Everaldo Alves da Costa

Automação da medição e segurança de dados em redes inteligentes: estudo da experiência brasileira

Dissertação de Mestrado

Dissertação apresentada como requisito parcial para obtenção do título de Mestre pelo Programa de Pós-Graduação em Metrologia (Área de concentração: Metrologia para Qualidade e Inovação) da PUC-Rio.

Orientador: Prof. Mauricio Nogueira Frota

Rio de Janeiro

Dezembro de 2012

Everaldo Alves da Costa

Automação da medição e segurança de dados em redes inteligentes: estudo da experiência brasileira

Dissertação apresentada como requisito parcial para obtenção do título de Mestre pelo Programa de Pós-Graduação em Metrologia (Área de concentração: Metrologia para Qualidade e Inovação) da PUC-Rio. Aprovada pela Comissão Examinadora abaixo assinada.

Prof. Mauricio Nogueira Frota
Orientador
Programa de Pós-Graduação em Metrologia - PUC-Rio

Prof. Reinaldo Souza Castro
Programa de Pós-Graduação em Metrologia - PUC-Rio

Profa. Elisabeth Costa Monteiro
Programa de Pós-Graduação em Metrologia - PUC-Rio

Jose Eugênio Leal
Coordenador(a) Setorial do Centro Técnico Científico - PUC-Rio

Rio de Janeiro, 27 de dezembro de 2012

Everaldo Alves da Costa

Formado em tecnologia da informação e pós-graduado pela UFRJ em gestão do conhecimento e inteligência empresarial. Há mais de sete anos no setor elétrico, como gestor de projetos inovadores para as áreas de planejamento de mercado, comercialização de energia e garantia de receita (recuperação de perdas comerciais e combate à inadimplência).

Ficha Catalográfica

Costa, Everaldo Alves da

Automação da medição e segurança de dados em redes inteligentes: estudo da experiência brasileira / Everaldo Alves da Costa; Orientador: Mauricio Nogueira Frota. - 2012.

131 f.: il. (color); 30 cm

Dissertação (mestrado) – Pontifícia Universidade Católica do Rio de Janeiro, Programa de Pós-Graduação em Metrologia para a Qualidade e Inovação, 2012. Inclui bibliografia e anexos.

1. Metrologia – Teses. 2. Metrologia. 3. Setor elétrico. 4. Medição inteligente. 5. Redes inteligentes. 6. Cyber segurança. 7. Norma. 8. Regulação. I. Frota, Mauricio Nogueira. II. Pontifícia Universidade Católica do Rio de Janeiro. Programa de Pós-Graduação em Metrologia para a Qualidade e Inovação. III. Título.

CDD: 389.1

Dedico este trabalho a meus pais que sempre
apoiaram minhas aventuras em busca da felicidade.
A Vinícius, meu sobrinho, um propagador incansável
da alegria de viver.

Agradecimentos

Finalizada mais uma etapa importante da minha vida, gostaria de agradecer a todos aqueles que sempre me apoiam, independente da caminhada, e contribuíram para a realização deste trabalho.

A Deus, em primeiro lugar, por me permitir viver tantos desafios como este e por me suportar nos momentos cinzentos da vida.

Ao professor Maurício Frota, o meu maior agradecimento pela incrível disponibilidade, pelo apoio incondicional e compreensão que sempre manifestou. Muito obrigado pela orientação efetiva e resolutiva.

A PUC-Rio por proporcionar-me condição única de avanço no campo do saber e por conceder-me isenção de grande parte dos investimentos necessários para obtenção do grau de mestre em uma instituição tão respeitada.

A Choice Technologies que me permitiu agarrar esta oportunidade, proporcionando-me crescimento profissional.

Aos entrevistados que, gentilmente, cederam tempo para as entrevistas em detrimento de suas atividades de trabalho. Em especial Luiz Renato, Cemig, que além de validar o instrumento de coleta de dados, contribuiu com o envio de textos pertinentes ao tema pesquisado.

A Elaine, pessoa incrível, que foi fundamental na conquista deste resultado. Mais do que isso, uma pessoa que admiro e respeito muito.

A Verônica e Anselmo pelo acolhimento na fase mais importante desta pesquisa.

Ao amigo André Nepomuceno que sempre teve parte neste processo contínuo de crescimento.

Por último, mas não menos importante, agradeço aos meus amigos, colegas de curso e a todos os professores que comigo partilharam do seu saber.

Resumo

Costa, Everaldo Alves; Frota, Mauricio Nogueira. **Automação da medição e segurança de dados em redes inteligentes: estudo da experiência brasileira.** Rio de Janeiro, 2012. 131p. Dissertação de Mestrado – Programa de Pós-Graduação em Metrologia (Área de concentração: Metrologia para Qualidade e Inovação), Pontifícia Universidade Católica do Rio de Janeiro.

Indutoras de inovação, as redes inteligentes de energia (*smart grid*) têm promovido mudanças significativas nos processos de fornecimento e controle de energia elétrica. Diante das oportunidades e desafios de incorporação da tecnologia de *smart grid* em suas práticas operacionais, as concessionárias de energia elétrica ficam expostas a novos riscos de segurança relacionados às suas necessidades de comunicação, automação de sistemas, introdução de novas tecnologias e tratamento de dados. O presente trabalho tem por **objetivo** mostrar que tais riscos podem ser minimizados pela adoção de recomendações normativas específicas. Objetiva, também, analisar parâmetros relacionados à segurança da informação na implantação da infraestrutura de medição inteligente no *smart grid*, assim contribuindo para a reflexão e produção de conhecimento na área. A experiência brasileira foi identificada a partir de uma pesquisa realizada junto a concessionárias inovadoras de energia elétrica que, tendo percebido a importância estratégica de adoção da tecnologia de redes inteligentes, já adotaram medidas estratégicas para a sua implantação. A pesquisa desenvolveu-se no **contexto** de cinco grandes vertentes de análise: contexto geral, segurança e vulnerabilidade da informação, impactos e aderência às normas aplicáveis. No Brasil, a **motivação** para o uso das redes inteligentes volta-se à confiabilidade do sistema elétrico nacional e ao combate às perdas não técnicas, refletindo compromisso com a melhoria da qualidade do serviço prestado ao consumidor final. Dentre os **resultados** do trabalho destacam o recenseamento da legislação aplicável e, à luz de iniciativas bem sucedidas de outros países em *smart grid*, o diagnóstico da experiência brasileira. Como **conclusão**, o trabalho (i) produz evidências de que as redes inteligentes contribuem para a redução de custos operacionais e perdas não técnicas e (ii) sinaliza para a necessidade de se intensificar a pesquisa sobre redes inteligentes como alternativa eficaz de superação da vulnerabilidade de acesso à informação imposta pelos medidores eletrônicos.

Palavras-chave

Metrologia; setor elétrico; medição inteligente; redes inteligentes; cyber segurança; norma; regulação.

Abstract

Costa, Everaldo Alves; Frota, Mauricio Nogueira (Advisor). **Automation of measurement and data safety in smart grid: study of the Brazilian experience.** Rio de Janeiro, 2012. 131p. MSc. Dissertation Programa de Pós Graduação em Metrologia (Área de concentração: Metrologia para Qualidade e Inovação), Pontifícia Universidade Católica do Rio de Janeiro.

Inducing innovation, the smart grids have promoted significant changes in electrical energy's supply and control processes. Given the opportunities and challenges for incorporating smart grid technology in their operating practices, the electrical utilities are exposed to new security risks related to their needs of communication, systems automation, new technologies introduction and data processing. This paper aims to show that these risks can be minimized by the adoption of specific policy recommendations. Also aims in analyzing parameters related to information security on the deployment of smart metering infrastructure on smart grids, this way contributing on reflection and knowledge production in the area. The Brazilian experience was idenified from a survey of innovative electrical utilities that, having realized the strategic importance of adoption of smart grid technology, were early adopters of strategic measures for its implementation. The research was developed in the context of five main pillars of analysis: general context, security and information vulnerability, impacts and adherence to applied standards. In Brazil, the motivation for the use of smart grids back to the national electrical system reliability and mitigation of non-technical losses, reflecting commitment to improve quality of service provided to the end consumer. Among the results of the survey it is highlighted the revision of legislation and, considering successful smart grid initiatives in other countries, the diagnosis of the Brazilian experience. In conclusion, the work (i) produces evidence that smart grids help reduce operating costs and non-technical losses and (ii) indicates the need to intensify research on smart grids as an effective alternative to overcome the vulnerability of access to information imposed by electronic meters.

Keywords

Metrology; electric sector; smart measurement; smart grid; cyber security; standard; regulation.

“Não importa o que fizeram de mim, o que importa é o que eu faço com o que fizeram de mim”.

Jean-Paul Sartre.

Sumário

1 **Introdução** **16**

1.1. Definição do problema de pesquisa 18

1.2. Objetivos: geral e específicos 19

1.2.1. Objetivo geral 19

1.2.2. Objetivos específicos 19

1.3. Motivação 19

1.4. Metodologia 20

1.5. Estrutura da dissertação 22

2 Redes inteligentes (*smart grid*) **24**

2.1. Conceitos e definições 24

2.1.1. Medição eletrônica 28

2.1.2. Comunicação 30

2.1.3. Sensoriamento e automação 32

2.1.4. Computação 32

2.2. *Smart grid e* o problema da segurança da informação 33

2.3. O custo do cybercrime no Brasil 34

2.4. Segurança da informação 36

2.5. Potenciais riscos e ameaças de ataques cibernéticos 37

2.6. AMI (*Advanced Metering Infrastructure*) - Vulnerabilidades 39

3 Redes de energia elétrica: perspectiva para uma revolução no setor **40**

3.1. Redes inteligentes: experiências relevantes 40

3.2. Desenvolvimento e difusão da tecnologia em nível mundial 42

3.3. Redes inteligentes: o novo paradigma brasileiro do setor 44

3.3.1. Desafios e oportunidades para o Brasil 45

3.3.2. Difusão de uso do *smart grid* no Brasil: principais iniciativas 48

3.4. Uma tecnologia para combate a perdas não técnicas 50

3.5. Desafios regulatórios à implantação de redes inteligentes no País 51

4 O papel das normas nas redes inteligentes **55**

4.1. Normalização 55

4.2. Sistema Brasileiro de Normalização 58

4.3. Normalização internacional 60

4.4. O esforço de normalização voltado para o *smart grid* 62

4.4.1. IEC *Smart grid* SG3 62
4.4.2. A experiência do NIST no *smart grid* 64
4.4.3. Normas globais de segurança cibernética para o *smart grid* 66
4.5. Normas aplicáveis à segurança da informação 70
4.6. Regulamentação brasileira aplicável à medição inteligente 71

5 Segurança da informação nas redes inteligentes de energia elétrica: estudo de caso de concessionárias no Brasil 72
5.1. Desenho da pesquisa 74
5.2. Tipo de estudo de caso e unidade de análise 75
5.2.1. Definição do tipo de estudo de caso 75
5.2.2. Unidade de Análise 76
5.3. Elaboração do instrumento de coleta de dados 77
5.4. Coleta de dados 78
5.5. Tratamento e análise dos dados 78
5.6. Resultados e discussão 79
5.6.1. Contexto geral 79
5.6.2. Segurança da informação 82
5.6.3. Vulnerabilidades 85
5.6.4. Impactos 88
5.6.5. Normas 90

6 Conclusões e recomendações 93
6.1. Sobre os objetivos 93
6.2. Sobre os resultados 94
6.3. Sobre os limites e limitações 95
6.4. Recomendações 96

7 Referências Bibliográficas 98

8 Apêndice A – Instrumento de coleta de dados 103

9 Anexos 107
9.1. Anexo I – Resultados da Audiência Pública nº 43/2010 107
9.2. Anexo II – Resolução normativa nº 502 128

Lista de quadros

Quadro 3.1 - Comparação da rede elétrica atual com as redes inteligentes. 26
Quadro 3.2 - Medição eletrônica 29
Quadro 2.1 - Principais iniciativas de implantação de redes inteligentes no mundo. 43
Quadro 2.2 - Relação de empresas e seus respectivos projetos de redes inteligentes. 49
Quadro 2.3 - Principais eventos para definição dos requisitos mínimos dos medidores inteligentes. 53
Quadro 4.1 – Principais razões para se utilizar normas 56
Quadro 4.2 - Descrição das instituições do Sistema Brasileiro de Normalização 59
Quadro 4.3 – Normas aplicáveis às redes inteligentes 63
Quadro 4.4 - Acervo normativo aplicável ao smart grid 67

Lista de figuras

Figura 1.1 - Desenho da pesquisa, seus componentes e métodos. 21
Figura 3.1 - O conceito *smart grid* 26
Figura 3.2 - Tecnologias viabilizadoras das redes inteligentes 27
Figura 3.3 - Aplicações de medição eletrônica. 29
Figura 3.4 - Principais tipos de crimes econômicos informados. 35
Figura 2.1 - Projetos de *smart grid* no mundo (2012). 41
Figura 2.2 - principais países investidores em tecnologias de *smart grid*. 42
Figura 2.3 - Temas de P&D de projetos *Smart grid* (em %). 48
Figura 2.4 - Perdas técnicas e não-técnicas por região. 50
Figura 4.1 - Sistema Brasileiro de Normalização 59
Figura 4.2 - Processo de elaboração de uma norma internacional 61
Figura 4.3 - Estágio e prazos para elaboração de uma norma 61
Figura 5.1 – Tipo de estudo de caso 73
Figura 5.2 - Fluxograma do desenvolvimento do estudo de caso 75
Figura 5.3 - Objetivos esperados pela implantação das redes inteligentes 80
Figura 5.4 - Atividades realizadas para assegurar garantia da segurança da informação nas redes inteligentes 83
Figura 5.5 - Escala de propagação de um ataque as informações dos consumidores 88
Figura 5.6 – Nível de impacto 89

Lista de tabelas

Tabela 5.1 - Garantia da segurança da informação 81
Tabela 5.2 - Política de segurança 82
Tabela 5.3 - Qualificação dos processos e atividades 84
Tabela 5.4 - Questões investigativas sobre a vertente vulnerabilidade 86
Tabela 5.5 - Tempo de recuperação 88
Tabela 5.6 - Nível de recuperação 89
Tabela 5.7 - Normas adotadas e grau de importância 91

Lista de Siglas e Abreviaturas

ABDI	Agência Brasileira de Desenvolvimento Industrial
ABNT	Associação Brasileira de Normas e Técnicas
ABRADEE	Associação Brasileira de Distribuidores de Energia Elétrica
APTEL	Associação de Empresas Proprietárias de Infraestrutura e de Sistemas Privados de Telecomunicações.
AMI	Advanced Metering Infrastructure
AMN	Associação Mercosul de Normalização
AMM	Advanced Meter Management
AMR	Automated Meter Reading
ANEEL	Agência Nacional de Energia Elétrica
ANSI	American National Standards Institute
CCM	Centro de Controle de Medição
COBEI	Comitê Brasileiro de Eletricidade, Eletrônica, Iluminação e Telecomunicações
CEFET	Centro Federal de Educação Tecnológica Celso Suckow da Fonseca
CEN	Comitê Europeu de Normalização
CSWG	Cyber Security Working Group
CONMETRO	Conselho Nacional de Metrologia, Normalização e Qualidade Industrial
CNI	Confederação Nacional da Indústria
CNN	Comitê Nacional de Normalização
CNPQ	Conselho Nacional de Desenvolvimento Científico e Tecnológico
CPFL	Companhia Paulista de Força e Luz
COPANT	Comissão Pan-Americana de Normas Técnicas
CPqD	Centro de Pesquisa e Desenvolvimento em Telecomunicações
COPANT	Comissão Pan-americana de Normas Técnicas
DEC	Duração Equivalente de Continuidade
DIC	Duração de Interrupção Individual por Unidade Consumidora
DMIC	Duração Máxima de Interrupção Contínua por Unidade Consumidora
DMS	Distribution Management System
DSM	Demand-Side Management
EDF	Électricité de France
EISA	Energy Independence and Security
EPE	Empresa de Pesquisa Energética
ERDF	Électricité Réseau Distribution France

EUA	Estados Unidos da América
FEC	Frequência Equivalente de Continuidade
FERC	Federal Energy Regulatory Commission
FIC	Frequência de Interrupção Individual por Unidade Consumidora
IEC	International Electrotechnical Commission
IEDs	Intelligent Electronic Devices
IEEE	*Institute of Electrical and Electronic Engineers*
IFMT	Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
ISA	International Federation of the National Standardizing Associations
ISO	International Organization for Standardization
ITU	International Telecommunications Union
GPRS	*General Packet Radio Service*
GSM	Global System for Mobile Communications
MC	Ministério das Comunicações
MCTI	Ministério da Ciência, Tecnologia e Inovação
MDIC	Ministério do Desenvolvimento, Indústria e Comércio Exterior
MDM	Meter Data Management
MME	Ministério de Minas e Energia
NIST	National Institute of Standards and Technology
OCDE	Organisation for economic co-operation and development
OFGEM	Office of the Gas and Electricity Markets
ONS	Operador Nacional do Sistema Elétrico
PLC	Power Line Communications
PMU	Phasor Measurement Unit
PUC-Rio	Pontifícia Universidade Católica do Rio de Janeiro
SBN	Sistema Brasileiro de Normalização
SINMETRO	Sistema Nacional de Metrologia, Normalização e Qualidade Industrial
SG	Strategic Group
SGCC	State Grid Corporation of China
SGSI	Sistema de Gestão de Segurança da Informação
SI	Sistema da Informação
SMB	Standardization Manangement Board
SMS	Short Message Service
SRA	Sistema de Reposição Automática
SRD	Superintendência de Regulação dos Serviços de Distribuição

TI	Tecnologia da Informação
UFF	Universidade Federal Fluminense
UNSCC	United Nations Standards Coordinating Committee
USP	Universidade de São Paulo
UFJF	Universidade Federal de Juiz de Fora
UFRGS	Universidade Federal do Rio Grande do Sul
UFRJ	Universidade Federal do Rio de Janeiro
UNSCC	United Nations Standards Coordinating Committee
UMTS	Universal Mobile Telecommunication System

1
Introdução

As redes inteligentes de energia (*smart grid*) surgem no cenário mundial como uma tecnologia inovadora, trazendo mudanças significativas nos processos de fornecimento de energia elétrica (Zhang, 2010). As práticas adotadas para implantação da arquitetura dessas redes inteligentes e os resultados esperados são estratégicos e com potenciais benefícios para as diversas partes envolvidas. Dentre estas, as concessionárias de energia elétrica, os reguladores, os consumidores, o poder público, os fornecedores, as instituições de pesquisa, os agentes de desenvolvimento e os financiadores do setor elétrico.

Para a maioria dos especialistas, as redes inteligentes serão compostas por um conjunto de tecnologias que integra sensoriamento, telecomunicações e processamento de dados ao sistema elétrico.

Dentre os principais benefícios, espera-se que esta tecnologia seja responsável por:

- Introduzir significativos ganhos de eficiência energética;
- Permitir automação e operação remota do sistema;
- Melhorar a fiscalização e monitoramento das condições de rede e qualidade de energia;
- Incrementar a capacidade de tomada de decisões nas empresas do setor;
- Viabilizar tecnicamente a o consumo programado, inteligente, de energia, dentre outros.

No contexto da abordagem técnica, uma das propostas das redes inteligentes é agregar inteligência digital ao setor elétrico. Essa transformação do setor vem se consolidando a partir de três pilares:

i. **o sensoriamento** — tecnologicamente representado pelos medidores eletrônicos (*smart meters*) — com a função de captar as informações de rede;
ii. **as telecomunicações**, com a função de transmitir as informações de rede. Estas se consolidam ou a partir de tecnologias que usam a própria rede elétrica para a transmissão de dados (*Power Line Communications*) ou a partir de tecnologias de transmissão de dados que atuam desvencilhadas da rede de energia elétrica (exemplo: GSM, GPRS, UMTS, SMS); e

iii. **o processamento**, com a função de “interpretar” as informações em trânsito, tomar decisões de forma independente etc.

Para que o conceito de redes inteligentes de energia elétrica seja consolidado no Brasil, diversos aspectos devem ser discutidos e avaliados. De acordo com Clements (2010), dentre os vários desafios que emergem destacam-se:

i. A compatibilização das funcionalidades requeridas;
ii. A interoperabilidade entre equipamentos;
iii. Os investimentos necessários e;
iv. Os riscos de ataques cibernéticos a que ficam expostas as concessionárias de energia elétrica com a implantação das redes inteligentes.

Recentemente, a McAfee[1] divulgou um relatório que abordava a situação da segurança energética no ambiente das redes inteligentes. O relatório discute as ameaças cibernéticas à rede. Em particular analisa (i) como as antigas redes se constituem em alvo preferencial de ataques de segurança e (ii) como deveriam funcionar os modelos de proteção a partir de sistemas críticos. De acordo com o relatório, a rede elétrica é a coluna principal sobre a qual tudo repousa. Um *cibercriminoso* constitui em grande ameaça para os sistemas instalados e cidades. Um único ataque à rede elétrica pode comprometer todo o sistema energético, impondo riscos à rede de iluminação e de abastecimento de eletrodomésticos, serviços de apoio, abastecimento de energia para hospitais e sistemas de defesa aérea. De acordo com a indústria de energia global, o relato mais comum de ameaça cibernética é a extorsão. Os criminosos ganham acesso ao sistema da concessionária, mostram que podem danificá-lo e exigem um valor para resgate. Outras ameaças adicionais incluem espionagem e sabotagem, que sempre tem um objetivo financeiro, além de roubo de dados e desativação de instalações.

Esta dissertação apresenta uma abordagem conceitual dos temas envolvidos e discute a rede inteligente e a segurança da informação. Estabelece, também, a conexão entre a literatura especializada sobre o tema e a visão dos principais responsáveis pela implantação de projetos de redes inteligentes no Brasil, à medida que investiga parâmetros relacionados à segurança da informação na implantação da infraestrutura de medição inteligente no país.

[1] McAfee, subsidiária integral da Intel Corporation (NASDAQ: INTC), é uma empresa dedicada à tecnologia de segurança com atuação no mercado mundial.

1.1.
Definição do problema de pesquisa

Em linhas gerais, a adoção de novas tecnologias de redes inteligentes requer cuidados e alterações na arquitetura de segurança da informação para blindar as concessionárias de indesejáveis ataques cibernéticos (Vieira, 2011). A partir de um sistema vulnerável, consumidores terão a oportunidade de reduzir o valor de suas faturas de energia elétrica, fraudando medidores eletrônicos ou invadindo os sistemas comerciais das concessionárias (Clements, 2010).

A segurança da informação nas redes inteligentes é reconhecida em nível mundial como uma questão crítica e transversal que deve ser discutida por todos agentes do setor elétrico. A implantação das redes inteligentes certamente introduzirá novas normas (NIST, 2010), especificações, requisitos técnicos e dispositivos regulatórios que deverão ser cumpridos pelos usuários da tecnologia.

No contexto dessas reflexões, a **questão principal da dissertação** foi assim formulada: Que recomendações devem ser formuladas com o propósito de orientar os agentes do setor elétrico na superação dos desafios impostos pela introdução de redes inteligentes de energia, particularmente no que se refere à segurança da informação?

Pela abrangência e complexidade do tema, a questão principal foi desdobrada nas seguintes **questões específicas** que a pesquisa de mestrado objetivou responder:

- Quais os fundamentos conceituais, regulatórios e normativos que deverão orientar a definição do marco regulatório das redes inteligentes de energia no Brasil?
- Quais vulnerabilidades na segurança da informação devem ser consideradas pelas concessionárias para superar os desafios impostos pela introdução das redes inteligentes (smart grid)?
- Em que medida as concessionárias reconhecem os riscos de ataque cibernético a que ficam expostas com a implantação das redes inteligentes?
- Qual a importância de se implantar um sistema de segurança da informação nas concessionárias de energia elétrica, fundamentado nas principais normas nacionais e internacionais aplicáveis e nas boas práticas de experiências bem sucedidas em outros países?

1.2.
Objetivos: geral e específicos

1.2.1.
Objetivo geral

Analisar parâmetros relacionados à segurança da informação na implantação da infraestrutura de medição inteligente no *smart grid* e mostrar que os riscos associados podem ser minimizados pela adoção de recomendações normativas específicas.

1.2.2.
Objetivos específicos

Deste desdobramento da questão central resultam os seguintes objetivos específicos:

- Apresentar os fundamentos conceituais, regulatórios e normativos que deverão orientar a definição do marco regulatório das redes inteligentes de energia no Brasil.
- Identificar vulnerabilidades na segurança da informação que devem ser consideradas pelas concessionárias para superar os desafios impostos pela introdução das redes inteligentes.
- Analisar em que medida as concessionárias reconhecem os riscos de ataque cibernético a que ficam expostas com a implantação das redes inteligentes.
- Discutir a importância de se implantar um sistema de segurança da informação nas concessionárias de energia elétrica, fundamentado nas principais normas nacionais e internacionais aplicáveis e nas boas práticas de experiências bem sucedidas em outros países.

1.3.
Motivação

A introdução de redes inteligentes na gestão e operação do sistema elétrico constitui tema central nos planejamentos estratégicos das principais concessionárias de energia elétrica em diversos países. No Brasil, algumas empresas já estão desenvolvendo projetos pilotos de implantação. Light, Cemig, AES Eletropaulo, Ampla, CPFL (Companhia Paulista de Força e Luz) são empresas brasileiras que veem investindo significativos recursos neste padrão de tecnologia ao longo dos últimos anos.

Para que cada uma dessas empresas alcancem seus objetivos é de grande importância que os projetos estejam alinhados com as principais normas

e recomendações técnicas de segurança, evitando assim problemas futuros oriundos de ataques cibernéticos.

Diante deste cenário, é esperado que os resultados desta dissertação possam trazer os seguintes benefícios para os diversos atores do setor elétrico brasileiro:

- Apontar os requisitos mínimos para a definição de uma arquitetura de segurança da informação relevante para as concessionárias de energia elétricas e agente regulador no Brasil.
- Oferecer subsídios para os tomadores de decisão e líderes das concessionárias com relação à importância da implantação de uma arquitetura adequada de segurança da informação para as redes inteligentes.
- Publicar os resultados do estudo de caso em nível nacional, focando na segurança da informação, uma vez que o tema é central nas discussões sobre redes inteligentes de energia.

Preocupado com a atualidade de suas linhas de pesquisa, o Programa de Pós-Graduação em Metrologia para Qualidade e Inovação (PósMQI/PUC-Rio) acaba de incorporar o tema “Redes inteligentes" dentre suas prioridades, criando uma linha específica de pesquisa para estudar o tema. Esta dissertação sobre segurança de dados de concessionárias que fazem uso da tecnologia das redes inteligentes contribui para o primeiro ciclo de pesquisas sobre o tema no âmbito do Programa.

1.4. Metodologia

Para a classificação da pesquisa, tomou-se como base a taxonomia apresentada por Vergara (2007), que classifica o trabalho quanto aos fins e quanto aos meios a que se propõe. Quanto aos fins, a pesquisa se classifica como descritiva, pois apresenta características claras e bem delineadas de determinada população ou fenômeno. Para tal envolve técnicas padronizadas e bem estruturadas de coletas de dados. Quanto aos meios de investigação, é uma pesquisa bibliográfica, já que inclui um extenso estudo sistemático de textos de autores credenciados e reconhecidos como referência sobre o tema, assim definindo a base teórica da dissertação. É de natureza documental, pela coleta de informações realizada em acervo oficial nas bases dos institutos de normalização e na base do Regulador do setor (a Aneel, Agência Nacional de Energia Elétrica). Inclui, ainda, pesquisa de campo pela aplicação de um questionário estruturado junto a concessionárias do setor elétrico brasileiro. Em

função da dinâmica e novidade inerente ao tema, fez uso de fonte de dados e informação atualizada, utilizando o noticiário da mídia impressa, revistas técnicas e artigos publicados e apresentados nos principais congressos do setor elétrico.

A Figura 1.1 apresenta o desenho da pesquisa segundo suas três grandes fases de desenvolvimento:

i. Pesquisa exploratória e descritiva;
ii. Pesquisa aplicada (estudo de caso);
iii. Pesquisa conclusiva e propositiva.

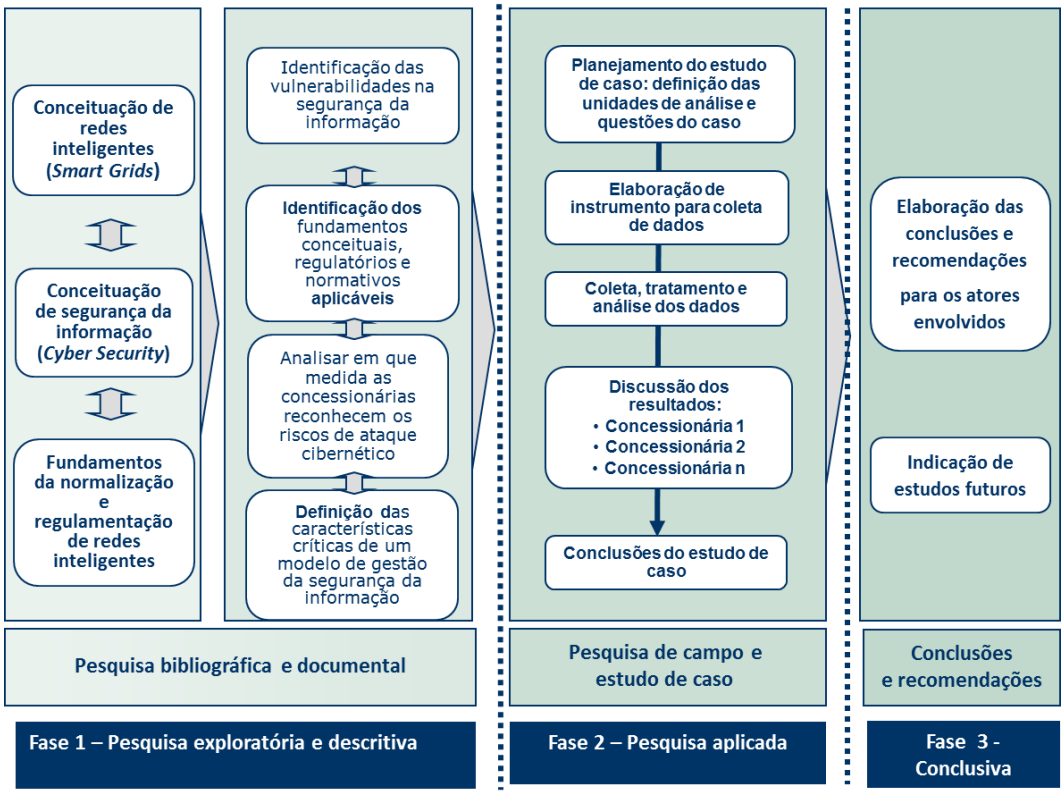

Figura 1.1 - Desenho da pesquisa, seus componentes e métodos.

Estudo de caso foi o método utilizado na fase da pesquisa de campo que compreendeu pesquisa operacional e aplicação de um questionário. O preenchimento do questionário contou com a participação de respondentes envolvidos na implantação de projetos de redes inteligentes.

Segundo Yin (2010), o estudo de caso é uma investigação empírica que: (i) investiga um fenômeno contemporâneo em profundidade e em seu contexto de vida real, especialmente quando (ii) os limites entre o fenômeno e o contexto não são claramente evidentes.

Ainda de acordo com Yin (2010), a investigação do estudo de caso (i) enfrenta a situação tecnicamente diferenciada em que existirão muito mais

variáveis de interesse do que pontos de dados, e, como resultado (ii) conta com múltiplas fontes de evidência, com os dados precisando convergir de maneira triangular, e como outro resultado (iii) beneficia-se do desenvolvimento anterior das proposições teóricas para orientar a coleta e a análise de dados.

A partir da tipologia apresentada por Yin (2010), selecionou-se o estudo de caso mais adequado para esta pesquisa: caso único holístico. Apesar de cada concessionária ser um sujeito de uma investigação de caso individual, a análise agrupada dos resultados faz com que o estudo de caso seja único, no qual as concessionárias tornaram-se parte de uma unidade de análise maior.

Finalmente, na terceira fase desta pesquisa (conclusiva e propositiva), buscou-se formular recomendações para aplicação prática nas concessionárias do setor elétrico brasileiro.

1.5. Estrutura da dissertação

A dissertação está estruturada em seis capítulos, incluindo esta introdução (1). São três capítulos de fundamentação teórica, abordando os temas centrais da dissertação: (2) evolução das redes elétricas, (3) redes inteligentes e segurança da informação. Um capítulo dedicado às normas aplicáveis ao tema redes inteligentes (4). O quinto capítulo apresenta o estudo de caso propriamente dito. E por fim, apresentam-se algumas conclusões e encaminham-se recomendações para trabalhos futuros (6).

O capítulo 2 — **Redes inteligentes (*smart grid*)** — conceitua as redes inteligentes e apresenta os três pilares que fundamentam esta tecnologia inovadora. Os principais recursos da tecnologia são descritos com maior ênfase para a tecnologia de comunicação por ser a principal porta de entrada para as invasões na rede. Concluindo o capítulo, é discutido o problema relacionado com a segurança da informação fragilizada pela exposição do sistema à rede inteligente.

