XIX SEMEAD
Seminários em Administração
novembro de 2016
ISSN 2177-3866

GOVERNANÇA E GESTÃO DA SEGURANÇA CIBERNÉTICA DE REDES INTELIGENTES (SMART GRIDS) EM CONCESSIONÁRIAS DE ENERGIA ELÉTRICAS NO BRASIL

DANIEL JARDIM PARDINI
UNIVERSIDADE FUMEC (FUMEC)
pardini@fumec.br

ASTRID MARIA CARNEIRO HEINISCH
UNIVERSIDADE FUMEC (FUMEC)
aheinisch@fitec.org.br

FERNANDO SILVA PARREIRAS
UNIVERSIDADE FUMEC (FUMEC)
fparreiras@gmail.com

Introdução
Apesar da ampla literatura, de natureza técnica e normativa, que trata das estruturas tecnológicas críticas voltadas à proteção dos sistemas de segurança nas organizações, são quase que desconhecidos os estudos que abordam a governança e a gestão da segurança cibernética, em especial, no setor elétrico. Diversas ações vêm sendo realizadas no sentido de modernizar o setor energético e mitigar os riscos de interrupção de energia. Dentre elas, destacam-se a implementação das redes inteligentes (Smart Grids), que objetiva tornar as redes de energia elétrica do futuro mais resilientes e seguras.

Problema de Pesquisa e Objetivo
Ainda prevalece a ausência de um campo teórico bem definido, em especial, para as concepções da governança e gestão corporativa no âmbito da segurança cibernética. A questão de pesquisa evidencia-se desta lacuna conceitual: quais seriam as dimensões da governança e da gestão corporativa em concessionárias de energia elétrica para a segurança cibernética dos smart grids? O artigo objetiva então identificar, avaliar e descrever as dimensões de governança e de gestão da segurança cibernética em concessionárias de energia elétrica brasileiras no contexto das redes inteligentes de energia elétrica.

Fundamentação Teórica
Abordou-se o arcabouço conceitual do ambiente dos smart grids, as concepções de gestão e governança do ambiente cibernético e suas dimensões e o modelo teórico-empírico da pesquisa. A segurança cibernética se refere a toda abordagem voltada a proteger dados, sistemas e redes de ataques deliberados e acidentais. Dois construtos são centrais no estudo: governança e gestão. O termo governança é usado para descrever um sistema de controle ou de regulação que inclui o processo de nomeação de controladores e reguladores. Já a expressão gestão é adotada para se referir às ações executivas.

Metodologia
O caminho metodológico foi trilhado em duas etapas. No primeiro momento resgatou-se na literatura estudada as variáveis que compõem as dimensões do modelo teórico-metodológico proposto para a estruturação do questionário. Na sequência validou-se e testou-se o instrumento de mensuração junto a especialistas do setor elétrico. Aqui utilizou-se o método Delphi realizado com especialistas (acadêmicos, pesquisadores e profissionais) e os testes estatísticos (análise fatorial, esfericidade, t de Student, Levene, Mann-Whithney e análise de variância) para a estruturação e validação do questionário.

Análise dos Resultados
A partir da literatura pesquisada foram identificadas as dimensões normativa, interacionista, transparência e fiscalização, Conselho de Administração e direito dos acionistas para o construto governança corporativa e, planejamento estratégico, gerenciamento de riscos, gerenciamento de ativos e gestão de recursos humanos para o construto gestão. A validação estatística do modelo permitiu sua aplicação no contexto da segurança cibernética dos smart grids em empresas de energia elétrica. A pesquisa revela um despreparo de decisões da alta administração nas concessionárias de energia brasileiras.

Conclusão
De uma forma geral, conclui-se que todas as dimensões descritas como resultados deste estudo atendem às concessionárias brasileiras de energia elétrica para a governança e a gestão da segurança cibernética no contexto das redes inteligentes de energia (Smart Grids). A dimensão que se mostrou melhor avaliada pelos especialistas, com base nos critérios de adoção pelas concessionárias brasileiras, foi o a dimensão de gestão que comporta o gerenciamento de ativos críticos. A dimensão pior avaliada foi a dimensão de governança que trata do direito dos acionistas.

