - 22

| | | | |
|---|---|---|---|
| **Hora de Início:** | 15:00 | **Elaborado por:** | José António Beleza de Carvalho |
| **Hora de Fim:** | 16:00 | **Data:** | 2020-07-22 |

| **Presentes** |
|---|
| Presidente do Júri: José António Beleza de Carvalho |
| Orientador: Isabel Cecília Correia da Silva Praça Gomes Pereira |
| Vogal: Sergio Filipe Carvalho Ramos |
| Vogal: Teresa Alexandra Ferreira Mourão Pinto Nogueira |
| |

**Assuntos Tratados:**

Ata da Reunião do Júri para discussão da Dissertação apresentada pelo Licenciado RAFAEL ALVES PORTE, para obtenção do grau de Mestre em Engenharia Eletrotécnica - Sistemas Elétricos de Energia - Mestrado (2011/2012), intitulada: "CLASSIFICAÇÃO E ANÁLISE DOS IMPACTOS DE ATAQUES CIBERNÉTICOS EM MERCADOS LOCAIS DE ENERGIA".

Aos vinte e dois dias do mês de julho do ano dois mil e vinte na sala do ISEP, nos termos do Decreto-Lei número setenta e quatro de vinte e quatro de março de dois mil e seis, republicado no anexo ao Decreto-Lei número cento e quinze de sete de agosto de dois mil e treze, reuniu para discussão da dissertação acima referida, o júri nomeado para o efeito com a presença dos elementos acima indicados.

As provas tiveram início às quinze horas, com o Presidente do júri cumprimentando os restantes membros, agradecendo a sua colaboração e desejando felicidades ao candidato.

De seguida, o candidato cumprimentou o júri e passou à apresentação oral da sua dissertação, com duração de vinte minutos.

Foi arguente Teresa Alexandra Ferreira Mourão Pinto Nogueira, que fez uma apreciação global do trabalho e colocou algumas questões ao candidato, a que este teve oportunidade de responder.

Terminada a discussão, o júri procedeu nos termos da lei (artigos vinte e dois e vinte e quatro do decreto lei citado), deliberando aprovar, por unanimidade, o candidato com a classificação de dezassete (17) valores, tendo o mesmo júri fundamentado esta classificação do seguinte modo:

ANÁLISE DO RELATÓRIO ESCRITO (40%): Conteúdo, redação, ilustrações, adequação da metodologia desenvolvida ao problema e resultados 16,86 valores;

RELEVÂNCIA DO TRABALHO (30%): Relevância social e ambiental, criatividade, Qualidade técnica / exigência programática 17,00 valores;

APRESENTAÇÃO E DEFESA PÚBLICA (30%): Qualidade dos meios, clareza da apresentação, capacidade de argumentação, domínio das temáticas relacionadas com o trabalho 16,00 valores;

Avaliação global da dissertação de Mestrado:
0,4 x 16,86 + 0,3 x 17,00 + 0,3 x16,00 = 16,6 valores

# ATA DE PROVAS DE MESTRADO

Nº: MEESEE / 3 / 2020

Data: 2020 - 07 - 22

Integrou o Júri das provas o Professor Rubipiara Calvalcante Fernandes, ao abrigo do programa de dupla titulação entre o ISEP e o Instituto Federal de Educação,Ciência e Tecnologia de Santa Catarina, Brasil.

Não havendo outros assuntos a tratar, a reunião foi dada por encerrada às dezasseis horas.

Da reunião foi exarada a presente ata que, depois de lida em voz alta, vai ser assinada por todos os membros do júri.

| Aprovado por: | Data |
|---|---|
| Ata assinada digitalmente.<br>Signature Not Verified<br>Digitally signed by Assinatura digital de atas de Projeto/Estágio/Tese<br>Date: 2020.07.27 09:27:33 +01:00<br>Reason:<br>Location: Porto | 2020-07-22 |

Trabalho dedicado a todos os brasileiros imigrantes, sobreviventes, que lutam todos os dias para sobreviver no velho continente.

# *Agradecimentos*

Primeiramente, gostaria de agradecer aos meus pais Silas Eduardo Porte e Josiane Helena Alves Porte e a toda minha família, os quais me proveram os recursos econômicos e incentivos psicológicos para o desenvolvimento deste estudo. Em seguida agradeço aos amigos Luis Santos Proença e Silvia Grade, os quais me acolheram na cidade do Porto e estiveram sempre a disposição em eventuais necessidades durante o ano em que passei em Portugal.

Agradeço a Professora Doutora Isabel Cecília Correia da Silva Praça Gomes Pereira, Professor Doutor Rubipiara Cavalcante Fernandes e Professor Doutor Sérgio Filipe Carvalho Ramos, os quais através de sua orientação possibilitaram a realização deste trabalho, além da paciência e disposição para sanar quaisquer dúvidas que ocorreram no decorrer da elaboração deste. Deixo também um agradecimento especial ao Pesquisador Científico do GECAD Rui Andrade, sem o qual não seria possível realizar as simulações utilizadas nos Casos de Estudo.

Ao Instituto Federal de Educação, Ciência e Tecnologia (IFSC), que, sem a oferta do programa de Dupla Titulação, não seria possível o ingresso ao Instituto Superior de Engenharia do Porto (ISEP).

Aos amigos e colegas que estiveram presentes durante todo o processo de elaboração do relatório, contribuindo de diversas formas para a conclusão do mesmo.

A todos, o meu sincero muito obrigado!

# *Resumo*

Os mercados locais de energia elétrica são uma forte tendência na evolução dos aspetos relacionados à comercialização de energia elétrica em todo o mundo. Consumidores produtores e outros agentes que compõem um mercado local de energia podem estar sujeitos a ataques cibernéticos em sua rede de dados, tais ataques podem ter impactos econômicos e sociais.

Desta forma, a presente dissertação apresenta uma revisão bibliográfica sobre os mercados de energia elétrica tradicionais, mercados locais de energia e seus modelos de negócio. Além disso, apresenta, ainda, as arquiteturas de *Smart Grids* e *Smart Homes*, que possibilitam o fluxo de dados para que seja possível estabelecer preços e quantidades de maneira dinâmica. Também é apresentada uma revisão bibliográfica sobre os riscos e objetivos de segurança aos quais estão submetidos esses sistemas. Por fim, são classificados os tipos de ataques e definidas as graduações de impacto considerando o que foi apresentado previamente além da listagem de metodologias utilizadas para a garantia dos critérios de segurança.

No âmbito da delimitação dos estudos de caso são definidos os métodos de precificação, bem como os modelos a serem analisados. Nos casos 1 e 2 há uma análise qualitativa daquilo que poderia acontecer em casos de ataques previamente definidos para uma rede de mercado local situada em Salamanca na Espanha. Já nos casos 3 e 4, os dados utilizados foram adquiridos de medições locais e inseridos em uma rede de mercado local estabelecida neste trabalho e simulada no software MASCEM [1].

***Palavras-Chave***

Mercados locais de energia, Mercado de energia, Segurança cibernética, MASCEM, *Smart Grid, Smart Home.*

# *Abstract*

The local electricity markets are a strong trend in the evolution of aspects related to the commercialization of electricity worldwide. Producing consumers and other agents that make up a local energy market may be subject to attacks on your data network, such attacks can have economic and social effects.

In this way, the present dissertation presents a bibliographic review on the traditional electric energy markets, local energy markets and their business models. In addition, it also features Smart Grids and Smart Homes architectures, which allow the flow of data so that it is possible to use prices and use the way of use. A bibliographic review on the security risks and objectives to which these systems are involved is also published. Finally, the types of attacks and the types of attacks that affect the levels of impact, considering what was presented in addition to the list of methods used to ensure safe use.

Within the scope of the case studies, pricing methods are defined as well as the models to be analyzed. In cases 1 and 2, there is a qualitative analysis of what could happen in cases of attack caused by a local market network located in Salamanca, Spain. In cases 3 and 4, the data used were purchased from local measurements and inserted in a local market network, in this work and simulated in the MASCEM software [1].

***Keywords***

Local energy markets, Energy market, Cybersecurity, MASCEM, Smart Grid, Smart Home

# *Índice*

# *Índice de Figuras*

# *Índice de Tabelas*

# *Acrónimos*

| | | |
|---|---|---|
| AA | - | *Attribute authority* - Autoridade de atributo |
| AC | - | *Attribute Certificates* - Certificados de Atributo |
| AES | - | *Advanced Encryption Standard* - Padrão Avançado de Criptografia |
| AMI | - | *Advanced metering infrastructure* - Infraestrutura de medição avançada |
| AT | - | Áustria |
| BAN | - | *Building Area Network* - Rede de área de construção |
| BE | - | Bélgica |
| BM | - | *Business Model* - Modelo de Negócio |
| CA | - | *Certification Authority* - Autoridade de Certificação |
| CAPEX | - | *Capital Expenses* - Despesas de capital |
| CIS | - | *Client information system* - sistema de informação do cliente |
| CP | - | Consumidor Produtor |
| CT | - | Consumidor tradicional |
| D&P | - | *Demonstration and pilot projects* - Projetos de demonstração e pilotos |
| D/C | - | Distribuidor e/ou comercializador |
| DE | - | Alemanha |
| DER | - | *Distributed Energetic Resources* - Recursos Energéticos Distribuídos |
| DK | - | Dinamarca |
| DR | - | *Demand response* - Resposta ativa à demanda |
| DRMS | - | *Demand response management system* – Sistema de gerenciamento de resposta ativa à demanda |
| DRP | - | *Demand response provider* - Provedor de resposta a demanda |
| DAS | - | *Digital Signature Algorithm* - Algoritmo de assinatura digital |
| DSM | - | *Demand Side Management* - Gerenciamento pelo lado da demanda |
| ECDSA | - | *Elliptic Curve Digital Signature Algorithm* Algoritmo de assinatura digital de curva elíptica |
| EMS | - | *Energy management system* - Sistema de gerenciamento energético |
| EPC | - | *Energy Performance Contracting* - Contratação de desempenho energético |

ES - Espanha

ESC - *Energy Supply Contracting* - Contratação de fornecimento de energia

ESCO - *Energy service company* - Empresas de Serviços Energéticos

ESI - *Energy systems integration* - Integrador de sistemas energéticos

FI - Finlândia

FIPS - *Federal Information Processing Standards*
Padrões Federais de Processamento de Informações (USA)

FR - França

G - Gerador

G.C - Grande Consumidor

GB - Reino Unido

GECAD - Grupo de Pesquisa em Engenharia e Computação Inteligente
para Inovação e Desenvolvimento Avançado

GG - Gerador de grande porte

GL - Gerador Local

GP - Gerador de pequeno porte

HAN - *Home Area Network* - Rede de área doméstica

HFID - *High Frequency Identity* - Identidade de alta frequência

HMAC - *Hash message authentication code* - Código de autenticação de mensagem

IAN - *Industrial Area Network* - Rede de área industrial

ICES - *Integrated Community Energy System* – Sistema Integrado de Energia Comunitária

ID - *Identity* - Identidade

IDS - *Identification System*- Sistema de deteção de intrusões

IP - *Internet Protocol* - Protocolo de Internet

IT - Itália

kW - Quilowatt

LFID - *Low Frequency Identity* - Identidade de baixa frequência

LMS - *Load management system* - sistema de gerenciamento de carga

MDMS - *Meter data management system* - Sistema de gerenciamento de dados medidos

ML - Mercado Local

MWh - Megawatt hora

NAN - *Neighborhood Area Network* - Rede da árear do bairro

| | | |
|---|---|---|
| NIST | - | *National Institute of Standards and Technology (USA)*<br>Instituto Nacional de Padrões e Tecnologia (USA) |
| NL | - | Países Baixos |
| OMS | - | *Output management system* - Sistema de gerenciamento de saída |
| P&D | - | Projetos em pesquisa e desenvolvimento |
| PEV | - | *Plug-in electric vehicle* - Veículo elétrico plug-in |
| PHEV | - | *Plug-in hybrid electric vehicle* - Veículo híbrido elétrico plug-in |
| PKC | - | *Public key certificate* - Certificado de chave pública |
| PR - | - | Consumidor prioritário |
| Prosumer | - | Consumidor produtor |
| PT | - | Portugal |
| PSS | - | *Product-service system* - Sistema de produto para serviço |
| PV | - | *Photovoltaic* - Fotovoltaico |
| RTU | - | *Remote Terminal Unit* - Terminal de unidade remota |
| SCADA | - | *Supervisory control and data acquisition*<br>Sistema supervisor de controlo e aquisição de dados |
| SE | - | Suécia |
| SG | - | *Smart Grid* - Rede Inteligente |
| SH | - | *Smart Home* - Casa Inteligente |
| SM | - | *Smart Meter* - Medidor Inteligente |
| SND | - | Serviços de Nutrição e Dietética |
| TCP | - | *Transmission Control Protocol* - Protocolo de Controle de Transmissão |
| TDES | - | *Triple Data Encryption Algorithm* - Algoritmo de criptografia tripla de dados |
| TIC | - | Tecnologias de informação e comunicação |
| UE | - | União Européia |
| WAN | - | *Wide Area Network* - Rede de área ampla |

# 1. INTRODUÇÃO

A evolução contínua dos setores elétricos espalhados pelo mundo é indiscutível. Devido à necessidade crescente da energia elétrica no cotidiano das pessoas, os setores elétricos de todos os países devem estar sempre em desenvolvimento, de maneira a se adequar aos hábitos de consumo de suas populações, aumentar a sua fiabilidade exploração, além de proporcionar ao meio ambiente um uso dos recursos de maneira sustentável sem deixar de lado o aspeto econômico e social do uso da eletricidade.

Considerando tais evoluções de hábito de consumo e sustentabilidade ambiental e econômica, mercados locais de energia são uma tendência. Nesta nova abordagem, consumidores assumem uma postura mais próxima de um fornecedor de maneira que podem, assim, definir de quem compram a energia elétrica necessária para suprir sua demanda energética, além de também poderem ser fornecedores, já que podem vender sua produção. A comercialização local de energia transcende tal postura por meio da possibilidade de vender energia elétrica gerada localmente, evitando perdas e, desta forma, sendo uma opção sustentável e barata do atendimento da demanda crescente.

Devido ao fato de mercados locais de energia serem, em comparação a tradicionais mercados grossistas, um campo ainda não muito explorado e relativamente novo, a relação que tais mercados devem ter diante das estruturas globais é um campo de estudo com elevado potencial bibliográfico. Diante deste fato, é notável que estruturas de mercado focadas na comercialização de energia elétrica são ambientes complexos e que dispõem um altíssimo volume de dados gerados num fluxo igualmente elevado. Para que seja possível

tomar decisões coerentes relacionadas à compra ou venda de energia elétrica, de acordo com um modelo de negócios e na conjuntura de mercados locais de energia, se faz relevante analisar os critérios de veracidade das informações coletadas e de segurança das redes de comunicação que transmitem os dados entre os agentes de geração e consumo e os agentes de mercado. Dentre os vários simuladores de mercados de energia encontrados na literatura, o *Multiagent Simulator of Competitive Electricity Markets* (MASCEM) [1] se mostra extremamente promissor, do ponto de vista técnico, para simular mercados locais de energia, razão pela qual foi usado nos cenários 3, 4 e 5 apresentados nesta dissertação.

Sendo assim, o presente trabalho foca-se na realização de um estudo sobre mercados locais de energia que relaciona a interação entre os agentes de mercado e a importância da veracidade das informações trocadas entre os agentes relacionados.

## 1.1. CONTEXTUALIZAÇÃO

De acordo com Lakatos e Marconi [2] a delimitação de um estudo acontece a partir do ato de colocar limites a uma investigação científica. Deste modo, os limites do presente estudo podem ser determinados por meio de três tópicos:

i. Assunto;

ii. Extensão;

iii. Série de fatores.

O assunto (i) foco da presente dissertação é relacionado aos mercados locais de energia elétrica e ligações com mercados num contexto global. Neste sentido, sobre a extensão (ii) do estudo, são considerados os riscos e critérios de segurança aos quais os mercados locais de energia devem ser submetidos e avaliados.

A série de fatores (iii) define-se como a aplicação de técnicas utilizadas no segmento de inteligência artificial e a descoberta de conhecimento fundamentais para que sejam criados diferentes cenários referentes à operação de mercados locais de energia, sua rede de comunicação de dados e segurança cibernética. O nível de profundidade bibliográfica adotado define-se como sendo o necessário para que os estudos de caso sejam fundamentados.

## 1.2. MOTIVAÇÕES

O desenvolvimento do presente estudo se deu em virtude de um conjunto de motivações as quais podem ser evidenciadas a partir da necessidade de dedicação, por parte da comunidade científica, focada no desenvolvimento de estudos referentes a mercados locais de energia.

A linha de estudo relacionada aos mercados locais de energia é considerada emergente no mundo. Ainda não é realidade na maioria dos mercados de energia, mas é um campo que dispõe de grande potencial de desenvolvimento em virtude da crescente disseminação de geração renovável de energia elétrica. Além disso, o uso de técnicas de inteligência artificial com grande potencial de inovação se traduz em uma motivação evidente e que pode ser vista como um conhecimento diferenciado para um engenheiro eletrotécnico. Com o aumento da implementação de mercados locais de energia elétrica e, sendo assim, o crescente fluxo monetário envolvido aumentam também as possibilidades de ataques a tais redes, desta forma o estudo e definição do impacto de ataques cibernéticos se faz pertinente.

## 1.3. OBJECTIVOS

A presente dissertação dispõe de cinco objetivos principais. São eles:

- Revisar o estado da arte sobre a organização de mercados de energia elétrica;
- Revisar o estado da arte sobre a organização de mercados locais de energia elétrica;
- Analisar estruturas de mercados locais de energia elétrica e a aplicação de modelos de negócios;
- Analisar os riscos e critérios de segurança que redes de mercados locais devem atender;
- Analisar, a partir de bibliografias e simulações realizadas com base em dados reais, os impactos de ataques cibernéticos a redes de mercados locais de eletricidade.

## 1.4. ORGANIZAÇÃO DO DOCUMENTO

A presente dissertação é composta por seis capítulos. Estes são desenvolvidos ao longo do trabalho para que os objetivos supracitados sejam alcançados. O capítulo 1 descreve uma contextualização sobre os temas abordados. Além disto, descreve também os objetivos e a estrutura do trabalho desenvolvido.

No capítulo 2 é realizada uma revisão do estado da arte no que se refere aos mercados de energia elétrica tradicionais, mercados locais de energia e os modelos de negócio para o setor elétrico.

O capítulo 3 introduz o tema de redes inteligentes, um âmbito geral dos desafios de segurança que uma rede de mercados locais está submetida e as arquiteturas de *Smart Homes* (SHs) e *Smart Grids* (SGs).

O capítulo 4, ainda no âmbito das redes inteligentes, tem por objetivo definir o que é segurança cibernética, explorando-a tanto para SGs quanto para SHs, a definição qualitativa dos objetivos de segurança, classificação das ameaças e avaliação de impactos para as redes e suas interligações.

O capítulo 5 discorre propriamente sobre os casos de estudo, os modelos utilizados de mercado (exemplo de um mercado local de Salamanca), definições de preço de mercado e determinação de cenários de ataque os quais são analisados hora qualitativa, hora quantitativamente.

No capítulo 6 são apresentadas as conclusões gerais e perspetivas de trabalhos futuros. Tais conclusões são baseadas nos contributos apresentados, resultados obtidos e nas análises realizadas.

# 2. ESTADO DA ARTE

## 2.1. MERCADOS DE ENERGIA ELÉTRICA

A energia elétrica foi "descoberta" no início do século XIX, porém somente consumida em larga escala nas últimas décadas desse mesmo século e posteriormente expandida já adentrando o século XX. A partir de então a eletricidade passou a ser um dos mais importantes elementos, se não o mais importante, no processo de modernização das sociedades, impulsionando a própria industrialização, alterando a estrutura urbana e refletindo na própria cultura. No entanto o setor elétrico é um sector particular, na medida em que se compõe de quatro atividades distintas, a produção, isto é toda a função para produzir a eletricidade; o transporte, que envolve todo o transporte de eletricidade na rede de alta e muito alta tensão (sem atividade de fornecimento); a distribuição, que envolve o transporte de eletricidade em postos de média e baixa tensão com o fim de fornecimento ao cliente final; e a comercialização que engloba a venda e revenda de eletricidade ao consumidor final e que inclui o serviço pós-venda [3].

Os setores de eletricidade em quase todos os lugares da Terra evoluíram com (principalmente) monopólios geográficos verticalmente integrados, pertencentes ao Estado ou a empresas privadas. Detidos e sujeitos a regulamentação de preço e entrada como monopólios naturais. Os componentes principais do fornecimento de eletricidade: geração, transmissão, distribuição, e fornecimento de varejo foram integrados em empresas elétricas

individuais consumidores comerciais e industriais de varejo em uma área geográfica definida [4].

Os mercados de energia elétrica, com os primeiros surgimentos a partir de 1980, tinham dominância de geração térmica movida a combustíveis fósseis. Desta maneira, como é comum neste tipo de mercado, a comercialização ocorre no curto prazo (mercados do dia seguinte) já que a dominância termoelétrica na geração conduz a uma fácil previsibilidade do preço da energia. Basicamente o preço da energia será o da térmica despachada (para atender a demanda) com maior custo de produção naquela hora. Isso se traduz em uma forte conexão entre o preço da energia e o preço dos combustíveis fósseis utilizados, no geral gás e carvão [5]. Com o avanço da geração alternativa, maneiras menos poluidoras, mais sustentáveis de geração de energia elétrica essa correlação deixa de ser tão relevante como anteriormente. A migração da geração energética para uma matriz mais limpa através de incentivos econômicos trás complicações técnicas de previsibilidade de preço ao mercado de energia.

Com as complicações técnicas de operação ocorre um aumento dos custos associados a este processo e desta forma surge a necessidade do aumento das tarifas de energia ou subsídio governamental [6]. Desta maneira é possível perceber que ao longo do tempo as atividades dos setores elétricos estão cada vez mais migrando para instituições privadas. O que acaba por mudar o panorama do mercado, uma vez que tais empresas carregam com sigo outro viés institucional e estão mais sujeitas as variações do mercado por não terem consigo o dinheiro do estado.