O capítulo 3 — **Redes de energia elétrica: perspectiva para uma revolução no setor** — apresenta a evolução das redes de energia elétrica no Brasil e discute o panorama da adoção das redes inteligentes no mundo. O capítulo discute ainda os principais desafios e oportunidades para a implantação desta nova tecnologia no contexto brasileiro e os principais motivadores para adoção das redes inteligentes no Brasil, destacando-se a sua aplicação ao combate às perdas não-técnicas e à inadimplência. E, também, os desafios

regulatórios e o papel da Aneel no processo de adoção das redes inteligentes no País.

No capítulo 4 — **O papel das normas para as redes inteligentes** — analisa-se a importância das resoluções e das normas para o ambiente das redes inteligentes no Brasil. As principais referências teóricas para este capítulo recaem sobre o documento publicado pelo NIST (*National Institute of Standards and Technology*) - *Guidelines for smart grid cyber security (2010)*, sobre a resolução normativa nº 502 (Anexo II), publicada pela Aneel em 07 de agosto de 2012, sobre os resultados da audiência pública nº 43/2010 e, por fim, sobre os esforços de normalização do *International Electrotechnical Commission* (IEC), através do grupo de trabalho *IEC Smart Grid SG3.*

O capítulo 5 — **Segurança da informação nas redes inteligentes de energia elétrica: estudo de caso de concessionárias no Brasil** — apresenta e discute os principais resultados do estudo de caso.

No último capítulo são formuladas as principais conclusões do trabalho. Propõem-se recomendações para as concessionárias com o propósito de orientá-las na superação dos desafios impostos pela introdução de redes inteligentes de energia, particularmente no que se refere à segurança da informação. Concluindo a dissertação, são formuladas algumas recomendações para desdobramentos futuros da pesquisa.

2
Redes inteligentes (*smart grid*)

2.1.
Conceitos e definições

Existem várias definições para a denominação *redes inteligentes* na literatura especializada e em uso no mercado mundial de energia elétrica. Pode-se dizer que embora a denominação s*mart grid* elucide diferentes significados para muitas pessoas, o seu entendimento guarda coerência entre as diferentes definições existentes. Sua primeira citação foi em 2005, no artigo "*Toward a Smart Grid*", de autoria de S. Massoud Amin e Bruce F. Wollenberg, publicado na revista IEEE P&E (Amin *et al*., 2005).

Atualmente, as tecnologias da informação, aliadas às de comunicação, permitem avanços significativos para processos que envolvem geração, transmissão e distribuição de energia elétrica. Medição eletrônica, comunicação, sensoriamento, energias alternativas, armazenamento de eletricidade são exemplos de tecnologias que compõem o conceito *smart grid*. Esses são conceitos que promovem novos serviços para os consumidores (Hledik, 2009**)**. Em última análise, parece não haver dúvida de que o acesso a novas informações irá melhorar os produtos e serviços que são oferecidos aos consumidores, levando a um consumo mais eficiente e mais racional.

O Departamento de Energia dos Estados Unidos afirma que as redes inteligentes agrupam um conjunto avançado de tecnologias, métodos de controle e comunicações que são integradas em uma rede elétrica (Rahman, 2009).

A expressão *smart grid* deve ser entendida mais como um conceito do que como uma tecnologia ou equipamento específico. Segundo Falcão (2010), as redes inteligentes (*smart grid*) baseiam-se na utilização intensiva de tecnologias de automação, computação e comunicação na rede elétrica. Estas tecnologias permitirão a implantação de estratégias de controle e otimização da rede elétrica de maneira muito mais eficiente (Falcão, 2010).

O grupo da comissão europeia, que trata do tema “Redes inteligentes”, propôs a seguinte definição:

> *Smart Grid é uma rede de energia elétrica que pode integrar eficientemente o comportamento e as ações de todos os usuários conectados a ela, a fim de garantir eficiência econômica, sistema de energia sustentável, com baixas perdas e elevados níveis de qualidade e segurança de abastecimento* (SGTF, 2011).

De acordo com Bouhafs (2012), as redes inteligentes poderiam ser caracterizadas por um fluxo bidirecional de energia elétrica e informação, onde as tecnologias de comunicação terão um papel determinante.

Há um consenso em formação de que a infraestrutura de comunicação, que atualmente suporta a operação das redes, precisa de modernização. A infraestrutura de comunicação presente nas concessionarias do setor elétrico brasileiro foi concebida para atender as necessidades de uma indústria com diferentes requisitos dos atuais.

A introdução do conceito de redes inteligentes produzirá uma convergência significativa entre as infraestruturas de geração, transmissão e distribuição de energia e a infraestrutura de comunicações digitais e processamento de dados. Esta última funcionará como uma Internet de equipamentos, interligando os chamados IEDs (*Intelligent Electronic Devices*). Trocará informações e ações de controle entre os diversos segmentos da rede elétrica. Essa convergência de tecnologias exigirá o desenvolvimento de novos métodos de controle, automação e otimização da operação do sistema elétrico.

De acordo com Falcão (2010), algumas das principais características geralmente atribuídas às redes inteligentes são:

- auto-recuperação: capacidade de automaticamente detectar, analisar, responder e restaurar falhas na rede;
- análise do comportamento dos consumidores nos processos de planejamento e operação da rede;
- tolerância a ataques externos: capacidade de mitigar e resistir a ataques físicos e cyber-ataques;
- qualidade de Energia: prover energia com a qualidade exigida pela sociedade digital;
- acomodação de uma grande variedade de fontes e demandas: capacidade de integrar de forma transparente (plug and play) uma variedade de fontes de energia de várias dimensões e tecnologia;
- redução do impacto ambiental do sistema produtor de eletricidade, reduzindo perdas e utilizando fontes de baixo impacto ambiental;
- resposta da demanda mediante a atuação remota em dispositivos dos consumidores;
- viabilização de mercados competitivos de energia;

A Figura 3.1 apresenta o conceito de redes inteligentes. Visão da Nansen (2010), que é fornecedora de soluções de medição para o setor de energia elétrica.

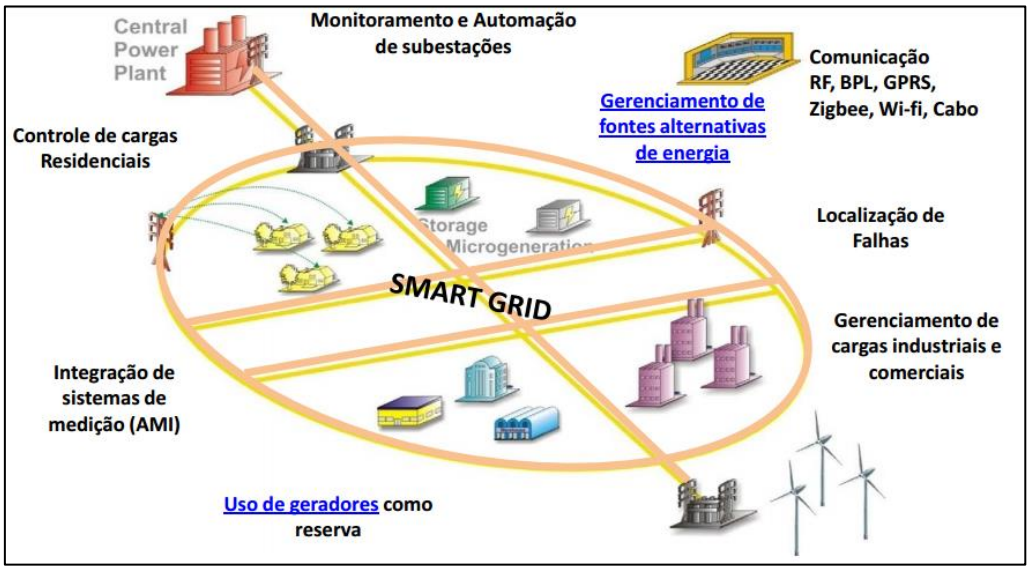

Figura 2.1 - O conceito *smart grid*.
Fonte: Nansen, 2010.

Para que o conceito de *smart grid* seja compreendido e implantado no Brasil, algumas transformações devem ser introduzidas no setor. Modernização da infraestrutura, instalação de camadas digitais, implantação de novos softwares e capacidade de processamento de dados, que são a essência da rede inteligente. O Quadro 3.1 traça um comparativo das principais características do padrão atual de rede de energia e das redes inteligentes.

Quadro 3.1 - Comparação da rede elétrica atual com as redes inteligentes.

Rede (padrão atual)	Rede Inteligente
Os consumidores estão desinformados e não participam do sistema.	As informações de preços estão disponíveis, assim o cliente tem a escolha de muitos planos, preços e opções de compra e venda.
Dominada pela produção centralizada, muito limitada na geração e armazenamento.	Recursos energéticos *plug and play* para complementar a produção centralizada.
Mercado limitado e não integrado.	Mercado integrado e que possibilita inovação.
Concentra-se em falhas ao invés da qualidade da energia.	Qualidade e prioridade, com uma variedade de opções de preço de acordo com as necessidades do cliente.
Inteligência da rede limitada.	Integração inteligente da rede com a gerência.

Rede (padrão atual)	Rede Inteligente
Foco na proteção após a falha.	Evita interrupções, minimiza o impacto e se recupera rapidamente de falhas.
Vulnerável a vândalos e a desastres naturais.	Detecta, atenua e se restaura rápida e eficientemente após desastres.

Fonte: Lopes, 2012.

Para que o processo de modernização da rede aconteça de forma eficiente, alguns conceitos devem ser observados (MME, 2010):

- Confiabilidade;
- Eficiência;
- Segurança;
- Questões ambientais;
- Competitividade.

As tecnologias envolvidas no conceito das redes inteligentes podem ser divididas em quatro grupos: medição eletrônica, comunicação, sensoriamento/automação e computação. A Figura 3.2 ilustra os grupos de tecnologias que viabilizam o conceito das redes inteligentes.

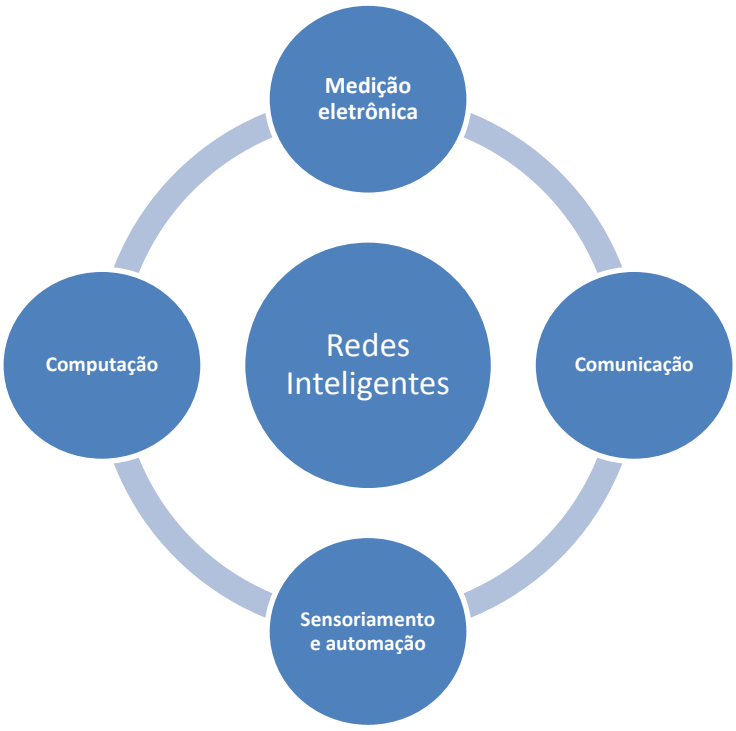

Figura 3.2 - Tecnologias viabilizadoras das redes inteligentes.

2.1.1.
Medição eletrônica

A medição eletrônica não se limita apenas à instalação de medidores eletrônicos nas residências ou estabelecimentos dos consumidores das concessionárias de energia elétrica. Toda a medição envolvida, da geração até o consumidor final, faz parte dessa categoria. Processos como controle de perdas, planejamento e operação da rede estão diretamente ligados a essa tecnologia.

Na medida em que as concessionárias fizerem a substituição dos medidores eletromecânicos por outros eletrônicos, uma grande massa de dados poderá ser alocada nos centros de controle das empresas, permitindo melhor planejamento e controle de toda a rede. A partir da utilização desses medidores, diversos novos serviços poderão ser ofertados ao consumidor, além de se mudar o conceito de utilização das cargas, que poderão ser controladas remotamente, tanto pelo consumidor, quanto pela concessionária.

Por exemplo, o despacho de equipes deverá ser bastante reduzido, já que o processo de interrupção e religação do fornecimento de energia poderá ser feito remotamente pela concessionária, graças ao poder de comunicação bidirecional dos novos medidores. Além disso, uma possível interrupção no fornecimento de energia, provocada por algum evento inesperado, será percebida pela concessionária quase que automaticamente, não havendo mais a necessidade de o consumidor avisar à empresa o fato.

A partir da implantação dos medidores eletrônicos, o consumidor terá mais condições de gerenciar seu uso de energia. Vários aplicativos já estão em desenvolvimento para proporcionar o acesso aos dados de medição, auxiliando na tomada de decisão (MME, 2010).

Alguns exemplos de interação entre o consumidor e a concessionária são: gestão do consumo em tempo real, equipamentos que mais consomem energia, valor a pagar até o momento, projeção de fatura no final do ciclo, etc. Antes mesmo de chegar à sua casa, o consumidor poderá programar qualquer equipamento conectado à rede elétrica (MME, 2010).

Uma transformação muito aguardada pelos atores desta indústria é a definição de vários níveis de tarifa de energia, pois a partir da medição eletrônica, o preço da energia poderá variar ao longo dia. Esse sinal tarifário proporcionará uma redução do pico de demanda, gerando uma economia em investimentos de geração e expansão de rede. A Figura 3.3 ilustra um esquema com as principais aplicações para as redes inteligentes.

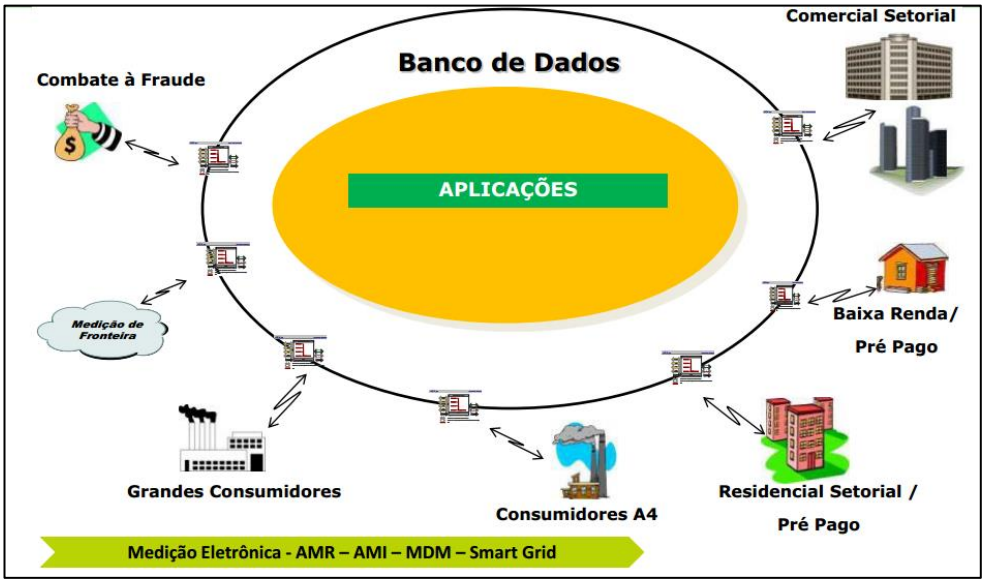

Figura 3.3 - Aplicações de medição eletrônica.
Fonte: Nansen, 2010.

Para melhor compreensão da medição inteligente, é importante definir alguns termos relacionados à evolução da mesma:

- *AMR (Automated Meter Reading);*
- *AMI (Advanced Metering Infrastructure);*
- *AMM (Advanced Meter Management);*
- *MDM (Meter Data Management)*

O Quadro 3.2 apresenta uma definição para cada um desses itens.

Quadro 3.2 - Medição eletrônica

Tecnologia	Definição
AMR (Automated Meter Reading), ou Leitura Automática do Medidor	Sistema que realiza a leitura automática de dados do medidor (e.g.: consumo e status), podendo ser eletrônico ou eletromecânico. Inicialmente visava aperfeiçoar o processo de faturamento ao permitir maior acurácia nas medições e economia de custos com pessoal de campo (leituristas). Este conceito foi lançado na década de 80, quando diversos países investiram em AMR com projetos priorizando a leitura remota dos medidores.
AMI (Advanced Metering Infrastructure), ou Infraestrutura de Medição Avançada	Sistema com capacidade de medição, leitura (programada ou por demanda) e validação de dados de uso de energia. Este modelo se comunica com medidores inteligentes de energia elétrica via diferentes meios de comunicação. A comunicação é estabelecida em via dupla. Em síntese, a AMI preparou o terreno para o surgimento da medição inteligente.
AMM (Advanced Meter Management), ou Gerenciamento do	Plataforma técnica de gerenciamento para medidores inteligentes (*smart meters*). Apresenta as seguintes funções básicas: (i) gerenciamento de dispositivo (p. ex., gestão de parâmetros dos

Tecnologia	Definição
Medidor Avançado	medidores), (ii) gestão de grupo, possibilitando o controle de grupos de dispositivos, como configuração e upgrade de firmware, e (iii) gestão de plataforma de comunicação, assegurando comunicação dupla via confiável entre medidores e CCM (Centro de Controle de Medição), reportando status de rede, desempenho da comunicação e situações de exceção.
MDM (Meter Data Management), ou Gerenciamento de Dados do Medidor	Processa e gerencia dados gerados pelos medidores, que devem experimentar crescimento exponencial com a exigência de menor intervalo entre leituras (a partir de 15 min.). Também fará registro de informações complementares (p. ex., fator de potência, DEC, FEC, DIC, FIC DMIC[2]), a fim de aperfeiçoar processos das concessionárias como faturamento, eficiência operacional, serviços ao consumidor, previsão de demanda de energia, gerenciamento do sistema de distribuição (*DMS: Distribution Management System*), gestão de fraudes, gestão de demanda, dentre outros.

Fonte: Vieira, 2011.

2.1.2. Comunicação

Uma importante funcionalidade dos medidores inteligentes é a sua capacidade de se comunicar com outros equipamentos instalados na rede ou nas unidades consumidoras. Essa inovação caracteriza uma relevante mudança na prestação de serviços do setor de energia.

Um sistema de comunicação constitui-se no componente-chave da infraestrutura de uma rede inteligente (Laverty, 2010). Com a integração de tecnologias e aplicações avançadas para alcançar uma forma mais inteligente de infraestrutura de rede, uma expressiva massa de dados geradas a partir de diferentes aplicações estará disponível para posterior análise e controle. Por isso, a definição dos requisitos de comunicação constitui variável crítica para as concessionárias de energia elétrica. O desafio que se impõe às tecnologias de comunicação refere-se à sua capacidade de operar com grande volume de dados de forma confiável, segura e a um baixo custo (Gungor, 2010).

Atualmente existe uma portfolio de tecnologia disponível no mercado com o objetivo de propiciar essa comunicação. Entre elas o *Power Line Communication* (PLC), *ZibBee*, redes *Mesh*, radiofrequência e redes celulares do tipo *General packet radio service* (GRPS).

A escolha da tecnologia de comunicação dependerá de uma série de fatores, dentre estes, topologia, preço, disponibilidade, alcance e viabilidade

[2] São indicadores que servem para monitorar a qualidade do fornecimento de energia elétrica pelas concessionárias. DEC (Duração Equivalente de Continuidade), FEC (Frequência Equivalente de Continuidade), DIC (Duração de Interrupção Individual por Unidade Consumidora), FIC (Frequência de Interrupção Individual por Unidade Consumidora) e DMIC (Duração Máxima de Interrupção Contínua por Unidade Consumidora).

(MME, 2010). Provavelmente, uma mesma concessionária fará uso de mais de uma tecnologia, já que atuam em áreas de concessão extensas e com grande variedade de terrenos e classes consumidoras.

O principal requisito da comunicação para as redes inteligentes é o protocolo. Segundo especialistas do setor, o uso de um protocolo proprietário e fechado poderá implicar no aumento dos preços e falta de competição. Por isso, acredita-se que a adoção de um protocolo público seria mais adequada. Esta prática poderá garantir a competição e a utilização de equipamentos de vários fabricantes, sem necessidade de mudança na contratação de serviços de comunicação de dados.

A comunicação em duas vias (concessionária → cliente e vice-versa) é fundamental para que o conceito de redes inteligentes seja totalmente viabilizado. Processos de interrupção e religação de fornecimento remotas, envio de informação sobre consumo em tempo real e definição de novos postos tarifários dependem dessa comunicação bidirecional.

Neste novo padrão de rede, os consumidores estão permanentemente conectados com a rede, gerando e recebendo informações. Isso permite que os consumidores façam uma gestão de seus gastos, além de possibilitar uma avaliação em relação à demanda e qualidade de serviço (Lopes, 2012).

De acordo com Gungor (2011), outro conceito muito importante é a interoperabilidade. Diversos sistemas e seus componentes precisam ter a capacidade de operar em conjunto. A interoperabilidade permite a integração, o funcionamento cooperado e a comunicação bidirecional entre os vários elementos interconectados do sistema elétrico. Para que seja efetiva, deverá ser estruturada uma padronização de interfaces, protocolos e outros elementos de interconexão.

Em resumo, do ponto de vista das redes de comunicação de dados, as redes inteligentes podem fazer uso potencial de um conjunto abrangente de tecnologias de rede, tais como (Lopes, 2012):

- PLC (Power Line Communications) – versões faixa larga e faixa estreita;
- Ethernet (E-Carrier, Gigabit, EPON e outras);
- IP/MPLS (MultiProtocol Label Switching) e IP/GMPLS (Generalized MPLS) (IP com comutação de circuito eficiente e restauração);
- IP/WDM (IP com redes óticas de alto desempenho);
- DCN (Dynamic Circuit Network) (redes com provisionamento de circuitos dinâmicos);
- Redes de Sensores sem Fio (WSN – Wireless Sensor Networks) e redes em malha (mesh);

- WiFi - IEEE 802.11;
- WiMax;
- Soluções tecnológicas baseadas na telefonia móvel (GSM, GPRS, 3G, 4G);
- ZigBee;
- Bluetooth;
- Outras.

2.1.3. Sensoriamento e automação

As redes inteligentes são amplamente baseadas no monitoramento, características fundamentais em todos os componentes da rede. Isso só é possível mediante o uso intensivo das tecnologias de comunicação que atuam na integração de vários componentes.

Para as transmissoras e distribuidoras de energia, a técnica de sensoriamento mais importante é o *phasor measurement unit* (PMU). Os PMUs são dispositivos de alta velocidade capazes de monitorar a qualidade da energia e, em alguns casos, atuar na rede automaticamente, de acordo com as medidas aferidas (Lopes, 2012).

Os sistemas avançados de controle e automação também constituem um grupo importante para as redes inteligentes. Eles monitoram e controlam os elementos essenciais da rede. Algoritmos inteligentes permitem a coleta e análise eficiente de dados, fornecem soluções para operadores humanos e também são capazes de atuar de forma autônoma (OECD, 2009).

Por exemplo, novos sistemas de automação de subestações foram desenvolvidos com a capacidade de monitorar as informações *in loco* ou remotamente. Considerando que a informação da subestação só estava disponível localmente nas redes tradicionais, novos subsistemas são capazes de tornar esta informação disponível em toda a rede e, assim, proporcionar melhor gerenciamento de energia. As falhas podem ser detectadas muito mais rápido do que nas redes tradicionais e os tempos de interrupção pode ser reduzido.

2.1.4. Computação

Um elemento chave das redes inteligentes são os programas de apoio à decisão e interfaces humanas. O volume de dados em redes inteligentes irá aumentar significativamente comparado às redes tradicionais.

Como Houseman e Shargal (2009) sugerem, "uma concessionária, com cinco milhões de consumidores terá mais dados na sua rede de distribuição do que o grupo *Wal-Mart*, que gerencia o maior repositório de dados do mundo". Um dos principais desafios das concessionárias refere-se à integração e gestão de todos os dados gerados. Consequentemente, outro desafio é disponibilizar estes dados para operadores e administradores de rede de forma amigável para apoiar suas decisões.

De acordo com pesquisadores do *Science Applications International Corporation* (2006), algoritmos de inteligência artificial e mineração de dados poderão contribuir para a gestão deste volume de dados e para criar um formato mais eficaz para a compreensão do usuário. Estas ferramentas têm características de aprendizado a partir de uma série histórica, ou seja, os algoritmos tem a capacidade de aprender e adaptar-se a fim de criar padrões que possam suportar a tomada de decisão.

Novas tecnologias de banco de dados e novos métodos de visualização permitem a integração de dados de diferentes fontes. Por exemplo, os operadores podem ter acesso às informações sobre o estado da qualidade da rede, identificando instabilidades e falhas. A área de planejamento poderá acompanhar o consumo horário de cada cliente, aprimorar todo o processo de compra e venda de energia, desenvolver programas de eficiência energética etc.

2.2. *Smart grid e* o problema da segurança da informação

Entende-se que as redes inteligentes serão capazes de introduzir novas funcionalidades ao sistema atual de energia elétrica. No entanto, elas também poderão introduzir vários novos riscos de segurança para o sistema. A dependência do uso de eletricidade para todos os setores produtivos de um país faz da rede de energia elétrica um bem essencial. A interrupção do fornecimento de energia elétrica sempre proporciona grandes impactos sociais, por isso a segurança da rede é uma questão de grande importância para todos. Na visão de especialistas, as redes inteligentes introduzirão novos riscos de segurança relacionados com as suas necessidades de comunicação, automação de sistemas, agregação de novas tecnologias e tratamento de dados (Baumeister, 2010).

A espinha dorsal das tecnologias que compõem as redes inteligentes é a própria rede. Sobre esta rede, diferentes componentes do *smart grid* estarão

conectados. A comunicação entre todos os componentes será bidirecional e os dados trafegarão pela própria rede elétrica. Segundo especialistas do setor, esta conexão introduzirá riscos de segurança para o sistema, apesar de ser fundamental para a implantação das principais funcionalidades das redes inteligentes.

A conexão dos diferentes componentes certamente aumentará a complexidade da rede de energia elétrica e o número de oportunidades para novas vulnerabilidades de segurança. Novos componentes funcionarão como pontos de entrada que poderão ser usados para obter acesso ao sistema de energia eléctrica.

Como se pode perceber, uma das grandes funcionalidades das redes inteligentes é a sua capacidade de transportar dados pela rede. Entretanto, este tipo de transporte pode gerar vulnerabilidade para o sistema. Alguns dos componentes da rede requerem dados em tempo real. A perda de dados ou a latência pode ter efeitos adversos sobre a rede de energia elétrica. Por exemplo, o *software* de gestão do estado do sistema poderá estar em risco de ser invadido por um código malicioso que altere sua funcionalidade. A interrupção da comunicação ou alteração do estado da rede pode levar a perda de energia.

A conexão dos diferentes componentes do sistema de energia elétrica exigirá a interação entre novas tecnologias. Essa interação entre diferentes tecnologias também introduzirá novos riscos de segurança. As redes inteligentes terão que apoiar os sistemas corporativos. Por sua vez, estes sistemas não possuem requisitos de segurança para suportar o novo modelo de rede, tornando-se o elo mais fraco para um ataque. Além disso, as novas tecnologias que estão sendo utilizadas nos componentes das redes inteligentes podem exibir vulnerabilidades de segurança que podem oferecer ameaças resultando em sérios problemas para a concessionária.

2.3.
O custo do cybercrime no Brasil

De acordo com os resultados de um estudo realizado pela Norton/Symantec (2012), o custo de crimes realizados através da internet no Brasil, incluindo fraude e roubo de informações bancárias pelo uso de vírus, é de cerca de R$ 16 bilhões anuais. Este montante representa 7% do prejuízo global causado pelo *cibercrime*.

Estimativas da Norton/Symantec indicam que o Brasil é o terceiro país mais afetado por atividade ilegal na rede, atrás apenas de China (R$ 92 bilhões), EUA (R$ 42 bilhões) e empatado com a Índia.

A PricewaterhouseCoopers também realizou uma pesquisa global sobre crimes econômicos em 2011. Os resultados desta pesquisa evidenciaram que, nos últimos dois anos, os crimes digitais passaram de irrelevantes ao segundo lugar na lista dos crimes econômicos sofridos por empresas brasileiras (Avruch, 2012). Apesar de as empresas estarem cada vez mais dependentes de tecnologia, elas ainda são despreparadas para tratar dos riscos associados aos ataques cibernéticos.

A pesquisa acima referida apresenta uma visão corporativa sobre crimes econômicos que estão em forte tendência de alta no Brasil, e focou nos crimes digitais – cometidos com a utilização de computadores e internet como elemento principal. Somente no país, 32% das empresas ouvidas foram vítimas desse tipo de ataque nos últimos 12 meses, contra 23% na média global (PwC, 2011). De acordo com a PricewaterhouseCoopers, em 2009, os respondentes não citaram os ataques cibernéticos entre os mais relevantes no Brasil. A Figura 3.4 apresenta os principais tipos de crimes econômicos de acordo com a pesquisa realizada pela PricewaterhouseCoopers.

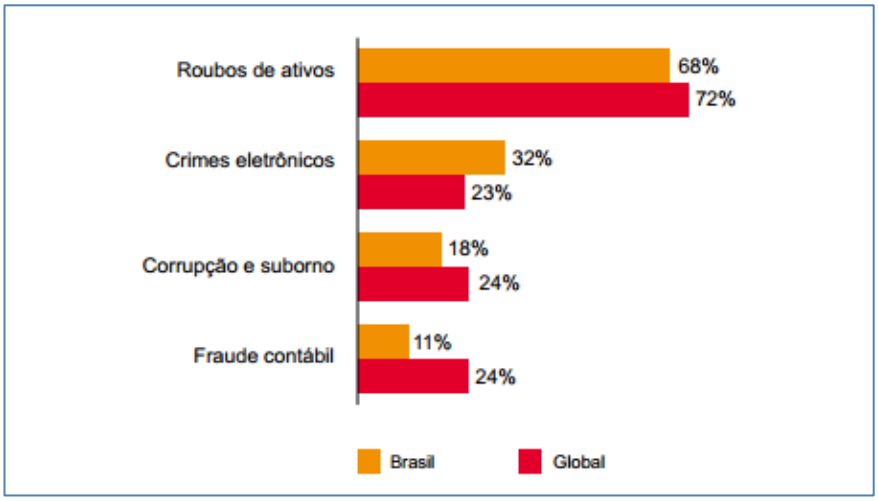

Figura 3.4 - Principais tipos de crimes econômicos informados.
Fonte (PwC, 2011).

Apesar do incremento do número de ataques virtuais, o estudo evidencia que os principais executivos e a diretoria das empresas ainda não adotaram processos de verificação de ameaças de crimes digitais ou os adotaram de

modo não formal, para fins específicos. Em linhas gerais, a maioria dos colaboradores das empresas não tem, ou não sabem da existência, de um plano de resposta a crises cibernéticas. 37% das empresas brasileiras (42% no mundo) não promoveram qualquer tipo de treinamento em segurança digital nos últimos 12 meses (PwC, 2011).

Em termos econômicos, a pesquisa evidencia números ainda mais preocupantes, pois os custos envolvidos com os crimes digitais são elevados. Oito em cada cem empresas afetadas no Brasil sofreram perdas superiores a US$ 5 milhões e 5 (cinco) em cada cem registraram prejuízos de US$ 100 milhões a US$ 1 bilhão (PwC, 2011).

Por referir-se a um conceito recente que se aplica a inúmeros elementos da rede de distribuição, o tema associado à segurança da informação nas redes inteligentes é extremamente complexo. Entendido como o indutor de uma revolução no setor elétrico como um todo, o tema vem sendo estudado e pesquisado de forma gradativa pelos diferentes atores que participam do setor. A segurança da rede e a blindagem dos sistemas operados pelas concessionárias devem ser avaliadas criticamente no âmbito de cada componente que integra a rede inteligente, levando-se em conta a conexão entre cada um desses elementos. Ciente da extensão do tema, esta pesquisa não tem a pretensão de exaurir o assunto, mas, tão somente, contribuir para a reflexão da problemática relacionada à segurança da informação no uso do *smart grid*, à luz dos objetivos propostos no capítulo 1 da dissertação.

2.4. Segurança da informação

A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma concessionária de energia elétrica e, consequentemente, necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades (ABNT, 2005).

As redes inteligentes precisam ser dotadas de uma nova arquitetura de segurança em função do arcabouço teórico exposto nos capítulos anteriores. Mesmo que cada fornecedor atente para o tema e faça uso de todas as normas de segurança, a conexão entre várias tecnologias pode se transformar em

vulnerabilidade para o sistema. Isso não significa que o atendimento às normas não seja suficiente, mas alerta para o fato de que a conexão de diferentes tecnologias pode apresentar novos requisitos de segurança. Tal situação pode expor as concessionárias às diversas ameaças. Na visão da Associação Brasileira de Normas Técnicas (ABNT), o organismo normalizador brasileiro, as principais causas de ataque a um sistema digital originam-se de fraudes eletrônicas, espionagem, sabotagem, vandalismo, *blackouts*, códigos maliciosos, *hackers*, entre outras (ABNT, 2005). Para a ABNT, segurança da informação (SI) tem como objetivo proteger a informação contra ameaças no intuito de garantir a continuidade, minimizar os danos e maximizar os investimentos e oportunidades do negócio. A segurança da informação é obtida com a utilização de controles: políticas, práticas, procedimento, estruturas organizacionais e infraestruturas de *hardware* e *software*.