Referências Bibliográficas
COUTINHO, Maurílio Pereira. Detecção de Ataques em infraestruturas críticas de sistemas elétricos de potência usando técnicas inteligentes. 2007. 260 f. Tese (Doutorado em Ciências em Engenharia Elétrica) – Universidade UNIFEI, Itajubá, 2007.
SOREBO, Gilbert N.; ECHOLS, Michael C. Smart Grid Security: An End-to-End View of Security in the New Electrical Grid. Boca Raton: CRC Press, 2012.
TURNBULL, Shann. Corporate Governance: Its Scope, Concerns and Theories. Scholarly Research and Theory Papers, v. 5, n. 4, Oct. 1997.

GOVERNANÇA E GESTÃO DA SEGURANÇA CIBERNÉTICA DE REDES INTELIGENTES (*SMART GRIDS*) EM CONCESSIONÁRIAS DE ENERGIA ELÉTRICA NO BRASIL

Introdução

Apesar da ampla literatura, de natureza técnica e normativa, que trata das estruturas tecnológicas críticas voltadas a proteção dos sistemas de segurança nas organizações, são quase que desconhecidos os estudos que abordam a governança e a gestão da segurança cibernética, em especial, no setor elétrico.

A energia elétrica é classificada como serviço essencial, elemento chave para a melhoria da qualidade de vida da população, a inclusão social e o desenvolvimento sustentável (LOBÃO, 2008, COUTINHO, 2007). Enquanto a demanda por energia vem crescendo em um ritmo maior que a sua capacidade, percebe-se que o sistema elétrico mundial tem se mantido, no decorrer dos últimos 30 a 50 anos, calcado em tecnologias desenvolvidas nas décadas de 1940 e 1950; o que, muitas vezes, resulta no congestionamento e estresse do sistema (GELLINGS, 2009).

Diversas ações vêm sendo realizadas no sentido de modernizar o setor energético e mitigar os riscos de interrupção de energia. Dentre elas, destacam-se a implementação das redes inteligentes (*Smart Grids*), objeto de análise deste estudo, que objetiva tornar as redes de energia elétrica do futuro mais resilientes, seguras, eficientes e confiáveis (MIT, 2011). Os *smart grids* consistem no uso extensivo de informação digital e tecnologia de controle para prover confiabilidade, segurança e eficiência à rede elétrica (*U.S., Title XIII of the Energy Independence and Security Act of 2007*).

Também denominadas de infraestruturas críticas, a segurança dos *smart grids*, em suas camadas física e de operação seguem as formas tradicionais de proteção. Porém, é na camada cibernética (infraestruturas de tecnologia de monitoramento das redes elétricas de transmissão e distribuição) que se encontram as questões mais preocupantes para os provedores dos serviços de energia elétrica. Isso ocorre muito em função das crescentes vulnerabilidades do sistema (COUTINHO, 2007) e do desconhecimento se as restruturas de administração estão preparadas para enfrentar estas ameaças.

O que se percebe é que ainda prevalece a ausência de um campo teórico bem definido, em especial, para as concepções da governança e gestão corporativa no âmbito da segurança cibernética. A questão de pesquisa evidencia-se desta lacuna conceitual: quais seriam as dimensões da governança e da gestão corporativa em concessionárias de energia elétrica para a segurança cibernética dos *smart grids*? Assim, pretende-se ampliar o conhecimento sobre a administração dessa nova concepção de energia elétrica. O artigo objetiva então identificar, avaliar e descrever as dimensões de governança e de gestão da segurança cibernética em concessionárias de energia elétrica brasileiras no contexto das redes inteligentes de energia elétrica (*smart grids*).