Nestes termos, em sistemas elétricos com predomínio de geração térmica tradicional, havendo concorrência plena, os preços tenderão a igualar os custos médios de produção. Se em algum momento os preços tenderem a superar consistentemente os custos médios de produção, novos geradores eficientes serão atraídos para o mercado e a oferta adicional reduzirá os preços de mercado de maneira que se estabeleça a igualdade de equilíbrio entre preços e custos médios de produção [5]. A ocasião onde os preços da energia elétrica estão abaixo do custo médio da produção acarreta na desativação de plantas geradoras e os preços relacionados ao consumo de energia elétrica são elevados em virtude da redução da oferta. No mesmo sentido, haverá o restabelecimento da igualdade de equilíbrio entre preços da energia elétrica e custos médios de produção [7].

A indústria de energia elétrica pode ser dividida em quatro modelos. O primeiro deles é definido como um monopólio tradicional vinculado a empresas verticalmente organizadas, onde não ocorre competição na geração, não ocorre escolha do distribuidor e tampouco escolha por parte do consumidor. O segundo modelo é um monopsónio, uma forma de mercado com apenas um comprador, caso inverso ao que ocorre no monopólio, e desta forma dispõe de competição na geração, porém com apenas um comprador desta energia gerada. A competição ocorre quando cogeradoras e produtores independentes são submetidos a certo grau de competição para suprir a demanda estabelecida pela agência compradora - comumente estatal. Este tipo de modelo infere em um nível de imposição da agência reguladora quanto ao preço a ser praticado. No terceiro modelo geradoras e distribuidoras competem para vender energia. Sendo assim é essencial que as empresas de ambos os segmentos assumam uma postura desverticalizada e tenham livre acesso ao sistema de transmissão. Neste modelo, empresas já estabelecidas precisam competir com as empresas iniciantes de tal forma que os preços médios da energia elétrica gerada tendem a diminuir. Já no modelo 4 também apresenta competição na geração e na distribuição de energia elétrica, porém com a ressalva de que há possibilidade de que os consumidores finais escolham de quem comprarão energia elétrica [8].

A redução de custos, em relação ao mercado tradicional de energia, é a maior vantagem na criação de um mercado competitivo de energia. Isso se justifica através da construção de estruturas de geração de energia mais eficientes visando maiores lucros. Além disso aumento da oferta acaba por reduzir o preço da energia elétrica de um modo geral. Boa parte dos ganhos em eficiência são transferidos ao consumidor [5]. De modo geral, se espera que a realização de uma reestruturação no setor elétrico de um determinado país tenha objetivo de viabilizar o beneficiamento da população no longo prazo. Estes benefícios são distribuídos da maneira mais adequada a cada usuário através de um sistema de preço que consiga alocar de maneira eficiente os custos econômicos envolvidos no setor elétrico [4].

Buscando estes objetivos, através do *The Electric Act,* em 1989 iniciou-se a reestruturação do Setor Elétrico do Reino Unido. Tal reestruturação serviu de gatilho para o processo de liberalização do setor e se tornou um marco que é referência para outras reformas ao redor do mundo [9].

São sete os elementos principais para implementação de um setor elétrico mais liberado [4]:

i. A desverticalização da indústria elétrica nas diferentes atividades: geração, transmissão, distribuição e comercialização;
ii. Privatização das empresas públicas;
iii. Restruturação horizontal da geração, a fim de criar várias empresas com capacidade de competição dentro do mercado;
iv. Redes, transmissão e distribuição, mantidas como monopólios naturais com tarifas definidas pelo Estado, através de uma Agência Reguladora;
v. A operação do sistema elétrico passou a ser executada por um operador independente;
vi. Criação do mercado atacadista de energia elétrica, no qual geradores vendem grandes blocos de energia;
vii. Competição no mercado de varejo através da liberalização de todos os consumidores, tornando livre a escolha do comercializador de energia.

Vários países seguiram o modelo inglês e liberalizaram os setores elétricos. Contudo, nem todos implementaram o mesmo modelo. A adoção de mecanismos de mercado é um traço comum, mas a estrutura do mercado varia bastante de país a país. Com a liberalização da indústria de energia elétrica e a introdução de mecanismos de mercado, os setores elétricos em todos os países analisados foram divididos em dois grandes mercados: o mercado de varejo e o mercado atacadista [6].

No mercado de varejo, a energia é vendida aos consumidores finais, tipicamente consumidores residenciais e comerciais com baixo consumo de energia elétrica. Já no mercado atacadista, a energia é vendida em grandes blocos pelos geradores aos comercializadores, distribuidores e grandes consumidores (contratos bilaterais). Já o mercado atacadista pode ser dividido em dois modelos de organização, o de comprador único e o que diferencia mercados de curto e longo prazo, conforme a Figura 1 [6].

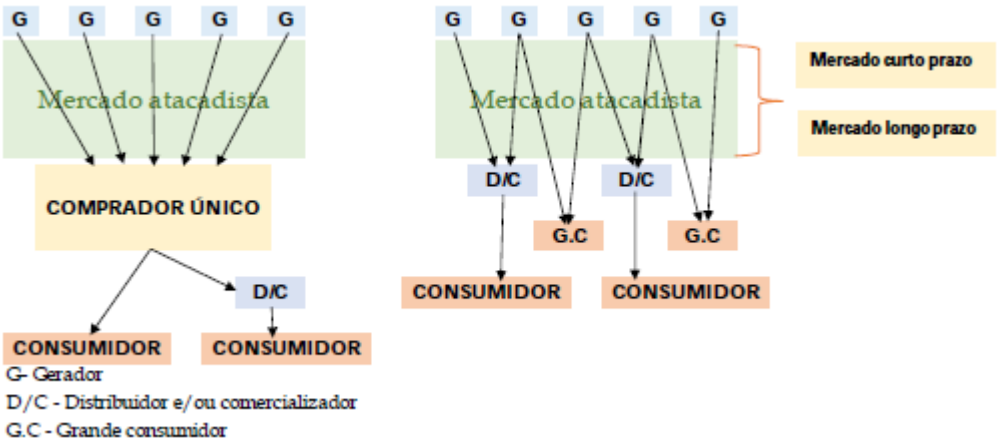



Figura 1 - Dois modelos de organização básica do mercado atacadista [6]

O esquema de comprador único de energia apresenta algumas características gerais, entre as quais destacam-se: o comprador único é uma empresa do Estado, normalmente proprietária das redes de transmissão e distribuição, e se encarrega de repassar a energia aos consumidores finais. Na atividade de geração, existem produtores públicos, os quais, em geral, são a parte de geração da empresa estatal que foi desverticalizada, autoprodutores e produtores independentes de energia. Já no esquema de curto prazo ocorre maior competitividade entre os agentes do setor. A ideia principal é aproximar o mercado atacadista de energia elétrica de um mercado de concorrência perfeita [6]. Mercados considerados de longo prazo têm tendência de apresentar maior previsibilidade nas relações entre os agentes. Os preços a serem pagos nos montantes de energia e as formas com que estes serão atualizados ao longo do tempo são, comumente definidos pelo agente vendedor (podendo ser um gerador, distribuidor ou comercializador) e o agente comprador [7].

Vale complementar que estas são as características essenciais de cada esquema e que, portanto, existem especificidades que variam de país para país. O estabelecimento destas especificidades provem de diferenças econômicas, políticas e sociais entre os estados, além de características geográficas de relações com os países vizinhos.

## 2.2. MERCADOS LOCAIS DE ENERGIA

Os mercados locais de energia elétrica podem ser entendidos como uma situação na qual consumidores individuais e consumidores produtores interagem com a finalidade de negociar energia elétrica numa determinada vizinhança. A idealização de tal situação é relativamente simples. Contudo, para a implementação prática de um mercado local, algumas barreiras técnicas devem ser ultrapassadas. Tais barreiras tangenciam temas relacionados à produção distribuída, mercados de energia elétrica e modelos de negócios, acabando por conceber linhas de pesquisa importantes para estudos de mercados de energia elétrica [7].

A produção de energia elétrica de maneira descentralizada é uma tendência global. Sendo assim muitas serão as mudanças técnicas relativas ao setor elétrico e por consequência o mercado também está sendo impactado, transações de compra e venda de energia já não são tratadas da mesma maneira que nas décadas anteriores. O crescente avanço da produção distribuída nos leva a um panorama onde em um curto espaço de tempo a maioria das unidades de consumo também irá dispor de unidades de produção própria de energia com o objetivo principal de suprir as necessidades energéticas destes consumidores, seja com painéis solares fotovoltaicos ou geradores eólicos, por exemplo. Em casos onde o suprimento de energia do consumidor seja realizado e, ainda assim, sobre energia, este excedente pode ser utilizado para suprir a demanda de seus vizinhos. Sendo assim, surge uma necessidade de comercialização local. A ideia de comercialização local de energia pode ter um grande impacto não somente quando se fala em redução de custos de transmissão mas também com relação a dinâmica de geração de energias renováveis através do compartilhamento de informações de montantes gerados nestes mercados locais, tendo em vista que a geração de energia através de recursos renováveis apresenta certa volatilidade associada às condições climáticas, como velocidade do vento, incidência solar e temperatura no local [10].

O aprimoramento da gestão pelo lado da demanda se torna muito importante com o desenvolvimento de mercados locais. O crescimento deste tipo de mercado pode estar diretamente relacionado ao desenvolvimento de cidades inteligentes, comunidades mais eficientes energeticamente. Estudos na área de sistemas elétricos de energia apontam que no futuro as cidades inteligentes serão ambientes extensos e de alta complexidade no que diz respeito às relações entre as entidades envolvidas no sistema elétrico. Os mercados

locais podem ser vistos como facilitadores para as relações entre as partes interessadas no contexto de uma cidade inteligente. Desta maneira pode-se dizer que ainda não é clara a forma com que tais mercados irão operar e nem os requisitos mínimos necessários para que haja funcionalidade e geração de benefícios para os participantes do mesmo [11].

No contexto de mercados locais, é considerável que haja uma relação direta entre consumidores produtores e demais agentes de mercado. Desta forma, tais agentes acabam por assumir uma postura de facilitadores na tarefa do operador de mercados, ou seja, registrar e monitorar diversos consumidores produtores inseridos em determinados mercados locais. As estruturas de *hardware* e *software* precisam dispor de confiabilidade para que o gerenciamento do mercado local seja viável em termos práticos. A segurança em termos de criptografia para a transferência de dados, tema que será mais amplamente discutido em um capítulo a parte, é extremamente relevante para a integração de mercados locais com o balanço de compra e venda de energia elétrica em um sistema elétrico de energia [7].

Entidades envolvidas em mercados locais, a produção distribuída de energia elétrica e a articulação com o mercado de energia são parâmetros importantes a levar em consideração para formação de um mercado local. Além disso o estudo dos modelos de negócio também se faz muito importante para a viabilização da expansão destes mercados locais.

## 2.3. MODELOS DE NEGÓCIO

Recentemente, estudiosos discutiram a necessidade de empresas de energia reformularem seu BM (sigla para modelos de negócio, do inglês – *Business Model*), substituindo a eletricidade como mercadoria para tratá-la como prestação de serviço. No entanto, a transição para um modelo de serviço contém muitos obstáculos e desafios [12]. Dentro do sistema convencional de energia prestou-se pouca atenção ao conceito BM. Consequentemente, este BM não evoluiu significativamente nos últimos anos. Isso se deve ao fato de, primeiro: o BM ser centrado em torno de mercadoria tangível, onde o valor intangível é uma reflexão tardia; segundo: a produção e distribuição desta mercadoria é protegida por regulamentação onde a concorrência tem sido muito limitada. Além disso, nesse sistema, agrega-se valor simplesmente vendendo eletricidade nos mercados estabelecidos. Não há necessidade de inovação, pois a receita cobre o custo fixo e variável da energia elétrica gerada. Ultimamente, novas tecnologias estão penetrando no setor de

energia e o mercado de energia começou a ser liberalizado. No mercado emergente de energia, os consumidores têm várias opções: relacionados aos diferentes custos de transação, como a heterogeneidade entre produtores. Além disso, há tendências ascendentes de redução do impacto ambiental entre os consumidores. A parcela de energia renovável no mercado está aumentando em relação a energia fóssil enquanto os preços das antigas tecnologias estão diminuindo [13]. Em resposta às emergentes mudanças, novas empresas foram posicionadas no setor de energia. Oferecendo novos produtos, serviços e condições de fornecimento de energia. Esses novos participantes estão construindo sua posição no mercado de eletricidade desenvolvendo novos BM's baseadas em serviços inovadores, criando um novo ecossistema e envolvendo novas parcerias [14].

O conceito de modelo de negócios recebeu crescente atenção de estudiosos e profissionais durante o período de *e-business* emergente em meados dos anos 90 do século passado. Apesar do grande uso desse conceito desde então, não há consenso entre estudiosos [15]. Recentemente foi usado de forma intercambiável por acadêmicos e profissionais como uma ferramenta analítica e de classificação [16]. Este conceito pode executar várias funções incluindo a articulação da proposição de valor, identificar um segmento de mercado, definir a cadeia de valor e a rede de valor, estimar a estrutura de custos e lucros e formular as estratégias competitivas [17]. Modelos de negócios abrem caminho para novas tecnologias para atuar nos mercados e criar valor para eles. Portanto, é considerado um agente que media o processo de criação de valor. Traduz os insumos técnicos para os domínios econômicos dos produtos [17].

Dois componentes principais formam o conceito de BM. Primeiro, a "Unidade de negócios" que se refere ao que as empresas estão oferecendo e o que o cliente está pagando. A unidade de negócios é fundamental para a escolha da estratégia [18]. O segundo são as "métricas principais" que se referem ao processo e às atividades que as empresas realizam para vender um produto ou serviço [19].

O ambiente externo, incluindo parceiros, fornecedores e clientes, é crucial no conceito de BM [13]. Os BMs esclarecem como o valor é criado e capturado [15]. Em grandes mudanças de infraestrutura, como a transição do combustível fóssil à energia renovável, o foco deve ser passar do desenvolvimento de tecnologias individuais para a criação de um sistema totalmente novo [20].

Desenvolver um BM é frequentemente necessário para a inovação tecnológica, facilita a introdução de invenções no mercado e satisfaz as novas necessidades do cliente. Da mesma forma, as tecnologias e a inovação por si só não garantem o sucesso dos negócios. O desenvolvimento de um novo BM requer uma profunda compreensão das necessidades fundamentais dos clientes, como os concorrentes não conseguiram satisfazer essas necessidades, e os aspetos tecnológicos e organizacionais. Enquanto projetar o BM desejado parece ser o mais importante, o processo de aprender e ajustá-lo também tem a mesma importância. Além disso, estimar os clientes e os concorrentes que comportam as mudanças do panorama inicial torna a adoção de um novo BM mais rápida e com menores riscos relacionados [21].

Estudos indicam que o PSS (do inglês - *product-service system*), como um instrumento funcional, é um conceito promissor em termos ambientais [22]. O emprego do PSS tem o potencial de aumentar a eficiência, oferecendo funcionalidade (por exemplo, pagamento por uso) em vez de simplesmente vender a propriedade da energia [23]. Fornecer fontes renováveis, energia eficiente e resposta à demanda por meio de um BM orientado a serviços detém o potencial de apoiar uma mudança para um meio mais sustentável de produção e consumo de energia [24][25].

### 2.3.1. MODELOS DE NEGÓCIO PARA O SETOR ELÉTRICO

São três as categorias de BMs descritas:

- BMs centrados no produto de propriedade do cliente;
- BMs centralizados na terceirização de serviços;
- BMs da comunidade energética.

#### 2.3.1.1. MODELOS DE NEGÓCIO CENTRADOS NO PRODUTO DE PROPRIEDADE DO CLIENTE

Nesses BMs o usuário final compra o sistema e financia ou realiza diretamente a instalação e manutenção do sistema. Por um lado, o consumidor pode comprar tecnologias de fontes renováveis de energia (por exemplo, painéis fotovoltaicos, PV) para gerar eletricidade. Por outro lado, o consumidor pode investir em Dispositivos de gerenciamento pelo lado da demanda (*Demand Side Management* - DSM), que incluem produtos de eficiência

energética (por exemplo, materiais de isolamento) e ferramentas de gerenciamento de energia (por exemplo, medidores inteligentes) [13].

#### 2.3.1.1.1. TECNOLOGIAS DE ENERGIA RENOVÁVEL DE PROPRIEDADE DO CLIENTE

Nesse BM, o consumidor se transforma em *prosumer* (produtor e consumidor). Na literatura acadêmica, várias designações descreveram este BM. "*Plug and play*" referente à maneira tradicional de compra direta de produtos [26], [27]. "*Host owned model*" [25,27], e "*Customer-owned PV BM*" [30].

A proposta de valor é a micro geração de eletricidade e seus serviços complementares. Os interessados neste mercado são os proprietários que possuam uma propriedade adequada que com energias renováveis (por exemplo, cobertura suficiente para energia fotovoltaica, sem sombra, etc.) [30] e quem pode assumir o risco dos investimentos. No entanto, a responsabilidade da implementação e a manutenção pode ser feita pelo consumidor ou pelo fornecedor. Este é um processo baseado em transações, portanto, o relacionamento entre o fornecedor do produto e o consumidor não é crucial [13].

A eletricidade gerada da micro geração pode ser alimentada na rede elétrica ou ser consumido pelo proprietário. O *prosumer* pode transmitir o excedente de eletricidade para a rede, o que depende das legislações e infraestrutura elétrica. Em ambos os casos, o modelo de receita é baseado no retorno de investimentos a longo prazo. No primeiro, a eletricidade é comprada a um preço competitivo por serviços públicos, enquanto no último; os consumidores terão uma troca na conta mensal de eletricidade. Em relação ao custo, os consumidores precisam enfrentar um alto investimento inicial, manutenção, risco de baixo desempenho e custo da transação da rede de interligação [28].

Um bom exemplo de sucesso implementação deste BM de propriedade do consumidor pode ser obtido na Alemanha. Muitos fatores contextuais incentivaram e facilitaram o desenvolvimento do BM. A Alemanha criou uma tarifa atraente de alimentação e propôs uma taxa de empréstimo a juros baixos para tecnologias de energia renovável. A baixa taxa de migração no setor da construção civil eliminou os problemas de senhorio e inquilino. Na transação o custo foi reduzido através da experiência local e baixo nível legal dos requisitos administrativos [29].

#### 2.3.1.1.2. GERENCIAMENTO PELO LADO DA DEMANDA DE PROPRIEDADE DO CLIENTE

O gerenciamento do lado da demanda é um método para ajustar os consumidores na demanda por eletricidade. O principal objetivo é reduzir o consumo do consumidor aumentando a eficiência ou alterando seu consumo do horário de pico da eletricidade para outros janelas de tempo, o que é chamado *Demand Response* (DR) [31]. Um modelo de negócios genérico foi proposto denominado "*energy efficiency service and devices sales*", um dos BMs convencionais de eficiência energética. Aqui o "*Demand Response Provider"* (DRP) vende um sistema/dispositivo que pode ajudar o cliente na redução do seu custo de energia. Outra variação desse BM é que o DRP conduz atividades de auditoria e estudos de custo/benefício para justificar a venda de um sistema/dispositivo mais eficiente ao consumidor [31]. O "*Value-Added Enabler Model*" emprega o DSM amplamente nos mercados de massa voltados para residências e pequenas empresas. Fornecendo elementos de controlo como termostatos inteligentes, monitores de energia e tecnologias de "*set and forget*" que fornecem dados de consumo de energia preditivos e em tempo real. Esses tipos de BM exigem a construção de plataformas de "*big data*", desenvolvem métodos inovadores para capturar, apresentar e compartilhar dados com cliente, conservando a segurança dos dados e ferramentas para facilitar e simplificar a tomada de decisão do consumidor [32].

### 2.3.1.2. MODELOS DE NEGÓCIO CENTRADOS NA TERCEIRIZAÇÃO DE SERVIÇOS

A base destes BMs é prestar um serviço e não um produto. No campo da energia, serviço é um conceito que se refere frequentemente à eficiência energética e está associado à Empresas de Serviços Energéticos (ESCOs). Além das ESCOs, esse BM está evoluindo para fornecer energia renovável, como um pacote de serviços, resposta à demanda e eficiência energética. Trabalhos de pesquisa recentes identificaram que os investidores preferem esse BM ao invés de BMs com foco na melhor tecnologia ou no menor preço [33].

#### 2.3.1.2.1. TECNOLOGIAS DE ENERGIA RENOVÁVEL DE PROPRIEDADE DE TERCEIROS

Neste BM, um terceiro oferece financiamento, instalação e manutenção de um sistema de energia renovável no local do consumidor. Além disso, mantém a propriedade e vende a eletricidade gerada através de um contrato de longo prazo (15-20 anos). Dois termos são usados na literatura: "*Third-party ownership BM*" [28][29] e "*Company-driven BM*" [26][27].

*SolarCity*, nos EUA, é um bom exemplo desse BM. Esta empresa empregou as inovações deste BM e especificamente a inovação financeira para ampliar seus negócios. Criou fortes parcerias com ambas as instituições financeiras para obter uma grande quantidade de capital e com parceiros a jusante para acelerar as vendas e minimizar os custos através de um processo vertical integrado ao longo da cadeia de valor [34].

A atratividade deste BM está na remoção do custo inicial e na compra de eletricidade a um preço competitivo. Ao fixar o preço da eletricidade para (15-20) anos, o risco de flutuação dos preços da eletricidade é eliminado. O proprietário do sistema possui dois fluxos de receita diferentes, oferecendo um arrendamento solar ou um contrato de compra de energia [30]. "*White label local BM*" é um fornecedor local de etiquetas que pode satisfazer as necessidades locais de energia renovável. Considerando que o custo de energia renovável é maior que a eletricidade da rede, as etiquetas podem usar medidores inteligentes e aplicativos móveis para otimizar o uso de energia dos consumidores, dando sinais de custo e consumo de energia diariamente. Este BM vincula uso de energia com atividades diárias através de tecnologias avançadas de informações e comunicação [35]. A atratividade deste modelo pode ser estendida para ir além do medidor (por exemplo, solar, armazenamento, etc.) desenvolvendo produtos alternativos no portfólio de geração [32].