Já na visão de Nordell (2012), a segurança da informação é caracterizada pela preservação da disponibilidade, integridade, confidencialidade e autenticidade da informação, e visa preservar a competitividade, o faturamento, a lucratividade, o atendimento aos requisitos legais e a imagem das concessionárias de energia elétrica. Nesse contexto, assim conceitua:

- **confidencialidade**: a propriedade de que informações confidenciais não serão divulgadas a pessoas não autorizadas, entidades ou processos.
- **integridade**: a propriedade que os dados sensíveis não foram modificados ou excluídos de forma não autorizada e sem ser detectado.
- **disponibilidade**: a propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada.
- **autenticidade**: a certeza de que o dado (em análise) provém das fontes anunciadas e que não foi alvo alterado ao longo de um processo.

2.5. Potenciais riscos e ameaças de ataques cibernéticos

Os riscos de segurança da informação se configuram pela potencial exploração de uma ou mais vulnerabilidades de um componente das redes inteligentes. Quer por parte de uma ou mais ameaças, quer por impacto negativo no processo de distribuição de energia.

Entende-se, assim, que a identificação das potenciais ameaças e vulnerabilidades da rede compreende um passo fundamental no tratamento deste tema. O Quadro 3.2 apresenta as principais fontes de ameaça, motivações e possíveis consequências de um ataque cibernético.

Quadro 3.2 - Principais fontes de ameaças.

Fontes de ameaça	Motivação	Possíveis Consequências
Hacher*, *cracker	Desafio Egocentrismo Protesto Rebeldia Status Dinheiro	*Hacking*; Engenharia social; Negação de serviço; Pichação de sites; Invasão de sistemas, infiltrações; Acesso não autorizado.
Criminosos digitais	Destruição de informações Acesso a dados sigilosos Divulgação ilegal de informações Ganho monetário Alterações não autorizadas de dados	Atos virtuais fraudulentos (interceptação de dados, ataque homem-no-meio, IP *spoofing*, etc.); Intrusão de sistemas. Suborno por informação; Ataques a sistemas (negação de serviço);
Terroristas	Chantagem Destruição Vingança Exploração Ganho político Cobertura da mídia	Ataques com bombas; Guerra de informação; Ataques a sistemas; Invasão e dominação de sistemas; Alteração de sistemas.
Espiões	Vantagem competitiva Espionagem econômica	Garantir vantagem de um posicionamento defensivo; Garantir uma vantagem política; Exploração econômica; Furto de informações; Violação da privacidade das pessoas; Engenharia social; Invasão de sistemas; Invasão de privacidade; Acessos não autorizados em sistemas
Pessoas: mal treinadas, insatisfeitas, mal-intencionadas, negligentes, imprudentes, desonestas, demitidas.	Curiosidade Egocentrismo Informações para serviço de Inteligência Ganhos financeiros Vingança Ações não intencionais ou omissões (erro na entrada de dados, erro na programação).	Agressão a funcionário; Chantagem; Busca de informação sensível; Abuso dos recursos computacionais; Fraudes; Furto de ativos; Suborno de informação; Inclusão de dados falsos; Corrupção de dados; Interceptação de informação; Desvio de informação; Uso de programas ou códigos maliciosos; Sabotagens; Invasão de sistemas; Acessos não autorizados a sistemas.

Fonte: ABNT, 2008.

2.6.
AMI (*Advanced Metering Infrastructure*) - Vulnerabilidades

A implantação da infraestrutura de medição avançada (AMI) é vista como um dos primeiros passos na digitalização dos sistemas da rede elétrica. Apesar do aumento da utilização desta tecnologia, pouco se tem pesquisado no sentido de identificar as necessidades de segurança para estes componentes. Os medidores inteligentes (*smart meters*), no entanto, são alvos atraentes para exploração e ataques às redes das concessionárias. Atualmente, nos Estados Unidos, estima-se que US$ 6 bilhões são perdidos através de fraudes (Amin, 2012).

Possíveis ameaças aos medidores eletrônicos resultam de atos relacionados a:

- fabricar leituras do medidor de energia;
- manipular os custos de energia;
- perturbar o equilíbrio de carga dos sistemas locais de repente aumentando ou diminuindo a demanda por energia;
- ganhar o controle de milhões de medidores e, simultaneamente, desligá-los;
- enviar sinais de comando falsos;
- desativar a rede de controle e sistemas de computador do centro de medição;
- desativar relés de proteção.

De acordo com Amin (2012), os requisitos de segurança devem ser observados em todos os níveis da rede para que o sistema seja confiável. Neste sentido, justifica-se o emprego de estratégias regulatórias, dentre as quais o estabelecimento e a adesão às normas técnicas, voltadas para a garantia da segurança da informação nas redes inteligentes.

No próximo capítulo, analisa-se a importância das resoluções e das normas para a segurança da informação no ambiente das redes inteligentes. As principais referências teóricas para este capítulo recaem sobre o documento publicado pelo NIST (*National Institute of Standards and Technology*) - *Guidelines for smart grid cyber security* e sobre a resolução normativa nº 502, publicada pela Aneel em 07 de agosto de 2012.

3
Redes de energia elétrica: perspectiva para uma revolução no setor

Muito se tem falado sobre as redes inteligentes e suas aplicações pelas concessionárias de energia elétrica de todo o mundo. Em linhas gerais, as empresas ao adotar esse tipo de tecnologia, esperam resolver questões intrínsecas ao padrão antigo de rede, melhorando a eficiência, a confiabilidade, a economia e a sustentabilidade dos serviços de eletricidade (Garcia, 2012).

A implantação das tecnologias de rede inteligente implicará na reformulação da indústria de serviços do setor elétrico. Não obstante o termo comumente referir-se à infraestrutura técnica, a sua aplicação é ampla envolvendo conceitos de tecnologia da informação (TI) que visam integrar sistemas de comunicação e infraestrutura de rede à infraestrutura da rede elétrica como um todo.

3.1.
Redes inteligentes: experiências relevantes

No contexto global, notadamente na Europa, as redes inteligentes estão sendo utilizadas para obter uma matriz energética compatível com as metas de emissão de poluentes e aprimorar ações de eficiência energética.

No que concerne o uso das redes inteligentes, a Europa se destaca pela sua aplicação em estágio avançado. O Plano 20-20-20[3] europeu tem por objetivo impulsionar ações de eficiência energética baseadas nas tecnologias de redes inteligentes em todo o continente. A Alemanha tem feito ambiciosos estudos no sentido de expandir a energia renovável a 100% da matriz até 2050. Desde já, tem incentivado o desenvolvimento de projetos em duas frentes: a microgeração distribuída e a redução de consumo (DECC, 2009).

O Reino Unido pretende reduzir em 80% as emissões de CO2 até 2050. Para alcançar esta meta, o governo vem promovendo diversas ações, dentre as quais está prevista a substituição de 53 milhões de medidores de gás e

[3] O plano da União Européia 20-20-20 estabelece objetivos para 2020 de melhoria da eficiência energética em 20%, reduzindo as emissões de CO2 em 20% e aumentando as fontes de energia renováveis para 20% das fontes de energia.

eletricidade até o final de 2019. Segundo as últimas estimativas do governo, o projeto tem um custo estimado de R$ 32 bilhões e promoverá uma economia anual média de R$ 67 por consumidor (DECC, 2009).

Nos Estados Unidos, as iniciativas estaduais isoladas foram impulsionadas pelo pacote federal de US$ 4,5 bilhões, que prevê o financiamento de 50% dos projetos de implantação de redes inteligentes. O ousado plano tem contribuído com um investimento da ordem de US$ 330 milhões alocando recursos em 11 projetos, em sua maioria no estado do Texas, cujos investimentos totalizam cerca de US$ 850 milhões (Zpryme, 2011).

A Figura 2.1 ilustra os principais projetos de redes inteligentes que estão sendo desenvolvidos ao redor do mundo.

Figura 3.1 - Projetos de *smart grid* no mundo (2012).
Fonte: Google Maps.

Em termos de investimento, a China apresenta-se como líder mundial no desenvolvimento de projetos de redes inteligentes. Os dados de 2012 assim se apresentam: China (US$ 7,32 bilhões); EUA (US$ 7,09 bilhões); Japão (US$ 849 milhões) e Coreia do Sul (US$ 824 milhões). A Europa, representada pela Espanha, aparece em quinta posição no investimento (US$ 807 milhões) (Zpryme, 2011). A Figura 2.2 ilustra os investimentos realizados por alguns países na tecnologia de redes inteligentes.

Figura 2.2 - principais países investidores em tecnologias de *smart grid*.
Fonte: Smartgridnews, 2012.

3.2.
Desenvolvimento e difusão da tecnologia em nível mundial

A despeito de a indústria reconhecer que existem incertezas associadas à evolução e difusão das redes inteligentes, as principais concessionárias do mundo estão desenvolvendo projetos para implantação dessas redes. Esses projetos refletem desenvolvimentos em grande escala ou projetos pilotos. No que concerne os projetos piloto, a prioridade sinaliza tecnologias candidatas que visam compreender os aspectos construtivos, evolutivos e operacionais das redes inteligentes (ABDI, 2012).

De acordo com a Agência Brasileira de Desenvolvimento Industrial (ABDI), as iniciativas observadas em alguns países europeus (e.g.: Reino Unido, França e Espanha), somam mais de 100 milhões de medidores. O Quadro 2.1 apresenta as principais iniciativas na implantação das redes inteligentes ao redor do mundo são:

Quadro 2.1 - Principais iniciativas de implantação de redes inteligentes no mundo.

País	Iniciativa
China	Desde 2010, a estatal chinesa *State Grid Corporation* of China (SGCC) iniciou um programa piloto voltado para o planejamento da implantação das redes até 2030. A partir de 2011, a implantação de medidores inteligentes ganha foco e os editais iniciais devem somar mais de 40 milhões de medidores, muitos deles com telemedição por meio da tecnologia PLC.
Estados Unidos	Desde 2009, os EUA destinaram cerca de U$ 4,5 bilhões para modernização das redes elétricas por meio do *American Recovery Reinvestment Act* dos quais, mais de U$ 600 milhões são para provas de demonstração. Estados que lideram as iniciativas são: Texas e Califórnia.
Japão	O programa das companhias elétricas japonesas prevê o desenvolvimento de redes do tipo *smart grid* que contemplem a geração de energia solar, até 2020, cujos investimentos governamentais superam U$ 100 milhões. Outras iniciativas são voltadas para o desenvolvimento de medidores inteligentes.
Coreia do Sul	O governo sul-coreano lançou, em conjunto com a indústria, programa piloto de U$ 65 milhões, voltado para a integração de geradores de energia eólica, linhas de distribuição e de 6000 residências na ilha de Jeju. O programa prevê implantação em nível nacional até 2030.
Espanha	Desde 2008, o governo espanhol estabeleceu a substituição dos medidores convencionais por medidores inteligentes, sem qualquer custo para o consumidor final. As distribuidoras Endesa e Iberdrola preveem juntas a implantação de mais de 23 milhões de medidores até 2015.
Alemanha	O programa nacional E-Energy possui diversos projetos com enfoque nas TICs aplicadas ao sistema energético alemão.
Austrália	Desde 2009, o governo australiano destinou U$ 100 milhões de dólares australianos, em iniciativa denominada "*Smart City*", voltada para piloto de demonstração em escala comercial.
Reino Unido	O órgão regulador OFGEM tem uma iniciativa denominada zona de energia registrada voltada 16 Relatório de Acompanhamento Setorial para estimular o desenvolvimento e implementação de soluções inovadoras para conectar geradores distribuídos à rede das empresas distribuidoras. Os recursos proveem do fundo para baixa emissão de carbono que destinará até £$ 500 milhões de libras para projetos que testem, operem e comercializem novas tecnologias.
França	Atualmente, a empresa de distribuição ERDF está implantando 300 mil medidores inteligentes em projetos piloto, utilizando protocolo de comunicação denominado Linky, já homologado pelo órgão regulador francês e operado por subsidiária da ERDF, denominada EDF. O sucesso da iniciativa determinará a utilização do protocolo na substituição de 35 milhões de medidores até 2016.
Itália	Em 2011, o órgão regulador italiano *Autorità per l'Energia Elettrica ed il Gas* aprovou oito projetos para a modernização do sistema de distribuição de média tensão, a serem financiados pelas tarifas de uso de energia, voltados para demonstrar o gerenciamento e a automação das soluções de integração do sistema, em escala comercial.

Fonte: ABDI, 2012.

3.3.
Redes inteligentes: o novo paradigma brasileiro do setor

As concessionárias e os clientes do setor elétrico brasileiro foram recentemente expostos a uma singular oportunidade de evoluir e encontrar soluções práticas que sejam capazes de refletir suas realidades e necessidades. Eficiência operacional, novas fontes de energia, menor emissão de carbono, tarifas mais ajustadas e maior participação do consumidor são somente algumas questões que se apresentam como desafios a serem vencidos por essa indústria brasileira de energia elétrica (CPqD, 2012).

O setor elétrico brasileiro possui características que o torna único no cenário mundial. A matriz energética brasileira é baseada principalmente em energias renováveis. O nível de integração das usinas e da infraestrutura para o transporte da energia, por exemplo, atingiu patamares continentais ainda não alcançados por países da Europa e pelos Estados Unidos. No Brasil, a interconexão dos sistemas representa um melhor balanceamento, mantendo certo nível de segurança da oferta de energia. A questão principal é que quanto mais pontos de interconexão, mais complexidade se evidencia no gerenciamento do sistema.

O contexto imposto pelas redes inteligentes é promissor em possibilidades tecnológicas enquanto a modernização do setor de energia oferece desafios e oportunidades. Se por um lado o uso das redes inteligentes impõe desafios à concessionária, por outro propicia benefícios para os consumidores. A nova realidade propiciada pelas redes inteligentes deve transformar o setor elétrico brasileiro em uma rede moderna e adaptada aos tempos atuais. Certamente passará a interferir na forma segundo a qual às concessionárias passarão a disponibilizar a energia e os consumidores dela fazerem um uso adequado e inteligente. De acordo com o CPqD (2012), no Brasil, as principais iniciativas dessa evolução estão focadas na implantação dos medidores eletrônicos de energia. Medidores esses que deverão ser capazes de permitir, no curto prazo, exercitar novas modalidades tarifárias e novos comportamentos de consumo.

Há consenso de que o os avanços do setor brasileiro de energia e o crescimento da economia nacional dependem dos avanços na sua infraestrutura de energia. E, por ser o nono maior consumidor de energia do mundo e o terceiro maior no hemisfério ocidental, perdendo apenas para EUA e Canadá, o Brasil já se mostra pressionado a modernizar sua infraestrutura (Zpryme, 2011).

Este fato deve-se, principalmente, à crescente demanda de energia elétrica, que aumenta a uma taxa acima da média mundial.

3.3.1.
Desafios e oportunidades para o Brasil

Seguindo o exemplo de outros países, o setor elétrico brasileiro está se definindo como um mercado potencial para a introdução de tecnologias de redes inteligentes. Preveem-se investimentos públicos e privados da ordem de alguns bilhões de dólares. Entretanto, a possibilidade de esses investimentos se concretizarem nos próximos anos está condicionada à superação de alguns desafios.

O organismo regulador brasileiro destaca em documento oficial do setor (Aneel, 2012) resultados da audiência pública que trata dos requisitos mínimos para implantação das redes inteligentes no Brasil. Esta publicação destaca que a diversidade do País constitui-se na sua característica mais marcante. Cada uma das 63 concessionárias de distribuição opera com realidades distintas e, para muitas das situações existentes, as diferenças ocorrem dentro da mesma área de concessão.

Outro desafio imposto pelo contexto brasileiro recai sobre os valores médios dos indicadores de continuidade na entrega da energia elétrica. Para este tema, percebe-se uma estagnação na melhoria da qualidade dos serviços de distribuição de energia. Problema que pode ser minimizado com a implantação das redes inteligentes. A sua adoção — solução técnica adequada para a detecção de falhas de forma mais rápida e precisa — permite a realização de manobras eficientes para isolar problemas de interrupção do fornecimento de energia (*self-healing*[4]).

A opção pelo uso de redes inteligentes no País, a exemplo do que ocorre na maioria dos países em desenvolvimento, justifica-se pelo aumento da demanda por energia, tendência crescente nesses últimos anos. Não obstante este aumento da demanda cabe observar que o consumo de energia *per capita* no Brasil ainda é expressivamente inferior àquele registrado em países desenvolvidos. Assim, no contexto da perspectiva brasileira, as redes inteligentes não visam conter o aumento de consumo a exemplo da experiência

[4] *Self-Healing* - ferramenta que atua como uma reconfiguração automática do sistema elétrico. Em caso de falta de energia, um sensor de tensão detecta a interrupção e envia informações ao sistema de gerenciamento da distribuição da companhia, que irá identificar outra possibilidade para restabelecer a eletricidade.

européia, mas racionalizar o atendimento da crescente demanda levando em conta a modicidade tarifária[5]. Esta se torna uma proposição factível quando se considera a aplicação de tarifas horárias em baixa tensão e a adoção de programas mais ousados de eficiência energética, iniciativas que se viabilizam pela adoção da tecnologia de redes inteligentes. A introdução de sensores em toda a rede e a sua automação certamente oferece maior segurança à ocorrência de apagões.

De acordo com a Empresa de Pesquisa Energética (EPE) — órgão de assessoria permanente do governo brasileiro para o setor de energia elétrica— a preocupação com a segurança cresce à medida que se espera uma expansão média do consumo de energia elétrica em torno de 4% ao ano (EPE, 2007). Esta previsão da EPE, documentada no Plano Nacional de Energia 2030, reflete a perspectiva de evolução do consumo de energia no País. Constata-se, assim, que as redes inteligentes podem representar o futuro da prestação de serviços de distribuição de energia elétrica no Brasil. Nas regiões onde a tecnologia está mais disseminada, notadamente na Europa, ela se apresenta como solução para modernização do sistema elétrico, de forma mais limpa e eficiente.

Não obstante o já estar consagrado no Brasil o conceito de redes inteligentes (inclusive a referência à denominação *smart grid*), o seu uso tem sido direcionado na perspectiva do equacionamento de problemas recorrentes do setor elétrico brasileiro. Com uma matriz energética limpa, custos operacionais relativamente baixos e reduzidos consumo energético (quanto comparado ao de países desenvolvidos), a prioridade do uso das redes inteligentes ainda não visa a preocupante redução de emissão de CO_2 ou a redução do consumo de energia elétrica. Entretanto, na perspectiva dos anseios da sociedade, o que deve motivar a adoção de redes inteligentes são serviços de melhor qualidade, transparência na tarifação e redução de perdas comerciais.

Dentre as razões que motivaram países da Europa e os Estados Unidos a implantar redes inteligentes destacam-se:

- redução da emissão de gases poluentes, com vistas à obtenção da sustentabilidade ambiental;

[5] **Modicidade tarifária** - busca -se o estabelecimento de tarifa justa a ser cobrada dos clientes do serviço monopolista de distribuição de energia elétrica. Para isso, o Regulador leva em consideração, dentre outros, dois componentes fundamentais: os custos operacionais vinculados à operação e manutenção dos ativos necessários para a prestação do serviço, gestão comercial dos clientes, direção e administração da empresa; a remuneração dos ativos efetivamente necessários para a prestação do serviço, com níveis de qualidade de modo a assegurar e sustentar adequadamente atividade econômica do negócio.

- redução do consumo de energia elétrica pelo uso da eficiência energética e da racionalização;
- redução de custos operacionais visando a eficiência econômica.

Razões essas que não refletem as motivações que levam as concessionárias brasileiras a fazerem uso de redes inteligentes. Segundo Alcântara (2012), o setor elétrico brasileiro assim justifica a sua opção pelas redes inteligentes:

- **O fator apagão** — O Brasil se apresenta como líder mundial em apagões, sendo que das seis maiores ocorrências registradas no mundo desde 1965, três são do Brasil. São elas: (i) em 11 de março de 1999 (97 milhões de pessoas sem energia); (ii) em 10 de novembro de 2009 (atingindo 60 milhões de consumidores) e (iii) em 03 de fevereiro de 2011 (interrompendo o abastecimento de energia elétrica de 53 milhões de usuários). O uso de uma rede inteligente aumentaria a segurança do setor elétrico brasileiro com a minimização de apagões (blecautes), automatização de equipamentos e sistemas de rede e sensoriamento de toda a rede.
- **O fator continuidade de abastecimento** — Elevados valores dos indicadores de continuidade no Brasil, hoje estimado (na média) em 18h de interrupção anual no fornecimento de energia. Uma rede inteligente aumentaria a qualidade do serviço de fornecimento de energia elétrica.
- **O fator consumo** — De acordo Agência Brasileira de Desenvolvimento Industrial (ABDI, 2012), a Aneel estima uma redução de cerca de 10% no consumo de energia no Brasil com a utilização de sistemas de rede inteligente (*smart grid*). Atualmente, as perdas totais (técnica e não técnica) de energia elétrica no Brasil são da ordem de 11,2% (valor médio). Com a introdução de sistemas de redes inteligentes estima-se um ganho de eficiência energética na distribuição e consumo de energia, iniciativa que reduzirá os elevados níveis de perdas técnicas e não técnicas.

Assim, o tema redes inteligentes deve ser avaliado na perspectiva das razões que motivam o seu uso. No caso do Brasil, a motivação recai no elevado grau de diversidade e nas particularidades de natureza elétrica e sócio-econômica do seu setor elétrico. Deve-se também levar em conta que o tema é novo no Brasil e que a literatura brasileira ainda é incipiente sobre o tema. Estudos acadêmicos e um considerável número de projetos-piloto em desenvolvimento pelas concessionárias do país certamente contribuirão para o planejamento das redes inteligentes no País.

Deve-se, portanto, incentivar estudos sobre o tema, assim assegurando um nível mínimo de padronização que seja capaz de evitar a estagnação do setor elétrico brasileiro e sua flexibilização. E assegurando, sempre que possível, as ações regionalizadas de melhoria.

3.3.2.
Difusão de uso do *smart grid* no Brasil: principais iniciativas

No Brasil, quer no ambiente empresarial quer no técnico-científico, o interesse pelas tecnologias de redes inteligentes tem aumentado de forma expressiva. De acordo com o relatório de acompanhamento setorial da Agência Brasileira de Desenvolvimento Industrial (ABDI), o Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) reconhece atualmente 08 grupos de pesquisa ativos e com projetos de redes inteligentes: Universidade Federal do Rio de Janeiro (UFRJ) (02), Centro Federal de Educação Tecnológica Celso Suckow da Fonseca (CEFET/RJ), Universidade Federal Fluminense (UFF), Universidade Federal do Rio Grande do Sul (UFRGS), Universidade Federal de Juiz de Fora (UFJF), Instituto Federal Mato Grosso (IFMT) e Mackenzie (ABDI, 2012). Adicionalmente, são reconhecidos os avanços alcançados pela Universidade de São Paulo (USP) e CPqD. Estas duas instituições constam entre as principais executoras de projetos do programa de Pesquisa & Desenvolvimento (P&D) regulado pela Agência Nacional de Energia Elétrica (ANEEL).

Em 2011, existiam 752 projetos de P&D cadastrados na base da Aneel. Deste total, 52 projetos tinham por objetivo avaliar os principais aspectos da implantação das redes inteligentes, entretanto nenhum destes projetos estava voltado à questão da segurança da informação. Os investimentos previstos totalizavam cerca de R$ 150 milhões, distribuídos conforme o gráfico abaixo. A Figura 2.3 ilustra a distribuição de projetos de pesquisa dentro do programa de P&D da Aneel.

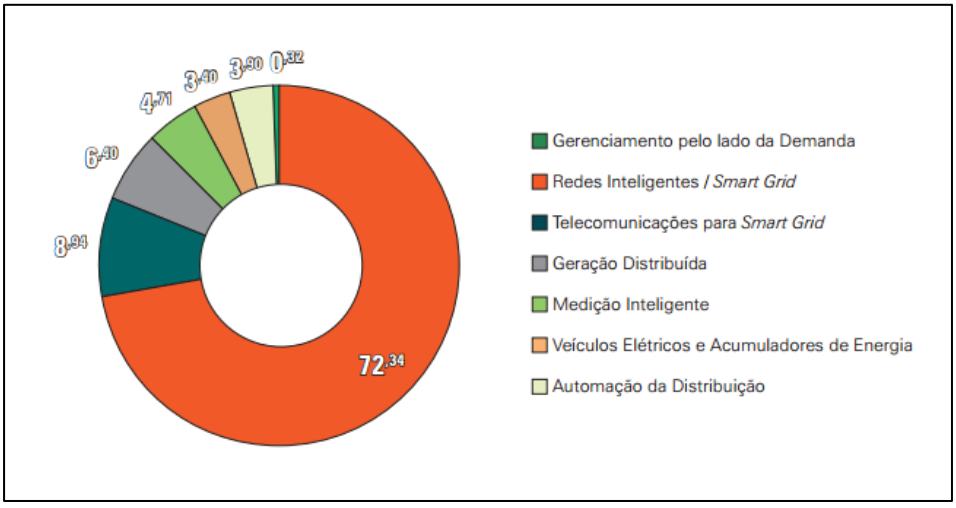

Figura 2.3 - Temas de P&D de projetos *Smart grid* (em %).
Fonte: ABDI (2012).

O Quadro 2.2 abaixo apresenta os principais projetos em desenvolvimento pelas concessionárias brasileiras de energia elétrica:

Quadro 2.2 - Empresas e seus respectivos projetos de redes inteligentes.

Empresa	Projeto
LIGHT	Baseado em diferentes modelos, o sistema de medição inteligente da Light foi desenvolvido em parceria com o fabricante de medidores CAS Tecnologia. Este sistema está em conformidade com as regulamentações da ANEEL e refere-se aos requisitos mínimos dos medidores. A estrutura tarifária encontra-se em fase de publicação. Preparado para funcionamento bi-direcional, o sistema possui capacidade para enviar e receber mensagens de outros dispositivos (medidor de água e gás, *smart appliances* etc.).
CEMIG	A Cemig iniciou o seu projeto de redes inteligentes denominado CIDADES DO FUTURO no município de Sete Lagoas (MG), envolvendo consumidores de todas as categorias. O projeto engloba desde a implantação de medidores inteligentes até a utilização de veículos elétricos, passando pela automação das redes, pela geração distribuída, implantação da infraestrutura de telecomunicações e de sensores, ferramentas de gerenciamento pelo lado da demanda (DSM) e de relacionamento com consumidores/parceiros. Observação: Juntas, Light e CEMIG pretendem investir R$ 65 milhões nos próximos três anos em temas de redes inteligentes, desde medidores eletrônicos até geração distribuída.
ELETROBRAS	Projeto com escopo amplo realizado no município de Parintins (AM), que visa a construção de um modelo de referência para aplicação em larga escala das tecnologias de redes inteligentes no mercado-alvo das empresas distribuidoras do grupo. O projeto prevê a implantação de 15 mil medidores inteligentes. Engloba outros aspectos, dentre eles: a automação das redes, a geração distribuída, a infraestrutura de telecomunicações e de sensores e as ferramentas de gerenciamento pelo lado da demanda (DSM) e de relacionamento com consumidores e parceiros. Tais ferramentas são voltadas para monitorar o perfil de uso e ampliar a interação com os clientes da empresa.
AMPLA	Projeto denominado CIDADE INTELIGENTE no município de Búzios (RJ), englobando Medição Inteligente, Telecomunicação, Automação, Geração Distribuída e Armazenamento, Prédio Inteligente e Veículos Elétricos. A abrangência do projeto envolverá a instalação de 10 mil medidores inteligentes e automação de 25 pontos da rede de média tensão.
COELCE	Projeto implantando no município de Aquiraz (CE) que consiste em um Sistema de Reposição Automática (SRA) e em um Sistema Inteligente para Mudança Automática de Ajuste do Sistema de Proteção (SIAP) na rede de média tensão.
CPFL	Projeto piloto no município de Morungaba (SP), que visa à automação da rede. Tem por objetivo o controle e a automação de subestações, com a inserção de equipamentos monitorados para manutenção, proteção, qualimetria e controle, conectados aos seus respectivos centros de gestão remota.
CELG	Projeto para avaliar diferentes plataformas de telecomunicações — tecnologia de redes cabeadas (modems ópticos, xDSL e PLC), tecnologias de rádio fixo (Ponto a Ponto, Ponto-Multiponto e Mesh) e tecnologias de rádio móvel (GPRS, 3G)— voltadas para a supervisão das redes de média e baixa tensão.

Empresa	Projeto
CEEE	Projeto-piloto para avaliar o desempenho da tecnologia PLC no monitoramento de consumo, parametrização e diagnóstico da rede elétrica de distribuição em baixa tensão.
BANDEIRANTE	Prevê-se a realização de projeto-piloto no município de Aparecida (SP) com o objetivo de implantar (i) um sistema completo de medição inteligente, nas unidades consumidoras e (ii) medidores em todos os alimentadores de média tensão e em todas as estações transformadoras.

Fonte: ABDI, 2012.

3.4.
Uma tecnologia para combate a perdas não técnicas

Uma questão já está clara para todos: a motivação brasileira para o uso de redes inteligentes é distinta daquela de outros países. Além de contribuir para a melhoria da qualidade do serviço prestado ao consumidor final, as redes inteligentes visam melhorar a confiabilidade do sistema elétrico nacional e reduzir os desperdícios. E mais, deverão contribuir para a redução das perdas não técnicas, notadamente expressivo furto de energia. Compete à Aneel contabilizar o nível dessas perdas no Brasil, hoje estimadas em cerca de 9% da energia total produzida; i.e.: equivale à produção futura Usina Hidrelétrica de Santo Antônio, no Rio Madeira (Aneel, 2010). A Figura 2.4 ilustra os percentuais de perdas técnicas e não-técnicas no território brasileiro.

Figura 2.4 - Perdas técnicas e não-técnicas por região.
Fonte: Aneel (2012).

Nos últimos anos, algumas distribuidoras desenvolveram projetos para substituição de medidores eletromecânicos por eletrônicos nas suas respectivas áreas de concessão. Basicamente, o retorno do investimento se deu em função da redução de perdas não técnicas e da melhoria da eficiência na medição do consumo de energia elétrica.

Até recentemente, a indefinição regulatória das funcionalidades mínimas dos medidores eletrônicos, levou as distribuidoras a apenas instalar equipamentos com funções mínimas para atender problemas relacionados tão somente ao furto de energia.

A regularização de um consumidor fraudador tem dois efeitos importantes: a *eficientização* do consumo e a desoneração dos demais consumidores, uma vez que estes pagam pela energia que é furtada por terceiros. Consequentemente, ações de combate às perdas têm importância econômica não somente para as concessionárias, mas, também, para a sociedade como um todo. Os sistemas avançados de medição têm como proposta dificultar o furto de energia na medida em que permitem sua detecção de forma mais rápida. Esses medidores são menos vulneráveis que os sistemas convencionais.

3.5. Desafios regulatórios à implantação de redes inteligentes no País

As agências reguladoras são os principais responsáveis pelo bom funcionamento do mercado de energia elétrica, o que beneficia todos os usuários da rede. Ao analisar o benefício global obtido pela implantação dos projetos de redes inteligentes para os usuários da rede, as agências se esforçam para definir uma abordagem centrada no usuário (Brekke, 2010).

A Aneel reconhece que existe uma tendência mundial de substituição da infraestrutura atual do sistema de energia elétrica por uma configuração que faça uso intensivo das recentes tecnologias de informação e comunicação (Aneel, 2009). Essa transformação proporcionará mudanças significativas na forma de relacionamento entre o órgão regulador e as concessionárias de energia elétrica e entre esta e seus consumidores (Leite, 2012). Por isso, não há dúvida que há grande interesse da agência reguladora nas questões decorrentes deste processo.

A Aneel tem desempenhado um papel relevante na condução de estudos sobre este tema, visando à publicação de regulamentos diretamente relacionados à implantação das redes inteligentes no Brasil.

Está claro para todos os atores do setor elétrico que as concessionárias de energia elétrica serão os principais motores da implantação dessa revolucionária tecnologia de redes inteligentes. Entretanto, o papel da agência reguladora configura-se como fundamental para que os benefícios das redes inteligentes sejam percebidos pelos consumidores brasileiros.

Uma das iniciativas da Aneel está relacionada com o desenvolvimento de um programa de P&D estratégico (Alcântara, 2012) com o intuito de desenvolver um Plano Nacional para Redes inteligentes. O estudo abordou sete temas relacionados às redes inteligentes:

- automação de subestações e redes elétricas;
- medição inteligente;
- comunicação de dados;
- tecnologia da informação voltada ao setor elétrico;
- veículos elétricos;
- geração distribuída;
- formulação de políticas públicas.

Nesse estudo, a Aneel realiza um diagnóstico do estado tecnológico das redes de distribuição no Brasil e traça um roteiro para se alcançar uma nova realidade de redes inteligentes no País.

Desde o início dos estudos, a Aneel concentrou os esforços na definição dos requisitos mínimos dos medidores inteligentes que gradativamente vem sendo implantados no Brasil por meio de projetos pilotos. A Aneel promoveu reuniões com fabricantes de medidores e sua associação, provedores de tecnologia de informação e telecomunicações, distribuidoras Instituto Nacional de Metrologia, Qualidade e Tecnologia (INMETRO), envolvendo outros agentes interessados no tema. Nesses encontros foram abordados aspectos relacionados à implantação dessa tecnologia no País e à regulamentação metrológica requerida.

Como se pode perceber, a Aneel tem percorrido um longo caminho de estudos e debates com os maiores especialistas do tema ao longo de quatro anos de intenso trabalho. Além das consultas públicas, que criaram oportunidades para que os agentes envolvidos pudessem opinar, a agência reguladora analisou iniciativas bem sucedidas realizadas em outros países (Aneel, 2012). O Quadro 2.3 apresenta as principais iniciativas da Aneel nos últimos anos, com objetivo de definir os requisitos mínimos para implantação de redes inteligentes no Brasil.

Quadro 2.3 - Principais eventos para definição dos requisitos mínimos dos medidores inteligentes.

ANO	EVENTO
2008	Em setembro de 2008, a ANEEL realizou em Brasília o "Seminário Internacional sobre Medição Eletrônica", estimulando a discussão sobre implantação de medição eletrônica em unidades consumidoras de baixa tensão, sobre abordagem regulatória, funcionalidades agregadas e experiências de implantação. Além de integrantes de empresas e associações do Setor Elétrico brasileiro, participaram do evento palestrantes internacionais da Itália, da Espanha e do Canadá. Foram discutidas as experiências desses países no uso da tecnologia *smart grid* e na substituição dos equipamentos e sua regulamentação.
2009	Na sequência, foi instaurada pela Superintendência de Regulação dos Serviços de Distribuição (SRD) a Consulta Pública 15/2009 para orientar as discussões a respeito do tema. Em abril de 2009, foi realizada, por servidores da Agência, missão técnica a Portugal, Espanha e Itália para conhecer e acompanhar as experiências desses países na implantação em grande escala da medição inteligente. Em setembro de 2009, foi realizada missão técnica para conhecer a experiência norte-americana na implantação da medição inteligente. Foram visitadas instituições com *know how* em medição eletrônica e redes inteligentes Em setembro de 2009, foi efetuada audiência para o público interno da ANEEL (API 3/2009), momento em que foi possível obter contribuições de diferentes áreas. Registra-se a participação da ANEEL no Grupo de Trabalho instituído pelo Ministério de Minas e Energia (MME) com o intuito de "[...] analisar e identificar ações necessárias para subsidiar o estabelecimento de políticas públicas para a implantação de um Programa Brasileiro de Rede Elétrica Inteligente (*smart grid)*". Além de integrantes da ANEEL, o Grupo de Trabalho era constituído por representantes da Empresa de Pesquisa Energética (EPE), do Centro de Pesquisas de Energia Elétrica (Eletrobrás) Cepel e do Operador Nacional do Sistema Elétrico (ONS).
2010	Já durante a AP 43/2010, a ANEEL recebeu pouco mais de 200 contribuições enviadas por consumidores e conselhos de consumidores, indústrias de tecnologia, distribuidoras de energia, entidades do Setor Elétrico e de defesa do consumidor, associações ligadas ao Setor, entre outras. Ou seja, se existe um tema que tenha exigido estudos e interação com a sociedade, o desta regulamentação pode ser citado como exemplo.
2011	Encerramento do prazo para recebimento de contribuições, com sessão presencial realizada em Brasília em 26 de janeiro de 2011. Ao fim desse período, a ANEEL recebeu 212 contribuições de 57 agentes, com sugestões de consumidores, consultores, distribuidoras, fabricantes de medidores, associações setoriais entre outros. Na Sessão presencial foram realizadas 19 exposições orais com apresentação de comentários e contribuições.
2012	Resultados da Audiência Pública nº 43/2010, que objetivou obter subsídios e informações adicionais para o estabelecimento de resolução normativa sobre os requisitos mínimos para os medidores eletrônicos de unidades consumidoras de baixa tensão.

A Aneel, desde 2008, tem atuado no sentido de viabilizar a implantação das redes inteligentes no Brasil, objetivando desenvolver uma rede de distribuição com mais funcionalidades e, consequentemente, mais benefícios para os consumidores. Com esse objetivo, a Aneel vem trabalhando no sentido

de estabelecer uma regulação necessária para a implantação das redes inteligentes no País. Cabe ressaltar que o programa ainda prioriza questões relacionadas aos medidores inteligentes de energia, uma vez que, nas redes inteligentes, ele é o elo de comunicação entre a empresa de energia e o consumidor.

O Brasil é um país de grandes dimensões e diversidade, onde realidades distintas convivem. Provavelmente, esta característica trará grandes desafios para os projetos de implantação das redes inteligentes. Em algumas regiões, a implantação da tecnologia de redes inteligentes será necessária para melhorar a qualidade do fornecimento. Mas em outras, a própria universalização do serviço ainda será um grande desafio.

4
O papel das normas nas redes inteligentes

A norma é um documento de caráter voluntário, normalmente produzido por um órgão oficialmente reconhecido e acreditado para tal, que estabelece regras, diretrizes, ou características sobre materiais, produtos ou serviços. Via de regra, cada país possui o seu organismo nacional de normalização. Compete a esses organismos nacionais de representar os interesses em normalização de seus países junto aos foros internacionais (e.g.: ISO, IEC, ITU) e regionais (e.g.: COPANT (Comissão Pan-Americana de Normas Técnicas), para as Américas; CEN (Comitê Europeu de Normalização), para a Europa) de normalização.

No âmbito global, compete às organizações internacionais de normalização articular e coordenar o diálogo entre as várias entidades nacionais de normatização. Como estratégia de implantação de um sistema compatível e harmonizado de normalização entre países com interesses econômicos comuns, cada vez mais os países priorizam a normalização internacional antes de considerarem a alternativa de introduzir uma norma nacional. Ao participar da elaboração de uma norma internacional e somente então adotá-la como norma nacional assegura equivalência e contribui para a harmonização dos sistemas normativos.

4.1.
Normalização

A normalização é a maneira de organizar atividades pela criação e utilização de regras e normas, elaboração, publicação e promoção de seu emprego visando assim contribuir para o desenvolvimento econômico e social de uma Nação (ABNT, 2012). As Normas estabelecem soluções para problemas de caráter repetitivo, existentes ou potenciais. Em conformidade aos preceitos da normalização, as normas objetivam:

- **Economia**: Proporcionar a redução da crescente variedade de produtos e procedimentos;
- **Comunicação**: Proporcionar meios mais eficientes na troca de informação entre o fabricante e o cliente;
- **Segurança**: Proteger a vida humana e a saúde;

- **Proteção do Consumidor**: Prover a sociedade de meios eficazes para aferir a qualidade dos produtos;
- **Eliminação de Barreiras Técnicas e Comerciais:** Evitar a existência de regulamentos conflitantes sobre produtos e serviços em diferentes países.

Amplamente disseminado pela Confederação Nacional da Indústria junto ao setor produtivo (CNI, 2002), tem-se a seguinte definição internacionalmente consagrada de normalização:

"Processo de formulação e aplicação de regras para um tratamento ordenado de uma atividade específica, para o benefício e com a cooperação de todos os interessados e, em particular, para a promoção da economia global ótima, levando na devida conta condições funcionais e requisitos de segurança."

A normalização é utilizada cada vez mais como um meio para se alcançar a redução de custo da produção e do produto final, mantendo ou melhorando sua qualidade.

O papel das normas é o de um facilitador técnico e um canal para a expressão do conhecimento coletivo sobre uma questão específica. Isto está longe de garantir que as etapas concretas necessárias serão de fato realizadas, ou que o desafio da energia será efetivamente resolvido (IEC, 2010).

O Quadro 4.1 apresenta, de acordo com, as principais razões para se utilizar normas.

Quadro 4.1 – Principais razões para se utilizar normas

Razão	Descrição
Melhorar produtos ou serviços	A aplicação de uma norma pode conduzir a uma melhora na qualidade de seus produtos ou serviços. Resultando, certamente no aumento das vendas. Alta qualidade é sempre uma poderosa proposta de venda. Consumidores são raramente tentados a comprar mercadorias de qualidade questionável. Além disso, agregar qualidade a seu produto ou serviço aumenta o nível de satisfação dos consumidores e é uma das melhores formas de mantê-los.
Atrair novos consumidores	Gerar a correta percepção de seu negócio e seus produtos ou serviços é vital quando você quer atrair novos consumidores. As normas são um caminho efetivo para convencer potenciais consumidores de que você atende aos mais altos e amplamente respeitados níveis de qualidade, segurança e confiabilidade.
Aumentar sua margem de competitividade	O atendimento às normas aumentará sua reputação de ter um negócio comprometido com a busca por excelência. Isto pode lhe dar uma importante vantagem sobre os seus concorrentes que não aplicam as normas – Auxiliando inclusive no ganho de concorrências. Além do que, muitos consumidores em certos setores só comprarão de fornecedores que podem demonstrar conformidade com determinadas normas.
Agregar confiança ao seu negócio	Acreditar na qualidade de seus produtos ou serviços é provavelmente uma das **razões chave** da existência de consumidores para esses

Razão	Descrição
	produtos ou serviços. Quando o consumidor descobre que normas são utilizadas, há o aumento da confiança em produtos ou serviços. Além do que, a utilização de certas normas (por exemplo, ABNT NBR ISO 14001) impacta positivamente na sua imagem.
Diminuir a possibilidade de erros	Seguir uma norma técnica implica em atender a especificações que foram analisadas e ensaiadas por especialistas. Isso significa que você terá, provavelmente, menos gasto de tempo e dinheiro com produtos que não tenham a qualidade e desempenho desejáveis.
Reduzir custos de negócio	A utilização de uma norma pode reduzir suas despesas em pesquisas e em desenvolvimento, bem como reduzir a necessidade de desenvolver peças ou ferramentas já disponíveis. Além disto, a utilização de uma norma de sistema de gestão pode permitir a dinamização de suas operações, tornando seu negócio muito mais eficiente e rentável.
Tornar produtos compatíveis	Aplicando as normas pertinentes, pode-se assegurar que seus produtos ou serviços são compatíveis com aqueles fabricados ou fornecidos por outros. Essa é uma das mais efetivas formas de ampliar o seu mercado, em particular o de exportação.
Atender a regulamentos técnicos	Diferentemente dos regulamentos técnicos, as normas são voluntárias. Não há obrigatoriedade em adotá-las. Entretanto, o atendimento a estas pode auxiliá-lo no cumprimento das suas obrigações legais relativas a determinados assuntos como segurança do produto e proteção ambiental. Haverá impossibilidade de vender seus produtos em alguns mercados a menos que estes atendam certos critérios de qualidade e segurança. Estar em conformidade com normas pode poupar tempo, esforço e despesas, lhe dando a tranquilidade de estar de acordo com suas responsabilidades legais.
Facilitar a exportação de seus produtos	A garantia de que seus produtos atendem a normas, facilita a sua entrada no mercado externo, devido á confiança gerada pela utilização de normas.
Aumentar chances de sucesso	Normas constituem parte de sua estratégia de marketing. Conferem ao produto oportunidade de sucesso. Isto porque – através de sua natureza colaborativa - a normalização auxilia na construção do conhecimento das necessidades de mercado e dos consumidores. Iniciativas de negócios em mercados que utilizam normas reconhecidas possuem maiores chances de sucesso.

Fonte: ABNT, 2012.

A normalização fundamenta-se em princípios, considerados estratégicos para que seus objetivos sejam atendidos, sua aplicação seja eficaz e o seu reconhecimento reconhecido por todos. Estes princípios norteiam a normalização no mundo (CNI, 2002). São eles:

- **Voluntariedade** – participar do processo de normalização não é obrigatório, mas sim uma decisão voluntária dos interessados. A vontade das partes envolvidas é fundamental para que o processo de normalização se estabeleça e aconteça, e deve ser aberto à participação dos interessados.
- **Representatividade** – É preciso que haja participação dos produtores, consumidores e de outras partes interessadas (universidades, laboratórios, institutos de pesquisa, governo), de modo que a opinião de todos seja considerada no estabelecimento da norma e que ela reflita de fato o entendimento comum.

- **Paridade** – Não basta apenas a representatividade, é preciso que as classes (produtor, consumidor e neutro) estejam equilibradas, evitando-se assim a imposição de uma delas sobre as demais por conta do número maior de representantes.
- **Consenso** – Processo pelo qual um texto é submetido à apreciação, comentários e aprovação de uma comunidade, técnica ou não, a fim de que se obtenha um texto o mais próximo possível da realidade de aplicação.
- **Atualização** – A normalização deve acompanhar a evolução tecnológica de maneira a que as novas técnicas que vão sendo adotadas sejam incorporadas, evitando-se que iniba a inovação tecnológica.

4.2.Sistema Brasileiro de Normalização

No Brasil existe um único Organismo Nacional de Normalização que é a Associação Brasileira de Normas Técnicas (ABNT). Criada em 1940, a ABNT iniciou o processo de elaboração de normas técnicas no Brasil. Sua criação resultou da identificação pela sociedade da necessidade de se desenvolver a normalização de forma sistemática.

A ABNT é membro fundador da ISO (International Organization for Standardization), da Comissão Pan-americana de Normas Técnicas (COPANT) e da Associação Mercosul de Normalização (AMN) e membro do IEC (organismo internacional de normalização para a área eletroeletrônica). No desempenho de sua missa institucional, a ABNT representa os interesses de normalização do Brasil junto a esses organismos internacionais e regionais de normalização.

De forma integrada, a ABNT coordena as atividades de normalização no âmbito das ações do Sistema Nacional de Metrologia, Normalização e Qualidade Industrial (SINMETRO), que integra as funções da tecnologia industrial básica (normalização, metrologia e avaliação da conformidade), que asseguram a qualidade de produtos e serviços e viabiliza a regulamentação técnica. A Figura 4.1 ilustra a estrutura desse subsistema do SINMETRO entendido como o Sistema Brasileiro de Normalização (SBN), cujas funções estão caracterizadas no Quadro 4.2 a seguir.

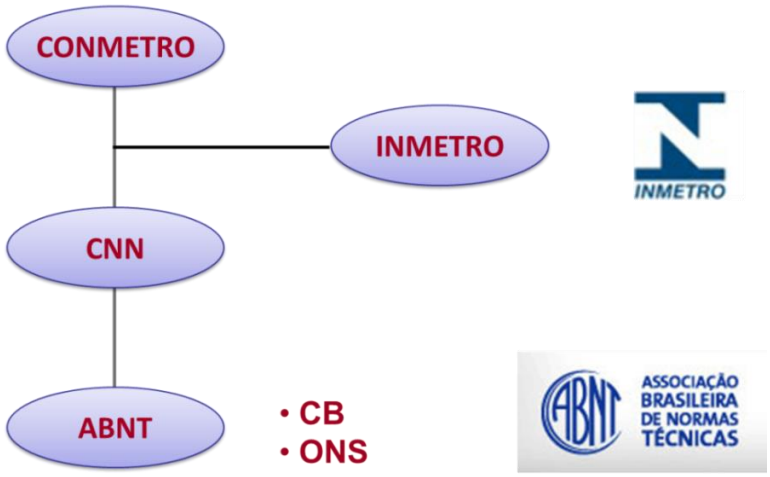

Figura 4.1 - Sistema Brasileiro de Normalização.
Fonte: CNI, 2002.

Quadro 4.2 - Descrição das instituições do Sistema Brasileiro de Normalização

Instituição	Descrição
SINMETRO – Sistema Nacional de Metrologia, Normalização e Qualidade Industrial	Sistema que integra o setor governamental e a iniciativa privada, articulando a infraestrutura de serviços tecnológicos para a qualidade e produtividade do país.
CONMETRO – Conselho Nacional de Metrologia, Normalização e Qualidade Industrial	Órgão normativo do SINMETRO, ao qual compete formular, ordenar e supervisionar a Política Nacional de Metrologia, Normalização Industrial e de Certificação da Qualidade de Produtos Industriais.
INMETRO – Instituto Nacional de Metrologia, Qualidade e Tecnologia	Órgão executivo do SINMETRO, Secretaria Executiva do CONMETRO e do CNN e fórum de compatibilização dos interesses governamentais.
CNN – Comitê Nacional de Normalização	Órgão assessor do CONMETRO, com composição paritária entre órgãos de governo e privados, com o objetivo de planejar e avaliar a atividade de normalização técnica no Brasil.
ABNT – Associação Brasileira de Normas Técnicas	Fórum nacional de normalização
As Normas Brasileiras são elaboradas na ambiência de dois órgãos distintos:	
ABNT/CB – Comitê Brasileiro	Órgão interno da ABNT, constituído pelos seus associados, e responsável pela coordenação e planejamento das atividades de normalização em uma área ou setor específico. Dentro do seu campo de atuação, é responsável, também, pela representação da ABNT no sistema de normalização regional e internacional.
NOS - Organismo de Normalização Setorial	Organismo público, privado ou misto, sem fins lucrativos, que tem atividade reconhecida no campo da normalização em um dado domínio setorial, mediante credenciamento pela ABNT, segundo critérios aprovados pelo CONMETRO. O ONS tem o papel de elaborar Normas Brasileiras para o setor que representa, bem como de representar o País na normalização regional e internacional, por delegação da ABNT, nas matérias relacionas ao âmbito de atuação para o qual foi credenciado.

4.3.
Normalização internacional

O setor eletrotécnico percebeu a necessidade da normalização internacional na virada do século XIX. Mais recentemente compreendida como processo indutor da inovação tecnológica, a normalização tem crescido de forma expressiva quer em âmbito internacional, regional e nacional. No ano de 1906 foi fundada a *International Electrotechnical Commission* (IEC), considerado o primeiro organismo internacional de normalização. Em 1926 foi criada a *International Federation of the National Standardizing Associations* (ISA), com 20 membros e ênfase em mecânica. Sofrendo o impacto desintegrador da II Guerra Mundial, os organismos de normalização — essencialmente um foro de especialistas representando interesses econômicos comuns de países parceiros comerciais — se viram forçados a interromper suas atividades. Assim ocorreu com a ISA, que encerrou suas atividades em 1942, enquanto organizações nacionais de normalização dirigiram seus esforços para a fabricação de armamentos.

A despeito do seu caráter avassalador, a guerra teve consequências importantes para a normalização (CNI, 2002). Os países aliados constituíram o *United Nations Standards Coordinating Committee* (UNSCC), que é o Comitê de Coordenação da Normalização das Nações Unidas, integrando 18 membros. Comitê que se manteve apenas no período da guerra, mas que desempenhou papel fundamental no esforço de guerra beneficiando-se dos princípios da normalização que sistematiza, otimiza e racionaliza a produção.

Resultado de uma iniciativa iniciada no pós-guerra, em 1946, envolvendo 25 países, dentre os quais o Brasil, foi criada a *International Organization for Standardization* (ISO) em 1947. No contexto de uma tendência de especialização da normalização internacional, em 1992, diversas iniciativas de normalização internacional na área de telecomunicações culminaram com a criação da *International Telecommunications Union* **(**ITU).

Aderentes aos princípios da normalização, normas Internacionais são desenvolvidas por especialistas dos países membros que integram os comitês técnicos da ISO, sempre assegurando amplo acesso de representação das partes interessadas. O processo de normalização se desenvolve segundo o seguinte processo evolutivo:

- Fase 1: proposta
- Fase 2: preparatória
- Fase 4: Comissão

- Fase 4: inquérito
- Fase 5: aprovação
- Fase 6: publicação

A Figura 4.2 ilustra o processo de elaboração de uma norma internacional.

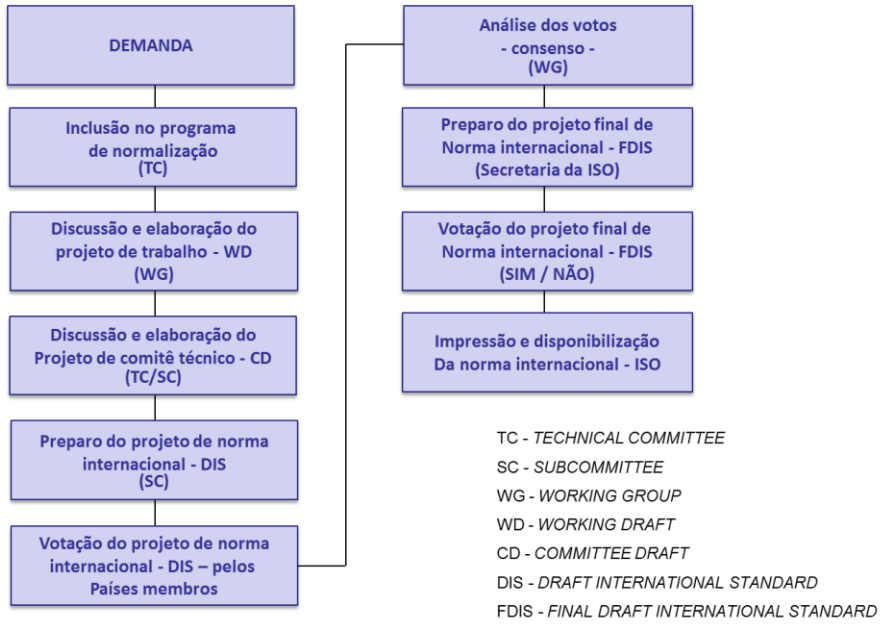

Figura 4.2 - Processo de elaboração de uma norma internacional.
Fonte: ISO, 2012.

A Figura 4.3 apresenta os estágios e ilustra os prazos (típicos) necessários para elaboração de uma norma internacional.

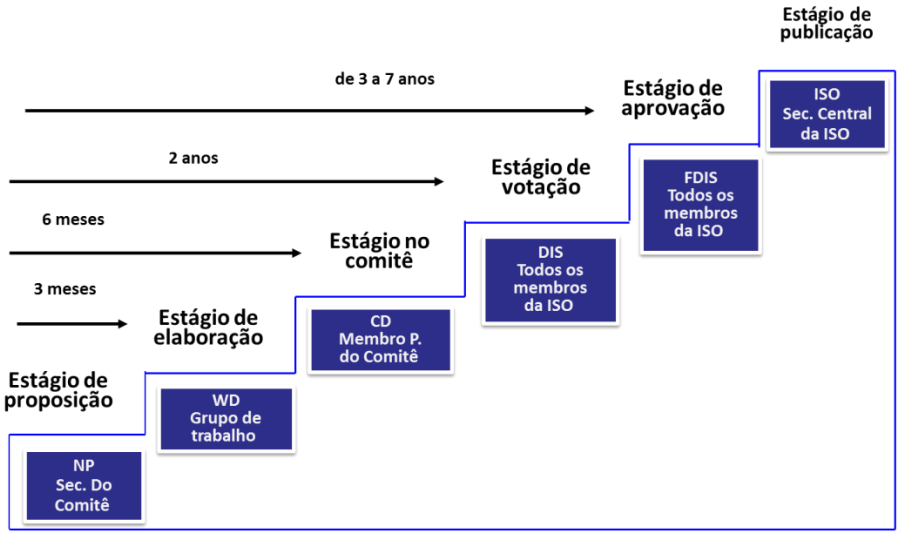

Figura 4.3 - Estágio e prazos para elaboração de uma norma.
Fonte: ISO, 2012.

4.4.
O esforço de normalização voltado para o *smart grid*

4.4.1.
IEC *Smart grid* SG3

O *International Electrotechnical Commission* (IEC) criou um grupo de trabalho para estudar as necessidades de normalização impostas pela introdução das redes inteligentes de energia (*smart grid*).

As normas internacionais do IEC (via de regra aplicáveis ao setor de eletrotécnica) englobam uma vasta gama de tecnologias de geração, transmissão e distribuição de energia para equipamentos domésticos e comerciais. Notadamente, semicondutores, fibra ótica, baterias, nanotecnologias, conversores de energia solar e energia marítima, para mencionar apenas alguns (IEC, 2010).

No âmbito de suas ações estratégicas, o *Standardization Manangement Board* (SMB) da IEC criou o *Strategic Group* (SG) com a tarefa de sinalizar para as necessidades de normalização resultantes da introdução de inovadoras ideias e tecnologias (IEC, 2012).

Anfitrião da iniciativa, o Brasil sediou em São Paulo, em 2008, a reunião do SMB/IEC que aprovou a criação de um Grupo Estratégico de *Smart Grid*, denominado de IEC SG3.

Como seu principal objetivo, o IEC SG3 desenvolveu um *framework* de normalização internacional que inclui os protocolos e modelo de normas para (i) assegurar a interoperabilidade de dispositivos e sistemas *Smart Grid* e (ii) otimizar o funcionamento, a manutenção e a evolução das redes elétricas (Pimentel, 2010).

Em 2010, o SG3 coletou informações junto à indústria, com o objetivo de desenvolver uma arquitetura-alvo capaz de ser mapeada e de auxiliar no desenvolvimento de um "*Generic Reference Architecture*" para o *Smart Grid* (IEC, 2010).

A expectativa das concessionárias é que o proposto *Generic Reference Architecture* constitua-se de fato numa referência para orientar o desafiador trabalho de implantação das redes inteligentes, indutoras de uma revolucionária transformação do setor. As diretrizes para implantação desse inovador sistema constam do IEC *Smart Grid Technical Reference Roadmap*.

No que concerne prioridades, o SG3 prevê as seguintes ações:

- Prevenção de Blackout;
- Gestão de Distribuição Avançada;
- Automação da Distribuição;
- Automação Inteligente da Subestação;
- Recursos Energéticos Distribuídos;
- Infraestrutura de Medição Avançada;
- Resposta à Demanda e Gestão de carga;
- Casa Inteligente e Automação Predial;
- Armazenamento de energia.

O IEC possui hoje um vasto acervo de normas com o escopo voltado para as redes inteligentes. Cerca de uma centena de normas IEC foram identificadas como relevantes para orientar o trabalho de introdução das redes inteligentes. Deste acervo, algumas normas possuem aplicação imediata para a consolidação do conceito de *Smart Grid*. Na visão de Pimentel (2010), um dos principais focos das atividades do IEC *Smart Grid* SG3 é o AMI (IEC 62051-62059; IEC TR 61334). A título de contextualização, o Quadro 4.3 relaciona um conjunto de normas aplicáveis às redes inteligentes.

Quadro 4.3 – Normas aplicáveis às redes inteligentes.

Nome	Descrição
IEC/TR 62357	Arquitetura Orientada a Serviços
IEC 61970	Interfaces de programação de aplicativos para sistemas de gestão de energia
IEC 61850	Automação de Subestação
IEC 61968	Troca de informações entre sistemas de distribuição elétrica
IEC 62351	Segurança
IEC 62056	Troca de dados na leitura do medidor, tarifa e controle de carga
IEC 61508	Segurança funcional de elétrica, eletrônico e eletrônico programável

O IEC, por meio da ação estruturada do SG 3, atua em sinergia com iniciativas de projetos de *Smart Grid* que se desenvolvem em diversos países. Dentre as iniciativas para introdução das redes inteligentes destacam-se projetos em desenvolvimento nos EUA pelo *National Institute of Standards and Technology* (NIST) e no Reino Unido, assistido pelo seu organismo nacional de normalização, o British Standard Institute (BSI). O esforço internacional de

normalização do IEC voltado ao *smart grid* conquistou reconhecimento mundial pelos diferentes agentes que participam, quer como usuários, quer como provedores de sistemas inteligentes para o sistema elétrico.

4.4.2. A experiência do NIST no *smart grid*

Fundada em 1901, o NIST é uma agência federal não regulamentadora vinculada ao Departamento de Comércio dos EUA. Sua missão institucional é promover a inovação e a competitividade industrial dos EUA por meio do avanço da ciência de medição, padrões e tecnologia de forma a aumentar a segurança econômica e melhorar a qualidade de vida.

Gestor do sistema metrológico americano, o NIST possui um papel fundamental na introdução das chamadas medições inteligentes, cerne da tecnologia *smart grid*. Desenvolve sistemas e conhecimento de suporte à implantação das redes inteligentes no país, provendo assist6encia tecnológica para fabricantes, consumidores, fornecedores de energia e reguladores que somam seus esforços e interesses comuns para viabilizar o desenvolvimento de "normas de interoperabilidade" do sistema. Em outras palavras, o NIST provê a base técnica para assegurar um desenvolvimento adequado dos componentes, subsistemas e sistemas que integram as redes inteligentes e sua implantação no amplo e complexo sistema elétrico americano, certamente suprindo a maior demanda por energia elétrica do planeta (NIST, 2012).

O NIST *Smart Grid Standards* tem a responsabilidade de coordenar o desenvolvimento de um framework que inclui protocolos e padrões para a gestão da informação. Na visão do NIST, as normas constituem insumo informacional indispensável para implantação e operação de todos os componentes das redes inteligentes.

Um vasto acervo normativo, que requer a definição de padrões e protocolos, será necessário para orientar a operação/implantação de uma rede inteligente e integrada, de forma eficiente e eficaz. Historicamente, o processo de desenvolvimento de uma norma é moroso, o que não deve ser compreendido como defeito da normalização já que o preceito do consenso das partes interessadas é que atribui robustez e isenção a uma norma. Este é o desafio que se descortina para o setor: como prover o acervo normativo de informações técnicas necessárias à implantação das redes inteligentes em tempo hábil sem violentar a lógica da normalização. Especialistas em normalização já preveem

expressiva demanda por normalização em *smart grid*, não apenas por normas especializadas como normas de gestão. Tal demanda se explica pela complexidade do sistema e pela interoperabilidade requerida para a sua implantação (NIST, 2012).

Dentre as principais referências que normalizam a interoperabilidade das redes inteligentes destacam-se:

- *NIST Identified Standards for Consideration by Regulators, Release 1.0*
- *NISTIR 7628 Guidelines for Smart grid Cyber Security (3 vols.)*
- *NIST to Launch Forum for Views on Consumer Interface to the Smart grid*
- *NIST Framework and Roadmap for Smart grid Interoperability Standards, Release 1.0*

O documento *NIST Framework and Roadmap for Smart Grid Interoperability Standards* (Release 1.0) aborda três requisitos básicos que refletem a necessidade de:

- descrever um modelo de referência de alto nível conceitual para as redes inteligentes,
- identificar normas que se aplicam (ou que possam ser aplicáveis) para o desenvolvimento de uma rede inteligente interoperável, e
- especificar um conjunto de lacunas e questões de alta prioridade relacionadas a normalização aplicável.

Em diagnóstico realizado sobre o setor, o NIST identificou (Documento de 6 de outubro de 2010) cinco famílias de normas que, na sua visão, devem merecer a atenção do regulador, notadamente nos aspectos necessários para se assegurar a interoperabilidade das redes inteligentes (NIST, 2010). São elas:

- **IEC 61970** e **IEC 61968** - Fornecem um modelo de informação padrão (CIM) necessários para o intercâmbio de dados entre dispositivos e redes, principalmente na transmissão (IEC 61970) e distribuição (IEC 61.968).
- **IEC 61850** - Facilita a automação e comunicação de subestações, bem como, a interoperabilidade através de um formato de dados padrão.
- **IEC 60870-6**: Facilita o intercâmbio de informações entre os centros de controle.
- **IEC 62351** - Aborda a segurança cibernética dos protocolos de comunicação definidas pelas normas anteriores IEC.

A introdução e operação adequada das redes inteligentes impõem novas e desafiadoras demandas por normalização e regulamentação aplicável a esses sistemas inteligentes. Especializando-se no setor, o NIST concentrou o seu primeiro esforço na identificação do acervo normativo requerido pela introdução da nova tecnologia de redes inteligentes. Priorizou a sua ação no atendimento

às necessidades do *Federal Energy Regulatory Commission* (FERC). Oito foram as necessidades apontadas:

- Resposta à demanda e Eficiência Energética do Consumidor
- Percepção situacional em uma Area Ampla
- Armazenamento de Energia
- Transporte Elétrico
- Infraestrutura Avançada de Medição
- Gestão da rede de distribuição
- Segurança Cibernética
- Rede de Comunicação

4.4.3. Normas globais de segurança cibernética para o *smart grid*

O *Energy Independence and Security* (EISA) atribui ao NIST a responsabilidade de elaborar e protocolos para interoperabilidade das redes inteligentes. O *Cyber Security Working Group* (CSWG) identificou um conjunto de normas entendidas relevantes para assegurar a segurança cibernética nas redes inteligentes. O Quadro 4.4 resume o escopo de cada uma dessas normas de segurança cibernética nas redes inteligentes[6].

- Nº – Índice da tabela;
- Organização – Identificação da organização que elaborou a norma;
- Norma - ID – Identificação da norma para referência;
- Norma - Nome – Nome detalhado da norma;
- Norma (sem custo) (S/N) – Identifica se a norma pode ser obtida via *download* direto na internet;
- Requerida por Regulação ou Lei (S/N) – Identifica se existe um órgão do governo que considere a norma exigida;
- Específica para *Utilities* (Y/N) – Indica se a norma é específica para as concessionárias.

[6] Á época do estudo nem todas as normas listadas estavam disponíveis para o *Cyber Security Working Group* (SGIP-CSWG), o que não permitiu a sua adequada caracterização.