O "*Cross-selling BM* ", refere-se a empresas não relacionadas a PV, que trabalham em diferentes setores, como empresas de construção envolvida na venda cruzada de sistemas fotovoltaicos que se beneficiam da boa relação pré-existente com os clientes [29]. A atratividade do modelo está na obtenção de um preço competitivo, baixo custo de transação e menor conta de eletricidade. O benefício financeiro para o consumidor é a economia de energia, enquanto o custo inicial do PV está embutido em alguma forma de garantia, como por exemplo na hipoteca da casa [29]. Da mesma forma, o modelo "*Partner of partner model*" prevalece quando há incrementos de tecnologia e escolha de energia, e os clientes estão buscando maneiras para simplificar seu estilo de vida. Empresas que procuram sucesso na busca por este BM "*Partner of partner*" devem criar um conjunto de parcerias

com empresas de solução e serviço, expandir seus canais de mercado, desenvolver várias ofertas e manter uma alta satisfação do cliente [32].

A transição energética para energias renováveis tem sido discutida do ponto de vista da concessionária de energia. Na tentativa de determinar o papel potencial da concessionária no futuro mercado, estruturas de BMs foram empregadas. Por esse motivo, dois BMs foram sugeridos: "*customer-side renewable energy BM*" e o "*utility-side renewable energy BM*" [36]. No primeiro, a concessionária produz eletricidade no local dos consumidores, com capacidade variável de poucos kWs. A proposta pode variar de serviço de consultoria simples para financiamento, propriedade e operação do ativo. Considerando que o BM de energia renovável é de grande escala de tecnologias de energia renovável que variam de uma a algumas centenas de megawatts [36].

O atual modelo de receita de serviços públicos é uma barreira que impede envolvimento no emergente sistema de energia renovável. O modelo tradicional baseia-se no consumo por kWh, portanto, seu retorno está associado ao consumo do consumidor [36]. A principal motivação das concessionárias mudar seu BM em direção a BMs orientado a serviços parece conter da erosão da renda das concessionárias e não do cliente e da mudança do mercado. A atual intensidade de capital e ativos tangíveis de concessionárias restringem sua capacidade de desenvolver BMs orientados a serviços o que depende mais de ativos intangíveis [37].

#### 2.3.1.2.2. TERCEIRIZAÇÃO DE SERVIÇOS DE RESPOSTA À DEMANDA

*"Business model involving load"* (modelo de negócios envolvendo a carga) visa reduzir custo da eletricidade da carga, vendendo assim flexibilidade de carga ao comprador de resposta à demanda [31]. Ao enviar sinais do preço da eletricidade, os usuários podem responder a esses sinais, modificar e priorizar suas ações. Esses ajustes podem ser alcançados conscientizando e trocando informações de preços sobre o consumo através de uma infraestrutura de medição ou fornecendo um sistema que reaja aos diferentes preços [31].

O BM "*local aggregator*" (agregador local de terceiros) vincula a demanda e o fornecimento local, fornecendo aos consumidores medidores inteligentes para influenciar o comportamento do consumidor e permitir que eles moldem seu padrão de consumo. A

medição de rede virtual permite a compensação fora do suprimento local do suprimento da concessionária [35].

O "*E-balance business model*" (modelo de negócios por equilíbrio eletrônico) visa integrar o consumidor em redes inteligentes através de soluções baseadas em Tecnologias de Informação e Comunicação (TIC) para aumentar eficiência e confiabilidade da rede de energia em nível local. Os ganhos são uma conta de energia elétrica mais baixa para o consumidor e um fluxo de energia estável para o operador da rede. Balanceamento, controlar e monitorar a eletricidade e permitir que consumidores comprem e vendam eletricidade são as principais atividades. Os parceiros podem ser fornecedores de dispositivos inteligentes, fornecedores de TIC, bancos e ESCOs. Incentivos de preços podem ser usados para orientar o relacionamento com o consumidor. A plataforma pode facilitar a comunicação entre agentes. O principal custo decorre de tecnologias avançadas, como sensores e aplicativos inteligentes, enquanto as receitas provêm do serviço de taxas mensais, como a análise da plataforma e de serviços correspondentes como intermediação entre fornecedores que não conseguem prever sua produção e os consumidores que começaram a tomar parte no mercado de energia e moldar seus perfis de consumo [40]. Esta posição da plataforma fornece duas funcionalidades: Primeiro, vender e comprar eletricidade para um ou diferentes recursos e, segundo: reduzir picos e otimizar o uso de eletricidade [41]. A plataforma intermediária divide os benefícios tradicionais do sistema elétrico em uma constelação de benefícios descentralizados, onde a cadeia de suprimentos verticalizada é transformada em redes de valor com vários pontos de entrada e saída, melhorando a eficiência do mercado e reduzindo os custos de transação. No entanto, um provedor de serviços de plataforma pode tomar algumas decisões em nome dos consumidores, a fim de limitar os efeitos ocasionados pelo comportamento individual destes, e controlar melhor o sistema [41].

#### 2.3.1.2.3. TERCEIRIZAÇÃO DE SERVIÇOS POR EFICIÊNCIA ENERGÉTICA

O conceito de BM também tem sido usado para analisar serviços de eficiência energética. O BM mais prevalente é o Serviço de Energia ESCO da empresa que se refere a uma prestação de serviços que uma empresa fornece ao consumidor a fim de reduzir o consumo de energia em vez de fornecer unidades de energia. Dois tipos de BM podem ser

observados para a ESCO. Primeiro, o "*Energy Supply Contracting*" ESC, que fornece energia (por exemplo, água quente, líquido de arrefecimento, eletricidade etc.), este PSS é orientado para o uso como um conversor primário (por exemplo, um gerador mais eficiente) é usado para converter energia em água quente como um exemplo. Em segundo lugar, "*Energy Performance Contracting*" (EPC), que fornece serviço de energia (por exemplo, luz ambiente, aquecimento ambiente etc.) é um resultado orientado a resultados PSS [12]. Do ponto de vista financeiro os modelos de negócios ESCO podem ser divididos em *"Shared Savings"* e *"Guaranteed Savins*". No primeiro, a ESCO fornece finanças e o consumidor tem que pagar uma parcela mensal da economia de energia, enquanto que, no segundo, o consumidor tem que financiar a ESCO e garantir uma economia suficiente para cobrir as dívidas anuais [43]. No entanto, a ESCO não se tornou uma componente principal do mercado emergente de energia e teve lenta difusão do mercado que pode ser atribuída ao fraco conhecimento e incerteza em torno das ESCOs [43], para "aprisionamento" do modelo tradicional do sistema energético e ao domínio das concessionárias de energia existentes [12].

#### 2.3.1.3. MODELOS DE NEGÓCIO DA COMUNIDADE ENERGÉTICA

Os BMs da comunidade de energia podem assumir muitas formas: pode ser uma fazenda de energia renovável em um único local ou pode ser um sistema renovável distribuído entre as casas dos membros. Os cidadãos têm a oportunidade de participar possuindo e/ou financiando cada um de acordo com sua capacidade. Este BM pode administrado pelos membros ou por terceiros. O principal incentivo além do desenvolvimento de uma comunidade de energia se dá pela possibilidade de controlar a origem da eletricidade. Os consumidores têm um alto nível de envolvimento em dois níveis. Em primeiro lugar, controlar e gerenciar a comunidade e, segundo, garantir o equilíbrio de oferta e demanda da micro rede [27]. Esse BM depende dos atores locais, portanto os mediadores locais e conhecidos incentivam comportamentos, alterações necessárias para estabelecer um relacionamento próximo e confiável. A construção de um modelo de negócios para uma comunidade pode ser organizada em nível local por meio da interação física entre os membros das cooperativas de energia renovável ou em nível nacional por meio da plataforma virtual de portal online. Na plataforma "*Grassroot P2P*", por exemplo, os membros organizam e administram a comunidade a fim de minimizar o custo e melhorar as

questões sociais ou ambientais [34]. Uma cooperativa de energia, como um BM de comunidade energética, é uma colaboração entre membros que visam produzir seus próprios recursos renováveis [44]. Iniciativas de Participação do Cidadão trazem um papel social ativo inovador dos cidadãos no financiamento e implementação de projetos de energia renovável [44]. O BM de comunidade energética tem muitas vantagens, minimiza as barreiras financeiras para indivíduos através da possibilidade de possuir uma parte do sistema de energia. Além disso, o processo coletivo de compra reduz o custo e, finalmente, elimina problemas como espaço disponível em telhados e sombreamento [28].

As comunidades energéticas não são entidades isoladas e podem afetar (e serem afetadas por) outras comunidades energéticas ou atores. A flutuação de energia renovável cria a necessidade de flexibilidade, melhor organizar e equilibrar a energia no nível local. *Integrated Community Energy System* – (Sistema Integrado de Energia Comunitária) leva em consideração o valor interno como eficiência e suficiência, bem como o valor externo da flexibilidade que outros atores como fornecedores, operadores de rede, agregadores e outras comunidades podem se beneficiar. A principal característica do ICES é a troca de energia local. Quando os consumidores locais aumentam sua cooperação, uma melhor viabilidade é alcançada no nível da comunidade devido a economias de escala (compras coletivas) e balanceamento local (por exemplo, otimizando o DSM), visando aliviar os problemas de espaço e variação temporal das energias renováveis e redução do risco associados à natureza estocástica dos recursos renováveis [44].

Vários BMs novos, entrantes no setor de energia, que podem ser adotados foram apresentados. Os três modelos de negócio permitem que novos empreendimentos considerem uma configuração de serviços do produto na proposta de valor (por exemplo, leasing ou venda de sistema fotovoltaico); os diferentes modelos financeiros na captura de valor (por exemplo, desempenho ou base mensal fixa) e valor diversificado, formas de entrega (por exemplo, site ou concessionária do cliente). O objetivo desta categorização é ajudar a repensar a forma BMs em mercados liberalizados de energia.

O conceito de modelo de negócio tem sido amplamente usado para lidar com a transição energética, no entanto, não há estrutura referente à sua implantação e aos novos papéis dos agentes. O documento descreve esses modelos em três categorias com base em revisão da literatura acadêmica e na tentativa de preencher a lacuna entre a necessidade urgente de modelos sustentáveis e a incerteza em relação ao papel dos novos participantes no mercado

emergente de eletricidade. O PSS tem sido amplamente utilizado para abordar o potencial de sustentabilidade em muitos setores, bem como no setor de energia. Ainda assim, o PSS recebeu pouca atenção em relação à sua potencial contribuição para a estruturação sustentável de modelos de negócio de energia e pode ser muito mais explorado no futuro [13].

# 3. REDES INTELIGENTES

A Todo o conceito de mercados locais se baseia na existência e inserção dos agentes deste mercado em uma *Smart Grid*. O conceito de *Smart Grid* carrega a ideia da utilização intensiva de tecnologia de informação e comunicação na rede elétrica [45].

A implantação de *Smart Girds (SGs)* tem por objetivo utópico melhorar a inteligência da interoperação do sistema de rede através do fornecimento de fluxo de informações multidirecionais entre duas ou mais unidades do sistema para alcançar uma indústria de energia revolucionária, fornecendo dados adequados da medição às subestações, distribuições, transmissão e gerações, maior segurança, resiliência e controle e monitoramento eficiente de ativos e serviços [46]. Na prática a ocorre a abertura a novos riscos a serem analisados e mitigados.

A inteligência é obtida pela incorporação de processadores em cada componente dos sistemas de potência, tendo cada componente um sistema operacional e agentes independentes conectados a sensores inteligentes ligados a seu próprio componente ou subestação para formar uma grande plataforma de computação distribuída, o que lhe permite acessar suas próprias condições operacionais e reportar a seus agentes vizinhos por meio dos caminhos de comunicação para os processadores [47].

Os sistemas convencionais de energia estão sendo atualizados em todo o mundo para oferecer essas vantagens, que incluem confiabilidade, segurança e flexibilidade na distribuição de energia, monitoramento do consumo de energia, gerenciamento do lado da demanda (DSM), aumento do tráfego otimizado da rede, tempos de inatividade mais curtos, falhas minimizadas, redução de perdas na rede, oferta e demanda reguladas, e operações e serviços de rede geralmente melhorados [48]. A maioria dos sistemas de rede de energia elétrica utiliza o fio terra com uma fibra ótica, operando eficientemente em longas distâncias com perdas reduzidas, tornando-o rápido, confiável e mais seguro [49].

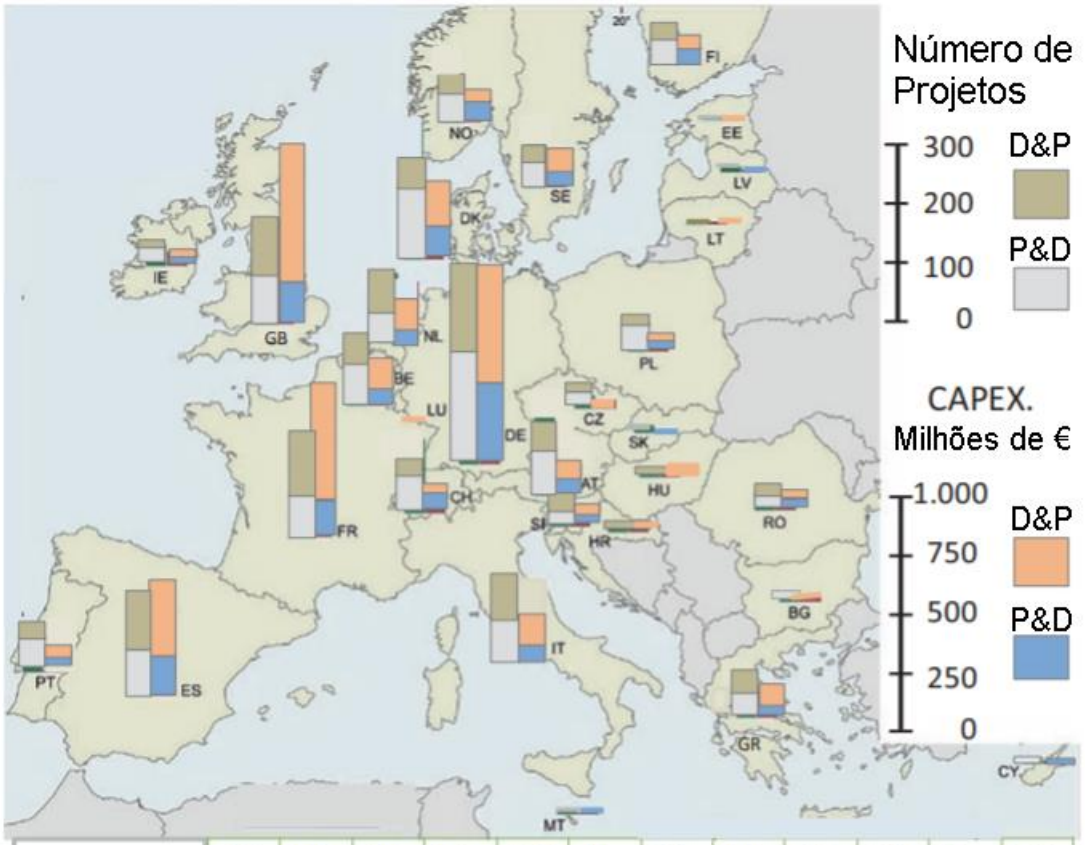
As fibras óticas facilitam a implantação de SGs, eliminando a necessidade de capacidade de comunicação adicional. Embora suportando os requisitos de SG, o protocolo TCP/IP atualmente em implantação não forneceu a segurança necessária para a comunicação entre os componentes de infraestrutura [50].

Em geral, a presença de nós de comunicação tornou o setor de energia mais vulnerável a *cyber* ataques e, portanto, a necessidade de uma inteligência operacional em tempo real de todos os componentes interconectados para melhorar a segurança, previsões de carga, gerenciamento pelo lado da demanda (DSM), informações de faturação e melhor utilização de sistemas de energia renovável [51].

Além disso, as vulnerabilidades poderiam ser exploradas por adversários para causar falhas no sistema na forma de possíveis falhas na sequência de transmissão, terrorismo, ataques cibernéticos, vândalos, roubo, etc. Outras ameaças possíveis incluem os desastres naturais e, possivelmente, de alguns distúrbios do sistema identificados, como instabilidade de tensão e frequência [50].

Vários trabalhos de pesquisa sobre SGs focam o envolvimento do consumidor na operação ativa do equilíbrio de poder, introduzindo sistemas técnicos de operação, bem como incentivos econômicos para facilitar demandas flexíveis [52]. Esses estudos e melhorias dos títulos operacionais são muito importantes, uma vez que o sistema é complexo e os recursos de infraestrutura associados são muito caros. Desde 2013, a UE publica resumos anuais dos projetos de redes inteligentes em Europa. O relatório para 2017 analisou 950 projetos com participantes de 50 países e implementações em 36 países. Os orçamentos dos projetos totalizaram 5 bilhões de euros [53]. A Figura 2 apresenta a distribuição dos projetos em relação ao número e aos orçamentos. O alto investimento neste tipo de

tecnologia demonstra o crescimento deste tipo de rede e desta forma devem ser tomadas as medidas de segurança necessárias para evitar danos que, por sua vez, possam representar perigo para as infraestruturas ou para o pessoal.




| País | DE | GB | FR | ES | DK | IT | NL | BE | SE | AT | FI | PT |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CAPEX | 809 | 774 | 680 | 521 | 278 | 239 | 208 | 190 | 171 | 152 | 106 | 100 |
| Número | 330 | 197 | 159 | 178 | 181 | 148 | 124 | 109 | 90 | 128 | 106 | 68 |

Figura 2 - Distribuição geográfica dos projetos nacionais de *Smart Grid* na Europa [53]

A SG é central para a operação da infraestrutura de energia e espera-se que amadureça no enfrentamento de futuras provisão de expansão. Isso exigiu o desenvolvimento de um mecanismo de monitoramento de defesa que possa processar eficientemente os dados complexos na avaliação do status do sistema, identificação de falhas ou ameaças, previsão de ameaças, sugestões de correção, assegurando de maneira confiável as provisões de segurança operacional adequadas da rede [50].

A seguir as ameaças identificadas à implantação dos SGs são classificadas e discutidas com base em informações técnicas e não técnicas. Espera-se que essa classificação forneça

uma estrutura explícita para facilitar o rastreamento e a contenção de ameaças em implantação de SGs.

## 3.1. DESAFIOS E OBJETIVOS DE SEGURANÇA DE REDES INTELIGENTES

O termo ameaça refere-se às várias ações possíveis que podem ser influenciadas por meios artificiais ou naturais, contra um sistema [54]. Essas ameaças não representam falhas, mas podem resultar em falha caso ações necessárias não forem tomadas. Daí a necessidade de estudar as ameaças e os desafios, bem como um objetivo definido para uma SG bem protegida.

## 3.2. ARQUITETURA E TECNOLOGIAS DE COMUNICAÇÃO

### 3.2.1. ARQUITETURA DE UMA *SMART GRID*

[55] NIST conceitualiza *Smart Grid* como um conjunto de sete domínios interconectados. Os quatro primeiros domínios (Geração, Transmissão, Distribuição e Clientes) são responsáveis pela geração, transmissão e distribuição de energia, mas também por garantir a comunicação bidirecional entre o lado do cliente e a medição avançada dos serviços públicos (AMI). As três entidades restantes (mercados, operações e prestadores de serviços) são responsáveis pela gestão do mercado de energia, energia gerenciamento de distribuição e prestação de serviços.

Uma arquitetura um pouco diferente, meramente inspirada no NIST modelo conceitual descrito acima, mas também por [56], [57] e [58], é adotado para os fins deste estudo. Esta arquitetura conceitualiza o Smart Grid, seguindo uma abordagem multicamada. Como mostrado na Figura 3.

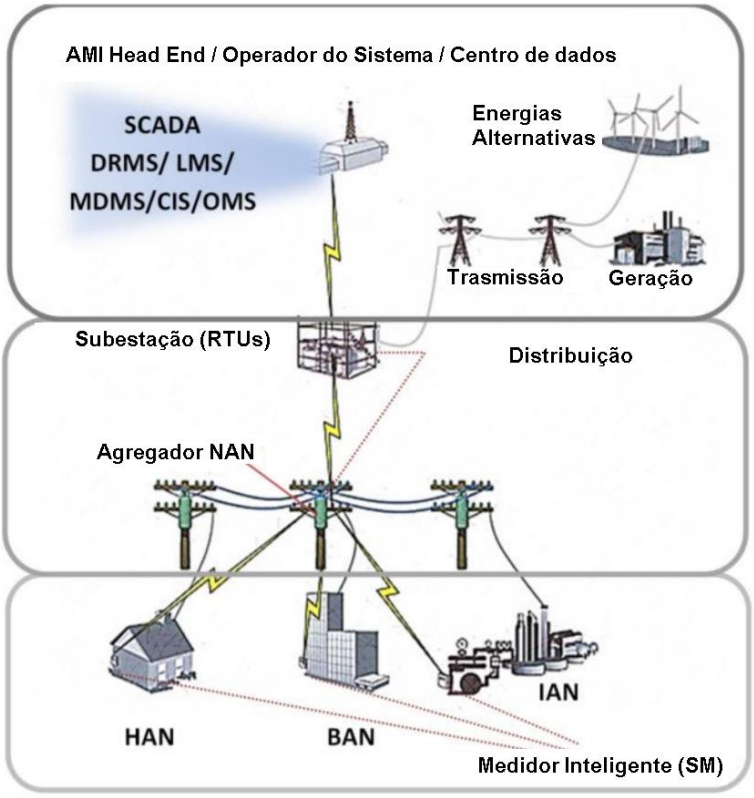



Figura 3 - Um modelo conceitual de várias camadas da arquitetura do *Smart Grid* [64]

Na camada inferior deste modelo, é possível encontrar redes de área doméstica (HANs), Redes de Área de Construção (BANs) e Redes de Área Industrial (IANs), ou seja, redes com ou sem fio nas instalações do cliente (residências, edifícios ou áreas industriais) que interligam aparelhos com medidores inteligentes e dispositivos de gerenciamento de energia, responsáveis por relatar as premissas de consumo à rede a qualquer momento, enquanto também transporta mensagens da rede de volta para o emissor da premissa [59].

Na camada do meio, pode-se encontrar a Rede da Área do Bairro (NANs), ou seja, redes que cobrem pequenas áreas geográficas responsáveis pela interconexão dos medidores inteligentes de diferentes tipos de instalações com um ponto de acesso de distribuição que agrega os dados coletados por eles encaminhando-os para a camada superior.