Quadro 4.4 - Acervo normativo aplicável ao *smart grid.*

No.	Organização	Norma - ID	Norma – Nome	Norma (sem custo) (S/N)	Requerida por Regulação ou Lei (S/N)	Específica para Utilities (Y/N)
1	IEC	IEC 62351 -1	Data and Communications Security Part 1: Introduction to Security Issues	Y	N	Y
2	IEC	IEC 62351 -2	Data and Communications Security	Y	N	
3	IEC	IEC 62351 -3	Data and Communications Security Part 3: Profiles Including TCP/IP	Y	N	Y
4	IEC	IEC 62351 -4	Data and Communications Security Part 4: Profiles Including MMS	Y	N	Y
5	IEC	IEC 62351 -5	Data and Communications Security Part 5: Security for IEC 60870-5 and Derivatives	Y	N	Y
6	IEC	IEC 62351 -6	Data and Communications Security Part 6: Security for IEC 61850	Y	N	Y
7	IEC	IEC 62351 -7	Data and Communications Security Part 7: Network and system management (NSM) data object models	When published	N	Y
8	IEC	IEC 62351 -8	Data and Communications Security Part 8: Role-based access control	When completed	N	Y
9	ANSI	ANSI C12.22	Meter and End Device Tables communications over any network	N	N	Y
10	DHS	DHS	Catalog of Control Systems Security: Recommendations for Standards Developers		N	N
11	IEEE	IEEE 802.11i	Part 11: Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) specifications, Amendment 6: Medium Access Control (MAC) Security Enhancements	Y		N
12	IEEE	IEEE 1547.3	Guide For Monitoring, Information Exchange, and Control of Distributed	Y	N	Y
13	IEEE	IEEE 1686	Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities	N	N	Y
14	IETF	SNMP	Simple Network Management Protocol (SNMP)	Y	N	N
15	ISA IEC	SP99 IEC 62443	Cyber security mitigation for industrial and bulk power generation stations	N		N
16	ISSO	ISO 27000	Information technology - Security techniques - Information security management systems - Overview and vocabulary	N		N
17	NERC	CIP 002 thru 009	NERC Critical Infrastructure Protection (CIP Standards)	Y	Y	Y
18	NIST	FIPS 140-2	Security Requirements for Cryptographic Modules	Y	N	N

No.	Organização	Norma - ID	Norma – Nome	Norma (sem custo) (S/N)	Requerida por Regulação ou Lei (S/N)	Específica para Utilities (Y/N)
19	NIST	FIPS 197	Cryptographic standard: Advanced Encryption Standard (AES)	Y	N	N
20	NIST	SP 800-53	Security controls required for federal information systems	Y	N	N
21	NIST	SP 800-82	DRAFT Guide to Industrial Control Systems (ICS) Security	Y	N	N
22	IEC	IEC 61850-3	General electrical and security requirements for substation IEDs	Y	N	Y
23	UCAIug	UCAIug AMI-SEC	System Security Requirements	Y	N	Y
24	OASIS	WS-Security	Web Services Security	Y		N
25	IEEE	802.1AR	Secure Device Identity	N	N	N
26	IEEE	802.1AE	Media Access Control Security Standard	Y	N	N
27	IEEE	802.1X-REV	Port Based Network Access Control	N	N	N
28	IETF	TLS	Transport Layer Security (TLS)	Y	N	N
29	IETF	DTLS	Datagram Transport Layer Security (DTLS)	Y	N	N
30	IETF	IPSec	Internet Protocol Security	Y	N	N
31	IETF	RFC3711	Secure Real-Time Transport Protocol	Y	N	N
32	IETF	RFC4962	Guidance for Authentication, Authorization, and Accounting (AAA) Key management	Y	N	N
33	IETF	RFC 3748	Extensible Authentication Protocol (EAP)	Y	N	N
34	IEEE	802.16e	Air Interface for Broadband Wireless Access Systems (WiMax)	N	N	N
35	NIST	SP 800-38(A-E)	Recommendations for Block Cipher modes	Y		
36	3GPP	TS 33.102	UMTS LTE 3G Security Architecture	Y	N	N
37	ISO/IEC	ISO/IEC 9798	Security Techniques - Entity Authentication (Parts 1 - 4)	N		N
38	ISO/IEC	ISO/IEC 11770	Security Techniques - Key Management (Parts 1 - 3)	N		N
39	ISO/IEC	ISO/IEC 13888	Security Techniques - Non Repudiation (Parts 1 - 3)			N
40	ISO/IEC	ISO/iEC 14888	Security Techniques - Digital Signatures (Parts 1 - 3)	N		N
41	ISO/IEC	ISO/IEC 15946-1	Cryptographic Techniques Based on Elliptic Curves -Part 1:General	N		N
42	ISO/IEC	ISO/IEC 18033	Security Techniques - Encryption Algorithms (Parts 1 - 4)	N		N

No.	Organização	Norma - ID	Norma – Nome	Norma (sem custo) (S/N)	Requerida por Regulação ou Lei (S/N)	Específica para Utilities (Y/N)
43	ISO/IEC	ISO/IEC 19772	Security techniques -- Authenticated encryption	N		N
44	W3C	XML Encryption	XML Encryption Syntax and Processing	Y	N	N
45	W3C	XML Signature	XML Signature Syntax and Processing	Y	N	N
46	W3C	Canonical XML	Canonical XML	Y	N	N
47	NERC CSSWG (1)37		Security Guidelines for the Electricity Sector: Control System Cyber Security Incident Response Planning	Y	N	Y
48	NERC CSSWG (2)		Security Guidelines for the Electricity Sector: Control System — Business Network Electronic Connectivity	Y	N	Y
49	NERC CSSWG (3)		Security Guidelines for the Electricity Sector: Patch Management for Control Systems	Y	N	Y
50	NERC CSSWG (4)		Security Guidelines for the Electricity Sector: Physical Security – Substations	Y	N	Y
51	NERC CSSWG (5)		Security Guideline for the Electricity Sector: Time Stamping of Operational Data Logs	Y	N	Y
52	IEEE	C37.231	Recommended Practice for Microprocessor-based Protection Equipment Firmware Control	N	N	Y
53	NIST	FIPS 198	The Keyed-Hash Message Authentication Code(HMAC)	Y		N
54	NIST	FIBS 180-2	Secure Hash Standard(SHS)	Y		N
55	ANSI	ANS X9.52-1998	Triple Data Encryption Algorithm Modes of Operation	N		N
56	NIST	FIPS 197	Advanced Encryption Standard(AES)	Y		N
57	NIST	FIPS 186-3	Digital Signature Standard(DSS)	Y		N
58	ANSI	ANSI X9.62	Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm(ECDSA)	N		N
59	PKCS	PKCS #1,#3,#5-#12,#15	RSA Public Key Cryptography Standards	Y		N
60	ANSI	ANSI X9.42	Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography	N		N
61	IETF	IETF 4120	The Kerberos Network Authentication Service (V5)	Y		N
62	ANSI/INCITS	INCITS 359	Information Technology - Role Based Access Control	N		N
63	NIST	SP 800-63	Electronic Authentication Guideline	Y	N	N

No.	Organização	Norma - ID	Norma – Nome	Norma (sem custo) (S/N)	Requerida por Regulação ou Lei (S/N)	Específica para Utilities (Y/N)
64	OASIS	XACML 2.0	eXtensible Access Control Markup Language	Y	N	N
65	OASIS	SAML 2.0	Security Assertion Markup Language	Y	N	N
66	OGC	GeoXACML	Geospatial exTensible Access Control Markup Language (GeoXACML)	Y	N	N

Fonte: NIST, 2012.

4.5.
Normas aplicáveis à segurança da informação

As normas aplicáveis à gestão de segurança da informação adotadas no Brasil são:

- **NBR ISO/IEC 27001:2006** - Requisitos para implantar um Sistema de Gestão de Segurança da Informação (SGSI)
- **NBR ISO/IEC 27002:2005** - Práticas para a gestão de um Sistema da Informação (SI)
- **NBR ISO/IEC 27005:2011** - Gestão de riscos de SI
- **27004:2009 e 27003:2011** - Gestão de SI (Medição) e Guia de Implantação de um SGSI
- **27007:2011** - Requisitos e Diretrizes para auditoria de um SGSI.

A ABNT NBR ISO/IEC 27002:2005 denota a edição brasileira da norma internacional de mesmo código. Esta norma estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Esta norma apresenta as diretrizes aja consensadas sobre a gestão de segurança da informação (ABNT, 2012).

A norma ABNT NBR ISO/IEC 17799:2005 é referenciada como indispensável para a aplicação da norma ABNT NBR ISO/IEC 27001, cabendo lembrar que a ABNT NBR ISO/IEC 17799:2005 foi cancelada e substituída pela ABNT NBR ISO/IEC 27002:2005.

4.6.
Regulamentação brasileira aplicável à medição inteligente

A diretoria do organismo regulador brasileiro para o setor elétrico — a Agência Nacional de Energia Elétrica (ANEEL) — aprovou, em agosto de 2012, a resolução que regulamenta os requisitos básicos para os sistemas de medição eletrônica de energia elétrica no Brasil (Aneel, 2012). Os medidores eletrônicos de energia elétrica constituem-se em pré-condição à implantação das redes elétricas inteligentes no Brasil.

A proposta de regulamentação dos requisitos mínimos para os medidores eletrônicos foi debatida na Audiência Pública 43/2010, que colheu contribuições da sociedade entre 1º de outubro de 2010 e 28 de janeiro de 2011. Tal iniciativa contou com uma sessão presencial realizada em Brasília em 26 de janeiro de 2011. Ao fim desse período, a ANEEL recebeu 212 contribuições de 57 agentes, com sugestões de consumidores, distribuidoras, indústrias, associações setoriais e outros segmentos da sociedade. Durante a sessão presencial foram realizadas dezenove manifestações, com apresentação de comentários e contribuições (Aneel, 2012).

A ANEEL já emitiu diversos regulamentos relacionados às redes inteligentes, dentre os quais destacam-se:

- Resolução Normativa nº 482, de 2012, que trata da conexão de micro e minigeração distribuída;
- Resolução Normativa nº 464, de 2011, que trata do estabelecimento da tarifa branca;
- Resolução Normativa nº 375, de 2009, que trata da regulamentação da utilização do PLC;
- Resoluções nº 345, de 2008, e nº 395, de 2008, que trata do uso compulsório de sistemas geoprocessados.

A título de contextualização, os resultados da Audiência Pública nº 43/2010 e a Resolução Normativa nº 502 (que Regulamenta sistemas de medição de energia elétrica de unidades consumidoras do Grupo B), foram incluídos como anexos desta dissertação.

5
Segurança da informação nas redes inteligentes de energia elétrica: estudo de caso de concessionárias no Brasil

Este capítulo discute um estudo de caso relacionado à segurança da informação nas redes inteligentes de concessionárias de energia elétrica no Brasil. A fundamentação teórica para enquadramento e desenvolvimento do caso se dá com base no trabalho de Yin (2010). Segundo sua taxonomia, o estudo de caso pode ser tratado como uma investigação empírica já que (i) investiga um fenômeno contemporâneo em profundidade no seu contexto de vida real e (ii) os limites entre o fenômeno e o contexto não são claramente evidentes.

O estudo de caso comumente se desenvolve na presença de excesso de variáveis, múltiplas fontes de evidência, podendo se beneficiar, entretanto, de desenvolvimentos anteriores e de proposições teóricas que orientam a coleta e a análise de dados.

Segundo Yin (2010) existem pelo menos cinco situações em que o estudo de caso se aplica:

- para explicar vínculos causais em intervenções complexas para estratégias experimentais da vida real;
- quando se faz necessário descrever intervenções no contexto em que ocorrem;
- para ilustrar determinados tópicos de uma investigação;
- para explorar uma situação complexa de resultados e
- como estratégia de meta-avaliação de determinados processos.

No presente estudo de caso entende-se que o fenômeno investigado (segurança da informação na implantação das redes inteligentes em concessionárias de energia elétrica) não poderia ser destacado de seu contexto original. Por essa razão, a investigação ocorreu em um determinado momento de observação no curso da trajetória original da intervenção, mais precisamente quando da implantação de redes inteligentes nas concessionárias estudadas.

Aderente à fundamentação teórica adotada, em função do contexto e da unidade incorporada de análise, quatro são os possíveis casos: únicos ou múltiplos, e holísticos ou integrados, conforme ilustrado pela Figura 5.1.

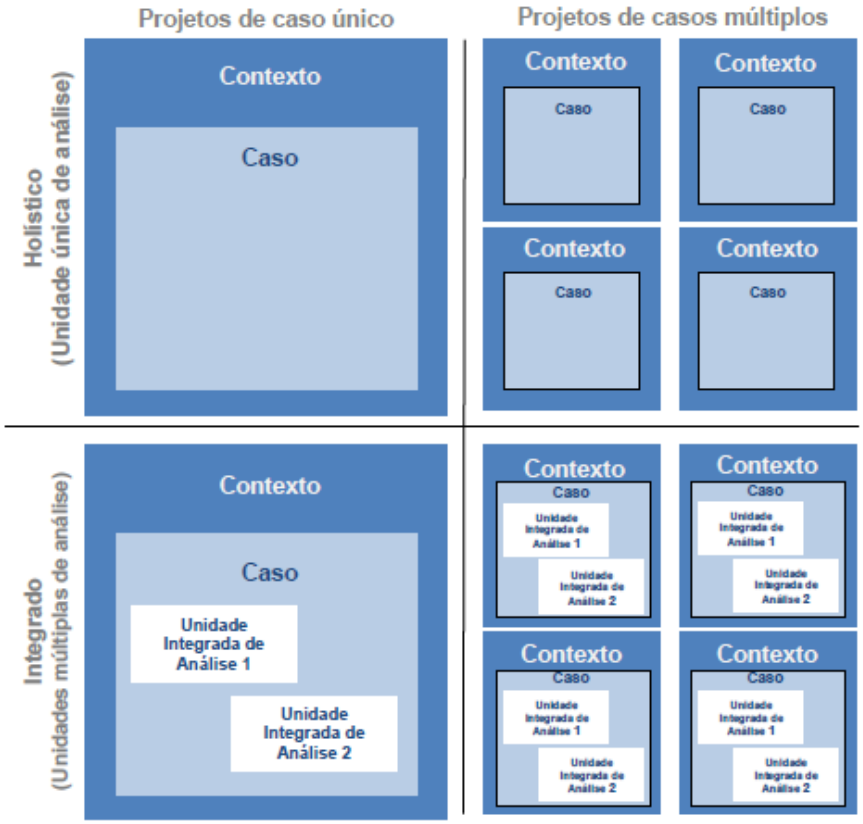

Figura 5.1 – Tipo de estudo de caso.
Fonte: Yin, 2010.

O ***estudo de caso único*** deve ser prescrito quando:

- representa o caso decisivo para testar uma teoria bem formulada, seja para confirmá-la, contestá-la ou para expandir a sua aplicação;
- representa uma situação rara ou extrema, comumente empregado em estudos relacionados à saúde (e.g.: casos patológicos incomuns);
- o caso único se mostra revelador, facultando ao pesquisador a oportunidade de observar um fenômeno anteriormente inacessível pela via da investigação científica, ou
- quando é utilizado como introdução a um estudo mais apurado ou como caso-piloto para a investigação.

No ***estudo de caso múltiplo***, a lógica a ser adotada na seleção dos casos é a de replicação (adota os mesmos procedimentos definidos no planejamento em mais de um caso), podendo ser por replicação literal (conduz a resultados semelhantes por motivos previsíveis); ou por replicação teórica (leva a resultados contrastantes por características de casos conhecidos).

O ***estudo de caso integrado*** é aquele no qual a situação é avaliada a partir de diferentes unidades ou níveis de análise com base em critérios distintos. Podem referir-se a setores diferentes de uma determinada instituição (e.g.:

setores de vendas e de produção) ou a atividades (e.g.: processo de planejamento e processo de implantação).

O ***estudo de caso holístico*** deve ser aplicado quando não é possível identificar uma "subunidade lógica". Nesse caso, o risco é induzir o pesquisador a ignorar pontos importantes de um processo já que não consegue isolá-los em unidades lógicas.

Para qualquer dessas abordagens metodológicas faz-se necessário delimitar o campo de trabalho, recorte a ser definido ao longo do estudo. A experiência mostra que é comum que tais condicionantes e determinantes serem alterados no curso do trabalho.

5.1. Desenho da pesquisa

Conforme definido no capítulo 1, a dissertação definiu como questão principal a análise dos parâmetros relacionados à segurança da informação na implantação da infraestrutura de medição inteligente (*smart grid*). Ou seja, mostrar que os riscos associados à adoção da tecnologia *smart grid* — que deixa vulnerável por exposição na rede inteligente o sistema informacional da concessionária de energia elétrica — podem ser minimizados pela adoção de recomendações normativas específicas. E, na busca das respostas cabíveis, quatro objetivos específicos foram definidos naquele capítulo introdutório como características críticas que devem ser incorporadas no modelo de gestão para assegurar a segurança da informação ameaçada pelas redes inteligentes.

O estudo de caso aqui desenvolvido compreendeu as seguintes cinco etapas, desenvolvidas segundo o fluxograma ilustrado na Figura 5.2:

i. seleção do tipo de estudo caso e definição da unidade de análise;
ii. elaboração do instrumento de coleta de dados;
iii. coleta de dados;
iv. tratamento e análise dos dados;
v. apresentação dos resultados.

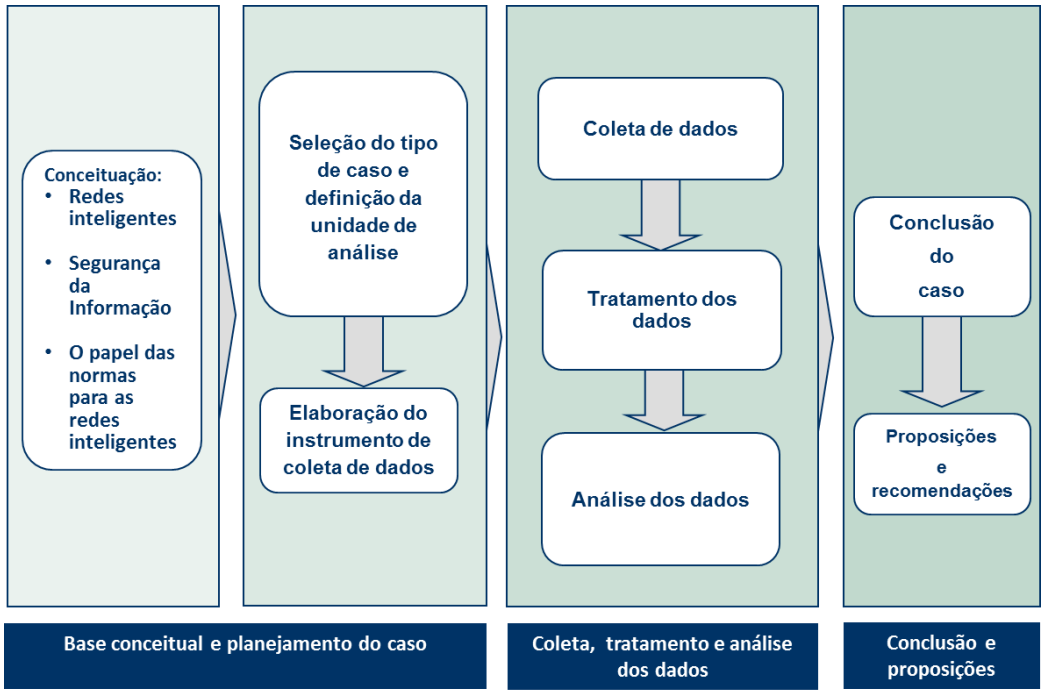

Figura 5.2 - Fluxograma do desenvolvimento do estudo de caso

A partir do referencial teórico apresentado (capítulos 2, 3 e 4) e da tipologia de estudo de casos (Figura 5.1), o tipo de estudo de caso foi selecionado e a unidade de análise definida. Na Fase 1 do trabalho foram desenvolvidos a base conceitual e o planejamento do caso, assim fundamentando a elaboração, pré-teste e validação do instrumento de coleta de dados, que orientou as entrevistas realizadas com gestores de projetos de implantação de redes inteligentes nas concessionárias que participaram da pesquisa (Apêndice A). A Fase 2, 3 e 4 compreendeu a coleta, tratamento e análise dos dados e a Fase 3 a elaboração das conclusões e formulação de recomendações para trabalhos futuros, sintetizando os resultados da pesquisa.

Nas seções a seguir são descritos os procedimentos e os resultados consolidados em cada uma das etapas do estudo de caso desenvolvido.

5.2. Tipo de estudo de caso e unidade de análise

5.2.1. Definição do tipo de estudo de caso

A revisão bibliográfica e o recenseamento do acervo normativo e técnico sobre os temas centrais da pesquisa orientaram o desenvolvimento da Fase 1

caracterizado no fluxograma da Figura 5.2. Como resultado dessa fase da pesquisa e com base nas premissas formuladas por Yin (2010), endossadas por Maffezzolli (2008), que reforça a escolha pela presença de dados quantitativos na pesquisa, optou-se pelo ***caso único integrado***, considerado o mais apropriado para consubstanciar o estudo de caso planejado. Esta classificação se configurou a partir da investigação de várias concessionárias de um mesmo setor, cujo diagnóstico contemplou a questão específica relacionada à segurança da informação nas redes inteligentes.

5.2.2.
Unidade de Análise

A unidade de análise é definida a partir do que se entende por "caso do estudo". Por exemplo, no estudo de um caso clássico, o "caso" pode ser um indivíduo, ou mesmo algum evento ou entidade a ele relacionado quando o indivíduo não é completamente definido. Assim, a orientação da unidade de análise (portanto, do caso) está relacionada à maneira pela qual as questões iniciais da pesquisa são definidas Yin (2010).

Na sua atual configuração integram o setor elétrico brasileiro sessenta e três[7] concessionárias de energia elétrica. De acordo com dados da Associação Brasileira de Distribuidores de Energia Elétrica (Abradee, 2012), juntas, as concessionárias brasileiras atendem a um contingente de cerca de setenta milhões de consumidores.

Este importante setor brasileiro é regulado por regras dispostas em resoluções da Agência Nacional de Energia Elétrica (Aneel), as quais se orientam pelas diretrizes estabelecidas nas leis aprovadas pelo congresso nacional e nos decretos estabelecidos pelo Executivo Federal. As concessionárias que compõem este setor estão distribuídas em todo o território nacional: Norte (9), Nordeste (11), Centro-Oeste (5), Sudeste (21) e Sul (17).

No início da década de 2000, antes da privatização do setor, a empresas eram verticalizadas e não havia separação dos negócios da cadeia produtiva (geração, transmissão e distribuição). Após a privatização, as concessionárias passaram a ser independentes, tornando-se a principal conexão entre o setor e a sociedade.

[7] Fonte: Aneel, 2012

5.3.
Elaboração do instrumento de coleta de dados

O Gabinete de Segurança Institucional da Secretaria Executiva do Departamento de Segurança da Informação e Comunicações da Presidência da República elaborou o Guia de Referência para a Segurança das Infraestruturas Críticas da Informação (Brasil, 2010). Este guia apresenta explanações sobre segurança cibernética e reúne métodos e instrumentos voltados para a garantia da segurança da informação em diferentes cenários considerados infraestruturas críticas da informação.

De acordo com o Gabinete de Segurança, as infraestruturas críticas são:

> *"definidas como as instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional."*

O Guia foi elaborado por grupos de trabalho com especialistas de diversos Ministérios e instituições públicas federais que reuniram estudos técnicos sobre o tema. A motivação se deu pelo entendimento de que ataques cibernéticos representam uma das maiores ameaças para a sociedade moderna. Neste sentido, a violação da segurança possibilitaria ações ofensivas por meio da penetração nas redes de computadores de setores estratégicos para a nação. Da mesma forma, estes ataques podem ocorrer em diferentes componentes das redes inteligentes, incluindo os medidores eletrônicos (inteligentes) de energia elétrica.

O tratamento dado no referido Guia ao tema *segurança da informação* é passível de ser apropriado ao contexto das redes inteligentes. Este documento visa assegurar, dentro do espaço cibernético, ações de segurança da informação consideradas fundamentais para garantir disponibilidade, integridade, confidencialidade e autenticidade da informação.

Organizações nacionais e internacionais beneficiam-se do trabalho de comitês técnicos e grupos de trabalho que objetivam estabelecer um conjunto de tecnologias, normas e padrões visando à segurança de dados nas redes inteligentes. Tais organizações têm produzido e divulgado documentos extremamente relevantes sobre o tema. Dentre os documentos produzidos e de interesse para este trabalho, destacam-se duas recentes publicações (2010): o "*Smart Grid Standardization Roadmap*" publicado pelo (*Smart Grid Strategic Group,* SG3) da IEC e o "*NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*", de autoria do NIST.

Levando em consideração as recomendações e premissas desses documentos foi elaborado o instrumento de coleta de dados da pesquisa (Apêndice). Estruturado segundo cinco vertentes de análise (contexto, segurança, vulnerabilidade, impactos e normas) inclui dezoito questões estruturadas (contexto: 3; segurança: 4; vulnerabilidades: 5; impactos: 4 e normas: 2). Sistematiza assim a pesquisa relacionada à segurança da informação na medição inteligente (*smart grid)*.

5.4. Coleta de dados

Dada a dinâmica e novidade inerente às redes inteligentes, procurou-se refletir na construção do instrumento de coleta de dados as ênfases atribuídas ao tema pelos recentes artigos publicados em revistas técnicas especializadas, conferências em congressos do setor elétrico e sua ampla discussão na mídia.

O instrumento de coleta de dados selecionado foi um questionário estruturado, testado com base em um caso piloto para refinamento das questões formuladas. Os critérios para a escolha do caso piloto foram: acessibilidade dos possíveis informantes, localização geográfica conveniente e riqueza da experiência na implantação das redes inteligentes.

Pré-aprovado o seu conteúdo por um grupo de trabalho constituído pela Associação Brasileira de Distribuidores de Energia Elétrica (ABRADEE), a aplicação do questionário se deu no âmbito de concessionárias do setor elétrico brasileiro. Caracterizada na seção 1.6 (resultados e discussão), o universo da pesquisa caracterizou-se pelas concessionárias que divulgaram a existência de projetos *smart grid,* independente do seu estágio de implantação. Representando as concessionárias que aceitaram participar da pesquisa, foram entrevistados profissionais-chave detentores de cargos gerenciais, envolvidos na implantação de projetos de medição inteligente. Não obstante o questionário ter sido enviado com uma carta de sensibilização pela pesquisa, em todos os casos o respondente foi pessoalmente constatado quer por telefone quer pessoalmente para dirimir qualquer dúvida sobre o conteúdo da pesquisa.

5.5. Tratamento e análise dos dados

As respostas de cada questionário foram tabuladas em planilha Microsoft Excel® e disponibilizadas de forma estruturada para análise. Incorporando

recomendação de Oliveira (2006), a análise do estudo de caso levou em conta as seguintes variáveis consideradas críticas:

- descrição dos procedimentos;
- anotações de campo;
- esquema de codificação;
- encadeamento de evidências;
- comparação dos casos;
- técnicas de análise;
- comparação dos resultados com a literatura.

A tabulação dos dados foi realizada de forma agregada para preservar a confidencialidade do respondente, a partir de medidas descritivas e por frequência de ocorrência.

5.6. Resultados e discussão

O instrumento de coleta de dados foi enviado para 26 concessionárias do setor elétrico brasileiro. A seleção desses respondentes fundamentou-se em dois critérios: nível de envolvimento com os projetos de implantação das redes inteligentes e nível de conhecimento do tema de estudo desta dissertação.

Algumas concessionárias são controladas por um mesmo grupo econômico, (e.g.: o grupo CPFL integra 8 concessionárias; AES, 2; Neoenergia, 3; Eletrobrás, 6 e Rede, 9). Assim, um mesmo respondente pode ser responsável pelo desenvolvimento de projetos de implantação de redes inteligentes em mais de uma concessionária de energia elétrica do grupo, o que aumenta a representatividade da amostra agregando informações sobre oportunidades, desafios e expectativas das concessionárias.

Dezessete das vinte e seis concessionárias convidadas aceitaram participar da pesquisa e, destas, quatorze responderam o questionário integralmente. Atribuindo relevância estatística à amostra, essas concessionárias contabilizam 26 milhões dos consumidores brasileiros de energia elétrica, representando 38% do total de consumidores do País.

5.6.1. Contexto geral

A vertente de análise “contexto geral” do instrumento de coleta de dados foi elaborada para abordar três questões da pesquisa; (i) identificação dos

principais objetivos a serem alcançados pelas concessionárias com a implantação das redes inteligentes; (ii) captura e percepção das concessionárias sobre quem deve recair a responsabilidade pela garantia da segurança no ambiente das redes inteligentes e, (iii) identificação da existência ou previsão de orçamento específico para segurança da informação nas redes inteligentes.

O gráfico apresentado na Figura 5.3 ilustra as escolhas feitas pelos respondentes sobre os objetivos pretendidos com a implantação das redes inteligentes. Conforme ilustrado, *redução de custos operacionais* foi a opção priorizada, reunindo 45% das indicações. A opção *redução de perdas não técnicas e inadimplência* contabilizou 33% das respostas, enquanto as opções *melhoria dos indicadores de qualidade e continuidade do fornecimento*" e *conhecimento do comportamento dos consumidores* receberam apenas uma indicação cada. Importante destacar que a opção *ganhos de eficiência energética* não foi indicada por nenhuma das concessionárias participantes da pesquisa.

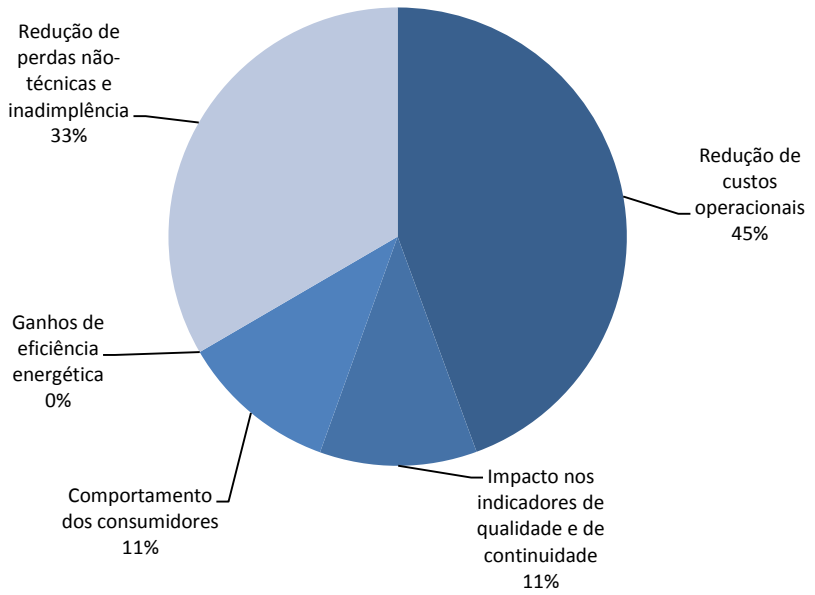

Figura 5.3 - Objetivos esperados pela implantação das redes inteligentes.

Este resultado pode ser justificado pelo fato de que, no Brasil, as perdas técnicas e os custos operacionais representam para as concessionárias uma perda financeira expressiva da sua receita comprometendo o seu plano de investimentos e, portanto, constituindo ameaças e desafios à modernização do setor.

De acordo com a ANEEL (2010), as perdas técnicas anuais correspondem a 7% da energia total gerada no país e, quando consideradas as perdas não-técnicas (notadamente furto de energia) o desperdício chega a 16% da geração total.

Corroborando com tal informação, Leite (2011) atribui à redução de perdas não-técnicas a principal motivação das concessionárias brasileiras para implantação de seus projetos de *smart grid*. Assim, a implantação das redes inteligentes contribui o alcance de três benefícios: (i) redução da energia requerida (eficiência energética); (ii) redução da tarifa de energia; (iii) maior retorno sobre os investimentos.

Por outra vertente, Lopes e colaboradores (2012) recomendam às concessionárias modernizar as redes a partir da introdução de novas tecnologias de informação e comunicação, assim permitindo que o sistema possa ser operado de forma mais eficiente e confiável, reduzindo os custos de operação.

É digno de nota o fato da opção *ganhos de eficiência energética* não ter sido considerada pelos respondentes. Nos EUA e Europa, o objetivo perseguido com a implantação das redes inteligentes está diretamente relacionado a ganhos de eficiência energética.

Em relação à percepção das concessionárias sobre a responsabilidade pela garantia da segurança nas redes inteligentes, 83,3% das concessionárias responderam que esse encargo compete à própria concessionária. Apenas 16,7% dos respondentes atribuem essa responsabilidade à agência reguladora (ANEEL).

Tabela 5.1 - Garantia da segurança da informação.

Responsabilidade pela garantia da segurança da informação nas redes inteligentes	**% (n)**
Agência Reguladora - Aneel	16,7 (1)
Concessionária	83,3 (5)
Fornecedores de tecnologia	0,0
Outro (s)	0,0

n= número de concessionárias

Apesar de apenas uma empresa entender que a Aneel é responsável pela garantia da segurança da informação, cabe considerar que, na audiência pública nº 43/2010 (Anexo I) que objetivou obter subsídios para o estabelecimento de resolução normativa sobre os requisitos mínimos para os

medidores eletrônicos de unidades consumidoras de baixa tensão, o tema não foi abordado. O que contribui para a percepção identificada no estudo.

A questão que objetivou investigar o orçamento destinado à segurança da informação recebeu o menor número de respostas. Apenas uma concessionária informou que o orçamento atual é de 10% do valor total investido na implantação das redes inteligentes. Os demais gestores de projetos não tinham conhecimento (ou preferiram não informar) este componente do orçamento. Mesmo na literatura consultada, não foi identificado padrão de investimento adequado, possivelmente, o montante investido tem relação com os ganhos auferidos com a redução de perdas e custos operacionais, sendo especifico em cada contexto.

5.6.2. Segurança da informação

O instrumento para coleta de dados estabeleceu quatro questões objetivas para investigar a vertente "segurança da informação". A Tabela 5.2, abaixo, apresenta os resultados sobre a situação da política da segurança da informação nas redes inteligentes. 50% das concessionárias declararam possuir uma política de segurança da informação implantada. Todas as empresas deste grupo relataram que há comprometimento da alta administração. Destas, 16,7% informaram que as responsabilidades não estão bem definidas e 33,3% que nenhum tipo de política de segurança da informação encontra-se implantada.

Tabela 5.2 - Política de segurança.

Situação da política de segurança da informação	% (n)
Implantada 1 [a]	33,3 (2)
Implantada 2 [b]	0,0
Implantada 3 [c]	16,7 (1)
Implantada 4 [d]	0,0
Não implantada 1 [e]	16,7 (1)
Não implantada 2 [f]	16,7 (1)
Sem resposta	16,7 (1)

a - Implantada. Responsabilidades bem definidas. Há comprometimento da alta administração; b - Implantada. Responsabilidades bem definidas. Sem comprometimento da alta administração; c- Implantada. Há comprometimento da alta administração. Responsabilidades ainda não foram totalmente definidas; d - Implantada. Não há comprometimento da alta administração. Responsabilidades ainda não foram bem definidas; e - Não implantada, mas está em processo de elaboração; f - Não implantada, e ainda não está sendo elaborada

n= número de concessionárias

No processo de desenvolvimento de uma política de segurança da informação, diferentes tipos de atividades devem ser executados simultaneamente (Brasil, 2010). Para as concessionárias analisadas, a implantação de uma base tecnológica com padrão de segurança em conformidade com normas nacionais e internacionais foi a opção que recebeu mais indicações. *Implantação de plano de contingência*, *identificação de vulnerabilidades* e *análise de riscos* ficaram empatadas como segunda opção de atividades que se encontram em desenvolvimento para assegurar a segurança da informação nas redes inteligentes.

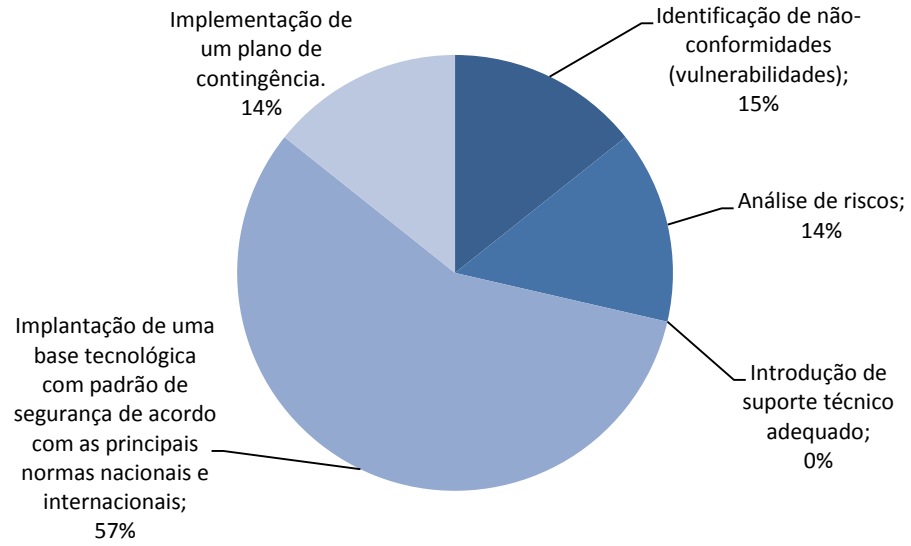

Figura 5.4 - Atividades realizadas para assegurar garantia da segurança da informação nas redes inteligentes.

Cerca de 40% dos respondentes considerou que os processos e atividades para garantia da disponibilidade, integridade, confiabilidade e autenticidade da informação são eficientes e eficazes.

Em relação aos *planos de contingência para mitigar problemas gerados por ataques cibernéticos às informações dos consumidores*, apenas 33,3% dos respondentes afirmaram ter este tipo de plano. Outros 33,3% informaram que esperam implantar planos de contingência no futuro e 16,7% informaram não possuir qualquer tipo de plano de contingência.

Tabela 5.3 - Qualificação dos processos e atividades.

Qualificação dos processos e atividades para assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação	
DISPONIBILIDADE	**% (n)**
Eficiente e eficaz	50,0 (3)
Eficiente e pouco eficaz	33,3 (2)
Pouco eficiente e eficaz	0,0
Pouco eficiente e pouco eficaz	0,0
Inexistente	0,0
Sem resposta	16,7 (1)
INTEGRIDADE	**% (n)**
Eficiente e eficaz	33,3 (2)
Eficiente e pouco eficaz	33,3 (2)
Pouco eficiente e eficaz	16,7 (1)
Pouco eficiente e pouco eficaz	0,0
Inexistente	0,0
Sem resposta	16,7 (1)
CONFIDENCIALIDADE	**% (n)**
Eficiente e eficaz	50,0 (3)
Eficiente e pouco eficaz	33,3 (2)
Pouco eficiente e eficaz	0,0
Pouco eficiente e pouco eficaz	0,0
Inexistente	0,0
Sem resposta	16,7 (1)
AUTENTICIDADE	**% (n)**
Eficiente e eficaz	33,3 (2)
Eficiente e pouco eficaz	33,3 (2)
Pouco eficiente e eficaz	16,7 (1)
Pouco eficiente e pouco eficaz	0,0
Inexistente	0,0
Sem resposta	16,7 (1)

Planos de contingência implementados para mitigar problemas gerados por ataques cibernéticos às informações	**% (n)**
SIM	33,3 (2)
NÃO	16,7 (1)
EXISTEM PLANOS FUTUROS	33,3 (2)
Sem resposta	16,7 (1)

n= número de concessionárias

Apesar de não haver uma inconsistência no conjunto de respostas, o resultado obtido evidencia que as concessionárias brasileiras não têm tratado deste tema de forma integrada. A Agência Internacional de Energia (IEA)

considera que o desenvolvimento de uma política de segurança da informação é parte indissociável de uma estratégia de implantação de redes inteligentes (IEA, 2010). Desta forma, o esperado seria que todas as empresas investigadas declarassem ter uma política e que esta fosse reconhecida pela alta administração e com atividades bem definidas, dado que já possuem em curso atividades para a implantação de redes inteligentes.

Em relação às atividades desenvolvidas para garantir a segurança da informação, Clements (2010) afirma que diferentes processos e atividades devem ser desenvolvidos no cumprimento de uma política de segurança. O autor ressalta que a combinação destas atividades potencializa o grau de proteção do sistema. O Gráfico 5.4 mostra que as concessionárias escolheram uma ou outra atividade, quando deveriam ter escolhido um conjunto de opções que melhor traduzissem suas políticas de segurança.

De acordo com a norma ABNT NBR ISO/IEC 27001:2006, os planos de contingência devem ser desenvolvidos e implantados para a manutenção ou recuperação das operações e para assegurar a disponibilidade da informação no nível requerido e na escala de tempo requerida, após a ocorrência de interrupções ou falhas dos processos críticos da concessionária. Ao verificar os resultados para esta questão é preocupante o fato de que nem todas as concessionárias envolvidas com projetos de implantação de redes inteligentes têm um plano de contingência implantado.

A implantação de uma política pode ser verificada de forma pragmática pela verificação da efetiva implantação dos processos críticos de uma determinada atividade. Sob esta ótica pode-se afirmar que não obstante 50% das concessionárias terem declarado que suas políticas já se encontram implantadas falhas contundentes foram identificadas. Falhas essas que têm consequências importantes para a disponibilidade, integridade, confidencialidade e autenticidade da informação.

5.6.3.Vulnerabilidades

A vertente "*vulnerabilidades*" do instrumento de coleta teve por objetivo identificar se as concessionárias estão atentas para o fato de que a implantação das redes inteligentes tornará o sistema elétrico mais vulnerável a ataques cibernéticos.

A Tabela 5.4, abaixo, apresenta os resultados de um conjunto de cinco quesitos que foram formulados aos respondentes envolvidos em projetos de

implantação de redes inteligentes. Dentre as respostas mais relevantes destacam-se:

- 100% dos entrevistados reconhecem que as concessionárias estarão mais expostas a ataques cibernéticos com a introdução do *smart grid;*
- 67% declararam que, com a introdução de novas tecnologias e novos pontos de conexão, as concessionárias poderão ficar expostas a rupturas da confidencialidade dos dados dos consumidores.
- 50% dos respondentes informaram que não possuem um método definido para identificar, classificar e analisar riscos de segurança potenciais (i.e.: o mesmo percentual atribuído à questão que sugere que *um ataque cibernético poderá resultar na interrupção do fornecimento de energia elétrica*).

Na visão das concessionárias que responderam o questionário, os dados de medição refletem a opinião de 87% dos respondentes que percebem um maior *risco de sofrer um ataque*.

Tabela 5.4 - Questões investigativas sobre a vertente vulnerabilidade.

Previsão de exposição a ataques cibernéticos	**% (n)**
SIM	100,0 (6)
NÃO	0,0

Crescimento dos pontos de conexão x comprometimento da confidencialidade dos dados	**% (n)**
SIM	67,0 (4)
NÃO	33,0 (2)

Método definido para IDENTIFICAR, CLASSIFICAR e ANALISAR riscos de segurança potenciais	**% (n)**
SIM	33,3 (2)
NÃO	50,0 (3)
Sem resposta	16,7 (1)

Previsão de vulnerabilidade a ataque cibernético que resulte em interrupção do fornecimento de energia ou comprometimento da integridade do sistema	**% (n)**
SIM	50,0 (3)
NÃO	33,3 (2)
Sem resposta	16,7 (1)

Categoria de informação que possui maior risco de sofrer um ataque cibernético	% (n)
Medição	83,0 (5)
Faturamento	17,0 (1)
Contabilidade	0,0
Regulação	0,0
Outra(s)	0,0

n= número de concessionárias

Certamente, o reconhecimento do risco contribui para a redução da vulnerabilidade a que se expõe o sistema de informação da concessionária. Entretanto tal redução só é significativa quando se faz um mapeamento detalhado das principais características do risco. Embora todas as concessionárias investigadas sejam capazes de prever o risco de exposição a ataques cibernéticos, quando investigadas as medidas para redução deste risco, percebe-se que nem todas possuem um método definido para identificar, classificar e analisar tais riscos.

Baumeister (2010) fez uma revisão da literatura sobre segurança da informação nas redes inteligentes e concluiu que a introdução de novas funcionalidades e novos componentes trará consigo muitos novos riscos de ataques, tornando o sistema ainda mais vulnerável. Neste sentido, as concessionárias brasileiras estão corretas na percepção de que o aumento dos pontos de conexão pode comprometer a privacidade dos dados dos consumidores.

Por outro lado, em relação à categoria da informação que apresenta maior risco de sofrer ataque cibernético, foi apontado, por ampla maioria das concessionárias pesquisadas, apenas a medição. Segundo McAFee (2012) um dos desafios para assegurar a segurança das redes inteligentes é que os ataques podem assumir diferentes formas e ocorrer em distintos componentes da rede elétrica. No estudo, a ignorância acerca dos outros possíveis pontos vulneráveis pode ter relação com o fato de que a tecnologia *smart grid* no Brasil tem sido adotada apenas para a medição.

No entanto, uma vez que as concessionárias deverão expandir a adoção dessa tecnologia para novos componentes, há a necessidade de se desenvolver métodos para identificar que parte do sistema se apresenta mais vulnerável a um ataque cibernético. E, também, definir qual é o nível de proteção exigido e o custo para estabelecê-la (McAFee, 2012).

5.6.4.
Impactos

Em relação aos *impactos provenientes de um ataque cibernético às redes inteligentes*, 50% dos respondentes informaram que não há previsão de tempo necessário para recuperar os dados dos consumidores; 33,3% relataram que há expectativa de recuperar tais dados em 24 horas.

Tabela 5.5 - Tempo de recuperação

Tempo estimado para recuperação de dados dos consumidores	% (n)
Até 02 horas	0,0
Até 10 horas	0,0
Até 24 horas	33,3 (2)
Até 72 horas	0,0
Mais de 72 horas	0,0
Não há previsão	50,0 (3)
Sem Resposta	16,7 (1)

n= número de concessionárias

Um dos grandes desafios à implantação de uma *política de segurança da informação* refere-se à proteção adequada para minimizar os desastrosos efeitos de um possível ataque ao sistema de informação da concessionária. Para a maioria dos entrevistados, um ataque pode se propagar para outros setores da empresa: 29% preveem consequências desse ataque em outras infraestruturas críticas da empresa. A Figura 5.5 resume os achados desta parte da pesquisa.

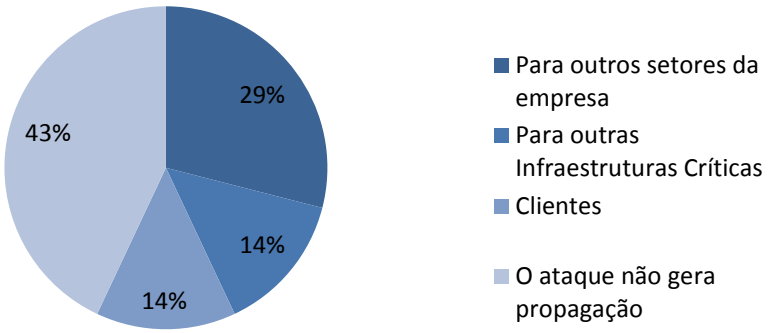

Figura 5.5 - Escala de propagação de um ataque as informações dos consumidores.

A Figura 5.6, abaixo, apresenta o nível de impacto proporcionado por um ataque cibernético. A apropriação indevida de dados dos consumidores foi a opção preterida pelos respondentes, reunindo o maior número de indicações (62,5%).

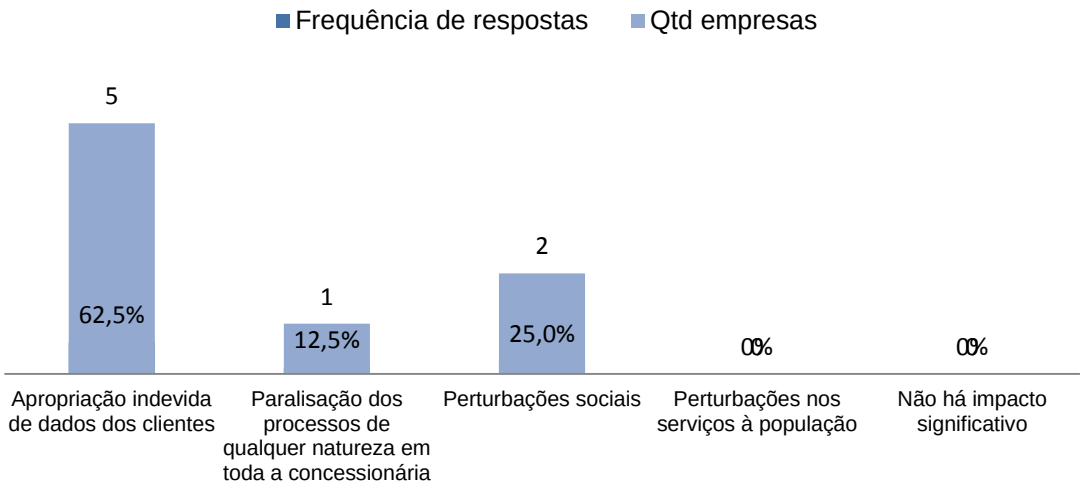

Figura 5.6 – Nível de impacto

Em relação ao que foi denominado *nível de recuperação dos dados do consumidor após um ataque cibernético*, cerca de 33% dos entrevistados relataram que possa haver recuperação total; os demais acreditam ser possível fazer uma recuperação parcial dos dados; mas, somente a metade dos respondentes acredita na possibilidade de perdas significativas resultarem de ataques cibernéticos.

Tabela 5.6 - Nível de recuperação

Nível de recuperação dos dados após ataque cibernético	**% (n)**
Recuperação total	33,33 (2)
Recuperação parcial com perdas insignificantes	33,33 (2)
Recuperação parcial com perdas significativas	33,33 (2)
Irrecuperável.	0,0

n= número de concessionárias

A vulnerabilidade de uma rede inteligente de energia elétrica é intrínseca à sua condição de existência, por isso o desenvolvimento de medidas de segurança é mandatório. Dentre as atividades voltadas para a garantia da

segurança, têm-se os modelos de previsão de propagação e impactos de um ataque a rede.

De acordo com Ardis (2012), um ataque a uma rede inteligente pode ser analisado sob a ótica de duas grandes categorias, que proporcionam diferentes impactos para rede. Na primeira categoria, o ataque é praticado individualmente, e tem como objetivo a manipulação dos dados para obter ganho particular. Nesta categoria a propagação é pequena e os prejuízos podem ser minimizados. Na segunda, o ataque pode ser uma ameaça social, incluindo atividades que redundem no mau funcionamento da rede. Neste caso, a propagação pode trazer prejuízos significativos, tanto para concessionária, quanto para a população em geral.

Prever os impactos de um ataque cibernético em uma rede inteligente está diretamente associado com o desenvolvimento dos métodos citados na vertente de análise denominada ***Vulnerabilidades***. Estes métodos devem estar voltados para identificar, classificar e analisar os riscos, no sentido de aumentar a resiliência das redes e, consequentemente, diminuir o impacto de eventos desfavoráveis, tais como os ataques cibernéticos.

Analisando a questão relativa ao tempo de retorno à normalidade em caso de ataque, é alarmante o resultado que aponta para um percentual elevado (50%) de concessionárias que não têm previsão do tempo para recuperação dos dados dos consumidores. É igualmente notório o fato de algumas concessionárias acreditarem que um ataque não gera propagação. De acordo com Morgan (2012), utilizando a rede americana como exemplo, um ataque de ordem social, com objetivo terrorista poderia provocar mais prejuízos ao sistema do que um desastre natural, a exemplo do que ocorreu com a passagem do furacão *Sandy*.

As respostas à questão sobre o nível de impacto esperado evidenciaram que a preocupação central é com a apropriação dos dados do consumidor, entretanto a coerência com a questão nível de recuperação desses dados não foi mantida, uma vez que 66,7% dos respondentes afirmaram que a recuperação total dos dados não é possível.

5.6.5. Normas

Para esta vertente da análise, duas questões foram formuladas: (i) permitir ao respondente identificar, dentre um conjunto de normas aplicáveis às redes

inteligentes listadas, aquelas com as quais estavam familiarizados e (ii) identificar a percepção do respondente sobre o grau de importância das normas aplicáveis à segurança da informação nas redes inteligentes.

Dentre as opções fornecidas na questão sobre *que normas estão sendo observadas*, apenas a norma NIST 800-53 foi reconhecida. Um dos entrevistados respondeu que a concessionária utiliza um conjunto de normas próprias (normas internas da empresa) para garantir a segurança da informação nas redes inteligentes. Um percentual elevado (66,6%) não respondeu a esta questão. Já em relação ao grau de importância das normas aplicáveis à segurança da informação, 100% dos entrevistados reconhecem a sua importância optando pela resposta “alto grau de importância”.

Tabela 5.7 - Normas adotadas e grau de importância

Normas de segurança da informação adotadas	**% (n)**
ABNR NBR 27002	0,0
NIST 800-53	16,7 (1)
NERC CIP	0,0
IEEE 1402-2000	0,0
Outras	16,7 (1)
Sem resposta	66,6 (4)

Grau de importância das normas aplicáveis à segurança da informação percebido	**% (n)**
Baixa	0,0
Média	0,0
Alta	100,0 (6)

n= número de concessionárias

Apesar de existirem poucas normas aplicáveis à segurança da informação nas redes inteligentes, muitas concessionárias têm prosseguido com implantações de seus projetos (Ardis, 2012). A implantação adequada das redes inteligentes impõe novas e desafiadoras demandas por normalização e regulamentação aplicável a esses sistemas inteligentes.

A literatura é uníssona ao apontar as consequências desastrosas que podem resultar das invasões às redes (Ardis, 2012), assim esperar-se-ia um maior comprometimento das concessionárias. No entanto, este comprometimento pode ser imposto por meio da regulação o que requer o

estabelecimento de medidas que minimizem os riscos relativos à implantação das redes inteligentes. Tal fato merece atenção do agente regulador, principalmente no que concerne ao desenvolvimento e à verificação da adoção de normas para setor.

6
Conclusões e recomendações

6.1.
Sobre os objetivos

Resgatando o objetivo central desta pesquisa de mestrado, i.e.: diagnóstico da segurança da informação na implantação das redes inteligentes, o trabalho confirma a tese de que, de fato, os riscos de ataques cibernéticos podem ser minimizados pela adoção de recomendações normativas específicas. Tais objetivos foram efetivamente alcançados já que o trabalho identificou questões críticas relevantes que devem ser tratadas na esfera normativa.

No que concerne os objetivos específicos originalmente formulados, esses foram igualmente alcançados. Quer com base na análise em profundidade dos documentos resgatados na pesquisa bibliográfica (que deram origem ao conteúdo explicitado no referencial teórico), quer pelos resultados da pesquisa de campo.

A revisão da literatura permitiu identificar que as normas recomendadas pelo documento ***NISTIR 7628 Guidelines for Smart Grid Cyber Security*** produzido pelo NIST são aplicáveis aos projetos de implantação de redes inteligentes que estão sendo desenvolvidos no Brasil. O diagnóstico realizado pelo NIST identificou cinco famílias de normas (**IEC 61970, IEC 61968, IEC 61850, IEC 60870-6 e IEC 62351**) que merecem atenção especial, tanto por parte do regulador (Aneel) ou diretamente pelas concessionárias.

A investigação junto às concessionárias brasileiras de energia elétrica pela via do estudo de caso permitiu a identificação de vulnerabilidades na segurança da informação. Dentre as detectadas destacam-se a ausência de método definido para identificar, classificar e analisar riscos de ataques cibernéticos.

A ausência destes métodos está relacionada com a indefinição ou ausência da política de segurança da informação para as redes inteligentes. Apesar das concessionárias investigadas estarem em fase de implantação de medidores inteligentes, esperava-se que todas declarassem dispor de uma política para segurança da informação, com atividades bem definidas e reconhecidas pela alta administração.

Todas as concessionárias investigadas reconhecem que a implantação das redes inteligentes de fato aumenta os riscos tornando o seu sistema informacional mais vulnerável a ataques cibernéticos. Entretanto, quando questionadas especificamente sobre que processos consideram mais críticos para a manutenção da segurança, são surpreendidas com a identificação de falhas contundentes que podem ter consequências marcantes para assegurar a disponibilidade, integridade, confidencialidade e autenticidade da sua informação.

A pesquisa realizada permitiu a conscientização de aspectos importantes relacionados aos riscos e impactos das falhas na segurança da informação. Explicitar esses aspectos mostrou-se estratégico para a concessionária permitindo-a evidenciar a necessidade da implantação de um sistema de segurança confiável nas concessionárias de energia elétrica brasileiras.

6.2. Sobre os resultados

Todas as vertentes de análise propostas contribuíram para a pesquisa realizada. No entanto, algumas questões do instrumento de coleta de dados não mereceu por parte da concessionária a atenção que se esperava. Até certo ponto é compreensível a omissão de alguns dados relacionados a investimentos de recursos financeiros pela concessionária para viabilizar a implantação de suas redes inteligentes, já que parte dessa informação é considerada confidencial por revelar sua estratégia corporativa. Entretanto, no que tange a adoção de normas voltadas para a garantia de informação, não existe explicação razoável para uma determinada concessionária mostrar desconhecimento sobre o acervo normativo relacionado à segurança da informação em suas redes inteligentes.

Em relação aos objetivos pretendidos pelas concessionárias que participaram da pesquisa — *redução de custos operacionais e perdas não-técnicas* — a pesquisa claramente evidenciou que estes são de fato os grandes desafios a serem vencidos no processo de modernização do setor elétrico brasileiro.

A vertente *segurança da informação* trouxe à luz duas situações preocupantes: (i) algumas concessionárias, mesmo em fase de implantação de medidores eletrônicos, não possuem um plano de segurança implantado e (ii) mesmo as concessionárias que o possuem, quando especificamente indagadas

sobre a execução de processos considerados críticos, revelaram fragilidade ao exibirem falhas contundentes que podem ameaçar seus sistemas.

Na vertente *vulnerabilidades* pode-se concluir que o reconhecimento do risco contribui para a redução da vulnerabilidade a que se expõe a concessionária. Entretanto, as características do risco precisam ser investigadas para se alcançar tal redução. Embora todas as concessionárias investigadas considerem real o risco de exposição a ataques cibernéticos, quando investigadas as medidas para redução desse risco, percebe-se que nem todas possuem uma estratégia definida para evitá-los; ou seja, para identificar, classificar e analisar tais riscos.

Os impactos de um ataque cibernético em uma rede inteligente estão diretamente associados ao desenvolvimento dos métodos citados na vertente de análise *vulnerabilidades*. Tais métodos devem ser capazes de identificar, classificar e analisar os riscos, com o objetivo de aumentar a resiliência da rede elétrica e, consequentemente, diminuir o impacto de eventos desfavoráveis.

Esta pesquisa evidenciou que as concessionárias de energia elétrica brasileiras desconhecem as normas aplicáveis à segurança da informação nas redes inteligentes. Pode-se observar que alguns projetos de implantação já se encontram em fase de execução sem que um plano de segurança tenha sido aplicado.

Por fim, o referencial teórico consolidado pela pesquisa produziu evidências de que a utilização das normas aplicáveis à segurança da informação podem sim minimizar os riscos de ataque. Fato esse que recomenda às concessionárias e ao regulador atenção especial às orientações específicas que emanam dessas normas.

6.3. Sobre os limites e limitações

Não obstante as limitações inerentes a qualquer estudo de caso (e.g.: falta de representatividade da amostra, significância estatística das respostas; limitação da visão especialista; representação do problema objeto do estudo pelo questionário), acredita-se que o estudo de caso atendeu aos seguintes critérios chave:

- definição clara dos objetivos da pesquisa;
- aderência aos preceitos do referencial teórico;
- desenvolvimento de um instrumento de coleta de dados alinhado com o objetivo geral da pesquisa.

- seleção das concessionárias com elevado potencial de contribuição para esta pesquisa;
- representatividade e significância estatística.

Dentre as limitações do estudo de caso destacam-se:

- dificuldade de envolvimento de um maior número de concessionárias, o que é compreensível neste momento crítico em que as concessionárias renegociam com o governo a renovação nº 579 de suas concessões;
- impossibilidade de captar uma visão média da concessionária sobre o tema, não obstante o único respondente da concessionária ter declarado possuir amplo conhecimento do seu projeto *smart grid*;
- entrevistas fundamentadas em experiência ainda incipiente das concessionárias que estão apenas em fase inicial de implantação de seus projetos *smart grid*.

6.4. Recomendações

Para fins de minimização das vulnerabilidades apontadas nas redes inteligentes por meio da adoção de recomendações normativas específicas, recomenda-se:

- desenvolver um modelo de referência de alto nível conceitual para as redes inteligentes;
- especificar um conjunto de lacunas e questões de alta prioridade relacionadas à normalização aplicável;
- implantar uma política de segurança da informação para as redes inteligentes com definição clara de métodos para identificar, classificar e analisar riscos de ataque ao sistema;
- desenvolver ações imediatas visando à normalização das redes inteligentes, através de participação ativa dos diversos atores (governo, concessionárias, institutos de pesquisa, fabricantes, consumidores, etc.) junto às entidades nacionais e internacionais de normalização (ABNT, IEC, ANSI, IEEE, etc.);
- Fomentar fóruns de discussões e criação de ambientes de cooperação para o tema ***segurança da informação nas redes inteligentes***, inclusive com a participação de organismos internacionais.

O referencial teórico desta pesquisa evidenciou que o conceito de redes inteligentes ainda está em fase de consolidação. Algumas tecnologias necessárias estão em fase inicial de desenvolvimento ou são apenas conceitos. Por esta razão, é necessário investir em trabalhos futuros de desdobramento desta pesquisa e aprofundamento dos resultados. Neste sentido, propõem-se o desenvolvimento de projetos de pesquisa para avaliação e gestão de riscos de ataques cibernéticos. Uma abordagem baseada em risco é uma forma potencial

para desenvolver soluções viáveis para tratar e medir a eficácia dessas soluções. Esta abordagem no âmbito das redes inteligentes suscita uma série de desafios de pesquisa. Três desses desafios são:

1. **análise do ataque cibernético**. Embora seja claro que os ataques cibernéticos representam uma ameaça significativa para as redes inteligentes, ferramentas avançadas e metodologias são necessárias para fornecer uma análise profunda dos ataques cibernéticos e suas consequências sobre a rede inteligente.
2. **medição do risco à exposição ao ataque cibernético**. Desenvolver ferramentas e técnicas avançadas que ofereçam noções quantitativas dos riscos, ou seja, ameaças, vulnerabilidades e consequências de ataque para as redes inteligentes, permitindo melhor proteção e regulação dos sistemas.
3. **definição do investimento adequado**. As soluções para segurança cibernética são implantadas para mitigar riscos. No entanto, é difícil avaliar em que medida tal risco foi mitigado. Por isso, uma questão relevante é saber que nível de investimento é apropriado para uma determinada concessionária. Investigação sobre as ferramentas e tecnologias avançadas baseada em noções de riscos quantitativos podem fornecer insights mais profundos para responder a esta pergunta.

7
Referências Bibliográficas

ARDIS, K. **Securing the Smart Meter**. USA, 2012. Disponível em: http://www.maximintegrated.com/app-notes/index.mvp/id/5337?utm_source=Metering.com&utm_medium=newsletter&utm_content=Push%20Email%20-%20AN%205337&utm_campaign=Smart%20Grid&utm_term=Q213

Associação Brasileira de Distribuidores de Energia Elétrica – Abradee. **Dados de mercado das empresas distribuidoras associadas**. 2012.

Associação Brasileira de Normas Técnicas - ABNT. **ABNT NBR ISO/IEC17799 - Tecnologia da informação - Técnicas de segurança – Sistemas de gestão de segurança da informação - Requisitos**. Rio de Janeiro, 2005.

Associação Brasileira de Normas Técnicas - ABNT. **ABNT NBR ISO/IEC 27002 - Código de Prática para a Gestão de Segurança da Informação**. Rio de Janeiro, 2005.

Associação Brasileira de Normas Técnicas - ABNT. **ABNT NBR ISO/IEC 27001 - Tecnologia da informação - Técnicas de segurança – Sistemas de gestão de segurança da informação - Requisitos**. Rio de Janeiro, 2006.

Associação Brasileira de Normas Técnicas - ABNT. **ABNT NBR ISO/IEC 27003 - Tecnologia da informação – Técnicas de segurança – Diretrizes para implantação de um sistema de gestão da segurança da informação**. Rio de Janeiro, 2011.

Associação Brasileira de Normas Técnicas - ABNT. **ABNT NBR ISO/IEC 27004 - Tecnologia da informação — Técnicas de segurança — Gestão da segurança da informação — Medição**. Rio de Janeiro, 2009.

Associação Brasileira de Normas Técnicas - ABNT. **ABNT NBR ISO/IEC 27005 - Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação**. Rio de Janeiro, 2011.

Associação Brasileira de Normas Técnicas - ABNT. **ABNT NBR ISO/IEC 27007 - Diretrizes para auditoria de sistemas de gestão da segurança da informação**. Rio de Janeiro, 2011.

Agência Brasileira de Desenvolvimento Industrial – ABDI. **Relatório de acompanhamento setorial – Smart grid: tendências no mundo e no Brasil e possibilidade de desenvolvimento produtivo e tecnológico**. 2012.

ALCÂNTARA, M. V. P., **Aspectos Regulatórios e Projetos de P&D na Implementação da Rede Inteligente**, apresentado no IV Fórum Latino-Americano de *Smart grid*, São Paulo, 2012.

Agência Nacional de Energia Elétrica - ANEEL. **Resoluções nº 345 - uso compulsório de sistemas geo-processados. Brasília, 2008.**

Agência Nacional de Energia Elétrica - ANEEL. Consulta pública nº 015/2009. **Análise das contribuições recebidas no âmbito da Consulta Pública nº 015/2009, instaurada com o objetivo de coletar subsídios sobre implantação de medidores eletrônicos em unidades consumidoras de baixa tensão**. Brasília, 2009.

Agência Nacional de Energia Elétrica - ANEEL. **Resolução Normativa nº 375 - regulamentação da utilização do PLC. Brasília, 2009.**

Agência Nacional de Energia Elétrica - ANEEL. **Chamada pública nº 011/2010 – Projeto estratégico: Programa brasileiro de rede elétrica inteligente**. Brasília, 2010.

Agência Nacional de Energia Elétrica - ANEEL. **Resolução Normativa nº 464 - estabelecimento da tarifa branca. Brasília, 2011.**

Agência Nacional de Energia Elétrica - ANEEL. **Resultados da Audiência Pública nº 43/2010**. Brasília, 2012.

Agência Nacional de Energia Elétrica - ANEEL. **ANEEL regulamenta medidores eletrônicos. Brasília, 2012.**

Agência Nacional de Energia Elétrica - ANEEL. **Resolução Normativa nº 482 - conexão de micro e minigeração distribuída. Brasília, 2012.**

AMIN, M; Wollenberg, B. **Toward a *Smart grid***. IEEE Power & Energy Magazine, 2005.

AMIN, M; GIACOMONI, A. ***Smart grid* – safe, secure, self-healing. Challenges and opportunities in power system security, resiliency e privacy**. IEEE Power & Energy Magazine, 2012.