Na camada superior desse modelo conceitual, pode-se encontrar redes de área ampla (WANs) interconectando várias NANs. Todos os dados coletadas pelas NANs (seja informação que descreva o estado atual da rede ou o consumo agregado de uma vizinhança ou qualquer outro tipo de informação) é entregue nesta camada superior. Nesta parte do sistema se encontram o sistema supervisor de controlo e aquisição de dados (SCADA),

responsável para aquisição, processamento, apresentação e gerenciamento dos dados recebidos, o sistema de gerenciamento de dados medidos (MDMS) responsável pelo faturamento dos clientes de acordo com seu consumo, os sistemas de gerenciamento de resposta à demanda (DRMS) e os sistemas de gerenciamento de carga (LMS), o sistema de gerenciamento de saída (OMS) e o sistema de informação do cliente (CIS), todos podem ser encontrados nesta camada [60]. Além disso, geração em massa, geração distribuída, redes de transmissão, redes de distribuição, mercados de energia e prestadores de serviços também são considerados parte camada superior.

### 3.2.2. ARQUITETURA DE UMA SMART HOME

Espera-se que o Energy Aware Smart Home esteja em interação constante com seus ambientes internos e externos. O ambiente externo de uma Casa Inteligente consiste em todas as entidades pertencentes ao Smart Grid e a única entidade responsável pela interconexão da Casa inteligente com a rede inteligente. O ambiente interno por outro lado, consiste em todos os aparelhos e dispositivos pertencentes à Smart Home, gerenciada centralmente por uma entidade nele. Tanto o ambiente interno quanto o externo são representados por entidades específicas dentro da Rede doméstica inteligente [61]. Uma entidade conhecida como Interface de Serviços de Energia (ESI) representa o “ambiente externo”, enquanto uma entidade conhecida como Sistema de gerenciamento de Energia (EMS) representa o “ambiente interno”.

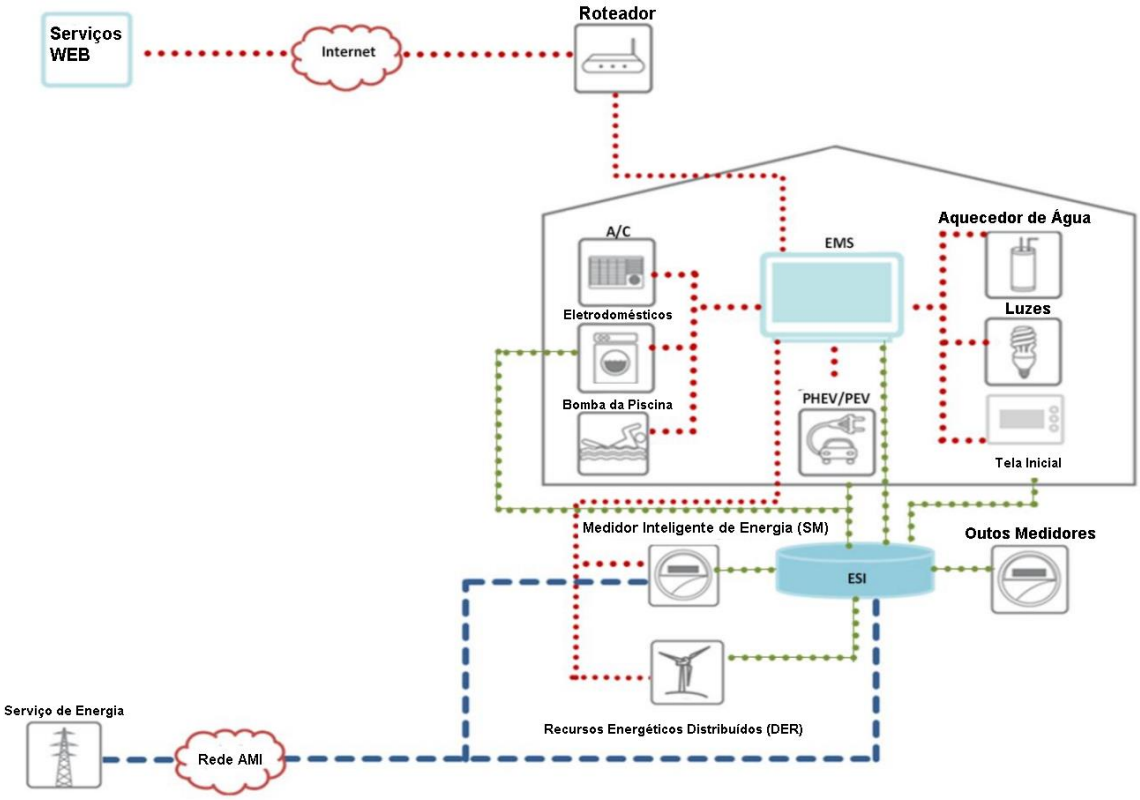



Figura 4 - Uma visão geral das arquiteturas dos ambientes interno e externo de uma SH [64]

O ESI (Figura 4) é a interface entre a Casa Inteligente e a Rede Inteligente. Permite o controlo remoto de dispositivos, o suporte de programas de resposta a demanda, o monitoramento dos Recursos Energéticos Distribuídos tais como turbinas eólicas pertencentes a instalações, os dados de consumo para os pontos de coleta do bairro (se atua como um medidor), permite a cobrança do consumo relativo a veículos híbridos (PEV/PHEV), etc. Apesar de sua separação lógica, as funcionalidades do ESI e do *Smart Meter* podem ser integradas em um único dispositivo físico devido a considerações de custo. O EMS (Figura 4), pelo contrário, é o sistema que permite o gerenciamento de vários aparelhos e sistemas na *Smart Home*, para ajudar a SH a adaptar seu perfil de energia para se adequar à rede. De interesse especial para nós, são os aparelhos controlados pelo EMS que fazem parte da categoria de "Grandes Cargas" controladas [62], como máquinas de lavar, termoacumuladores e sistemas de ar condicionado cuja operação sobrecarrega significativamente a rede. Também são controlados pelo EMS termostatos, interruptores de luz, e bombas de piscina. A Figura 4 ilustra o ESI e o EMS junto com as

entidades conectado a eles. As linhas a traço interrompido verdes representam as entidades conectadas ao ESI, enquanto as linhas pontilhadas em vermelho representam as entidades conectadas ao EMS. A linha azul tracejada representa a comunicação entre a Smart Home e seu ambiente externo.

# 4. *CYBER SECURITY*

Segurança de computadores ou *CyberSecurity* é a proteção de sistemas de computadores contra roubo ou danos ao hardware, software ou dados eletrônicos, bem como a interrupção ou desorientação dos serviços que estes fornecem [52]. Neste âmbito se faz pertinente analisar critérios e objetivos de segurança para os integrantes de um mercado local.

## 4.1. SEGURANÇA EM *SMART GRIDS / SMART HOMES*

### 4.1.1. OBJETIVOS DE SEGURANÇA EM SMART GRIDS

Dada a relação de interdependência das infraestruturas, a demanda por um sistema de fornecimento de eletricidade confiável e resiliente é, portanto, essencial e deve ser bem estruturada para um fornecimento de energia seguro e eficiente [63]. Portanto, objetivos de segurança bem articulados são geralmente considerados para garantir uma operação eficiente e confiável. Esses objetivos devem abranger todos os planos de expansão e melhoria possíveis para redes futuras. Além disso, a expansão da rede para integração em larga escala da energia renovável no suprimento de eletricidade também é de extrema prioridade, já que aumenta ainda mais a garantia de fornecimento através do atendimento dos requisitos entre produção de eletricidade e demandas dos consumidores [52].

As seis metas comumente adotadas como aa mais importante para a segurança do *Smart Home / Smart Grid* são [62]:

- Confidencialidade: a garantia de que os dados serão divulgados apenas para indivíduos ou sistemas autorizados;

- Integridade: a garantia de que a precisão e consistência de dados serão mantidos. Nenhuma modificação não autorizada, destruição ou perda de dados não serão detetadas;

- Disponibilidade: a garantia de que qualquer recurso de rede (dados /largura de banda/equipamento) estará sempre disponível para qualquer entidade autorizada. Esses recursos também são protegidos contra qualquer incidente que ameace sua disponibilidade;

- Autenticidade: a validação de que as partes que se comunicam são quem afirmam ser e que as mensagens supostamente enviadas são realmente enviados por eles;

- Autorização: a garantia de que os direitos de acesso de todos os entidade no sistema são definidas para fins de acesso ao controle;

- Não repúdio: a garantia de que uma prova inegável existirá para verificar a veracidade de qualquer reivindicação de uma entidade.

Na Tabela 1 estão enumerados os objetivos de segurança analisados por [64].

Tabela 1 - Objetivos de Segurança em SGs/SHs [64]

| Objetivos de Segurança | nº |
|---|---|
| Confidencialidade | 1 |
| Integridade | 2 |
| Disponibilidade | 3 |
| Autenticidade | 4 |
| Autorização | 5 |
| Não Repudio | 6 |

### 4.1.2. CLASSIFICAÇÃO DAS AMEAÇAS À SEGURANÇA DA REDE INTELIGENTE POR FONTES

Ameaças de segurança em *Smart Home / Smart Grid* geralmente tentam comprometer uma ou mais das metas descritas anteriormente. Essas ameaças podem ser classificadas em duas grandes categorias [64].

Na primeira categoria, “ataques passivos”, realizam-se ataques tentando aprender ou fazer uso de informações de um sistema sem afetar os recursos do sistema. Ataques passivos podem assumir a forma de intercetação ou análise de tráfego. A intercetação não autorizada de um dispositivo é aquela na qual ocorre comunicação sem o consentimento da rede para fins de obtenção de informação desta rede. A análise de tráfego trata de algo mais subtil, em vez de tentar se apossar do conteúdo da mensagem, o adversário monitora padrões de tráfego para deduzir informações úteis. Ambos os ataques são considerados difícil de detetar, pois eles não alteram os dados. Assim, ao lidar com eles, o foco é a prevenção, e não deteção.

A segunda categoria, “ataques ativos”, é a categoria em que se realizam ataques tentando alterar recursos do sistema ou afetar sua operação. Ataques ativos podem envolver alguma modificação nos dados ou a introdução de dados fraudulentos no sistema. Os ataques mais comuns deste tipo são realizados mascarando, reproduzindo e modificando informações, ou ainda através de softwares maliciosos. Um ataque mascarado ocorre quando um intruso finge ser uma entidade legítima para obter privilégios. Um ataque de reprodução envolve a captura passiva de mensagens em uma comunicação e sua retransmissão para produzir um efeito não autorizado. Um ataque de modificação de mensagem envolve a alteração do conteúdo de uma mensagem legítima ou o atraso ou reordenação de um fluxo de mensagens, com o objetivo de produzir efeito não autorizado. Um ataque de negação de serviço visa interromper temporariamente ou permanentemente ou suspender a disponibilidade dos recursos de comunicação de um sistema. Ataques de software malicioso, são ataques que visam explorar vulnerabilidades internas para modificar, destruir e roubar informações ou obter acesso não autorizado aos recursos do sistema [64].

Na Tabela 2 estão enumeradas as ameaças analisadas por [64].

Tabela 2 - Riscos de segurança em SGs /SHs [64]

| Tipos de Ameaça | n |
|---|---|
| Espionagem | 1 |
| Análise de Tráfego | 2 |
| Modificação de Mensagens | 3 |
| Ataques de "ver novamente" | 4 |
| Reprodução EMS | 5 |
| Repúdio | 6 |
| Violação/Reversão/Remoção do Medidor | 7 |
| Modificação/Atualização ilegal de software | 8 |
| Reprodução do cliente | 9 |
| Reprodução de Dispositivo | 10 |
| Interceptação | 11 |
| Informações publicamente disponíveis | 12 |
| Configuração fraca de plataforma | 13 |
| Vulnerabilidades de software | 14 |
| Malware | 15 |
| Ataques internos | 16 |
| Reconexão com rede passiva | 17 |
| Fabricação de mensagens | 18 |
| Ataques de reprodução | 19 |
| Alteração de arquivos (sistema/não do sistema) | 20 |
| Injeção falsa de dados | 21 |
| Negação de serviço | 22 |
| Representação ESI | 23 |
| Ataques de interferência | 24 |
| Reprodução de Medição | 25 |
| Representação do DRMS/LMS | 26 |
| Reenvio de Mensagens Anteriores | 27 |
| Ataque de falsa sincronização | 28 |
| Acesso ao servidor DRM/LMS | 29 |
| Representação do ESP | 30 |

### 4.1.3. AVALIAÇÃO DE IMPACTO

Para a avaliação da criticidade e sensibilidade de certas interações e avaliação do nível de impacto das ameaças nas interações no ambiente SH/SG, adota-se o FIPS 199, critério de avaliação do nível de impacto [65]. O FIPS 199 caracteriza o impacto potencial de ameaças como baixa, moderada ou alta.

Impacto Baixo, se a violação de uma ou mais das metas de segurança, descritas anteriormente, pode ter um efeito adverso limitado nas operações. Isso pode significar degradação da capacidade de uma entidade de executar com eficiência sua função, danos materiais menores, perdas financeiras menores ou dano menor aos indivíduos.

Impacto Moderado, se a violação de um ou mais dos elementos de segurança tenham um efeito adverso nas operações da SH/SG. Efeito adverso significativo pode significar degradação significativa da capacidade de uma entidade de eficientemente desempenhar suas funções principais, danos significativos a ativos, perdas financeiras significativas ou danos significativos a indivíduos (não incluindo perda de vidas ou ferimentos graves).

Impacto Alto, se a violação de um ou mais dos elementos de segurança tenham um efeito adverso catastrófico nas operações SH/SG. Efeito adverso grave ou catastrófico pode significar degradação grave ou perda da capacidade da entidade de desempenhar suas funções principais, danos a ativos, grandes perdas financeiras ou danos graves a indivíduos (que podem até resultar em perda de vida ou vida lesões ameaçadoras).

Na Tabela 3 estão listados os impactos analisados por [64].

Tabela 3 - Nível de Impacto das ameaças analisadas [64]

| Impactos | Rótulo |
|---|---|
| Baixo | B |
| Médio | M |
| Alto | A |

### 4.1.4. PROBLEMAS DE SEGURANÇA EM *SMART HOMES*

O EMS é a principal entidade do ambiente interno no qual os aparelhos se conectam, relatam seu consumo e recebem sinais de ligar/desligar. O ESI também foi apresentado como a entidade que vincula o SH ao seu ambiente externo. Várias interações entre entidades do SH podem se tornar alvos para um ataque cibernético ou físico por um adversário ou mesmo por um cliente. A seguir, apresentam-se alguns dos cenários:

1) Ataques que ameaçam relatórios bem-sucedidos de consumo de energia do dispositivo

Espera-se que os medidores inteligentes de uma SG sejam capazes de fornecer informações detalhadas sobre o consumo em cada casa em que estão conectados em intervalos de 15 minutos (em vez de dados referentes a um mês, como é o caso da rede tradicional) [66]. Tal desenvolvimento se torna sinônimo de coleta e transmissão de maiores volumes de dados de consumo dos aparelhos SH e cria um risco maior contra a privacidade do cliente. Durante a transmissão destes dados de aparelhos para o EMS uma escuta inserida por um adversário, por exemplo, poderia resultar em dados de consumo valiosos vazando para o adversário que pode assim deduzir muito sobre o estilo de vida de um cliente [67].

2) Ataques visando sinais de importação / exportação de energia em o ESI / HAN

O SG fornece o consumidor a oportunidade de se tornar um produtor de energia bem como consumidor. Instalando energia distribuída recursos em suas instalações, um cliente pode gerar energia que ele pode vender para a rede quando a demanda supera a oferta. Além disso, usando seu veículo elétrico plug-in como bateria, o cliente não apenas pode armazenar, mas também devolver energia a rede quanto pertinente. Mensagens solicitando a exportação ou importação de energia da rede, que chegue ao ESI / HAN do SG de forma incorreta pode trazer riscos.

3) Violação / reversão ou remoção do medidor físico

Incidentes de adulteração de medidores físicos são comuns mesmo antes das redes inteligentes [68][69]. Com os medidores se tornando mais esperados, esperamos mais incidentes físicos adulteração do medidor ou no software do medidor. Clientes mal-intencionados, tentando remover o medidor, inverter a medição ou alterar seu software, em

um esforço para diminuir suas contas de energia elétrica, podem tornar-se um caso comum no futuro do SG.

4) Ataques contra monitoramento doméstico remoto e controle.

Um adversário pode se passar pelo cliente enviando mensagens para o ESI/HAN, solicitando que todos os dispositivos permaneçam ligados ou desligados [64]. Um ataque de personificação de dispositivo, realizado por um adversário, é outro exemplo. Em tal ataque, o cliente acredita que está controlando remotamente um dispositivo quando, na realidade, ele controla outro (por exemplo, em vez de ajustar o forno para 120 ° C pode-se definir a temperatura da sauna a 120 ° C) [64].

5) Ataques visando pedidos de dados de uso de energia.

O cliente na SH pode solicitar a qualquer momento tempo, para receber seu perfil de consumo detalhado. As informações de consumo são coletadas gradualmente por Medidores inteligentes na SH, responsáveis por encaminhar ao sistema MDMS, que processa os dados de medição para aplicar as informações de cobrança eles. O MDMS se comunica com o CIS para armazenar informações de consumo de cada cliente, que podem ser enviadas a ele, mediante solicitação, juntamente com feedback e sugestões [70].

A Tabela 4 sintetiza os riscos de segurança para SHs discriminando as possíveis ameaças para cada cenário (conforme Tabela 2), os objetivos de segurança comprometidos em casa situação (conforme Tabela 1) e seu nível de impacto (conforme Tabela 3) para cada cenário.

Tabela 4 - Riscos de Segurança em SHs [64]

| **Smart Home - Riscos de Segurança** | | | |
|---|---|---|---|
| Cenários | Ameaças Possíveis | Objetivos de segurança Comprometidos | Nível de Impacto |
| 1 | 1,2,3,4,5 | 1,2,4 | B-M |
| 2 | 3,4,6 | 2,4,6 | M |
| 3 | 7,8 | 2,4, | B |
| 4 | 3,4,6,9,10 | 2,4,6 | B-A |
| 5 | 1,3,9,11 | 1,2,4 | B-M |

### 4.1.5. PROBLEMAS DE SEGURANÇA EM *SMART GRIDS*

As entidades do SG também podem se tornar alvos de ataque. A Tabela 5 fornece uma visão mais concisa das ameaças apresentadas em cada cenário descrito nesta seção, as metas de segurança violadas e uma avaliação de impacto. No começo da análise dos casos são apresentados três cenários envolvendo ataques nos servidores principais da *Smart Grid*, cada um dos quais visa atingir um golpe diferente [69].

1) Ataques com o objetivo de roubar dados de servidores públicos;

2) Ataques com o objetivo de assumir o controlo de servidores utilitários;

3) Ataques com o objetivo de derrubar servidores utilitários.

Todos os três cenários descritos acima, definem os servidores principais da SG como seu principal objetivo, visando obter informações valiosas sobre o sistema ou acessá-lo, para roubar dados ou exercer controlo. A coleta de informações valiosas sobre o sistema permite que o adversário planeje um ataque direcionado ao SG enquanto obtém acesso ao sistema, dá ao adversário a oportunidade de interagir da maneira que quiser.

4) Ataques contra equipamento de medição de área ampla.

Ataques nos quais adversários manipulam medições de dispositivos de campo e dispositivos de medição na SG introduzir erros nas medições destinadas a central de medição. Medições falsas passando pelo algoritmo de estimativa de estado resulta em uma estimativa de estado que não condiz com o estado real da rede. Desta forma ocorrem acionamentos de cargas ou resposta à demanda em horários errados, estimativas erradas da demanda do dia seguinte, aumentando as chances de instabilidades ou apagões contínuos, etc. [71].

A Tabela 5 sintetiza os riscos de segurança para SGs discriminando as possíveis ameaças para cada cenário (conforme Tabela 2), os objetivos de segurança comprometidos em casa situação (conforme Tabela 1) e seu nível de impacto (conforme Tabela 3) para cada cenário.

Tabela 5- Riscos de segurança em SGs [64]

| Smart Grid - Riscos de Segurança | | | |
|---|---|---|---|
| Cenários | Ameaças Possíveis | Objetivos de segurança Comprometidos | Nível de Impacto |
| 1 | 12,13,14,15,16 | 1,2,3,4,5 | M-A |
| 2 | 12,13,14,15,17,18,19,20 | 1,2,3,4,5,6 | M-A |
| 3 | 1,2,3,10,19,20,23 | 1,2,3,4,5 | A |
| 4 | 15,21 | 2,3 | M-H |

### 4.1.6. PROBLEMAS DE SEGURANÇA -*SMART HOMES* PARA *SMART GRIDS*

Tendo adquirido uma visão mais abrangente sobre ameaças à SH e à SG individualmente, pode -se identificar algumas das principais ameaças que visam a interação entre eles. Primeiramente apresentam-se as ameaças que começam afetando entidades na SH, e evoluem de maneira a afetar o ambiente da SG.

1) Ataques visando a resposta à demanda sinais no ESI/HAN

Nesse cenário, um adversário pode invadir o ESI/HAN para intercetar os sinais de resposta a demanda pretendidos, para substituí-los por dados mais antigos (como parte de um ataque de repetição). Pode-se realizar também a modificação dos sinais recebidos pelo ESI/HAN (como parte de um ataque de modificação de mensagem) [62].

Ataques nesse cenário também podem ser iniciados pelo cliente. Mais especificamente, um cliente mal-intencionado que concordou em participar da resposta à demanda, porém realiza alterações nas medições de maneira a não ter o uso limitado de nenhum de seus dispositivos [64].

2) Ataques que ameaçando a comunicação de interrupções

As ameaças em potencial nesse caso podem se referir a ataques ao medidor. Assim, mensagens mais antigas (relatórios de falta de energia) enviadas ao operador são reproduzidas mesmo quando não há interrupção para que o pessoal seja despachado para áreas específicas quando na verdade não há necessidade [70].

3) Ataques que ameaçam o DER relatórios de desligamento / isolamento

Representações do medidor, ataques de repetição e mensagens ataques de modificação são apenas alguns dos possíveis ataques nesse cenário.

4) Ataques contra o agregador NAN.

Os ataques nesse cenário podem envolver a interceção passiva de dados a serem transferidos do ESI/HAN para o SM (e então para a NAN agregadora) ou uma modificação ativa dos dados/ injeção de novos dados na rede.

A Tabela 6 sintetiza os riscos de segurança de SHs para SGs discriminando as possíveis ameaças para cada cenário (conforme Tabela 2), os objetivos de segurança comprometidos em casa situação (conforme Tabela 1) e seu nível de impacto (conforme Tabela 3) para cada cenário.

Tabela 6 - Riscos de segurança de SHs para SGs [64]

| **Smart Home para Smart Grid - Riscos de Segurança** | | | |
|---|---|---|---|
| Cenários | Ameaças Possíveis | Objetivos de segurança Comprometidos | Nível de Impacto |
| 1 | 3,6,10,19,23,24 | 2,4,5,6 | B-M |
| 2 | 19,25 | 2,4,5 | B |
| 3 | 3,19,25 | 2 | B-M |
| 4 | 1,3,21,22 | 1,2,3 | B-A |

### 4.1.7. PROBLEMAS DE SEGURANÇA -*SMART GRIDS* PARA *SMART HOMES*

A última categoria de ameaças que se apresenta é a de ameaças que começam afetando entidades na SG, e evoluem de maneira a afetar o ambiente da SH.

1) Ataques visando sinais de resposta à demanda para o ESI/HAN

Possíveis ataques nesse cenário, poderia incluir a representação do sistema DRMS (sistemas de gerenciamento de resposta à demanda) por um adversário, que poderia repetir mensagens de uma resposta de demanda mais antiga como parte de um ataque de repetição.

2) Ataques visando desligamento direto de carga sinais para o ESI / HAN

Quando a demanda por eletricidade excede o suprimento disponível, interrupções planejadas do suprimento na forma de desligamento de carga, pode ter que ser realizado para evitar instabilidades na rede que possam danificar seus equipamentos. Essas interações na fonte de alimentação são acionadas por um LMS (servidor responsável pela

emissão e encaminhamento comandos para instalações em áreas específicas de acordo com horário predeterminado) [66]. Um ataque a este servidor pode ser caracterizado dentro deste tipo de ameaça.

3) Ataques visando Importação/Exportação de sinais de energia para o ESI/HAN

Ataques de repetição estão entre os mais propensos a ocorrer em tais cenários [70]. Neste tipo de ataques as mensagens para importação / exportação de energia são reproduzidas, independentemente das necessidades da rede, fazendo com que a energia seja extraída da rede elétrica em momentos de alta demanda ou energia sendo liberada para a rede nos momentos em que não é necessário.

4) Ataques visando dados relacionados ao cliente encaminhado para um terceiro ESP confiável

Ataques altamente prováveis nesse cenário poderiam envolver a representação de um adversário de terceiros ou espionagem, para que o adversário receba as mensagens de consumo de energia e urgência. Assim, violando a privacidade do cliente e potencialmente interrompendo a comunicação, impedindo-o de agir em proveito do cliente.

A Tabela 7 sintetiza os riscos de segurança de SGs para SHs discriminando as possíveis ameaças para cada cenário (conforme Tabela 2), os objetivos de segurança comprometidos em casa situação (conforme Tabela 1) e seu nível de impacto (conforme Tabela 3) para cada cenário.

Tabela 7 - Riscos de segurança de SGs para SHs [64]

| **Smart Grid para Smart Home - Riscos de Segurança** | | | |
|---|---|---|---|
| Cenários | Ameaças Possíveis | Objetivos de segurança Comprometidos | Nível de Impacto |
| 1 | 3,26,27,28 | 2,4 | B-M |
| 2 | 4,22,28,29 | 2,3,4,6 | B-A |
| 3 | 3,4,22 | 2,3,4 | M-A |
| 4 | 1,3 | 1,2,4 | B-M |

## 4.2. CONTRAMEDIDAS

### 4.2.1. GARANTIR CONFIDENCIALIDADE

A técnica mais básica para obter confidencialidade hoje em dia é através de criptografia. Modernas técnicas de criptografia disponíveis hoje, podem ser classificadas em duas categorias de acordo com o tipo de chave que eles usam. A primeira categoria, inclui algoritmos de chave simétrica e também é conhecida como criptografia de chave privada, pois o remetente e o recetor compartilham uma chave secreta para sua comunicação. A segunda categoria inclui algoritmos de chave assimétrica e também é conhecido como criptografia de chave pública, pois cada uma das partes comunicantes tem sua chave pública (conhecida por todas as outras partes) e sua chave privada (que é mantida em segredo) [72][73]. Em geral algoritmos simétricos (como os padrões AES e TDES) são utilizados para fins de dados criptografia dentro do *Smart Grid*. Algoritmos assimétricos por outro lado, (como o DSA, ECDSA etc.) são utilizados para fins de digitalização de mensagens [66].

### 4.2.2. GARANTIR PRIVACIDADE

Desde a sua aparição, implantações de medição inteligente têm levantado inúmeras preocupações por ser potencialmente invasiva a privacidade. Os dados de consumo coletados por medidores inteligentes podem revelar muito sobre o comportamento, atividades e hábitos dos moradores dentro de uma premissa, causando medo aos clientes. Até a presente data, vários modelos foram propôs os para garantir a privacidade de dados de medição dentro do ambiente SH/SG [70]. Algumas técnicas para garantia de privacidade são brevemente apresentadas abaixo:

- Anonimização: um processo que remove o link entre os dados e sua origem de tal maneira que o utilitário pode receber os dados necessários para transportar seus cálculos, mas não pode atribuir os dados recebidos para um medidor específico;

- Agregadores confiáveis: o medidor ou um terceiro confiável são consideradas entidades confiáveis que podem lidar com a agregação de dados de medição e seu encaminhamento para o utilitário. A utilidade nesse caso pode usar apenas os agregados de dados sem ser capaz de ter acesso ao consumo individual informações dos medidores participantes;

• Criptografia Homomórfica: um esquema de criptografia que permite o trabalhar com dados criptografados sem a necessidade de descriptografa-los, minimizando a possibilidade de exposição das informações;

• Modelos de perturbação: modelos que introduzem ruído aleatório de uma distribuição conhecida para os dados de medição sensíveis à privacidade, antes de serem transmitido à concessionária. O utilitário que recebe os dados perturbados reconstrói uma aproximação dos dados originais. Uma troca entre o nível de privacidade alcançada e a perda de informações existe;

• Modelos de computação verificáveis: modelos nos quais o agregador fornece uma prova junto com o agregado de dados de medição, que o cálculo foi realizado conforme reivindicado. Essa prova pode ser fornecida através de um sistema à prova de conhecimento zero, com o medidor inteligente sendo o provador e o utilitário o verificador. Na prova de zero conhecimento, o verificador apenas confirma que o provador tem o conhecimento que ele afirma ter e nada mais do que isso;

• Técnicas de ofuscação de dados: baseadas em abordagens que visam ocultar a quantidade de energia consumida liberando sua carga. Trata-se de um método para anonimizar com segurança os dados de medição elétrica. Sua abordagem distingue dois tipos de tráfego transportado por um medidor inteligente. Dados de baixa frequência, necessários para fins de cobrança ou gerenciamento de contas que precisa ser atribuível e coletado todos os dias / semana / mês etc. e dados de alta frequência, necessários para operação eficiente do SG (programas de resposta à demanda, estimativa de demanda etc.), que devem ser coletados a cada minuto / cinco minutos. Os medidores neste esquema têm dois IDs incorporados um para dados de alta e outra para dados de baixa frequência [75]. O ID da frequência (LFID) será público, para que possa ser usado pelo serviço de energia para cobrar um cliente pelo consumo. O ID de alta frequência (HFID), por outro lado, deve permanecer oculto, para que ninguém seja capaz de identificar a fonte de dados de medição específicos. A fim de manter seu sigilo, o ID de alta frequência deve ser codificado no dispositivo considerando que para efeitos de verificação de um HFID é válido um protocolo diferente, combinando técnicas de anonimização com computação verificável sem implicar confiança em qualquer *gateway* ou terceiro [76]. Seu protocolo consiste essencialmente em dois subprotocolos um subprotocolo de faturamento e um subprotocolo de relatório de carga. Um medidor inteligente usa o protocolo de faturamento para enviar o

consumo de energia elétrica à concessionária, criptografado e assinado assimetricamente. Durante o processo de faturamento, as identidades do cliente e do medidor são mantidas em público. O protocolo de relatório de carga explora uma ideia nomeada esquemas de assinatura de grupos. Para efeitos deste protocolo diz-se que todo medidor inteligente pertence a um grupo (cujo gerente de grupo é o fornecedor de energia). Sempre que um medidor deseja relatar seu consumo assina usando o nome do grupo.

### 4.2.3. GARANTIR INTEGRIDADE

Os ataques contra a integridade não se limitam apenas a modificações de mensagens. Ataques de injeção de dados falsos, de repetição, de personificação de dispositivos e ataques esparsos são também considerados grandes ameaças a integridade do sistema. A seguir são citadas duas metodologias desenvolvidas na tentativa de garantia de integridade.

Para garantia da integridade pode ser utilizada a técnica de marca d'água [77]. A marca d'água digital é uma técnica de incorporação de dados digitais nas leituras do medidor em tempo real, com uma marca d'água com informações exclusivas sobre o proprietário da leitura. O objetivo da marca d'água é validar a integridade dos dados. Dados com marca d'água são enviados do medidor ao gerador de energia através de redes não seguras de alta velocidade propenso a ataques de injeção de dados falsos. Para garantir o sucesso na deteção desses ataques, os medidores usam taxa baixa e canais seguros para transmitir com segurança as marcas d'água. O gerador recebe, assim, as marcas d'água e dados com marca-d'água, para correlacioná-los e detetar falsos ataques de injeção de dados [77].

Mesmo um adversário sem conhecimento da topologia da rede elétrica pode lançar com êxito ataques de injeção de dados ruins. Quando o sistema é pequeno e pode ser aproximado linearmente, uma análise independente de componentes pode ser aplicada para calcular a matriz jacobiana que, se multiplicada pelos vetores próprios da matriz de covariância das variáveis de estado pode expor informações necessárias a um adversário que deseja lançar um ataque de injeção de dados falsos sem ser notado. Como contramedida pode-se implementar um algoritmo recursivo de soma cumulativa, que compreende de duas etapas intercaladas. A primeira introduz o solucionador linear de parâmetros desconhecidos enquanto a segunda aplica o algoritmo com várias ameaças. A defesa proposta por este mecanismo visa detetar ataques o mais rápido possível com um número mínimo de observações, mantendo um nível satisfatório de precisão [78].

### 4.2.4. GARANTIR DISPONIBILIDADE

Ataques potenciais contra a disponibilidade da SG visam saturar os recursos da rede para impedir que ela seja acessível a seus usuários legítimos. Vários ataques introduzidos foram ataques na camada física. Os ataques de camada física foram os ataques de injeção de dados falsos e ataques de interferência. A melhor maneira de defender contra interferência intencional é usar vários canais de frequência alternativos quando for detetada interferência o canal atual. A AMI e todos os nós dentro dele, podem ser programados para se mover através de uma sequência de canais comum e predefinida, codificada, se o canal padrão sofrer perdas de pacotes que estão acima de um limite aceitável, por um período especificado [57]. Todo nó que é introduzido na rede AMI e autenticado a ele, recebe um salto de canal predefinido em sequência criptografada com a chave pública do cliente. O nó recupera a sequência descriptografando com a chave privada do cliente e começa a se comunicar no canal atualmente utilizado. Devido à pseudo-aleatoriedade da sequência de salto de canal, é considerado difícil para o adversário prever qual canal é para ser usado a seguir e, portanto, para executar um ataque de interferência contra isso [57].

Igualmente capazes de comprometer a disponibilidade da SG são Ataques de negação de serviço que ocorrem em camadas superiores à camada física. A prática comum contra esses ataques é a implantação de sistemas de deteção de intrusões (IDS). Os sistemas de deteção de intrusão podem ser classificados em três categorias amplas [79]:

- Com base em assinaturas;
- Com base em especificações;
- Com base em anomalias.

Um IDS baseado em assinatura reconhece invasões usando uma lista negra de padrões de ataque conhecidos. Enquanto um IDS baseado em especificação deteta ataques usando um conjunto restrições (regras) que definem a operação correta de um programa ou protocolo. Um IDS baseado em anomalia reconhece desvios do que é considerado normal, construindo um modelo de comportamento normal do sistema onde qualquer desvio do normal é identificado como uma intrusão [79].

Oura abordagem sugere a instalação, em pontos-chave da rede, de sensores de intrusão baseados em mecanismos de deteção adequados para detetar intrusões nas camadas da

aplicação, transporte e rede. Os autores detetam o comportamento esperado dos medidores na camada de rede com base na especificação de protocolos usados por esses medidores. Este comportamento é modelado em um diagrama de estado simples representando todos os estados e transições possíveis de um medidor para outro. Uma máquina de estado semelhante para a camada da aplicação também é apresentada. Cada estado dessas máquinas de estado define um conjunto diferente de direitos e funcionalidades. Qualquer operação do medidor que se comporta de maneira não esperada e não respeita o conjunto esperado de regras é considerado suspeito [80].

### 4.2.5. GARANTIR AUTENTICIDADE

Garantir a autenticidade é garantir que possamos provar a veracidade de qualquer alegação relativa a transações dentro do SG. *Hashes* (dispersões) criptográficas são atualmente usados para garantir a integridade da mensagem contra alterações deliberadas, da mesma forma que as somas de verificação são usadas para detetar os inadvertidos. Semelhante as *hashes* criptográficas, com exceção de que eles fazem uso de uma chave secreta, são os códigos de autenticação de mensagens como HMAC (códigos de autenticação de mensagem) que estão entre as abordagens mais usadas para alcançar autenticidade na atualidade [81]. Tais esquemas também podem ser usados dentro da SG, assim como esquemas de assinatura digital que garantem a autenticidade da mensagem por meio de criptografia. Esses esquemas operam com a premissa de que todas as entidades comunicantes possuem seu próprio par de chaves público-privado.

Antes de enviar uma mensagem criptografada com chave pública, o remetente pode dispersar a mensagem e assinar tal dispersão com sua chave privada. Ao receber a mensagem, o recetor usa sua chave privada para descriptografá-la e avaliar sua dispersão e a chave pública do remetente para descriptografar a dispersão original [81]. As duas dispersões são então comparadas, se corresponderem a integridade da mensagem é comprovada e também é autenticidade (já que ninguém, além do remetente, poderia ter assinado a mensagem com a chave privada do remetente).

### 4.2.6. GARANTIR AUTORIZAÇÃO

O penúltimo objetivo de segurança em que nos concentramos é a autorização, ou seja, Autorização é o atestado de que nenhuma entidade dentro do ambiente SH/SG pode ter acesso a informações ou serviços além de sua autoridade [66]. Apesar disso, sua importância para a segurança deste ambiente, a literatura sobre autorização é ainda limitada.

A autorização pode ser garantida através de um esquema com o uso de um atributo variante de criptografia modificada específica, de acordo com as necessidades da rede inteligente. Desta forma, a RTU coleta dados de diferentes unidades, criptografa dados sob um conjunto de atributos antes de enviá-los para os dados de repositório em que devem ser mantidos. Esses atributos podem ser qualquer informação relacionada a esses dados, como a fonte de energia (por exemplo, energia solar, eólica, combustível fóssil), o tipo de consumidor (por exemplo, indivíduo, empresa, veículo), o tipo de equipamento (por exemplo, secador, aquecedor), o tempo de uso (por exemplo, pico, fora de pico) etc. Dessa forma, a RTU cria uma política de acesso para os dados e coloca no repositório. Assim, usuários que desejam ter acesso a eles devem primeiro adquirir chaves secretas correspondentes aos atributos de seu interesse, de um KDC (centro de distribuição de chaves). Dessa forma, os usuários só podem descriptografar os dados para os quais eles têm atributos correspondentes, portanto o controle de acesso é alcançado [82].

A garantia de autorização pode ainda ser baseada em atributos específicos para Sistemas de Automação de Subestações. Esta abordagem explora a ideia de certificados de chave públicos e nenhum uso de sistemas de conhecimento para fins de autenticação, mas sim a ideia de certificados de atributo (ACs). Um certificado de atributo pode ser considerado como complementar a um certificado de chave pública. Um certificado de chave pública (PKC) é emitido por uma autoridade de certificação (CA) e é usado para verificar a identidade de seu proprietário, assim como um Passaporte. Por outro lado, é emitido também outro certificado, por uma autoridade de atributo (AA), e é usada para caracterizar ou autorizar seu titular, assim como um visto dá pessoa a permissão para viver/trabalhar em um local específico por um período de tempo. Sempre que um usuário solicita acesso a um ID de uma subestação, tanto o usuário quanto o ID são autenticados. Após a autenticação, a subestação controladora fornece ao usuário seu certificado de atributo (definindo suas permissões). A partir desse momento, toda vez que um usuário desejar ter

acesso ao ID, ele envia sua assinatura solicitação, seu PKC e seu AC que serão usados para garantir autenticidade e autorização [83].

### 4.2.7. GARANTIR O NÃO REPÚDIO

Por último, de maneira complementar ao realizado para obtenção da autenticidade, onde se utilizam técnicas de dispersão e assinatura do remetente, o não repúdio também pode ser alcançado se o remetente exige um reconhecimento assinado do recetor, verificando se ele realmente recebeu a mensagem [81]. Outra maneira eficiente de garantia do não repúdio é a instalação de dois medidores inteligentes com um fio elétrico que conecta o lado de envio com o lado de recebimento. O medidor de um lado representa a leitura do assinante enquanto o medidor no outro lado representa a leitura do provedor. Estes dois nem sempre esperam que as leituras sejam iguais, mesmo sob circunstâncias normais devido a perdas de energia durante a transferência de energia, problemas de sincronização e outros atrasos. Contudo, às vezes, sua inconsistência pode sugerir medidores comprometidos, interferência ou qualquer outro tipo de ataque. Em tais casos, as leituras dos dois extremos são trocadas e a inconsistência é verificada em relação a um limite aceitável. Se a leitura provar ser o resultado de um comprometimento, se inicia assim uma investigação adiciona [84].

Uma síntese das metodologias de garantia aqui explanadas pode ser encontrada na Tabela 8.

Tabela 8 - Revisão das contramedidas de segurança por objetivo [64]

| Medidas de Segurança por Objetivo |
|---|
| **Confidencialidade e Privacidade** |
| *Algoritmos de criptografia simétrica/assimétrica |
| *Anonimização |
| *Agregadores confiáveis |
| *Criptografia Homórfica |
| *Modelos de perturbação |
| *Modelos de computação verificáveis - sistemas à prova de conhecimento zero |
| *Ofuscação de dados |
| **Integridade** |
| *Técnicas de hash criptográfico |
| *Marca d'água digital |
| *Algoritmo de soma cumulativa adaptativa |
| *Instalação de PMUs seguras conhecidas na rede |
| *Perfil de carga |
| *Timestamps |
| *Números de sequência |
| *Chaves de sessão |
| *Nonces |
| **Disponibilidade** |
| *Canais alternativos de frequência de acordo com a sequência codificada |
| *Encontro de quorum de frequência |
| *IDSs baseados em anomalias |
| *IDSs baseados em especificação |
| **Autenticidade** |
| *Funções de hash criptográfico com chave |
| *Funções fisicamente não clonáveis |
| *Códigos de autenticação baseados em hash |
| *Mensagens anexadas a MAC e assinadas por HORS |
| **Autorização** |
| *Criptografia baseada em atributos |
| *Certificados de atributo |
| *Sistema de controle de acesso baseado em atributos baseado em XACML |
| **Não Repúdio** |
| *Inspeção mútua com medidores inteligentes |
| *Chaves exclusivas para comunicação AMI do cliente |
| *Registro de transação AMI |

# 5. CASOS DE ESTUDO

Posteriormente aos estudos apresentados nos Capítulos 2, 3 e 4, se faz pertinente a estruturação de um caso de estudo que relacione a segurança cibernética de *Smart Grids* e *Smart Homes* a mercados locais de energia. A ideia é estabelecer uma relação de impacto entre os preços de energia executados nos mercados locais e ataques cibernéticos.

## 5.1. MODELO 1

O modelo 1 adotado para embasar o primeiro estudo de caso proposto é fundamentada a partir de um modelo físico da smart city, GECAD-BISITE, estruturada a partir da cidade de Salamanca na Espanha [85]. Este modelo local de mercado teve como base, para definições de cálculos de preço de compensação, a miniaturização do mercado grossista. De forma resumida, a cidade é composta por um conjunto específico de agentes apresentados na Tabela 9.

Tabela 9 - Descrição dos agentes para definição do mercado local de energia – Modelo 1 [85]

| | Quantidade | Numero de barramentos | Representação % na geração no mercado local [%] | Representação % no consumo no mercado local [%] |
|---|---|---|---|---|
| Geradores Locais (GL) | 2 | 7,11 | 8,74 | 0 |
| Consumidores Produtores (CP) | 10 | 2,4,5,6,7,11,12 | 11,3 | 5,13 |
| Consumidores Tradicionais (CT) | 5 | 3,8,10 | 0 | 3,69 |
| Gerador Comercial de Grande Porte (GG) | 1 | 9 | 0,3 | 7,8 |
| Geradores Comerciais de Pequeno Porte (GP) | 7 | 2,4,5,6,7,9,12 | 0 | 79,85 |
| Consumidores Prioritários (PR) | 2 | 3,13 | 0,38 | 3,53 |

As seis categorias que descrevem os agentes inseridos no mercado local são a base para a realização das simulações. Vale ressaltar que a representatividade remanescente de 79,28 %, referente à geração necessária para o mercado local, é suprida através da relação com o mercado de energia elétrica num nível global [7].

Para que seja possível ilustrar a rede elétrica no modelo de mercado local considerado para o presente estudo, expõem-se na Figura 5 um esquema do sistema elétrico de energia da rede local [7].