AVRUCH, M. **Um terço das empresas brasileiras foi vítima de crime digital no último ano**. PricewaterhouseCoopers, 2012. Disponível em: http://www.pwc.com.br/pt/sala-de-imprensa/assets/press-release/pesquisa-crimes-economicos-press-release.pdf

BAUMEISTER, T. **Literature Review on *Smart grid* Cyber Security**. University of Hawaii, 2010.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Guia de referência para a segurança das infraestruturas críticas da informação.** Brasília: GSIPR/SE/DSIC, 2010.

BREKKE, K.; VAILATI, R.; EVANS, G.; ESTEVES, J.; KAPETANOVIC, T.; FRIEDL, W.; STEINER, M.; SCHOTMAN, H.; HEMBERGER, K.; FERRIERES, F. **Aspectos regulatórios das redes inteligentes de energia**. Trabalho apresentado no Cired Workshop 2010. Lyon, France.

BOUHAFS, F.; MACKAY, M.; MERABTI, M. **Links to the Future: Communication Requirements and Challenges in the *Smart grid***. Power and Energy Magazine. IEEE, 2012

CLEMENTS, S; KIRKHAM, H. **Cyber-security considerations for the *smart grid***. Power and energy society general meeting. IEEE, 2010.

Centro de Pesquisa e Desenvolvimento em Telecomunicações – CPQD. ***Smart grid*: energia inteligente no Brasil**. 2012. Disponível em: http://www.cpqd.com.br/solucoes-e-produtos/smart-grid.html.

Confederação Nacional da Indústria (CNI). **Normalização: conhecendo e aplicando na sua empresa.** Brasília, 2002

Departament of Energy Climate Change – DECC. **Impact Assessment of the Climate Change Act**. United Kindon, 2009. Disponível para download em: http://www.decc.gov.uk/en/content/cms/legislation/cc_act_08/cc_act_08.aspx

Empresa de Pesquisa Energética – EPE. **Plano Nacional de Energia 2030 – Capítulo: Eficiência Energética**. Brasília, 2006-2007.

FALCÃO, D. M. **Integração de Tecnologias para Viabilização da *Smart grid***. Anais do III Simpósio Brasileiro de Sistemas Elétricos (SBSE). Pará, 2010. Disponível em: http://labplan.ufsc.br/congressos/III%20SBSE%20-%202010 /PDF/SBSE2010-0241.pdf.

GARCIA, D. A. A; JUNIOR, F. E. D. **Aspectos de evolução do *smart grid* nas redes de distribuição**. Revista: O setor elétrico, ed. 75. 2012. Disponível em: http://www.osetoreletrico.com.br/web/a-revista/edicoes/836-capitulo-iii-aspectos-de-evolucao-do-smart-grid-nas-redes-de-distribuicao.html

GUNGOR, V.C.; LU, B.; HANCKE, G.P. **Opportunities and Challenges of Wireless Sensor Networks in *Smart grid***. IEEE on Trans. Ind. Electron., 2010.

GUNGOR, V.C., SAHIN, D., KOCAK, T., ERGUT, S, BECCELLA, C., CECAT, C., HANCKE, G. ***Smart grid* Technologies: Communication Technologies and Standards**. IEEE, 2011.

HLEDIK, R. How Green Is the SmartGrid? The Electricity Journal. Elsevier Inc, 2009. Disponível em: http://www.sciencedirect.com/science/article/ pii/ S1040619009000608.

International Electrotechnical Commission (IEC). **Lidando com o Desafio da Energia - O Papel da IEC**. Genebra, 2010.

International Electrotechnical Commission (IEC). **SG 3 - Strategic Group on *Smart grid***. Genebra, 2012.

Institute of Electrical and Electronic Engineers (IEEE). **IEEE 1402-2000 - IEEE Guide for Electric Power Substation Physical and Electronic Security**, 2000.

Laverty, D. M.; MORROW, D. J.; BEST, R.; CROSSLEY, P. A. Telecommunications for *Smart grid*: Backhaul solutions for the distribution network. IEEE Power and Energy Society General Meeting, 2010.

LEITE, D. R. V.; Lamin, H.; Albuquerque, J. M. C.; CAMARGO, I. M. T. **Regulatory Impact Analysis of Smart Meters Implementation in Brazil**. IEEE, 2012.

LOPES, Y., FRANCO, R., MOLANO, D., SANTOS, M., CALHAU, F., BASTOS, C., MARTINS J., FERNANDES, N. ***Smart grid* e IEC 61850: Novos desafios em redes e telecomunicações para o Sistema Elétrico**. XXX Simpósio Brasileiro de Telecomunicações. Brasília, 2012.

MAFFEZZOLLI, E. C.; BOEHS, Carlos Gabriel Eggert. **Uma reflexão sobre o estudo de caso como método de pesquisa**. Revista da FAE, v. 11, p. 95-110, 2008.

McAfee, inc. **Smart protection for the *smart grid***. Canada, 2012.
Disponível em: http://www.mcafee.com/ca/resources/reports/rp-smarter-protection-smart-grid.pdf

Ministério de Minas e Energia (MME). **Relatório *Smart grid***. 2010. Disponível em: http://www.mme.gov.br/mme/galerias/arquivos/acoes/Energia/Relatxrio_GT_Smart_Grid_Portaria_440-2010.pdf

Morgan, M. G. **U.S. power grid 'inherently vulnerable' to terrorist attacks**. Washington, 2012
Disponível em: http://www.metering.com/node/21830

Nansen S. A. Instrumentos de Precisão (Nansen). **Redes inteligentes: como passo inicial do conceito *Smart grid***. Belo Horizonte, 2010.
Disponível em: http://www.tec.abinee.org.br/2010/arquivos/s04.pdf

NORDELL, D. **Terms of protection**. IEEE power & energy magazine, 2012

National Institute of Standards and Technology (NIST). ***Smart grid* Cyber Security Strategy, Architecture and High Level Requirements**. U. S. Department of Commerce, 2010.

National Institute of Standards and Technology (NIST). **NIST & the *Smart grid***. 2012. Disponível em: http://www.nist.gov/smartgrid/nistandsmartgrid.cfm

National Institute of Standards and Technology (NIST). **Identified Standards for Consideration by Regulators, Release 1.0**. U.S. Department of Commerce, 2010.

National Institute of Standards and Technology (NIST). **NISTIR 7628 Guidelines for *Smart grid* Cyber Security (3 vols.)**. U.S. Department of Commerce, 2010.

National Institute of Standards and Technology (NIST). **NIST to Launch Forum for Views on Consumer Interface to the *Smart grid***. U.S. Department of Commerce, 2010.

National Institute of Standards and Technology (NIST). **NIST Framework and Roadmap for *Smart grid* Interoperability Standards**, Release 1.0. U.S. Department of Commerce, 2010.

Norton/Symantec. **Norton Cybercrime Report**. 2012. Disponível em: http://now-static.norton.com/now/en/pu/images/Promotions/ 2012/ cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

OLIVEIRA, M., MAÇADA, A. C. G., GOLDONI, V. **Análise da Aplicação do Método Estudo de Caso na Área de Sistemas de Informação**. 30º encontro da ANPAD. Salvador, 2006.

Organisation for economic co-operation and development – OECD. **Smart Sensor Networks: Technologies and Applications for Green Growth**. OCDE, 2009. Disponível em: http://www.oecd.org/sti/44379113.pdf

PIMENTEL, P. **Normas Globais para *Smart grid*s**. IEEE/PES, 2010.

PricewaterhouseCoopers (PwC). **Crimes digitais - como combater a ameaça crescente**. 2011. Disponível em: http://www.pwc.com.br/pt_BR/br/publicacoes/ assets/pesquisa-crimes-digitais-11.pdf

PEARSON, I. ***Smart grid* cyber security for Europe**. Elsevier Energy Policy, 2011.

RAHMAN, S. ***Smart grid* expectations - what will make it a reality**. IEEE power & energy magazine, 2009.

SMB *Smart grid* Strategic Group (SG3). **IEC *Smart grid* Standardization Roadmap**. 2010. Disponível em: http://www.iec.ch/smartgrid/downloads/ sg3_roadmap.pdf

Science Applications International Corporation (SAIC). **San Diego *Smart grid* Study Final Report**. San Diego, 2006.

SHARGAL, M. and HOUSEMAN, D. **The Big Picture of Your Coming *Smart grid***. *Smart grid* News, 2009. Disponível em: http://www.smartgridnews.com/artman/publish/commentary/ The_Big_Picture_of_Your_Coming_Smart_Grid-529.html

The *Smart grid*s Task Force – SGTF. **Regulatory recommendations for data safety, data handling and data protection**. European Commission, 2011. Disponível em: http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/ expert_ group2.pdf.

VERGARA, Sylvia Constant. **Projetos e relatórios de pesquisa em administração**. 9 ed. São Paulo: Atlas, 2007.

VIEIRA, J., GRANATO, S. **Medição inteligente e a *smart grid***. *Smart grid* News, 2011. Disponível em: http://smartgridnews.com.br/conheca-com-exclusividade-o-primeiro-trabalho-sobre-smart-grid-desenvolvido-por-pesquisadores-brasileiros/

YIN, Robert K. **Estudo de caso: planejamento e métodos**. 4 ed. Porto Alegre: Bookman, 2010.

ZHANG Zhigang, et al. **Information Security Requirements and Challenges in *Smart grid***. IEEE, 2011.

Zpryme Research & Consulting. **Brazil – The *Smart grid* Network. 2011**. Disponível em: http://smartgridresearch.org/wp-content/uploads/sgi_reports/ Brazil _The_Smart_Grid_Network_October_2011_Zpryme_Research.pdf

8
Apêndice A – Instrumento de coleta de dados

Pesquisa sobre Segurança de dados no ambiente Smart Grid

Prezado Respondente,
Em cooperação com a ABRADEE, a Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio) está desenvolvendo uma pesquisa com o objetivo de propor modificações na arquitetura de segurança das redes convencionais de informação assim orientando as concessionárias a superar vulnerabilidades impostas pela implantação de seus projetos de redes inteligentes de energia (*smart grids*). Para assegurar rigor acadêmico ao trabalho, a pesquisa desenvolve-se na forma de uma dissertação de Mestrado do Programa de Pós-Graduação em Metrologia para Qualidade e Inovação da Pontifícia Universidade Católica do Rio de Janeiro.

As informações serão tratadas no conjunto das respostas; nenhuma informação individual será divulgada assim assegurando a completa confidencialidade dos respondentes. O questionário foi construído para ser objetivo e rapidamente respondido. Ao solicitar a sua visão especialista sobre esse importante tema relacionado à segurança da informação no âmbito das redes inteligentes, assumimos o compromisso de resguardar a confidencialidade da sua opinião e de compartilhar os resultados finais da pesquisa na dissertação de mestrado. Antecipadamente agradecemos pela sua valiosa participação.

Atenciosamente,
Everaldo Costa <everaldo.costa@choice.com.br>
Eventuais dúvidas deverão ser encaminhadas à Coordenação do Programa de Pós-Graduação em Metrologia para Qualidade e Inovação da PUC-Rio: Prof. Mauricio N. Frota <mfrota@puc-rio.br>

Nome do Respondente:
Concessionária: AMPLA
Email:
Nota: Se conveniente favor recomendar Nome/E-mail de outro Respondente

---

BLOCO 1: VISÃO GERAL

1) Quais são os principais objetivos estratégicos que a empresa espera alcançar pela implantação das tecnologias de Smart Grid?

[ ] Redução de custos operacionais (racionalização do consumo; reposição de medidor com defeito; leitura, corte e religação);
[ ] Impacto nos indicadores de qualidade e de continuidade;
[ ] Comportamento dos consumidores;
[ ] Ganhos de eficiência energética
[ ] Redução de perdas não-técnicas e correção de inadimplência;

2) Qual é o principal responsável pela garantia da segurança da informação no ambiente Smart Grid?

[ ] Agência Reguladora - Aneel
[ ] Concessionária
[ ] Fornecedores de tecnologia
[ ] Outro (s) _____

3) Qual é a situação da política de segurança da informação e comunicações da organização?

[ ] Implantada. Responsabilidades bem definidas. Há comprometimento da alta administração;
[ ] Implantada. Responsabilidades bem definidas. Sem comprometimento da alta administração;
[ ] Implantada. Há comprometimento da alta administração. Responsabilidades ainda não foram totalmente definidas;
[ ] Implantada. Não há comprometimento da alta administração. Responsabilidades ainda não foram bem definidas;
[ ] Não está implantada, mas está em processo de elaboração;
[ ] Não está implantada, e ainda não está sendo elaborada.

4) Quais atividades estão sendo realizadas para garantir a segurança da informação no ambiente Smart Grid?

[ ] Identificação de não-conformidades (vulnerabilidades);
[ ] Análise de riscos;
[ ] Introdução de suporte técnico adequado;
[ ] Implantação de uma base tecnológica com padrão de segurança de acordo com as principais normas nacionais e internacionais;
[ ] Implementação de um plano de contingência.

5) Qual é a situação atual dos processos e atividades necessários para assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação de cada cliente?

Disponibilidade:

[ ] Eficiente e eficaz;
[ ] Eficiente e pouco eficaz;
[ ] Pouco eficiente e eficaz;
[ ] Pouco eficiente e pouco eficaz;
[ ] Inexistente.

Integridade:

[ ] Eficiente e eficaz;
[ ] Eficiente e pouco eficaz;
[ ] Pouco eficiente e eficaz;
[ ] Pouco eficiente e pouco eficaz;

[ ] Inexistente.

Confidencialidade:

[ ] Eficiente e eficaz;
[ ] Eficiente e pouco eficaz;
[ ] Pouco eficiente e eficaz;
[ ] Pouco eficiente e pouco eficaz;
[ ] Inexistente.

Autenticidade:

[ ] Eficiente e eficaz;
[ ] Eficiente e pouco eficaz;
[ ] Pouco eficiente e eficaz;
[ ] Pouco eficiente e pouco eficaz;
[ ] Inexistente.

6) Existem planos implementados de contingência para mitigar os problemas gerados por ataques cibernéticos às informações dos clientes?

[ ] SIM; [ ] NÃO; [ ] EXISTEM PLANOS FUTUROS PARA IMPLEMENTÁ-LOS

7) Considerando o orçamento total do projeto de implantação das redes inteligentes (smart grid), qual é o percentual destinado à segurança da informação?

Percentual: _____

BLOCO 2: RISCOS DE UM ATAQUE CIBERNÉTICO

8) Existe alguma metodologia ou processo definido para IDENTIFICAR, CLASSIFICAR e ANALISAR riscos de segurança potenciais?
[ ] SIM [ ] NÃO

9) É sabido que a adoção de tecnologias Smart Grid expõe o sistema de dados da concessionária. Com a adoção do Smart Grid essa concessionária antevê algum risco de exposição a potenciais ataques cibernéticos?
[ ] SIM [ ] NÃO

10) A partir da adoção de tecnologias de Smart Grid, a concessionária prevê um aumento da vulnerabilidade e a ocorrência de um ataque cibernético capaz de resultar em interrupção do fornecimento de energia ou comprometimento da integridade de softwares e sistemas?
[ ] SIM [ ] NÃO

11) O crescimento dos pontos de conexão e caminhos para potenciais ataques pode comprometer a confidencialidade dos dados, incluindo a violação da privacidade do cliente?
[ ] SIM [ ] NÃO

12) Que categoria de informação possui maior risco de sofrer um ataque cibernético?
[ ] Medição
[ ] Faturamento
[ ] Contabilidade
[ ] Regulação
[ ] outra(s) _____

BLOCO 3: IMPACTOS

13) Qual a estimativa de retorno à normalidade caso ocorram incidentes que comprometam informações relativas ao cliente?

[ ] Até 02 horas;
[ ] Até 10 horas;
[ ] Até 24 horas;
[ ] Até 72 horas;
[ ] Mais de 72 horas.
[ ] Não há previsão

14) Um ataque realizado aos dispositivos que armazenam as informações dos clientes poderá se propagar em que escala?

[ ] Para outros setores da empresa;
[ ] Para outras Infraestruturas Críticas;
[ ] Clientes;
[ ] O ataque não gera propagação.

15) Em caso de ataque, qual é o nível de impacto esperado?

[ ] Apropriação indevida de dados dos clientes;
[ ] Paralisação dos processos de qualquer natureza em toda a concessionária;
[ ] Perturbações sociais;
[ ] Perturbações nos serviços à população;
[ ] Não há impacto significativo.

16) Quanto à capacidade de recuperação do ativo de informação e das operações:

[ ] Recuperação total;
[ ] Recuperação parcial com perdas insignificantes;
[ ] Recuperação parcial com perdas significativas;
[ ] Irrecuperável.

BLOCO 4: NORMAS

17) Em relação à segurança da informação, que NORMAS estão sendo observadas?

[ ] ABNR NBR 27002
[ ] NIST 800-53
[ ] NERC CIP
[ ] IEEE 1402
[ ] Outras (favor indicar): _____

18) Como a Concessionária avalia a importância de conformidade às NORMAS aplicáveis a para segurança da informação?

[ ] Baixa
[ ] Média
[ ] Alta

9
Anexos

9.1.Anexo I – Resultados da Audiência Pública nº 43/2010

PROCESSO: 48500.005714/2009-46
INTERESSADO: Distribuidoras e Consumidores
RELATOR: Diretor André Pepitone da Nóbrega
RESPONSÁVEL: SUPERINTENDÊNCIA DE REGULAÇÃO DOS SERVIÇOS DE DISTRIBUIÇÃO - SRD
ASSUNTO: Resultados da Audiência Pública nº 43/2010, que objetivou obter subsídios e informações adicionais para o estabelecimento de resolução normativa sobre os requisitos mínimos para os medidores eletrônicos de unidades consumidoras de baixa tensão.

I. R E L A T Ó R I O

A Audiência Pública – AP 43/2010 objetivou obter subsídios e informações adicionais para o estabelecimento de resolução normativa acerca dos requisitos mínimos para os medidores eletrônicos a serem empregados em unidades consumidoras de baixa tensão.

2. Na AP 43/2010, além da minuta de resolução, também foi disponibilizada a Nota Técnica no 44, de 17 de setembro de 2010, emitida pela Superintendência de Regulação dos Serviços de Distribuição – SRD, que apresentou a análise e a fundamentação da proposta para debate com a sociedade.

3. O prazo para recebimento de contribuições foi de 1o de outubro de 2010 a 28 de janeiro de 2011, com sessão presencial realizada em Brasília em 26 de janeiro de 2011. Ao fim desse período, a ANEEL recebeu 212 contribuições de 57 agentes, com sugestões de consumidores, consultores, distribuidoras, fabricantes de medidores, associações setoriais entre outros. Na Sessão presencial foram realizadas 19 exposições orais com apresentação de comentários e contribuições.

4. A SRD, pela Nota Técnica nº 98, de 29 de junho de 2012, analisou as contribuições recebidas na Audiência Pública e consolidou a proposta final de regulamento.

5. Dentre as 212 sugestões recebidas, 16 foram aceitas e 65, parcialmente aceitas, com as respectivas implicações inseridas no texto da minuta de resolução revisada, como demonstrado no Quadro 1. A Nota Técnica nº 98, de 2012, contém Anexo intitulado “Relatório de Análise de Contribuições” com o exame e a sugestão sobre o aproveitamento de cada uma das contribuições recebidas na Audiência Pública, assim como a minuta de resolução proposta pela área técnica.

Quantidade de Contribuições				
Aceita	**Parcialmente aceita**	**Não aceita**	**Não aplicável**	**Total**
16 (7,5%)	65 (30,7%)	126 (59,4%)	5 (2,4%)	212 (100%)

Quadro 1 – Número de contribuições recebidas por meio da AP no 43/2010
Fonte: Nota Técnica no 98/2012-SRD/ANEEL.

6. A Procuradoria-Geral da ANEEL conheceu da minuta de resolução normativa e a referendou.

II. F U N D A M E N T A Ç Ã O

7. Preliminarmente, destacam-se os motivadores e os passos percorridos pela ANEEL a fim de regulamentar os sistemas de medição eletrônica a serem instalados em unidades consumidoras de baixa tensão.

8. Os sistemas elétricos de distribuição passarão, nos próximos anos, por mudanças significativas provenientes da integração das redes de distribuição com as tecnologias de automação, informação e telecomunicações, o que transformará a rede elétrica de baixa tensão na nova supervia para transportar elétrons.

9. Tais mudanças serão impulsionadas, sobretudo, com o aumento significativo das fontes de geração distribuída, permitindo que milhões de brasileiros produzam a própria energia para compartilhar o excedente entre os pares.

10. O conceito de redes inteligentes - Smart Grid constitui, em síntese, a infraestrutura que integra equipamentos e redes de comunicação de dados ao

sistema de fornecimento de energia elétrica; isso transformará a rede elétrica existente em uma “Internet” de energia, aliando transporte de elétrons e de informação. Assim, os medidores digitais de energia elétrica representam o primeiro passo para o desenvolvimento das redes elétricas inteligentes.

11. Ouso dizer, concordando com Jeremy Rifkin[8], que as redes inteligentes impactarão tão significativamente as nações no século XXI quanto a Primeira Revolução Industrial o fez no século XIX: incentivando a energia renovável; transformando residências e edificações em microgeradores de energia, que injetam energia oriundas de fontes limpas (eólica ou fotovoltaica) na rede local; permitindo o uso da tecnologia da Internet para transformar a rede elétrica de todo o país em uma rede de compartilhamento de energia que age como a Internet.

12. Recentemente, em reportagem jornalística veiculada em jornal de circulação nacional[9], foi dito que o mercado brasileiro de redes inteligentes será o terceiro maior do mundo.

13. A necessidade de integrar e harmonizar toda essa tecnologia tornou-se clara para a ANEEL Desse modo, a Agência tem realizado diversas ações no sentido de preencher lacunas regulatórias, permitindo a introdução de tais mudanças no setor de distribuição de energia elétrica.

14. Em setembro de 2008, a ANEEL realizou em Brasília o “Seminário Internacional sobre Medição Eletrônica”, estimulando a discussão sobre implantação de medição eletrônica em unidades consumidoras de baixa tensão, sobre abordagem regulatória, funcionalidades agregadas e experiências de implantação.

15. Além de integrantes de empresas e associações do Setor Elétrico brasileiro, participaram do evento palestrantes internacionais da Itália, da Espanha e do Canadá, os quais apresentaram suas experiências sobre o tema, uma vez que esses Países já desenvolveram estudos, regulamentação e, em alguns casos, a própria substituição dos equipamentos.

16. Na sequência, foi instaurada pela SRD a Consulta Pública 15/2009 para orientar as discussões a respeito do tema. Em abril de 2009, foi realizada, por

[8] RIFKIN, Jeremy. **A terceira Revolução Industrial** – Como o poder lateral está transformando a Energia, a economia e o mundo.

[9] Setti, Rennan. Smart Grid vai turbinar a rede elétrica do país. **O GLOBO**, Rio de janeiro, 20 mai. 2012. Disponível em: <http:// http://oglobo.globo.com/tecnologia/smart-grid-vai-turbinar-rede-eletrica-do-pais-4952797>

servidores da Agência, missão técnica a Portugal, Espanha e Itália a fim de conhecer e acompanhar as experiências desses Países na implantação em grande escala da medição inteligente[10].

17. Além da realidade europeia, servidores da Agência também acompanharam as iniciativas que vêm sendo adotadas nos Estados Unidos da América. Em setembro de 2009, foi realizada missão técnica para conhecer a experiência norte-americana na implantação da medição inteligente. Foram visitadas instituições com *know how* em medição eletrônica e redes inteligentes.

18. Em setembro de 2009, foi efetuada audiência para o público interno da ANEEL – API 3/2009[11], momento em que foi possível obter contribuições de diferentes áreas.

19. Registra-se a participação da ANEEL no Grupo de Trabalho instituído[12] pelo Ministério de Minas e Energia – MME com o intuito de "[...] analisar e identificar ações necessárias para subsidiar o estabelecimento de políticas públicas para a implantação de um Programa Brasileiro de Rede Elétrica Inteligente - Smart Grid". Além de integrantes da ANEEL, o Grupo de Trabalho era constituído por representantes da Empresa de Pesquisa Energética - EPE, do Centro de Pesquisas de Energia Elétrica - Eletrobras Cepel e do Operador Nacional do Sistema Elétrico - ONS. Durante as reuniões do Grupo, a minuta de resolução posteriormente submetida à Audiência Pública 43/2012 foi levada ao debate e recebeu contribuições dos participantes.

20. Acentua-se também que, desde o início dos estudos, a ANEEL tem promovido reuniões com fabricantes de medidores e sua associação, provedores de tecnologia de informação e telecomunicações, distribuidoras, Instituto Nacional de Metrologia, Normalização e Qualidade Industrial - INMETRO, entre outros agentes envolvidos no tema. Em tais encontros foram abordados aspectos relacionados à implantação dessa tecnologia no País tais como tecnologias utilizadas e regulamentação metrológica associada.

21. Constata-se, portanto, que a ANEEL percorreu logo caminho, de aproximadamente 4 anos de estudos e debates com os maiores especialistas do tema, bem como analisou diversas iniciativas bem sucedidas em outros países.

[10] A Nota Técnica nº 59/2009-SRD/SRC/ANEEL contém o relato e as conclusões da visita.

[11] A Nota Técnica no 117/2009-SRD/ANEEL consolidou as contribuições recebidas.

[12] Portaria MME nº 440, de 15 de abril de 2010.

Ressaltam-se as viagens técnicas de seus servidores, inclusive deste Relator, envolvidos diretamente nos trabalhos.

22. Já durante a AP 43/2010, a ANEEL recebeu pouco mais de 200 contribuições enviadas por consumidores e conselhos de consumidores, indústrias de tecnologia, distribuidoras de energia, entidades do Setor Elétrico e de defesa do consumidor, associações ligadas ao Setor, entre outras. Ou seja, se existe um tema que tenha exigido estudos e interação com a sociedade, o desta regulamentação pode ser citado como exemplo.

Iniciativas internacionais

23. Os estudos relacionados às redes inteligentes vêm se desenvolvendo em todo o mundo, e a ANEEL sempre buscou verificar como o tema está sendo tratados em diversas nações. Com isso, foi possível compreender os motivos que as levaram a introduzir comunicação nas redes elétricas, as circunstâncias que conduziram a essa decisão, as dificuldades encontradas e os benefícios alcançados. Desse conhecimento, pôde-se identificar o que é aplicável ao Brasil.

24. A observância às experiências internacionais constitui etapa relevante para os estudos do assunto no Brasil. Neste ponto, é essencial que se discorra, embora resumidamente, sobre os principais casos no mundo. Em 2009, a União Europeia publicou a Diretiva no 2009/72/CE, a qual estabeleceu a obrigatoriedade dos estados-membros de avaliar a implantação da medição inteligente.

25. Antes da implantação, entretanto, a Diretiva determinou que os estados-membros avaliem a economia advinda da substituição dos medidores até setembro de 2012. Se a análise de custos e benefícios for positiva, as autoridades devem determinar que pelo menos 80% dos consumidores sejam contemplados com sistemas inteligentes de medição até 2020.

26. A Diretiva também pretende promover a eficiência energética no continente europeu e ajudar no alcance de duas metas do Plano de Ação 20/20/20: poupar 20% do consumo energético da União Europeia e alcançar 20% de uso de fontes renováveis na geração de energia elétrica até 2020.

27. Verifica-se que a celeridade com que o processo de substituição de medidores roll-out ocorre é distinta de país para país. Em 2011, Itália e Suécia já

se encontravam praticamente com 100% dos medidores inteligentes instalados. Notícias anteriores ao agravamento da crise econômica relatam que Dinamarca, Finlândia, Holanda e Islândia haviam iniciado a troca de medidores, enquanto Grécia, Espanha e Reino Unido já haviam decidido iniciá-la.

28. Nota-se, na Europa, que a decisão de implantar medidores inteligentes e começar a disseminação das redes inteligentes partiu de diretivas da União Europeia e foi replicada pelos governos dos países-membros. Assim, há políticas governamentais específicas para redes inteligentes. O intuito é aumentar a confiabilidade da rede, reduzir os custos com a manutenção, manter registros mais exatos do uso por cliente e, sobretudo, reduzir as emissões de CO2.

29. Os Estados Unidos também exibem importantes iniciativas relacionadas às redes elétricas inteligentes. Em todo o País, há diversas experiências-piloto, mas o uso mais expressivo de medição inteligente é encontrado no Texas e na Califórnia, cujos principais vetores são a redução da demanda no horário de pico e a promoção da eficiência energética.

30. Na esfera federal norte-americana, foi lançado em 2009 o Plano de Recuperação e Reinvestimento, o qual destinou US$ 3,4 bilhões à implantação de redes inteligentes. Na visão do Governo norte-americano, a tecnologia possibilita sistema elétrico mais confiável, ganhos ambientais, geração de dezenas de milhares de empregos e economia de US$ 20 bilhões durante a próxima década.

31. Nos Estados Unidos, assim como na Europa, a geração de empregos e a recuperação da economia também são razões para a implantação da tecnologia. O estímulo ao uso de redes inteligentes também partiu de políticas públicas.

32. Na China, as redes inteligentes são necessárias para reduzir a dependência do carvão, integrar veículos elétricos e garantir o crescimento dos centros urbanos. Ademais, o País almeja se tornar referência no desenvolvimento da tecnologia. Na Coreia do Sul também há o uso disseminado de redes inteligentes com foco na eficiência energética. Já no Japão, há diversos projetos-piloto integrando telecomunicação, geração renovável e controle de demanda por meio da tecnologia. Também nesses Países as redes inteligentes passaram a ser fortemente estudadas a partir do desenvolvimento de estratégias governamentais.

Comparação entre as experiências internacionais e a realidade brasileira

33. Hajam vista as experiências internacionais, salienta-se o que as difere do caso brasileiro. As diferenças são, basicamente, a motivação e o caráter político da decisão de incentivar o uso de redes inteligentes. Na grande maioria dessas Nações, a decisão de implantar redes inteligentes e, consequentemente, a substituição de medidores partiu do estabelecimento de políticas públicas específicas. No Brasil, embora diversos ministérios – principalmente Ministério de Minas e Energia - MME, Ministério do Desenvolvimento, Indústria e Comércio Exterior - MDIC, Ministério da Ciência, Tecnologia e Inovação - MCTI e Ministério das Comunicações - MC – já tenham iniciado estudos relacionados ao tema, ainda não há política pública estabelecida nem definição governamental a respeito do tema.

34. Quanto ao outro aspecto – os motivos –, nota-se que o caso brasileiro difere dos demais em razão de o País ter uma matriz energética limpa. Em 2010, 86% da energia gerada para atender à demanda e suportar o crescimento econômico originaram-se de fontes renováveis (hidráulica, eólica, bagaço de cana-de-açúcar). Já nos países-membro da OCDE, apenas 18% da energia gerada em 2010 advieram de fontes renováveis, representando 68% da produção proveniente de combustíveis fósseis.

35. Mundo afora, as redes inteligentes foram encaradas como ferramenta para solucionar problemas e alcançar metas relacionadas principalmente à redução das emissões de CO2; porém, destaca-se a racionalidade no consumo de energia elétrica, a redução dos custos operacionais, a liberalização do mercado, entre outros. Ao se analisar cada um desses motivos no Brasil, é possível constatar que não se aplicam ao País na mesma medida.

Histórico de implantação no Brasil

36. O Brasil possui as próprias motivações, que levam o regulador a contemplar o estudo de implantação de redes inteligentes: melhorar a qualidade no serviço prestado de baixa tensão, reduzir as perdas no fornecimento de energia e os custos operacionais, dentre outras.

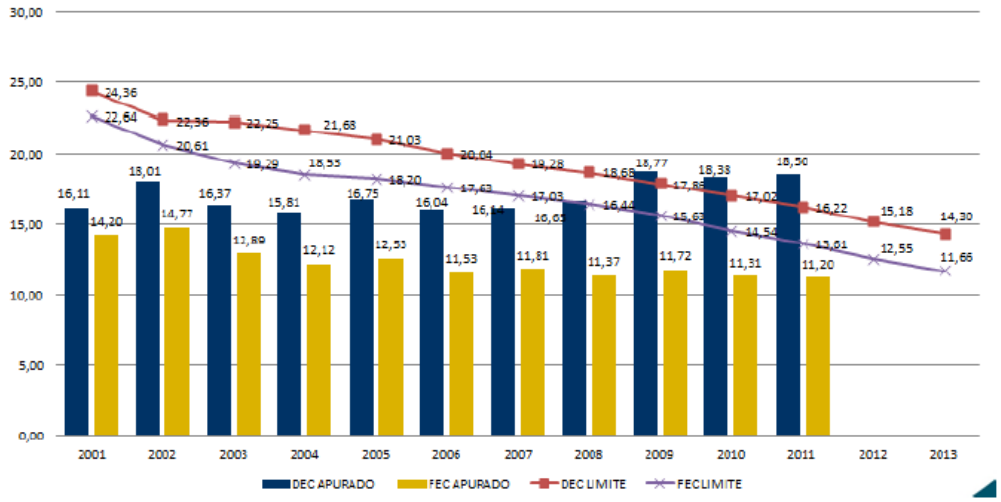

Gráfico 1 – Qualidade do Serviço - DEC / FEC Brasil 2001 a 2011
Fonte: SRD/ANEEL.

37. Do Gráfico 1, depreende-se que as concessionárias de distribuição, desde 2009, não alcançam o nível de qualidade estabelecido pelo regulador, com o número de interrupções acima do desejado, embora pratiquem a tarifa de energia calculada (a tarifa calculada sugere o nível de qualidade do serviço prestado). Em razão disso, pagaram de indenização ao consumidor em 2010, R$ 360.797.553,60 milhões, e em 2011, R$ 385.187.839,38 milhões. Para o primeiro semestre de 2012, esse valor é de R$ 129.334.586,38 (valor ainda passível de verificação de consistência).

38. Quando se realiza a comparação com parâmetros mundiais, os números de interrupções destoam. Recentemente, na plenária internacional conjunta com a finalidade de compartilhar conhecimentos sobre o estado da arte em redes inteligentes de eletricidade, evento promovido pelo Comitê Europeu de Normalização Eletrotécnica – CENELEC, órgão integrante do Comitê Europeu de Normalização – CEN, que contou com a participação de mais de 100 delegados dos 27 países integrantes da Comunidade Europeia, em Bruxelas, na Bélgica, nos debates promovidos, quando apresentei o slide do Gráfico 1, mostrando que em 2011 a média de interrupção tolerada para as 63 concessionárias do País era de 16,22h e que o apurado era de 18,50h, fui informado que no Japão a tolerância anual era de 16 min; nos Estados Unidos, o valor médio chegava a 240 minutos. Já nos países-membro da Comunidade Europeia, falava-se em 140 min, sendo Portugal o que apurava maiores valores, chegando a 200 minutos.

39. A Figura 1 apresenta as perdas técnicas e não-técnicas por região. Deduz-se então que os níveis de perdas praticados no Brasil são bem elevados quando comparados com paradigmas mundiais.

Figura 1 – Perdas por região
Fonte: SRD/ANEEL.

40. Recentemente, algumas distribuidoras iniciaram a substituição de medidores eletromecânicos por eletrônicos nas respectivas áreas de concessão, com o intuito de promover a redução de perdas não-técnicas e melhorar a eficiência na medição do consumo de energia elétrica.

41. Por ausência de determinação regulatória no que diz respeito às funcionalidades mínimas dos medidores eletrônicos, as distribuidoras vêm instalando equipamentos com funções que atendam apenas à solução de problemas localizados.

42. Diante de tal cenário, a ANEEL iniciou estudos para promover a regulamentação do tema com vistas a garantir que os usuários do serviço público de distribuição de energia elétrica sejam tratados com atenção pelas permissionárias e pelas concessionárias de serviço público de distribuição, buscando redução de custos e melhoria do sistema como um todo.

43. Verifica-se que, além da melhoria na qualidade do serviço, é possível obter da redução de perdas com a implantação das redes inteligentes no Brasil. Logo, por razões distintas daquelas encontradas em outros países, também é positivo implantá-las, ainda que em escala diferente. Não se pode perder de perspectiva, contudo, os custos decorrentes dessa implantação, os quais são representativos.

44. O Brasil é um país de grandes dimensões e diversidade, onde realidades distintas convivem. Em algumas regiões, a implantação das redes inteligentes é necessária para melhorar a qualidade do fornecimento. Ao mesmo tempo, em outras, a própria universalização do serviço ainda é um desafio.

45. Deve-se, portanto, buscar mecanismos regulatórios para que a implantação das redes inteligentes – impulsionada pela troca de medidores – comece pelas áreas que realmente dela necessitem prioritariamente, observando os diferentes motivos expostos.

Princípios que orientaram a nova proposta

46. Antes de apresentar a avaliação sobre a Audiência Pública no 43/2010, relevam-se os princípios gerais que orientaram a proposta. A definição das funcionalidades deve tomar como base a busca de solução para determinados problemas – apuração da qualidade e do custo da energia elétrica ao consumidor final, por exemplo – e benefícios que seriam usufruídos pelo consumidor e pelo sistema elétrico como um todo, favorecendo a sociedade em geral.

47. Entretanto, a obtenção dos benefícios traz consigo determinados custos, os quais serão aportados, em última instância, pelo consumidor de energia elétrica, visto que os medidores irão integrar a base de remuneração das respectivas concessionárias, como já o é hoje. Sem se afastar da relação benefício esperado versus custo decorrente, é função do regulador procurar o adequado equilíbrio entre a modernidade do serviço e a modicidade tarifária.

48. A adoção dos medidores inteligentes agrega muitos benefícios para a sociedade, que, conforme estudos internacionais6, neste momento não são passíveis de quantificação. Entre eles, cita-se a criação das condições para difundir a microgeração distribuída, para permitir a introdução das redes inteligentes. Dentre os mensuráveis, elencam-se:

a) redução do consumo, motivado por melhor informação;

b) otimização das redes de distribuição;

c) leituras remotas;

d) redução da emissão de CO2;

e) melhor monitoramento da rede;

f) redução de perdas técnicas e não-técnicas;

g) controle de fraude;

h) adiamento de investimentos em geração e transmissão;

i) novos serviços aos consumidores;

j) adoção do pré-pagamento – redução da inadimplência;

k) gestão de carga na ponta – peak load management.

49. Ao longo das discussões no ambiente da Audiência Pública no 43/2010, foi possível concluir que vários dos pontos positivos enumerados poderiam ser igualmente obtidos sem a instalação de um mesmo medidor padrão em todas as unidades consumidoras do País.

50. Em outras palavras, há benefícios relacionados a determinados grupos de consumidores com características peculiares, de modo que a instalação irrestrita do mesmo padrão de medidor eletrônico em todas as unidades consumidoras da área de concessão ou permissão poderia se configurar em opção não viável e economicamente desfavorável. Ao se considerar como referência esse ponto de vista, buscou-se fornecer mais flexibilidade na definição das funcionalidades que devem compor o medidor eletrônico de cada unidade consumidora.

51. É fato que a implantação de redes inteligentes é benéfica ao País e será realizada em processo paulatino. Nesse sentido, a ANEEL já emitiu diversos regulamentos relacionados ao tema, dentre os quais se destacam:

a) Resolução Normativa no 482, de 2012, que trata da conexão de micro e minigeração distribuída;

b) Resolução Normativa no 464, de 2011, que trata do estabelecimento da tarifa branca (PRORET);

c) Resolução Normativa no 375, de 2009, que trata da regulamentação da utilização do PLC;

d) Resoluções no 345, de 2008, e no 395, de 2008, que trata do uso compulsório de sistemas geoprocessados (PRODIST).

52. Além desses, mencionam-se outros estudos relacionados às redes inteligentes tais como o pré-pagamento, recentemente submetido à Audiência

Pública no 48/2012, e o sistema de monitoramento da qualidade, o qual comentarei com mais detalhes adiante.

53. Assim, a definição das funcionalidades mínimas – objeto da AP no 43/2010 – deve ser entendida como etapa de um projeto estratégico mais abrangente. A norma resultante da Audiência Pública estará integrada a outras paralelas, das quais se espera contribuição significativa para viabilizar a modernização do ambiente de baixa tensão de energia elétrica no País.

54. A Resolução não define a estratégia do uso de medidores inteligentes nem finda a discussão acerca das funcionalidades mínimas. É ponto inicial de um processo de modernização e, como tal, será uma ação monitorada e, se necessário, ajustada ao longo do tempo.

55. Na discussão das funcionalidades mínimas, considerou-se a sua importância para a disseminação das redes inteligentes e a ideia de que esse é apenas mais um passo. Daí, destacam-se dois aspectos: a tecnologia está em pleno desenvolvimento e o dever de manter a modicidade tarifária.

56. Atualmente, dezenas de projetos-piloto sobre temas relacionados às redes inteligentes estão em andamento no País. Paralelamente, fabricantes e distribuidoras vêm buscando soluções técnicas que melhor se adaptem ao mercado nacional, e pesquisas estão sendo cada vez mais incentivadas. A padronização excessiva nesse momento pode desestruturar o pleno desenvolvimento da tecnologia em vez de estimulá-la.

57. Portanto, na atual conjuntura, o ritmo de disseminação dos medidores e das redes inteligentes deve ser estabelecido de modo a minimizar potenciais aumentos tarifários. Caso haja uma política governamental que indique fontes específicas de financiamento, o ritmo de implantação poderá ser acelerado, a exemplo do que ocorreu nos programas de universalização.

58. Mais uma vez, recorro à experiência internacional, para apontar que na França existe a expectativa de se realizar a troca de 95% do parque de medição até 2016 e na Holanda, até 2018. Constata-se que na Europa o período de implementação em alguns países varia entre 5 e 8 anos. Mas pode-se citar um exemplo onde o roll-out foi mais arrojado. No caso da Suécia, a troca dos medidores foi bem mais célere, foi promovida a substituição de 70% dos medidores do País, o que representa 5 milhões de unidades, em apenas 18 meses.

Abordagem revisada dos modelos de medidores

59. Quanto aos modelos de medidores, na versão submetida à Audiência Pública no 43/2010, pretendia-se definir um único modelo a ser utilizado nas novas ligações ou quando da substituição dos equipamentos existentes. Nessa situação, a troca do medidor ocorreria alheia ao interesse do consumidor ou da distribuidora.

60. A nova proposta estabelece dois tipos de medidores. Um será implantado quando o usuário aderir à modalidade tarifária branca. Nesse caso, os critérios comerciais serão posteriormente estabelecidos em regulamentação específica (Resolução Normativa no 414, de 2010), conforme previsto na Agenda Regulatória 2012/2013 da ANEEL, devendo o medidor registrar o consumo em postos tarifários e ser fornecido sem ônus.

61. O outro modelo aplicar-se-á aos casos em que o consumidor deseje ter acesso a informações específicas individualizadas sobre o serviço prestado. Ao solicitar o equipamento, a instalação pela distribuidora ocorrerá de forma onerosa ao consumidor requerente. A instalação de medidores com mais funcionalidades (e consequentemente de maior custo) não ocorrerá de forma compulsória em todas as unidades consumidoras, mas por solicitação do equipamento pelo consumidor que desejar acesso a dados individualizados. As especificidades de cada equipamento serão detalhadas na sequência.

62. Os sistemas de medição inteligente começarão a ser instalados nas unidades consumidoras em que os usuários efetivamente utilizarão suas funcionalidades. Os consumidores deixarão de receber informações apenas ao final de cada ciclo de faturamento e passarão a ter papel mais ativo no relacionamento com a distribuidora e o sistema elétrico.

63. Assim como na Holanda, o que se propõe é a instalação do medidor de maneira voluntária, do ponto de vista do consumidor.

Abrangência da resolução

64. Relativamente às unidades consumidoras que serão abrangidas pela resolução normativa, a minuta submetida à AP no 43/2010 restringia a aplicação àquelas pertencentes aos subgrupos de consumidores residenciais (B1) não

classificados como de baixa renda e de consumidores comerciais e industriais (B3).

65. Quanto à exclusão dos consumidores de baixa renda, que hoje constituem cerca de 10 milhões de unidades consumidoras, recomenda-se mantê-la pelas mesmas razões discutidas quando da aprovação do PRORET, que criou a tarifa branca, que não prevê tarifa horária para essa subclasse. O mesmo vale para o subgrupo B4 – Iluminação Pública.

66. Já os consumidores rurais - B2 - devem ser incluídos, pois podem optar pela tarifa branca e apresentam cargas moduláveis, de forma que as informações trazidas pelos medidores podem ser importantes aos usuários desse Subgrupo.

67. Ressalta-se que a Agência acompanhará o processo de implantação dos novos medidores eletrônicos e, eventualmente, poderá avaliar a necessidade de estabelecer forma mais coordenada de sua instalação. Neste caso, consoante apontado por algumas das contribuições da Audiência Pública, a implantação intensificada poderá contar com mais planejamento da distribuidora em termos da definição de áreas ou grupos de consumidores prioritários. Por ora, o uso de medidores eletrônicos além das funcionalidades mínimas propostas fica a critério da distribuidora.

Prazo inicial

68. A minuta de resolução normativa da AP no 43/2010 trazia prazo (18 meses) para início da instalação dos medidores eletrônicos nas novas unidades consumidoras ou por substituição. Esse prazo visava fornecer intervalo de tempo de adaptação para o mercado, particularmente fabricantes, distribuidoras e Inmetro, considerando as novas necessidades e obrigações. Grande parte das contribuições recebidas sinalizou a necessidade de dilatação desse prazo de adaptação, sem apresentar justificativas adequadas.

69. Ao se entender que o tempo decorrido desde o início dessa Audiência já possibilitou certo nível de previsibilidade aos fabricantes e às distribuidoras e que a instalação dos novos medidores passará a ocorrer inicialmente por solicitação, julga-se não haver necessidade de acrescer o prazo proposto na minuta. Assim, recomenda-se a manutenção do prazo de dezoito meses a partir da data de publicação do ato normativo aqui em análise.

70. Fica, entretanto, mantida a excepcionalidade de prazo para aquelas permissionárias de distribuição que celebrarem Contrato de Permissão posteriormente à data de publicação da resolução. Para estas, o prazo de dezoito meses vale a partir do início da vigência do Contrato.

Grandezas medidas e funcionalidades complementares

71. A minuta submetida à AP no 43/2010 definiu as grandezas que deverão ser apuradas pelos medidores novos e por aqueles instalados por substituição: tensão, energia ativa em postos tarifários, energia reativa, data e hora de início e fim das interrupções de curta e de longa duração e transgressões de tensão, além de comunicação e atuação remota.

72. Como resultado da análise das contribuições recebidas durante a Audiência, a proposta revisada sugere o estabelecimento de dois modelos de medidor: um deles aplicável aos consumidores que fizerem adesão à tarifa branca e outro aos que optarem por acesso a maior quantidade de dados individualizados.

73. Especificamente para a definição das grandezas do medidor eletrônico instalado nas unidades consumidoras que optarem pela modalidade tarifária branca, propõe-se somente a inclusão da funcionalidade responsável pela medição de energia elétrica ativa consumida em quatro postos tarifários, assim como a identificação do posto vigente.

74. Em se adotando a tarifa branca, o preço da eletricidade na rede vai variar em três períodos distintos, durante as 24 horas do dia – ponta, pré-ponta e fora ponta. O medidor permitirá a disponibilização dos preços de maneira dinâmica, permitindo aos consumidores aumentarem ou diminuírem o uso da energia automaticamente, dependendo do preço. Logo, aqueles que responderem ao sinal econômico de maneira adequada terão a chance real de reduzir a fatura de energia elétrica ao final do mês.

75. Em termos das funcionalidades de apuração de continuidade (DIC, FIC e DMIC) e de conformidade (DRP e DRC), propõe-se o aperfeiçoamento da regra levada à Audiência. O objetivo principal dessas funções é o aprimoramento da apuração dos índices de qualidade. A área técnica entende, todavia, que o objetivo de melhor apuração não passa necessariamente pelo registro de interrupções e de níveis de tensão em todas as unidades consumidoras.

76. Sugere-se, alternativamente, a apuração em pontos estrategicamente determinados – tal como no secundário dos transformadores de distribuição de média tensão, por exemplo – em vez de ser necessariamente em cada medidor individualmente.

77. Essa opção resulta em redução dos custos de cada medidor e dos processos de armazenamento, leitura e processamento. Ao mesmo tempo, acredita-se que a apuração dos indicadores acontecerá de forma mais rápida, uma vez que a proposta levada à Audiência Pública demoraria um pouco mais, pois ensejaria a substituição de todo o parque de medição nacional algo de aproximadamente 70 milhões de medidores.

78. Já no caso do consumidor que demonstrar interesse em possuir dados individualizados sobre o serviço prestado, o sistema de medição aplicável (com funcionalidades complementares) deverá ser instalado com custos adicionais diretamente atribuídos ao solicitante, conforme procedimentos a serem estabelecidos em regulamentação comercial específica. Ressalta-se que a solicitação por tal sistema de medição independe da adesão da unidade consumidora à modalidade tarifária branca. Ou seja, o consumidor poderá requisitar o medidor com funcionalidades complementares, mas sem necessariamente ser faturado segundo postos tarifários.

79. Resta, então, ponderar quais grandezas e quais funcionalidades devem compor tal sistema de medição, partindo-se do modelo sugerido na AP no 43/2010. Além dos requisitos comuns ao medidor instalado para adesão à modalidade tarifária branca (valor de energia elétrica ativa consumida por posto tarifário e identificação do posto tarifário vigente, caso aplicável), recomenda-se que as seguintes informações sejam disponibilizadas pelo medidor com funcionalidades complementares (cujo custo adicional será atribuído ao consumidor solicitante):

- valores de tensão e de corrente de cada fase;
- data e hora de início e fim das interrupções de curta e de longa duração ocorridas nos últimos três meses e
- últimos doze valores calculados do Índice de Duração Relativa da Transgressão para Tensão Precária – DRP e do Índice de Duração Relativa da Transgressão para Tensão Crítica – DRC, conforme legislação específica.

80. A proposta também estabelece que essas informações devam estar disponíveis por meio de saída específica para captura de dados, existente no

próprio equipamento, enquanto o sistema de comunicação, este sim, que leva informação à rede, esteja disponível.

81. Assim, permite-se que o consumidor tenha acesso aos dados coletados pelo medidor em tempo real e possa utilizá-los em procedimentos específicos, por exemplo, de eficiência energética e gerenciamento pelo lado da demanda.

82. Além desses casos compulsórios, fica a critério da distribuidora o uso de sistemas de medição dotados de funcionalidades adicionais. A empresa é a maior conhecedora de sua área de atuação e, portanto, a mais indicada para buscar soluções individualizadas aplicáveis apenas a grupos de consumidores específicos. Dessa forma, aconselha-se que, observada a prudência dos investimentos e a modicidade tarifária, a distribuidora possa adotar sistemas de medição com requisitos adicionais ao mínimo necessário em qualquer unidade consumidora. Quando a iniciativa partir da distribuidora, ela não poderá onerar o consumidor.

83. Destaco, ainda, que o consumo de energia elétrica do medidor e do eventual sistema de comunicação associado não deve ser oneroso ao consumidor. Esse comando foi estabelecido na própria Resolução - art. 10. De todo modo, tal disposição não recepciona o consumo de energia relativo a dispositivos internos para visualização do consumo, tais como in home displays ou terminais de consulta individuais.

Sistema de comunicação

84. Na proposta submetida à Audiência Pública, os medidores deveriam possuir dispositivos que possibilitassem a comunicação bidirecional entre o medidor e o centro de medição da distribuidora. Além disso, as atividades de suspensão e religação do fornecimento, assim como monitoramento e controle de determinados parâmetros do medidor, deveriam poder ser remotamente realizadas pela distribuidora.

85. A proposta baseava-se no fato de que a implantação de sistema de comunicação e a decorrente possibilidade de operação remota podem trazer redução de custos operacionais, promover ações de eficiência energética e disseminar a inteligência na rede. Entretanto, as discussões realizadas durante todo o processo de regulamentação trazem informações dos custos associados

à implantação da infraestrutura de comunicação. Tais dados, segundo a SRD, são corroborados por informações provenientes dos projetos-piloto em desenvolvimento no País e pelo custo de implantação em outros países.

86. Esse aspecto é reforçado quando se observa o valor de determinadas atividades operacionais da distribuidora – tais como a leitura do medidor, o corte e o restabelecimento da ligação da unidade consumidora –, os quais, no Brasil, ainda são relativamente baixos quando comparados com os de outros países que estão expandindo o uso de redes inteligentes.

87. Em outras palavras, embora alguns países venham adotando sistema de comunicação como forma de redução de custos operacionais, não se observa essa realidade em todas as áreas de atuação das distribuidoras, haja vista o alto custo da infraestrutura de comunicação e o relativo baixo custo da mão de obra no país.

88. Assim, em termos de comunicação entre o medidor e o centro de medição, no primeiro momento, sugere-se que seu uso não seja compulsório e que a avaliação de quais medidores devem possuir comunicação remota seja da distribuidora. Esta poderá planejar a implantação desses sistemas de forma otimizada, priorizando inicialmente agrupamentos de unidades consumidoras conforme os benefícios sejam mais relevantes. É o caso, por exemplo, das áreas densamente povoadas em que a infraestrutura de comunicação alcance maior número de unidades consumidoras.

89. Caso a distribuidora opte por utilizar sistemas de comunicação integrados a seus medidores eletrônicos, esta deve garantir a segurança da informação, preocupação externada nas contribuições à AP n.o 43/2010. Nesse sentido, o regulamento deve dispor que a distribuidora garanta a segurança dos dados trafegados e, especialmente, das informações de caráter pessoal coletadas das unidades consumidoras na hipótese de utilizar comunicação remota.

90. Por fim, a questão da interoperabilidade foi tema de diversas contribuições. Na minuta da AP no 43/2010, já havia previsão de que o protocolo de comunicação fosse aberto no intuito de assegurar a interoperabilidade. A intenção era que o tráfego de informações fosse o mais independente possível de marcas, modelos ou fabricantes específicos, de modo a não restringir a atuação da distribuidora a poucos fornecedores.

91. No entanto, embora esse cuidado seja pertinente, as distribuidoras também compartilham a mesma preocupação, como já ocorre na aquisição de outros

equipamentos que compõem seu sistema elétrico. Além disso, o uso de protocolo público ou aberto não garante a interoperabilidade entre os equipamentos. Mesmo que a ANEEL defina o uso compulsório de protocolo público ou aberto, ou determine qual protocolo deve ser utilizado, não se garante a livre troca de informações entre os equipamentos.

92. Adicionalmente, a determinação de protocolos específicos – ainda que públicos ou abertos – na fase inicial de implantação pode restringir o uso de tecnologias pelas distribuidoras. Ou seja, poderá haver casos em que soluções que não utilizem tal tipo de protocolo possam se mostrar mais adequadas para serem utilizadas em determinados consumidores ou áreas dentro da concessão ou da permissão da distribuidora.

93. Assim, por mais adequada que seja uma solução que utilize protocolo privado, determinação regulatória em contrário impedirá o seu uso e as possibilidades de implantação da distribuidora estarão restringidas. Logo, propõe-se não padronizar o tipo de protocolo a ser utilizado.

Monitoramento da qualidade

94. A questão da qualidade do serviço prestado pela distribuidora sempre foi objeto de preocupação da ANEEL. Nos últimos anos, tem-se enfatizado o assunto pelos anseios da sociedade e pela estagnação dos indicadores de continuidade, que, em média, não melhoraram nos últimos anos. Esse cenário pode ser aprimorado com a disseminação das redes inteligentes.

95. Na proposta inicial da AP no 43/2010, pensou-se em aliar a substituição dos medidores à apuração da qualidade. Nesse sentido, foi sugerido que os medidores deveriam registrar data e hora de início e fim das interrupções. Dessa maneira, poder-se-ia lançar estratégias de redução das interrupções, direcionando ações de melhoria das distribuidoras e de fiscalização do regulador, além de dar mais transparência ao consumidor.

96. No entanto, apesar de ser indubitável a necessidade de se aprimorar a apuração dos indicadores, isso não resolveria os problemas de confiabilidade por si só. A questão é mais abrangente e não deve ser tratada como mera funcionalidade adicional dos medidores.

97. Embora a questão da qualidade não seja o foco específico da Audiência aqui tratada, a ANEEL gerou forte expectativa na sociedade acerca da melhoria na apuração, de modo que não seria adequado postergar a decisão sobre o assunto. Dessa forma, propõe-se a instauração de processo específico para o aprimoramento da apuração dos indicadores de continuidade do serviço.

98. Tem-se que se ter presente no desenvolvimento de tal trabalho que a apuração dos indicadores de continuidade do serviço em local diferente da unidade consumidora possui imprecisões que devem ser superadas. Ou seja, o consumidor deve ter garantido que os níveis de continuidade do serviço serão apurados de maneira precisa.

Necessidade de acompanhamento contínuo

99. Ao longo do tempo, o tema será acompanhado e sua abordagem poderá ser aprimorada pela Agência de acordo com os dados advindos do processo de implantação tais como a evolução dos custos de medidores, o custo dos sistemas de telecomunicações, o percentual de adesão dos consumidores à modalidade tarifária branca, entre outros.

100. Entende-se que o regulador deve utilizar os instrumentos regulatórios para que as distribuidoras promovam a modernização do parque de medição sem, entretanto, eleger uma solução técnica única e padronizá-la em todo o País. Tão essencial quanto as redes inteligentes é a adoção de soluções técnicas específicas para auxiliar em temas particulares de cada região do Brasil.

101. Nesse aspecto, as distribuidoras têm papel importante na escolha das ferramentas personalizadas por possuírem conhecimento detalhado de sua área de atuação. Ao regulador, com visão mais ampla, caberá utilizar os instrumentos regulatórios adequados para induzir o operador da rede a melhorar os serviços ao menor custo possível, garantindo a prestação do serviço adequado.

102. Sempre se deve lembrar que a questão da medição eletrônica está inserida em um projeto de longo prazo que visa à disseminação das redes inteligentes no Brasil. A proposta baseou-se em experiências internacionais, projetos-piloto, reuniões técnicas e vários anos de estudos. Mais do que isso, o regulamento ora proposto considerou a conjuntura atual, que, evidentemente, pode mudar no futuro.

103. Efetivamente se acredita que os benefícios das redes inteligentes e da troca de medidores transcendem o Setor Elétrico. Assim, incentiva-se a busca por outras fontes de rateio dos custos da implantação, que também podem extrapolar o Setor. Logo, estimula-se que o tema continue a ser alvo de preocupação e acompanhamento por órgãos governamentais no intuito de avaliar a conveniência do estabelecimento de políticas públicas sobre o assunto.

104. Hoje se dá o primeiro passo para transformar a rede elétrica de baixa tensão em uma verdadeira “Internet” da energia. O que está por trás de tudo isso é tornar a rede elétrica uma rede interativa de infoenergia e em última instância beneficiar o consumidor de energia elétrica.

III. D I R E I T O

105. A legalidade do assunto encontra amparo nas seguintes normas:

a) Lei n.o 9.427, de 26 de dezembro de 1996;

b) Decreto n.o 2.335, de 6 de outubro de 1997.

IV. D I S P O S I T I V O

106. Fundado nesse exame e nas considerações efetuadas no Processo no 48500.005714/2009-46, voto pela aprovação da regulamentação dos sistemas de medição de energia elétrica de unidades consumidoras do Grupo B, como a minuta de Resolução em anexo.

107. Decido, ainda, pela instauração de processo para o aprimoramento da apuração dos indicadores de qualidade, com a participação da Superintendência de Regulação dos Serviços de Distribuição – SRD e da Superintendência de Fiscalização dos Serviços de Eletricidade – SFE, sob a liderança da primeira.

Brasília, 7 de agosto de 2012.

ANDRÉ PEPITONE DA NÓBREGA

Diretor

9.2.
Anexo II – Resolução normativa nº 502

AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA – ANEEL

RESOLUÇÃO NORMATIVA Nº 502, DE 7 DE AGOSTO DE 2012

Regulamenta sistemas de medição de energia elétrica de unidades consumidoras do Grupo B.

O DIRETOR-GERAL DA AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA – ANEEL, no uso de suas atribuições regimentais, de acordo com deliberação da Diretoria, tendo em vista o disposto na Lei nº 9.427, de 26 de dezembro de 1996, com base no art. 4º, inciso XX, Anexo I, do Decreto nº 2.335, de 6 de outubro de 1997, o que consta do Processo nº 48500.005714/2009-46 e considerando:

a Consulta Pública nº 15/2009, realizada entre 30 de janeiro e 30 de abril de 2009, e a Audiência Pública nº 43/2010, realizada no período de 1º de outubro de 2010 a 26 de janeiro de 2011, resolve:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Regulamentar, na forma desta Resolução, sistemas de medição de energia elétrica de unidades consumidoras do Grupo B.

§ 1º As distribuidoras, compreendendo as concessionárias e as permissionárias do serviço público de distribuição, devem adotar sistemas de medição na forma desta Resolução em até 18 (dezoito) meses após a data de sua publicação.

§ 2º Para as permissionárias que celebrarem contrato de permissão após a publicação desta Resolução, o prazo referido no § 1º é contado a partir da data de vigência do referido Contrato.

§ 3º Ficam excluídas da abrangência estipulada no caput as unidades consumidoras classificadas em qualquer subclasse baixa renda do subgrupo B1 – Residencial e as do subgrupo B4 – Iluminação Pública.

CAPÍTULO II
SISTEMAS DE MEDIÇÃO

Art. 2º O sistema de medição das unidades consumidoras enquadradas na modalidade tarifária branca deve apurar, observando a regulamentação técnica metrológica específica, o consumo de energia elétrica ativa em pelo menos 4 (quatro) postos tarifários, devendo ser programáveis o início e o fim de cada posto.

§ 1º Em complemento aos requisitos metrológicos referentes à apresentação de informações ao consumidor, devem estar disponíveis por meio de mostrador existente no próprio medidor ou em dispositivo localizado internamente à unidade consumidora:

I – o valor de energia elétrica ativa consumida acumulada por posto tarifário; e

II – a identificação do posto tarifário corrente.

§ 2º A critério da distribuidora, as informações referenciadas no § 1º podem ser adicionalmente disponibilizadas por meios alternativos com vistas a facilitar o acesso às informações pelo consumidor.

§ 3º O sistema de medição deve ser instalado pela distribuidora conforme prazos e critérios estabelecidos em regulamento específico.

§ 4º Caso a unidade consumidora não faça adesão ao faturamento na modalidade tarifária branca, a instalação do sistema de medição referenciado no caput não é obrigatória.

Art. 3º Os titulares das unidades consumidoras abrangidas por esta Resolução, independentemente da adesão ao faturamento na modalidade tarifária branca, observando a regulamentação técnica metrológica específica, podem solicitar à distribuidora a disponibilização de um sistema de medição capaz de fornecer cumulativamente as seguintes informações:

I – valores de tensão e de corrente de cada fase;

II – valor de energia elétrica ativa consumida acumulada por posto tarifário;

III – identificação do posto tarifário corrente, se aplicável;

IV – data e horário de início e fim das interrupções de curta e de longa duração ocorridas nos últimos 3 (três) meses; e

V – últimos 12 (doze) valores calculados dos indicadores Duração Relativa da Transgressão de Tensão Precária – DRP e Duração Relativa da Transgressão de Tensão Crítica – DRC.

§ 1º Em complemento aos requisitos metrológicos referentes à apresentação de informações ao consumidor, as informações referenciadas nos incisos I a III devem estar disponíveis por meio de mostrador existente no próprio medidor ou em dispositivo localizado internamente à unidade consumidora.

§ 2º As informações referenciadas nos incisos I a V devem estar disponíveis por meio de saída específica para aquisição de dados existente no próprio medidor.

§ 3º As informações referenciadas nos incisos IV e V, a critério da distribuidora, podem ser contabilizadas pelo próprio medidor ou por dispositivo externo, e devem estar disponíveis por meio de mostrador existente no medidor ou de forma remota.

§ 4º A critério da distribuidora, as informações fornecidas pelo medidor podem ser adicionalmente disponibilizadas por meios alternativos com vistas a facilitar o acesso às informações pelo consumidor.

§ 5º O sistema de medição deve ser instalado pela distribuidora conforme prazos e critérios estabelecidos em regulamento específico, devendo a diferença de custo entre o sistema de medição descrito neste artigo e o sistema de medição de que trata o art. 2º ser de responsabilidade do consumidor interessado.

§ 6º Na hipótese de solicitação pelo consumidor, a distribuidora, a seu critério, pode fornecer sistema de medição que disponibiliza informações adicionais àquelas estabelecidas neste artigo.

Art. 4º Eventuais diferenças entre os indicadores de qualidade informados pela distribuidora e os registrados com base no sistema de medição referenciado no art. 3º devem ser justificados pela distribuidora sempre que solicitado pelo consumidor, conforme disposto no Módulo 8 do PRODIST.

Art. 5º Observada a prudência dos investimentos e a modicidade tarifária, a distribuidora pode adotar sistemas de medição com requisitos adicionais aos dispostos nesta Resolução em qualquer unidade consumidora.

Art. 6º Para faturar a unidade consumidora na modalidade tarifária branca, a distribuidora deve utilizar sistema de medição com a funcionalidade de apuração do consumo de energia elétrica em postos tarifários aprovado pelo Instituto Nacional de Metrologia, Qualidade e Tecnologia – Inmetro.

CAPÍTULO III
SISTEMA DE COMUNICAÇÃO REMOTA

Art. 7º Na hipótese de o sistema de medição ser provido de sistema de comunicação remota, a distribuidora deve adotar procedimentos e tecnologias que assegurem a segurança dos dados trafegados e, especialmente, das informações de caráter pessoal coletadas das unidades consumidoras.

Parágrafo único. É vedado à distribuidora disponibilizar dados coletados das unidades consumidoras a terceiros sem a autorização do titular.

CAPÍTULO IV
DISPOSIÇÕES GERAIS

Art. 8º Faculta-se à distribuidora a instalação de equipamentos de medição em local externo à unidade consumidora, incluindo sistema de medição centralizada, desde que também sejam respeitados os critérios e procedimentos definidos em regulamentação específica.

Art. 9º Para as unidades consumidoras em que os sistemas de medição de que trata esta Resolução vierem a ser instalados, os consumidores devem ser informados, previamente à instalação, acerca das funcionalidades do referido sistema e das informações que lhes passarão a ser disponibilizadas.

Art. 10. O consumo de energia elétrica do medidor e do eventual sistema de comunicação associado não deve ser considerado como consumo da unidade consumidora.

Art. 11. Esta Resolução entra em vigor na data de sua publicação.

NELSON JOSÉ HÜBNER MOREIRA

Este texto não substitui o publicado no D.O. de 14.08.2012, seção 1, p.30, v. 149, n. 157.