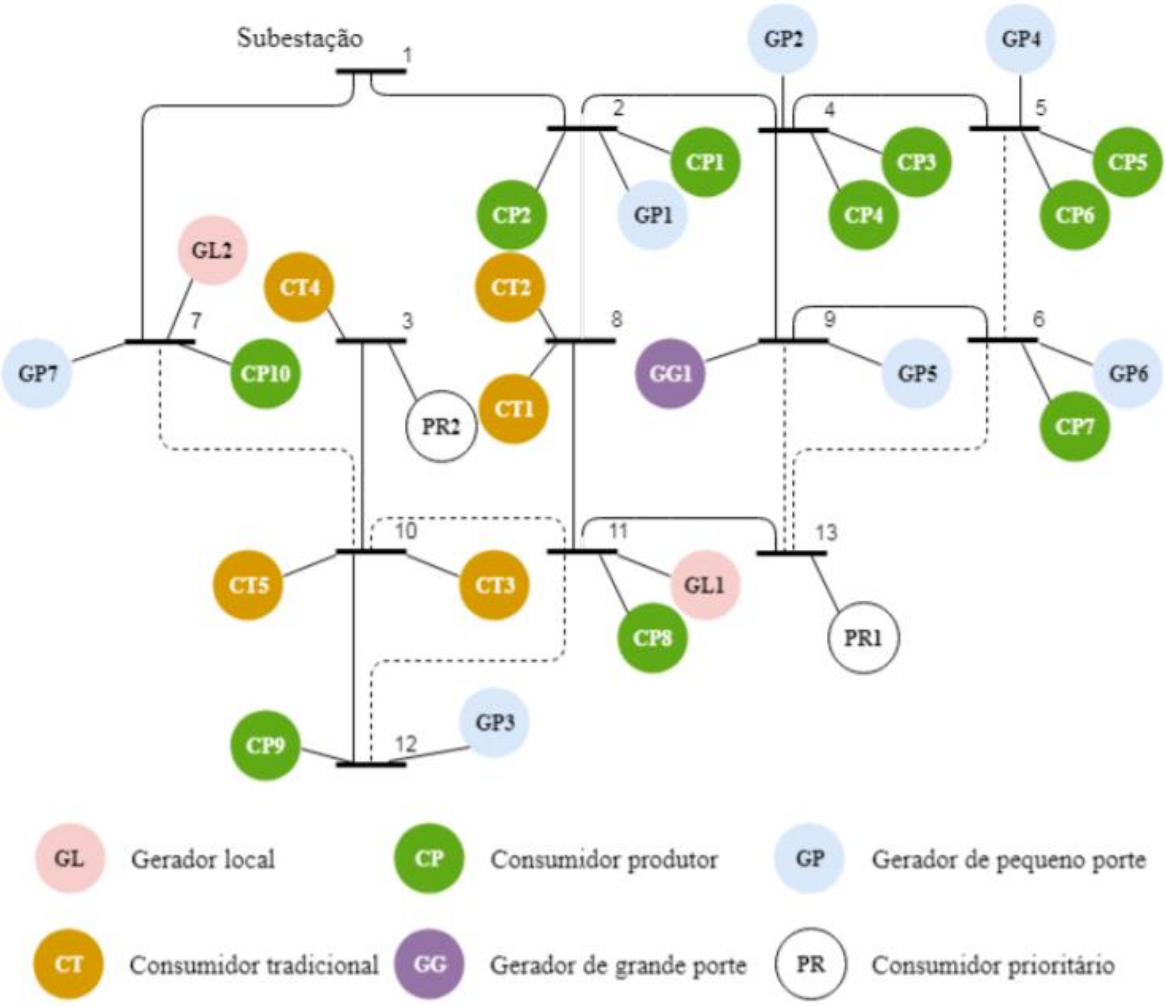



Figura 5 - Esquema do sistema elétrico estruturado para o mercado local de energia – Modelo 1 [7]

A disposição dos agentes do mercado local, apresentada na Figura 5, leva em consideração as características da cidade modelo de Salamanca [85].

Os dois GLs levados em conta são entidades exclusivamente geradoras de energia elétrica. No contexto examinado, tais geradores produzem energia elétrica através de geração eólica, ou seja, renovável. Estes geradores estão atrelados às gerações de energia de menor proporção e distribuídas em locais mais próximos de centros de consumo [7].

Os CPs são consumidores residenciais que possuem geração local e podem ser vistos como elementos principais na estruturação do mercado local já que são responsáveis por boa parte da geração 11,3% (fotovoltaica) e 5,13% do consumo [7].

Os CTs são consumidores que não possuem qualquer tipo de geração de energia elétrica associada. Sua representatividade no mercado local restringe-se à compra de energia de outros agentes em mercados locais ou do mercado global [7]. A tendência é que com o passar do tempo estes agentes passem a ser também produtores.

No modelo considerado, é apontado um gerador comercial de grande porte (GG). Tal gerador pode ser visto como uma grande indústria que produz uma parte de seu consumo de energia através de uma geração local com base na combustão de resíduos resultantes de seu processo produtivo. Tal agente necessita de uma considerável quantidade de energia elétrica para suprir sua demanda. Desta forma, este agente pode ser visto como um consumidor produtor que apresenta características de consumo mais substanciais [7].

Os geradores comerciais de pequeno (GP) porte são edifícios comerciais com geração fotovoltaica agregada, como galerias comerciais, supermercados e lojas em geral. A atividade foco deste tipo de agente não é a geração de energia elétrica, mas sim outras atividades comerciais. A condição destes geradores comerciais de pequeno porte é semelhante à situação dos consumidores tradicionais, com a ressalva de que há geração fotovoltaica que não supre o consumo de energia em período algum, ou seja, o mercado local enxerga tais agentes como sendo consumidores tradicionais de grande consumo [7].

Os dois consumidores prioritários (PR) são evidenciados na cidade modelo e representam um prédio do corpo de bombeiros, conectado na barra 13, e um hospital, conectado na barra 3. Os PRs apresentam características diferenciadas em relação aos outros consumidores devido ao impacto que a interrupção de fornecimento pode trazer, seja na perda de vidas ou prejudicando a manutenção da segurança pública. Atrelar a geração de energia elétrica às incertezas associadas às condições climáticas acaba por não ser a melhor opção para este tipo de agente. Desta forma, estes agentes dispõem de um regime de cogeração a diesel para gerar energia elétrica de maneira instantânea no caso de uma ausência de fornecimento [7].

### 5.1.1. PREÇO

Para o estudo de caso considerado é necessário que os valores de preços de compra e venda de energia no mercado local sejam definidos. Tais preços devem ser menores ou iguais ao preço do mercado global, estabelecido como referência para o período considerado. A dinâmica de precificação do mercado local é definida de acordo com o tipo de investimento. O sistema dispõe de três modalidades de investimento para geração distribuída, sendo elas: fotovoltaica comercial, fotovoltaica residencial e eólica. Considera-se como preço base (100%) o valor da energia do mercado global para o período.

A avaliação econômico-energética de autoconsumo de energia fotovoltaica no setor não residencial, aponta que o investimento em produção fotovoltaica para setores comerciais pode reduzir até 50 % da fatura de energia elétrica [86]. Sendo assim, pode-se considerar que o preço de venda para esta modalidade de geração no mercado local é de pelo menos 50% do preço do mercado global [7].

Levando em consideração a avaliação econômico-energética de projetos fotovoltaicos residenciais e o preço imediato, de sistemas fotovoltaicos nesta modalidade, o preço da energia é tido como 25 % maior quando comparado ao preço para a modalidade não residencial [87]. Sendo assim, o preço de venda de energia no mercado local para tal modalidade é de, no mínimo, 62,5 % do preço de referência de mercado global [7].

Para a geração eólica, a avaliação econômico-energética deve considerar os custos de aquisição, custos de geração de energia elétrica, energia produzida, custo de oportunidade e tempo de vida útil [88]. Desta forma, ao observar a razão do preço de venda estimado de mercado e o preço da energia efetivamente gerada por fonte eólica, pode-se definir que o preço de venda de energia no mercado local é de no mínimo 80,9 % do preço do mercado global [7]

### 5.1.2. PREÇO DE COMPENSAÇÃO DO MERCADO

A fixação de preços em mercados competitivos de energia segue os mesmos princípios econômicos que ditam os resultados dos preços em outros mercados competitivos de mercadorias ou produtos. Leilões de Energia podem ser projetados para definir um preço único e uniforme. Em um leilão competitivo de energia, o preço que os compradores pagam e os vendedores recebem sempre satisfaz um princípio econômico fundamental: todas as avaliações dos compradores vencedores da mercadoria são iguais ou superiores ao

preço e custo de produção dos vendedores vencedores são menores ou iguais ao preço. A regra é: compradores cuja avaliação da mercadoria é menor que o preço não a comprarão e os fornecedores cujo custo para produzir a mercadoria é mais alto que o preço não será exigido para produzi-lo [89].

O preço que satisfaz a demanda agregada dos compradores vencedores e cobre os custos agregados dos vendedores vencedores é chamado de preço de compensação do mercado, no jargão do setor de eletricidade. Esse preço libera o mercado em que a quantidade agregada demandada (a soma de todas as quantidades demandadas de compradores individuais) e quantidade agregada fornecida (a soma de todas as quantidades fornecidas pelos vendedores individuais) são iguais, uma condição referida por economistas como equilíbrio de mercado. Se o preço de mercado fosse menor, haveria mais quantidade demandada do que seria suprida e, se fosse estabelecida mais alta, haveria menos quantidade demandada do que suprida, em outras palavras, o mercado não estaria em equilíbrio [89].

Mercados bilaterais descentralizados levam naturalmente a múltiplos preços determinados através de contratos privados negociados entre pares de compradores e vendedores e dependentes de informações e fatores relevantes para cada parte da transação. Então, pode parecer que esses mercados podem não obedecer ao princípio. No entanto, se todas essas negociações privadas preços e quantidades correspondentes seriam revelados publicamente e agregados, o conjunto de preços bilaterais satisfariam o princípio, com o preço mais alto atuando como preço de compensação [89]. Sendo assim pode-se dizer que a formação do preço de compensação (Figura 6) ocorre de maneira semelhante em mercados locais de energia.

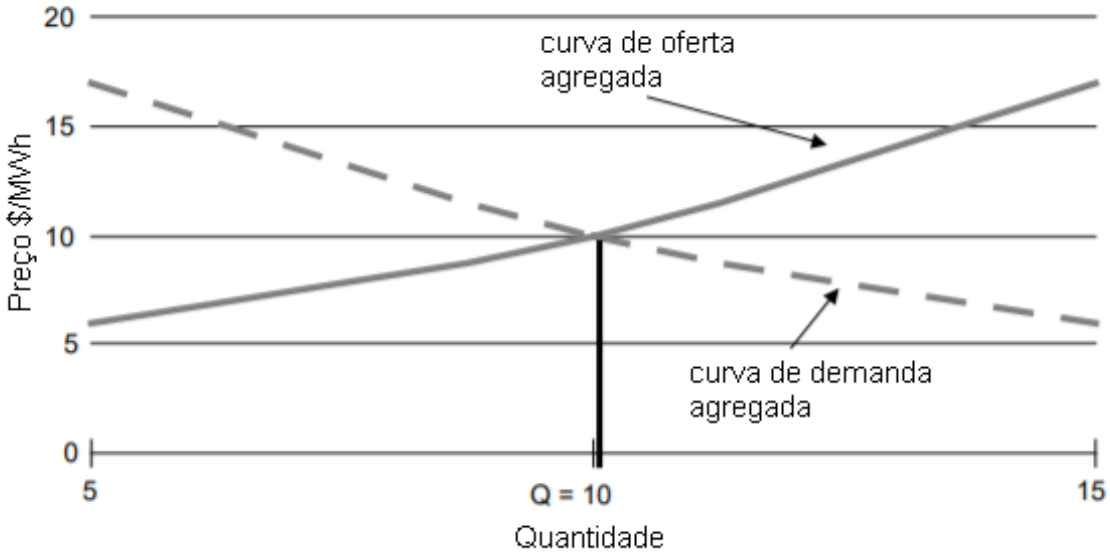



Figura 6 - Oferta e Demanda Agregadas: Determinação do preço de compensação do mercado [89]

### 5.1.3. DEFINIÇÃO DOS CENÁRIOS DE ESTUDO – MODELO 1

Para definição dos cenários de estudo cabe analisar o impacto que cada cenário de ataque a SGs e a SHs já previamente analisados poderiam ter na formação de preço de um Mercado Local. Para tanto se desenvolveu a análise que segue.

Problemas de segurança para Mercados Locais de Energia

O Mercado Local EMS é a entidade maior do ambiente em análise. Nele os aparelhos conectados à rede, que relatam seu consumo e recebem sinais de ligar/desligar, são traduzidos na precificação da energia. Trata-se da entidade que reúne todas as informações até então disponibilizadas e atua efetivamente de maneira econômica. Conforme já citado anteriormente, várias interações entre entidades do SH e SG podem se tornar alvos para um ataque cibernético ou físico por um adversário ou mesmo por um cliente de maneira a impactar nos dados que chegam ao mercado. A seguir, apresentam-se os cenários já utilizados anteriormente, agora de maneira compacta na Tabela 10:

Tabela 10 - Cenários para mercados locais e suas origens

| Mercado Local - Cenários | | |
|---|---|---|
| nº | Cenários | Onde Ocorre |
| 1 | Ataques que ameaçam relatórios bem-sucedidos de consumo de energia do dispositivo | SH |
| 2 | Ataques visando sinais de importação / exportação de energia em o ESI / HAN | |
| 3 | Violação / reversão ou remoção do medidor físico | |
| 4 | Ataques contra monitoramento doméstico remoto e controle. | |
| 5 | Ataques visando pedidos de dados de uso de energia. | |
| 6 | Ataques com o objetivo de roubar dados de servidores públicos. | SG |
| 7 | Ataques com o objetivo de assumir o controle de servidores utilitários. | |
| 8 | Ataques com o objetivo de derrubar servidores utilitários. | |
| 9 | Ataques contra equipamento de medição de área ampla. | |
| 10 | Ataques visando a resposta à demanda sinais no ESI/HAN | SH to SG |
| 11 | Ataques que ameaçando a comunicação de interrupções | |
| 12 | Ataques que ameaçam o DER relatórios de desligamento / isolamento | |
| 13 | Ataques contra o agregador NAN. | |
| 14 | Ataques visando sinais de resposta à demanda para o ESI/HAN | SG to SH |
| 15 | Ataques visando desligamento direto de carga sinais para o ESI / HAN | |
| 16 | Ataques visando Importação/Exportação de sinais de energia para o ESI/HAN | |
| 17 | Ataques visando dados relacionados ao cliente encaminhado para um terceiro ESP confiável | |

A Tabela 11 sintetiza os riscos de segurança para MLs discriminando as possíveis ameaças (conforme Tabela 2) para cada cenário descrito na Tabela 10, os objetivos de segurança comprometidos em casa situação (conforme Tabela 1) e seu nível de impacto (conforme Tabela 3) para cada cenário.

Tabela 11 - Riscos de Segurança para ML

| Mercado Local - Riscos de Segurança | | | |
|---|---|---|---|
| Cenários | Ameaças Possíveis | Objetivos de segurança Comprometidos | Nível de Impacto |
| 1 | 1,2,3,4,5 | 1,2,4 | B |
| 2 | 3,4,6 | | B |
| 3 | 7,8 | | B |
| 4 | 3,4,6,9,10 | | B |
| 5 | 1,3,9,11 | | B |
| 6 | 12,13,14,15,16 | 1,2,3,4,5 | M-A |
| 7 | 12,13,14,15,17,18,19,20 | | M-A |
| 8 | 1,2,3,10,19,20,23 | | A |
| 9 | 15,21 | | M-A |
| 10 | 3,6,10,19,23,24 | 2,4,5,6 | B |
| 11 | 19,25 | | B |
| 12 | 3,19,25 | | B |
| 13 | 1,3,21,22 | | B |
| 14 | 3,26,27,28 | 2,4 | B-M |
| 15 | 4,22,28,29 | | B |
| 16 | 3,4,22 | | M |
| 17 | 1,3 | | B-M |

Desta forma, visando elucidar a respeito de formas de ataques de maior impacto e consideradas factíveis desenvolveu-se o estudo apresentado nos cenários de estudo 1 e 2.

### 5.1.4. CENÁRIO DE ESTUDO 1

O cenário de estudo 1 tem como base ataques contra equipamentos de medição de área ampla (9 na Tabela 10). Tal ataque é considerado por este trabalho como de médio a alto impacto (Tabela 11), variando de acordo com a amplitude de área, ou seja, onde está localizado o medidor na topologia em questão.

Para realização de tal ataque o atacante deve considerar que o ponto de acesso de mais impacto para a rede está localizado no barramento 1, onde se localiza a subestação. Tal ponto recebe as informações referentes a todos os agentes integrantes da rede. Considerando que se pode discernir quanto ao caminho da informação que chega à subestação o agente atacante opta então por realizar alteração dos dados referentes ao maior número de GPs possível (grande percentual de consumo de energia elétrica). Sendo assim o ramo em destaque (Figura 7) passa a ter suas informações alteradas com a intenção de realizar uma alteração impactante nos dados de consumo.

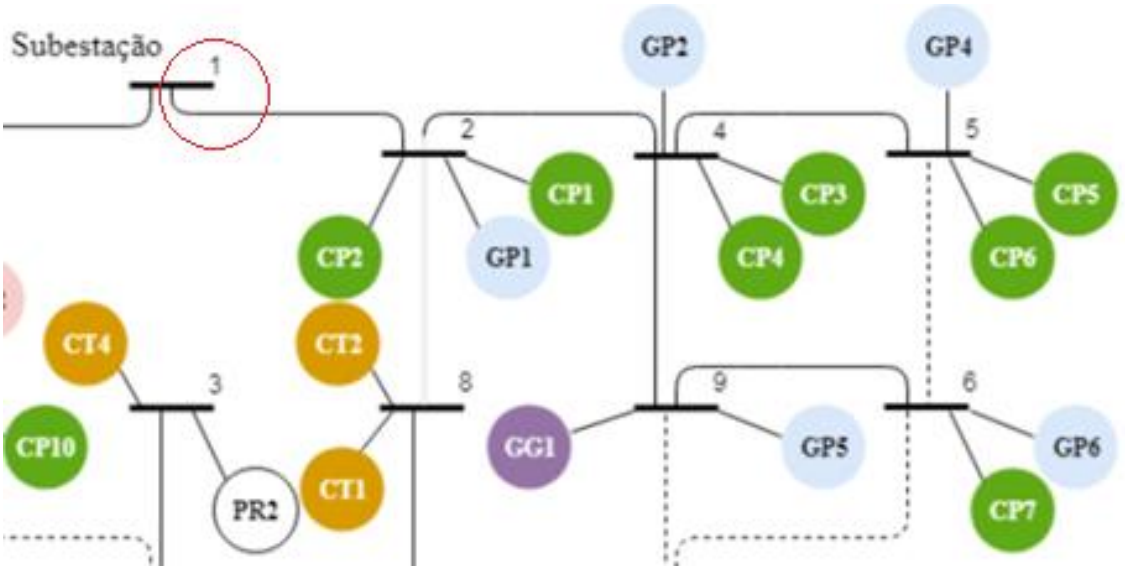



Figura 7 – Definição do Ponto de ataque, cenário 1

#### 5.1.4.1. POSSÍVEIS IMPACTOS PARA O CENÁRIO 1

Tendo em consideração a fixação de preços nos mercados de energia [89] o preço de compensação do mercado pode ser deslocado por um atacante alterando os dados de consumo para mais ou para menos. Um deslocamento da curva de geração não será considerado para tal ataque já que os agentes envolvidos não têm expressiva importância na energia gerada pelo mercado local.

##### 5.1.4.1.1. ATACANTE ALTERANDO OS DADOS DE CONSUMO PARA MAIS

Um atacante que deseje aumentar o preço de compensação do mercado através da alteração da curva de demanda, como proposto no cenário 1, estaria deslocando a curva de demanda agregada para cima (considerando um ataque a um consumidor de alto impacto) e desta forma deslocando também o preço para cima, conforme Figura 8 [89].

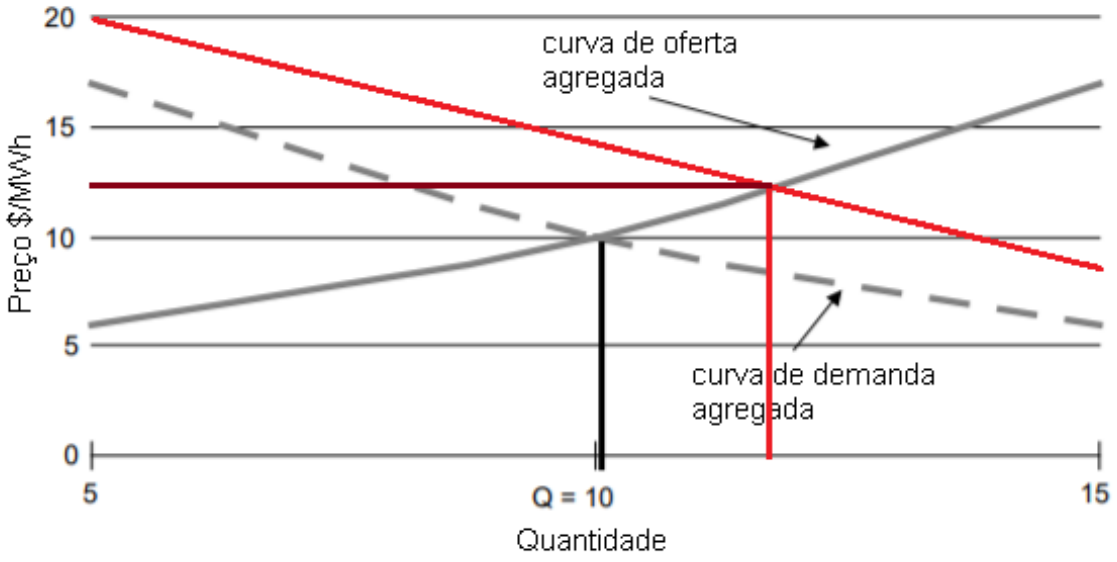
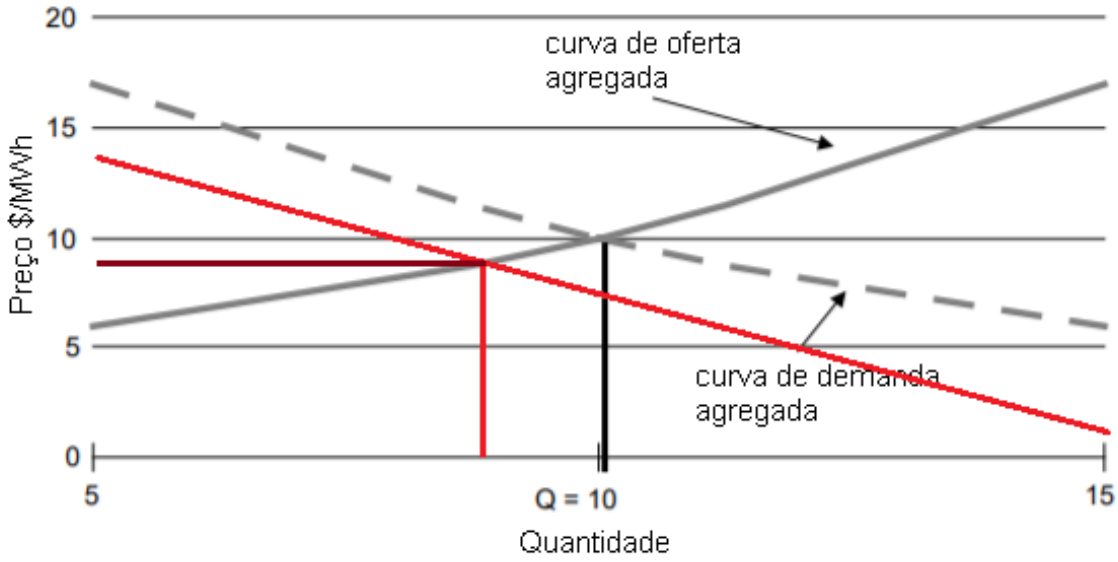



Figura 8 - Determinação do preço de compensação do mercado com curva de demanda deslocada para mais

Tal efeito teria também um impacto relacionado à quantidade de energia a ser despachada e traria um impacto de desvio não somente no preço da energia, bem como uma alteração na curva de oferta que não está sendo considerada de maneira a simplificar os resultados.

#### 5.1.4.1.2. ATACANTE ALTERANDO OS DADOS DE CONSUMO PARA MENOS

Um atacante que deseje diminuir o preço de compensação do mercado através da alteração da curva de demanda, como proposto no cenário 1, estaria deslocando a curva de demanda agregada para baixo (considerando um ataque a um consumidor de alto impacto) e desta




forma deslocando também o preço para baixo, conforme Figura 9 [89].

Figura 9 - Determinação do preço de compensação do mercado com curva de demanda deslocada para menos

Tal efeito teria também um impacto relacionado a quantidade de energia a ser despachada e traria um impacto de desvio não somente no preço da energia, bem como uma alteração na curva de oferta que não está sendo considerada de maneira a simplificar os resultados.

### 5.1.5. CENÁRIO DE ESTUDO 2

O cenário de estudo 2 terá como base ataques contra monitoramento doméstico remoto e controle (4 na Tabela 10). Tal ataque é considerado de baixo impacto (Tabela 11) quando se analisa o macro, porém será analisado para verificação do que aconteceria se um sensor em uma SH fosse invadido.

Para realização de tal ataque, onde não necessariamente o atacante precisa ter tanta informação referente à rede em comparação ao cenário 1, o atacante visa interferir nos dados de medição de determinado sensor que realiza alguma leitura em um determinado equipamento de uma SH. Para tal análise será considerado a alteração nos dados referentes

aos agentes PR. Tais agentes têm em seu suprimento energético uma importância ainda mais elevada, uma vez que são serviços de extrema importância para a sociedade como um todo.

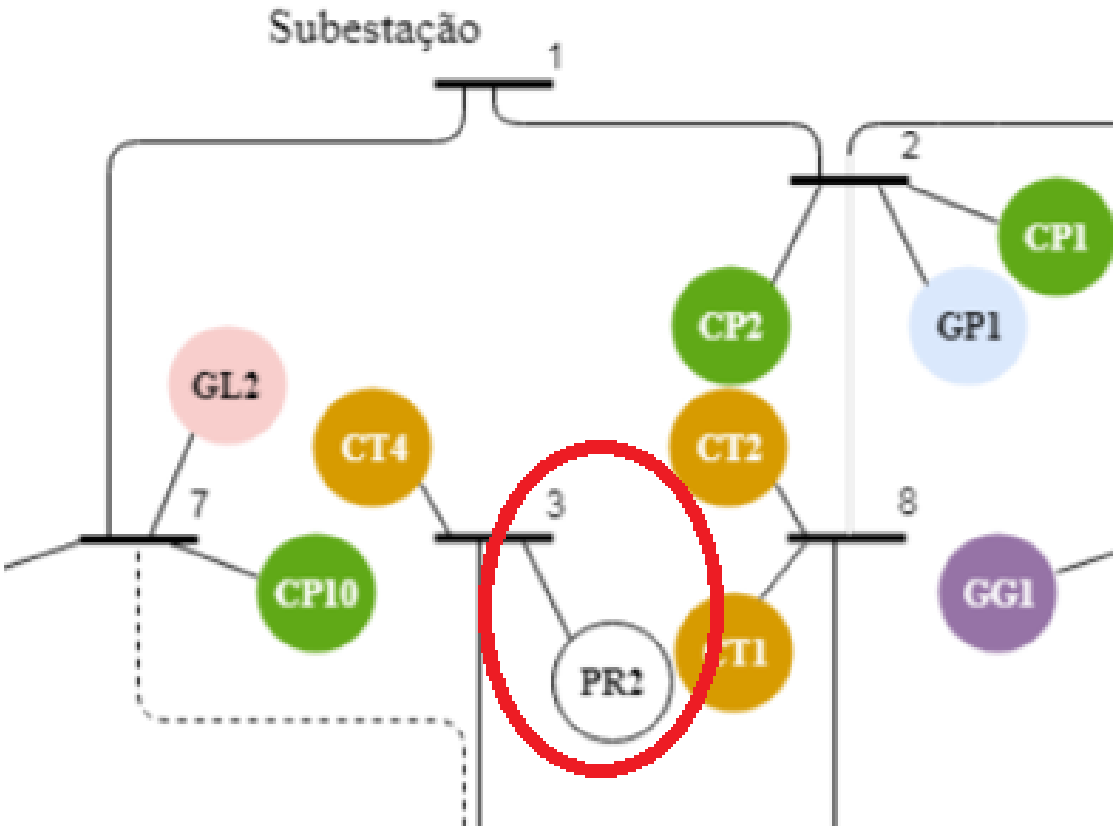



Figura 10- Definição do Ponto de ataque, cenário 2

#### 5.1.5.1. POSSÍVEIS IMPACTOS PARA O CENÁRIO 2

Considerando que para o cenário 2 a alteração dos dados de medição de temperatura do sensor central do agente PR2 (Figura 10) não traria grandes impactos de deslocamento na curva de demanda energética para o cálculo de preço de compensação do mercado, os impactos correlacionados a tal ataque podem trazer outros riscos. Uma vez que a realização deste ataque se dá em um ambiente crítico, onde pessoas estão em condições de saúde não ideais e a propagação de doenças é facilitada, a alteração nos dados de sensoriamento pode trazer riscos que vão além do econômico, mas sim a vida humana.

O calor é largamente utilizado no ambiente hospitalar, nas operações de limpeza, desinfeção e esterilização dos artigos e áreas hospitalares. Também, no preparo de alimentação pelos Serviços de Nutrição e Dietética (SND) e nos laboratórios de análise clínica no preparo de soluções especiais. Há, ainda, o uso do calor para geração de condições de conforto ambiental, principalmente em regiões de clima frio [90]. Um erro de leitura de um sensor de temperatura em um ambiente cirúrgico por exemplo pode levar a complicações durante o procedimento e até eventual perda do paciente.

## 5.2. MODELO 2

O modelo 2 adotado para embasar o segundo estudo de caso proposto é fundamentada a partir de bases de dados reais (disponibilizados pelo GECAD) referentes a 13 agentes de mercados locais, constituídos por 10 consumidores e 3 produtores. De forma resumida, a caraterização do mercado local é apresentada na Tabela 12.

Tabela 12 - Agentes componentes do mercado local - Modelo 2

| | Name | Start | End | Days | Days for negotiation | min bid €/MWh | max bid €/MWh |
|---|---|---|---|---|---|---|---|
| Consumption | Private Home 1 | 03/06/2011 | 18/06/2011 | 16 | 7 | 34 | 46 |
| | Private Home 2 | 16/07/2012 | 26/07/2012 | 11 | 7 | 34 | 46 |
| | Private Home 3 | 23/01/2013 | 07/02/2013 | 16 | 7 | 36 | 48 |
| | Private Home 4 | 06/01/2014 | 30/01/2014 | 25 | 7 | 36 | 48 |
| | Private Home 5 | 04/08/2011 | 18/08/2011 | 15 | 7 | 38 | 48 |
| | Private Home 6 | 25/12/2011 | 15/03/2013 | 447 | 7 | 38 | 48 |
| | Private Home 7 | 26/09/2011 | 03/10/2011 | 8 | 7 | 38 | 50 |
| | Private Home 8 | 01/06/2012 | 15/06/2012 | 15 | 7 | 38 | 50 |
| | Private Home 9 | 29/12/2012 | 12/01/2013 | 15 | 7 | 40 | 50 |
| | Private Home 10 | 01/06/2012 | 30/06/2012 | 30 | 7 | 40 | 50 |
| Generation | Generator 1 | 01/01/2011 | 15/12/2011 | 349 | 7 | 40 | 52 |
| | Generator 2 | 01/06/2014 | 10/06/2014 | 10 | 7 | 42 | 52 |
| | Generator 3 | 01/12/2013 | 10/12/2013 | 10 | 7 | 40 | 52 |

Nota-se que a quantidade de dados referente a cada agente é diferente, e desta maneira decidiu-se realizar simulação referente a um horizonte de uma semana. Para efeitos de simulação e cálculo foi utilizada uma ferramenta (script) desenvolvido a partir de uma simplificação, considerando somente a parte econômica, do simulador MASCEM [1].

### 5.2.1. DEFINIÇÃO DOS CENÁRIOS DE ESTUDO – MODELO 2

Tendo como partida os valores de referência do Modelo 2 e considerando os tipos de ataque previamente estudados, foram definidos para efeito de simulação alguns cenários de ataque observando que ocorre a convergência do preço de compensação do mercado local ao preço sugerido por um dos geradores e fazendo assim uma análise de qual dos geradores estaria a impor o preço. Através da observação dos dados obtidos a partir da simulação do caso base, conforme a Figura 11 (variação do preço de energia elétrica ao longo do tempo ), foi possível estabelecer que o **Gerador 2** foi o que teve seu preço elencado a preço de compensação mais vezes (97 vezes), seguido pelo Gerador 1 (52 vezes) e em seguida pelo Gerador 3 (19 vezes).

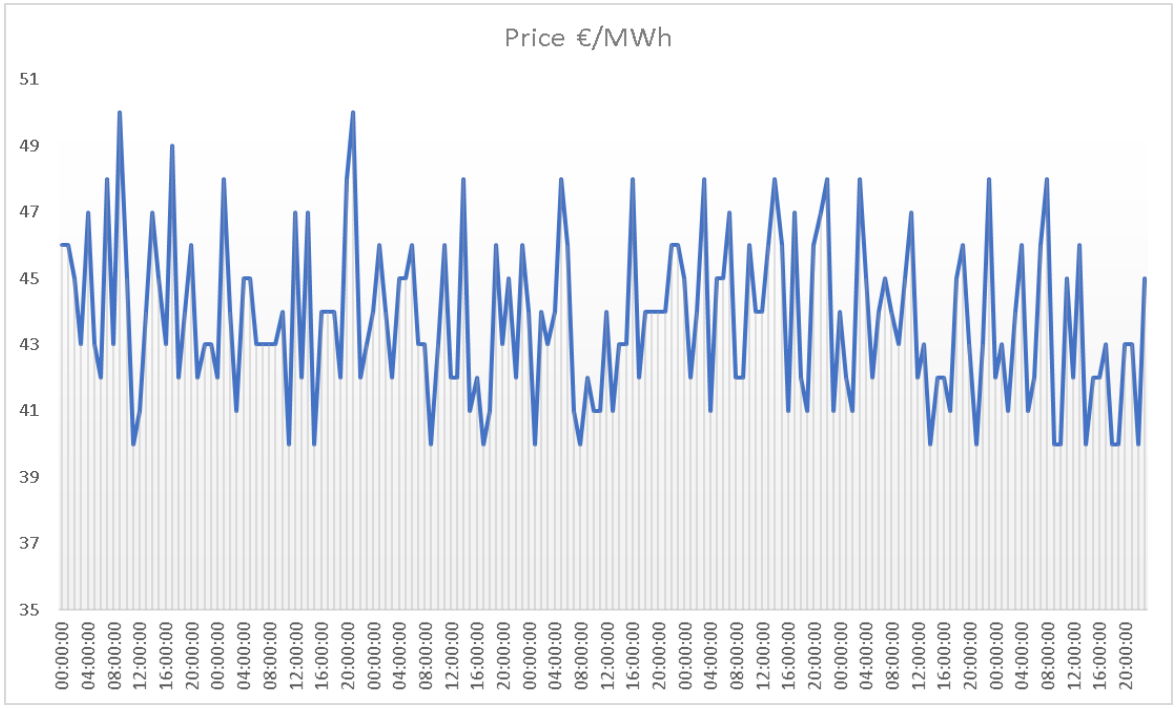



Figura 11 - Curva de Preço de compensação Caso Base

### 5.2.2. CENÁRIO DE ESTUDO 3

Após a identificação do agente mais preponderante na imposição do preço de compensação deste mercado local, para este horizonte temporal (Gerador 2), foi possível estabelecer o cenário de ataque número 3.

Para este cenário foi considerado um ataque de alteração dos dados (aumento da sugestão de preço do Gerador 2) de venda de eletricidade em 3 €/MWh. Os dados oriundos da simulação estão apresentados na Figura 12.

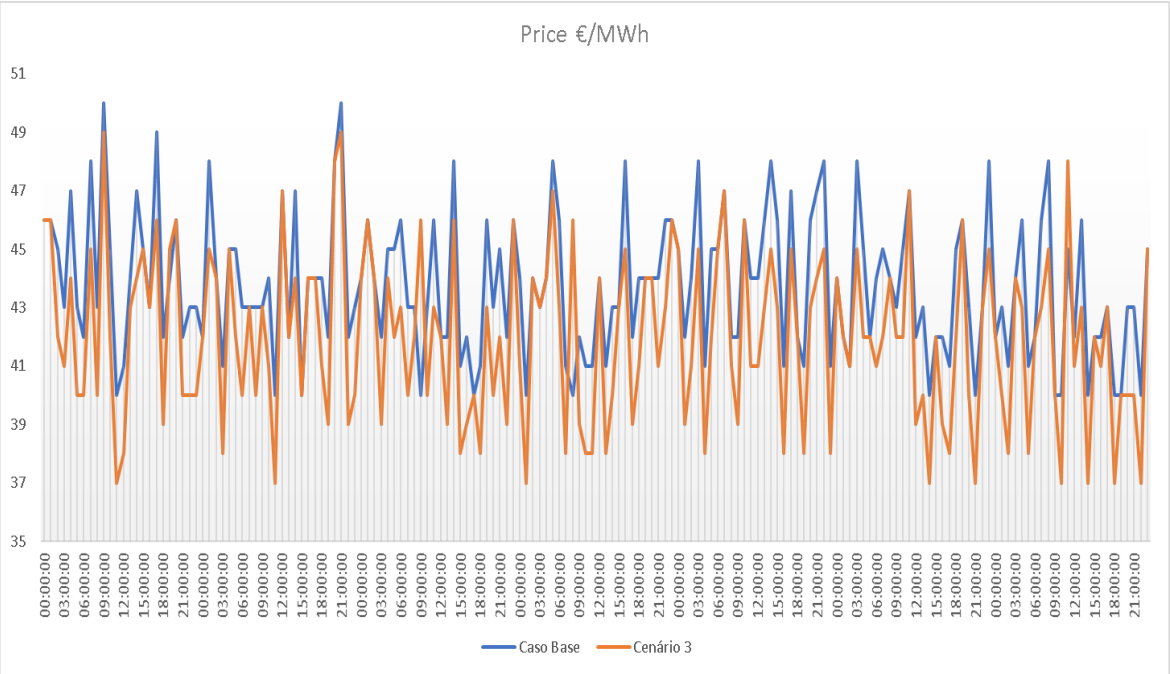



Figura 12 - Curva de Preço de compensação Caso Base x Cenário 3

#### 5.2.2.1. IMPACTOS PARA O CENÁRIO 3

Para os valores simulados, em comparação ao Caso Base no qual o preço médio do MWh para o período foi de 43,73 €, houve uma diminuição de 4,02%. Desta forma o valor médio do MWh para o período foi de aproximadamente 41,97 €. Assim, o impacto deste possível ataque foi a alteração do valor final de mercado para cada hora (diminuição relativa do seu valor), conforme ilustrado na Figura 12.

### 5.2.3. CENÁRIO DE ESTUDO 4

A partir daquilo que foi verificado no cenário 3, partindo para uma modificação do gerador classificado como segundo maior impositor do preço de compensação no período de referência, foi considerado um ataque de alteração aumento da sugestão de preço do Gerador 1 em 3 €/MWh. Os dados oriundos da simulação estão apresentados no Figura 13.

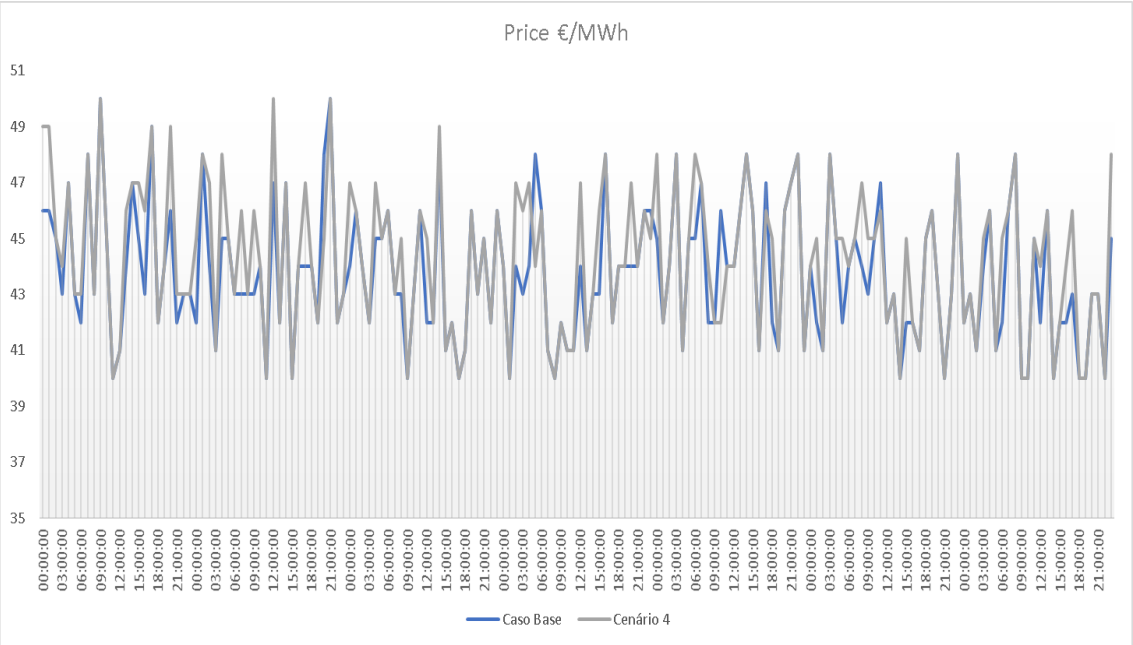



Figura 13 - Curva de Preço de compensação Caso Base x Cenário 4

#### 5.2.3.1. IMPACTOS PARA O CENÁRIO 4

Para os valores simulados, em comparação ao Caso Base no qual o preço médio do MWh para o período foi de 43,73 €, houve um aumento de 1,28%. Desta forma o valor médio do MWh para o período foi de aproximadamente 44,29 €. Deste modo, o impacto deste ataque foi o do aumento (embora residual) do valor final do preço de mercado. Este impacto não se observou tão evidente quanto o anterior (Figura 13), dado que o agente tem menos influência no fechamento do valor de preço final de mercado.

### 5.2.4. CENÁRIO DE ESTUDO 5

A partir daquilo que foi verificado no cenário 4, partindo para uma modificação do gerador classificado como menor impositor do preço compensação no período de referência, foi considerado um ataque de alteração aumento da sugestão de preço do Gerador 1 em 3 €/MWh. Os dados oriundos da simulação estão apresentados no Figura 14.

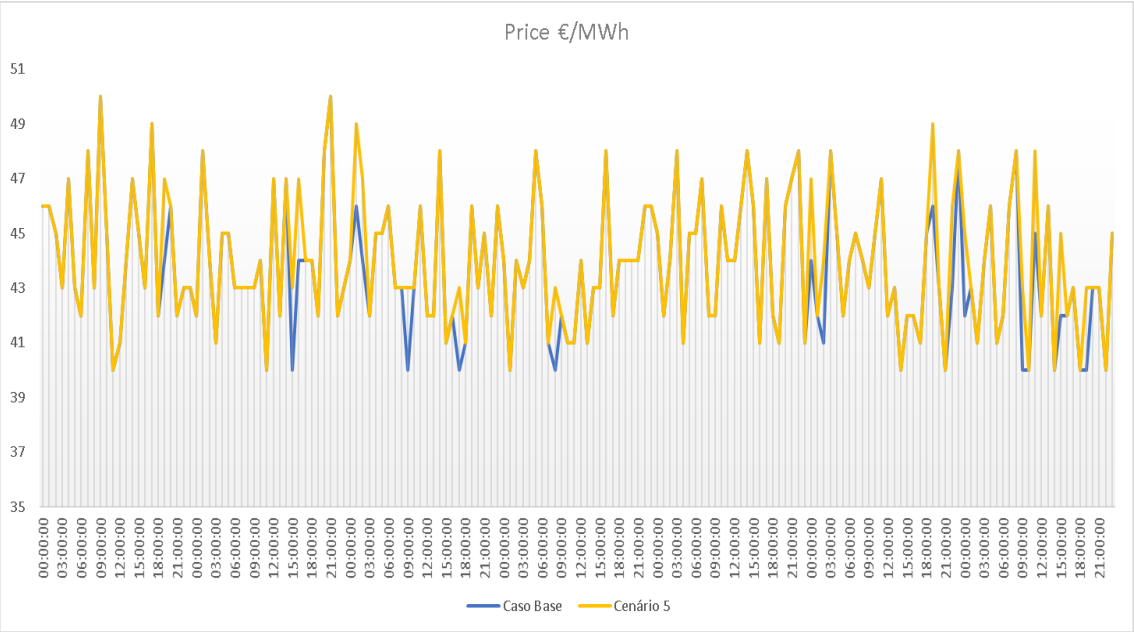



Figura 14 - Curva de Preço de compensação Caso Base x Cenário 5

#### 5.2.4.1. IMPACTOS PARA O CENÁRIO 5

Para os valores simulados, em comparação ao Caso Base no qual o preço médio do MWh para o período foi de 43,73 €, houve um aumento de 0,69%. Desta forma o valor médio do MWh para o período foi de aproximadamente 44,03 €. À semelhança do cenário de estudo 4, o impacto deste ataque foi o da variação do valor do preço de mercado (Figura 14), embora uma variação menos significativa que o cenário 3, aquando do ataque ao gerador mais influente no preço de mercado.

## 5.3. ANÁLISE FINAL DOS MODELOS E CENÁRIOS APRESENTADOS

No âmbito do Modelo 1, e considerando seus dois cenários de ataque propostos, pode-se concluir que ataques bem-sucedidos de *hackers* mal-intencionados em agentes de um ML podem não somente ter impactos econômicos e elétricos, bem como trazer riscos a vida humana. Destaca-se também a importância da garantia dos objetivos de segurança nas redes de dados dos Mercados Locais.

No âmbito do Modelo 2, e considerando seus três cenários de ataque propostos, pode-se concluir que o gerador com maior influência na determinação do preço de compensação, como alvo do ataque, ocasionou uma maior variação da curva de preço e, consequentemente, do preço médio pago por cada unidade de MWh durante o período em análise.

# 6. CONCLUSÕES GERAIS E PERSPETIVAS FUTURAS

A título de fechamento do trabalho, são apresentadas as conclusões obtidas a partir do estudo realizado. Para complementar o encerramento, são apresentadas sugestões para trabalhos futuros que estão relacionados com os temas discutidos.

## 6.1. CONCLUSÕES

A presente dissertação evidenciou temas que, ao serem alinhados, geram importantes análises para a evolução de mercados de energia elétrica em todo o mundo. Os objetivos da presente dissertação foram:

- Revisar o estado da arte sobre a organização de mercados de energia elétrica;
- Revisar o estado da arte sobre a organização de mercados locais de energia elétrica;
- Analisar estruturas de mercados locais de energia elétrica e a aplicação de modelos de negócios;
- Analisar os riscos e critérios de segurança que redes de mercados locais devem atender;

- Analisar, a partir de bibliografias e simulações realizadas com base em dados reais, os impactos de ataques cibernéticos a redes de mercados locais de eletricidade.

Os mercados de energia elétrica evoluíram a partir de uma estrutura de monopólios fortemente afetada pela variação dos preços de combustíveis utilizados na geração térmica de eletricidade. Com o advento e a popularização da inserção de fontes renováveis nos sistemas elétricos ao redor do mundo, houve uma drástica alteração neste cenário. Surge então a ideia de Mercado Local, uma maneira de reduzir perdas e adequar-se a padrões de consumo mais sustentáveis.

Do estudo dos Mercados Locais de energia, concluiu-se que tais organizações impulsionam a produção distribuída de energia elétrica, de maneira a resultar na redução de perdas associadas ao fluxo de potência da rede elétrica, além de tornar consumidores parte ativa do setor elétrico e desenvolver o conhecimento da eletricidade em um âmbito geral, para todas as pessoas.

Adicionalmente, a implementação de mercados locais de eletricidade possibilita a participação ativa de consumidores, produtores, consumidores-produtores no próprio mercado que, de outra, e no que respeita aos modelos de mercados grossistas, não teriam qualquer possibilidade de atuação.

O estudo e desenvolvimento de modelos de negócios é uma importante ferramenta para que mercados locais sejam instaurados de forma prática em diferentes realidades. Através deste estudo foi possível evidenciar as condições básicas para disseminação de Mercados Locais ao redor do globo. Sendo assim, o objetivo relativo à análise de mercados locais de energia elétrica e a importância da definição de modelos de negócios, previsto neste trabalho, foi cumprido.

No âmbito da análise dos riscos e critérios de segurança relativos às redes de Mercados Locais, interligações entre consumidores e geradores, foram explicitadas as classificações de riscos e os impactos através de bibliografias especializadas. A elucidação quanto à importância e aos critérios de segurança a serem seguidos, além de medidas para garantir tais critérios também foram apresentados. Desta forma, tal objetivo também foi cumprido.

A modelagem a partir do caso de estudo, baseado na estruturação de um mercado local com características da cidade de Salamanca – Espanha, permitiram realizar uma análise,

através de recursos bibliográficos, de cenários de ataque aos quais este Mercado Local pode estar submetido. Utilizando-se de dados reais (o que confere casos de estudo realísticos) disponibilizados pelo GECAD foi possível delimitar um segundo modelo, o qual pode ser simulado através de algoritmos obtidos do simulador MASCEM, de onde foi possível realizar conclusões quantitativas em relação ao que poderia acontecer em caso de ataque cibernético a um agente de um mercado local de energia. Da observação dos resultados provenientes da simulação de *cyber*-ataques, concluiu-se que o impacto na formação do valor do preço de mercado é proporcional à importância (influência) que os agentes têm na formação do preço de mercado (no caso de estudo: Gerador 2). Assim, os agentes de mercado mais preponderantes devem ter uma preocupação acrescida na "*veracity*" dos seus dados transmitidos ao operador de mercado. Este objetivo proposto: análise do impacto de ataques cibernéticos a mercados locais de energia, foi, igualmente, cumprido.

Através dos argumentos apresentados, conclui-se que as análises relacionadas aos mercados locais de energia são importantes para a evolução das formas de comercialização de eletricidade

## 6.2. CONTRIBUTOS

Diante das conclusões apresentadas no Tópico 6.1., é importante evidenciar de forma efetiva os principais contributos do autor aquando da realização da presente dissertação. Assim, as principais contribuições no âmbito deste trabalho foram:

• Estudo de mercados locais de energia elétrica, tendo em vista que são organizações emergentes e, por isso, ainda em fase de iniciação. De notar que a bibliografia relacionada com este tópico é, ainda, diminuta, quando comparada com outro tipo de organização de mercados de eletricidade;

• Descrição de modelos de negócios específicos voltados para a implementação de mercados locais de energia;

• Classificação e agrupamento dos ricos e impactos de ataques cibernéticos a rede de mercados locais, bem como a descrição de metodologias de garantir os critérios de segurança descritos;

• Análise de um estudo de caso que, a partir de bibliografias e simulações, descrevendo possíveis impactos de ataques cibernéticos no preço de mercados locais de energia.

## 6.3. TRABALHOS FUTUROS

Pela crescente tendência da inserção e surgimento de novos mercados locais de energia pelo mundo se faz extremamente relevante que mais trabalhos relacionados a estes sejam desenvolvidos na literatura.

Desta forma, como sugestões para trabalhos futuros é pertinente:

• Simular mercados locais de energia considerando operações em tempo real sendo atacados ciberneticamente;

• Analisar a inserção de condições complexas para agentes inseridos no contexto de mercados locais de energia e simulados no simulador MASCEM;

• Utilizar outros simuladores de mercados de energia que tenham diferentes técnicas de análise para comparação do que foi obtido;

• Simular outras estruturas de mercado local submetidas a outros tipos de ataque.

# *Referências Bibliográficas*

[1] Praça, Isabel; Ramos, Carlos; Cordeiro, M.; “MASCEM: A Multi-Agent System that Simulates Competitive Electricity Markets”, IEEE Intelligent Systems, vol. 18, no. 6, pp. 54–60, 2003.

[2] M. A. Marconi e E. M. Lakatos, Fundamentos da Metodologia Científica, São Paulo: Atlas S.A., 2003

[3] R. A. G. Pimpão, "O processo de liberalização do mercado da energia elétrica: O caso português em perspetiva comparada", ISCTE – Instituto Universitário de Lisboa, 2013.

[4] P. L. Joskow, “Lessons Learned From Electricity Market Liberalization,” The Energy Journal, pp. 1-39, 2008.

[5] N. de Castro, R. Brandão, N. Hubner, G. Dantas e R. Rosental, “A Formação do preço da energia elétrica: Experiências internacionais e o modelo brasileiro,” GESEL-IEUFRJ, Rio de Janeiro, 2014.

[6] N. de Castro, R. Brandão, G. Dantas, P. Vardiero e P. Dorado, “Análise comparative internacional e desenhos de mercados atacadistas de energia,” GESEL-IE-UFRJ, Rio de Janeiro, 2017.

[7] A. S. da Silva, “Análise e simulação de mercados locais de energia elétrica,” Instituto Superior de Engenharia do Porto, 2019.

[8] S. Hunt e G. Shuttleworth, “Competition and choice in electricity,” Wiley, West Sussex, 1996.

[9] D. V. Rotaru "The UK electricity market evolution during the liberalizationprocess". CES Working Paper 2013.

[10] D. Ilic, P. G. Da Silva, S. Karnouskos e M. Griesemer, “An energy market for trading electricity in smart grid neighbourhoods,” Research gate, 2012

[11] S. Karnouskos, “Demand Side Management via Prosumer Interactions in a Smart City

Energy Marketplace," IEEE, pp. 1-7, 2011.

[12] M.J. Hannon, T.J.Foxon, W.F.Gale "The co-evolutionary relationship between Energy Service Companies and the UK energy system: Implications for a low-carbon transition". Energy Policy 2013

[13] M. Hamwi "A review of business models towards service-oriented electricity systems". ScienceDirect, 2017

[14] H. Overholm "Collectively created opportunities in emerging ecosystems: The case of solar service ventures". Technovation, 2015

[15] C. Zott, R. Amit,L. Massa "The business model: recent developments and future research". Journal of Management 2011;37:1019–1042.

[16] C. Baden-Fuller, M.S.Morgan "Business models as models". Long Range Planning 2010;

[17] H. Chesbrough ,R.S. Rosenbloom "The role of the business model in capturing value from innovation: evidence from Xerox Corporation's technology spin-off companies". Industrial and Corporate Change 2002;

[18] R.G. McGrath "Business models: a discovery driven approach". Long Range Planning 2010;43:247–261.

[19] A. Osterwalder "The business model ontology: A proposition in a design science approach". 2004.

[20] M.W. Johnson, J. Suskewicz "How to jump-start the clean economy". Harvard Business Review 2009.

[21] D.J. Teece "Business models, business strategy and innovation". Long Range Planning 2010; 43:172–94.

[22] A. Tukker "Eight types of product-service system: Eight ways for sustainability? Experiences from SUSPRONET". Business Strategy and the Environment, 2004.

[23] N.M.P. Bocken, S.W. Short, P.Rana, S. Evans "A literature and practice review to develop sustainable business model archetypes", Journal of Cleaner Production, 2014.

[24] M.J. Hannon, T.J.Foxon, W.F.Gale "Demand pull government policies to support Product-Service System activity: the case of Energy Service Companies (ESCOs) in the UK", JOURNAL OF CLEANER PRODUCTION, 2015.

[25] A. Plepys, E. Heiskanen, O. Mont "European policy approaches to promote servicizing", Journal of Cleaner Production, 2015.

[26] M. Provance, R.G. Donnelly, E.G. Carayannis "Institutional influences on business model choice by new ventures in the microgenerated energy industry", Energy Policy, 2011

[27] R. Sauter, J. Watson "Strategies for the deployment of microgeneration: Implications for social acceptance", Energy Policy, 2007

[28] S. Zhang "Innovative business models and financing mechanisms for distributed solar PV (DSPV) deployment in China", Energy Policy, 2016

[29] L. Strupeit, A. Palm "Overcoming barriers to renewable energy diffusion: business models for customer-sited solar photovoltaics in Japan, Germany and the United States", Journal of Cleaner Production, 2016

[30] J. Huijben, G.P.J. Verbong "Breakthrough without subsidies? PV business model experiments in the Netherlands", Energy Policy, 2013

[31] M. Behrangrad "A review of demand side management business models in the electricity market", Renewable and Sustainable Energy Reviews, 2015

[32] P. Nillesen, M. Pollitt "New Business Models for Utilities to Meet the Challenge of the Energy Transition" Future of Utilities-Utilities of the Future: How Technological Innovations in Distributed Energy Resources Will Reshape the Electric Power Sector, 2016

[33] M. Loock "Going beyond best technology and lowest price: on renewable energy investors' preference for service-driven business models", Energy Policy, 2012

[34] M.E. Wainstein, A.G. Bumpus "Business models as drivers of the low carbon power system transition: a multi-level perspective". Journal of Cleaner Production, 2016

[35] S. Hall, K. Roelich "Business model innovation in electricity supply markets: The role of complex value in the United Kingdom", Energy Policy, 2016

[36] M. Richter "Utilities' business models for renewable energy: A review", Renewable and Sustainable Energy Reviews, 2012;

[37] T. Helms "Asset transformation and the challenges to servitize a utility business model", Energy Policy, 2016

[38] E.L. Apajalahti, R. Lovio, E. Heiskanen "From demand side management (DSM) to energy efficiency services: A Finnish case study", Energy Policy, 2015

[39] B.E. Matusiak, K. Piotrowski, F. Melo "Energy management using the business model approach", 2015 12th International Conference on the European Energy Market (EEM), IEEE, 2015

[40] Weiller CM, Pollitt MG. Platform markets and energy services 2014.

[41] S. Pätäri, S. Annala, A. Jantunen, S. Viljainen, A. Sinkkonen "Enabling and hindering factors of diffusion of energy service companies in Finland—results of a Delphi study", Energy Efficiency, 2016

[42] Ö. Yildiz "Financing renewable energy infrastructures via financial citizen participation–The case of Germany", Renewable Energy, 2014

[43] S. Hatzl, S. Seebauer, E. Fleiß, A. Posch "Market-based vs. grassroots citizen participation initiatives in photovoltaics: A qualitative comparison of niche development", Futures, 2016

[44] B.P. Koirala, E. Koliou, J. Friege, R.A. Hakvoort, P.M. Herder "Energetic communities for community energy: A review of key issues and trends shaping integrated community energy systems", Renewable and Sustainable Energy Reviews, 2016

[45] D. M. Falcão "Smart grids e microredes: O futuro já é presente", COPPE/UFRJ,

[46] L. M. Camarinha-Matos "Collaborative smart grids – a survey on trends". Renew. Sustain. Energy Rev. 65, 283-294, 2016

[47] J. Gao, Y. Xiao, J. Liu, W. Liang, C.P. Chen “A survey of communication/networking in Smart Grids” Future Generation Computer System, 2012

[48] C. Clastres “Smart grids: Another step towards competition, energy security and climate change objectives”, Energy Policy, Volume 39, Issue 9 , 2011

[49] W. Wang, Y. Xu, M. Khanna, “A survey on the communication architectures in smart grid”, Department of Electrical and Computer Engineering, North Carolina State Universit, 2011

[50] S. Goel, S., Y. Hong, “Security Challenges in Smart Grid Implementation Smart Grid Security”, Springer, 2015

[51] I. Doh, J. Lim, K. Chae “Secure authentication for structured smart grid system”. Paper presented at the 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2015

[52] H. Lund, A. N. Andersen, P.A. Østergaard, B.V. Mathiesen, D. Connolly “From electricity smart grids to smart energy systems – a market operation based approach and understanding” Energy Volume 42, Issue 1 ,2012

[53] F. Gangale, J. Vasiljevska, C. F. Covrig, A. Mengolini, G. Fulli “Smart grid projects outlook 2017: facts, figures and trends in Europe”, JRC Science for Policy Report,European Commission, 2017

[54] J. Mendel “Smart Grid Cyber Security Challenges: Overview and Classification”, e-mentor, 2017

[55] U.S. Department of Commerce, National Institute of Standards and Technology (2010,January) NIST Special Publication 1108, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0

[56] Xu Li; Xiaohui Liang; Rongxing Lu; Xuemin Shen; Xiaodong Lin; Haojin Zhu, "Securing smart grid: cyber attacks, countermeasures, and challenges," Communications Magazine, IEEE , vol.50, no.8, August 2012,pp.38-45

[57] Young-Jin Kim; M. Thottan, V. Kolesnikov, L. Wonsuck, "A secure decentralized data-centric information infrastructure for smart grid," Communications Magazine, IEEE , vol.48, no.11, November 2010, pp.58-65

[58] Y. Zhang, L. Wang, W. Sun, R. C. Green II, and M. Alam, “Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids,” IEEE Transactions on Smart Grid, vol. 2, no. 4, Dec. 2011,pp. 796– 808,.

[59] ENISA (2012, June) Annex I. General Concepts and Dependencies with ICT of ENISA study ‘Smart Grid Security: Recommendations for Europe and Member States

[60] IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads," IEEE Std 2030-2011 , pp.1-126, Sept. 10, 2011

[61] OpenHAN Task Force of the Utility AMI Working Group, (2008,August), Utility AMI 2008 Home Area Network System Requirements Specification,Version 1.0 [Online]

[62] V. Aravinthan, V. Namboodiri, S. Sunku, W. Jewell, "Wireless AMI application and security for controlled home area networks," Power and Energy Society General Meeting, 2011 IEEE , pp.1-8, 24-29 July 2011

[63] M. Amin, “Toward self-healing infrastructure systems”, Computer 33 (8), 2000

[64] N. Komninos, E. Philippou, A. Pitsillides "Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures" IEEE Communications Surveys & Tutorials, 2014

[65] Computer Security Division Information Technology Laboratory National Institute of Standards and Technology (2004, February), Standards for Security Categorization of Federal Information and Information Systems, FIPS PUB 199, [Online]

[66] The Smart Grid Interoperability Panel – Cyber Security Working Group, Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security - All Volumes, September. 2010.

[67] I. Ghansah , (2009). Smart Grid Cyber Security Potential Threats, Vulnerabilities And Risks California Energy Commission, PIER EnergyRelated Environmental Research Program.CEC-500-2012-047.

[68] F.M. Cleveland, , "Cyber security issues for Advanced Metering Infrasttructure (AMI)," Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008

[69] J. Liu, Y. Xiao, S. Member, S. Li, W. Liang, and C. L. P. Chen, “Cyber Security and Privacy Issues in Smart Grids,” vol. 14, no. 4, 2012, pp. 981–997.

[70] Xantus Consulting International, (2009), White Paper for NIST CSWG: Cyber Security Requirements for Business Processes Involving Home Area Networks (HAN), [Online]

[71] Cyber-Physical Systems Security for Smart Grid Future Grid Initiative White Paper (2012,February), PSERC, [Online]

[72] J. Benoit, “An Introduction to Cryptography as Applied to the Smart Grid,” Cooper Power Systems, February 2011.

[73] “Cryptographic Key Management for the Advanced Metering Infrastructure.” [Online].

[74] M. Jawurek, F. Kerschbaum, and G. Danezis, “SoK?: Privacy

Technologies for Smart Grids – A Survey of Options .”

[75] C. Efthymiou, G. Kalogridis, , "Smart Grid Privacy via Anonymization of Smart Metering Data," Smart Grid Communications (SmartGridComm), pp.238,243, 4-6 Oct. 2010

[76] T. Jeske, "Privacy-preserving Smart Metering without a Trusted-thirdparty", in Proc. SECRYPT 2011, Seville, Spain, 18 - 21 July, 2011, pp.114-123.

[77] S. Bhattarai, G. Linqiang, and Y. Wei, “A novel architecture against false data injection attacks in smart grid,” in 2012 IEEE International Conference on Communications (ICC) ,10-15 June 2012

[78] Y. Huang, H. Li, K. A. Campbell, and H. Z, “Defending false data injection attack on smart grid network using adaptive CUSUM test,” 45th Annual Conference on Information Sciences and Systems. IEEE, 23-25 March 2011.

[79] M. A. Faisal, Z. Aung, J. R. Williams, and A. Sanchez, “Using Intrusion Detection System with Data Stream Mining” in Intelligence and Security Informatics Pacific Asia Workshop, PAISI 2012, Kuala Lumpur, Malaysia, May 29, 2012, ProceedingsSeries: Lecture Notes in Computer Science,vol.7299, pp. 96–111

[80] R. Berthier and W. H. Sandersm, “Specification-Based Intrusion Detection for Advanced Metering Infrastructures,” 2011 IEEE 17th Pacific Rim International Symposium on Dependable Computing, December 2011, pp. 184–193

[81] J. Benoit, “An Introduction to Cryptography as Applied to the Smart Grid,” Cooper Power Systems, February 2011.

[82] S. Ruj, , A. Nayak, , & I. Stojmenovic, “A security architecture for data aggregation and access control in smart grids”, 2011

[83] B. Vaidya, D. Makrakis, and H. T. Mouftah, “Device authentication mechanism for Smart Energy Home Area Networks,” 2011 IEEE International Conference on Consumer Electronics (ICCE).

[84] Z. Xiao, Y. Xiao, and D. H.-C. Du, “Non-repudiation in neighborhood area networks for smart grid,” Communications Magazine, IEEE, vol. 51, no. 1, pp. 18 – 26, 2013

[85] B. Canizes, T. Pinto, J. Soares, Z. Vale, P. Chamoso e D. Santos, “Smart City: A GECAD-BISITE Energy Management Case Study,” em Smart City: A GECADBISITE Energy Management Case Study, Porto, Springer Nature, 2018, p. 92–100.

[86] Maleitas e P. F. H, “Viabilidade Económica do Autoconsumo de Energia Fotovoltaica no Setor Não Residencial,” Faculdade Nova de Lisboa, Lisboa, 2015.

[87] R. C. Torres, “Energia solar fotovoltaica como fonte alternativa de geração de energia elétrica em edificações residenciais,” Universidade de São Paulo, São Carlos, 2012. 124

[88] C. A. A. Macedo, A. A. Albuquerque e H. F. Moralles, “Análise de viabilidade econômico-financeira de um projeto eólico com simulação Monte Carlo e avaliação de risco,” SciELO, São Carlos, 2017

[89] Morey, Mathew J (2001). “Power Market Auction Design: Rules and Lessons In Marketbased Control for the New Electricity Industry”

[90] ANVISA, “SEGURANÇA NO AMBIENTE HOSPITALAR” Disponível em: http://portal.anvisa.gov.br/documents/33852/271855/Seguran%C3%A7a+no+ambiente+hospitalar/473c5e32-025a-4dc2-ab2e-fb5905d7233a