No desenvolvimento do artigo aborda-se, na sequência, o arcabouço conceitual do ambiente dos smart grids, as concepções de gestão e governanca do ambiente cibernético e suas dimensões, o modelo teórico-empírico da pesquisa, a metodologia de pesquisa, a validação e aplicação do modelo no contexto das concessionárias de energia brasileira e a conclusão do estudo.

O contexto das redes inteligentes de energia (*smart grids*): o espaço cibernético e as ameaças dos ambientes organizacionais

Smart grid é a rede de transmissão e distribuição de eletricidade que usa sensoriamento, monitoramento, comunicação bidirecional e sistemas de controle distribuídos no fornecimento de energia (NEWTON'S TELECOM DICTIONARY, 2009). O sistema de controle das redes de energia elétrica incorpora tecnologias de informação e telecomunicação que têm como objetivo monitorar toda a cadeia de valor energética – geração, transmissão, distribuição e consumo (MIT, 2011; NIST, 2010; SOREBO; ECHOLS, 2012).

Para garantir a confiabilidade e a eficiência operacional dessas redes de inteligência de energia as organizações (concessionárias) envolvidas devem proceder a otimização dinâmica de recursos e operações da rede voltada para a segurança cibernética, desenvolver e incorporar respostas em tempo real, automatizadas e interativas direcionadas à demanda e geração de energia, utilizar tecnologias de corte de pico de consumo e armazenamento avançado de energia e prover informações oportunas sobre a medição de energia consumida e opções de controle ao consumidor (MIT, 2011).

Além dos consumidores e das concessionárias de energia, compõem as partes interessadas (*stakeholders*) na implantação e funcionamento de *smart grids* (MOMOH, 2012): os órgãos reguladores, os provedores, desenvolvedores e integradores dos serviços de tecnologia de informação, pesquisadores e instituições de pesquisa e desenvolvimento (P&D). A identificação e o mapeamento das interações entre a organização e seus stakeholders pode auxiliar no entendimento que as partes interessadas e outros elementos representam nos riscos organizacionais.

Hatch (1997) identifica três componentes que explicam a dinâmica de interação entre a organização e o ambiente. São eles: as redes interorganizacionais, o ambiente geral e o ambiente internacional e global. Quanto à rede interorganizacional, tem-se que qualquer organização interage com outras organizações, seja para contratar empregados, garantir capital, obter conhecimento ou ainda para estruturar, alugar ou comprar infraestruturas e equipamentos.

Já no ambiente geral considera-se aquelas dimensões que de forma direta ou indireta impactam nas atividades organizacionais, quais sejam: as variáveis social, cultural, legal, política, econômica, tecnológica e física. No ambiente internacional e global, incluem-se os aspectos que vão além dos limites nacionais ou aqueles organizados em escala global. Destacam-se aqui as instituições que tratam de interesses comuns e dos diversos ambientes gerais (HATCH, 1997).

Se formos definir as camadas ambientais do espaço cibernético dos *smarts grids* das concessionárias de energia elétrica teríamos o esboço ilustrado na Fig. 1 com as respectivas ameaças dos ambientes externos. O ambiente cibernético se traduz no conjunto de infraestruturas de tecnologia da informação e comunicação (TIC) de uma organização, que incluem a internet, as redes de telecomunicações, os sistemas computacionais, os dispositivos pessoais, sensores, processadores e controladores neles embutidos (BODEAU et al., 2010).

Neste contexto podem ser identificados dois grandes componentes do ambiente cibernético: a rede de comunicação que suporta os dados do sistema de controle e monitora os processos organizacionais físicos reais e o ambiente de rede interna de computadores usados para operações não críticas e tarefas administrativas (AITEL, 2013). Além dessas duas infraestruturas, cabe acrescentar os dados operacionais que se referem aos processos críticos da organização. A criticidade das informações é refletida também pela criticidade dos ativos, denominados ativos críticos cibernéticos, envolvidos nas trocas de dados. São esses ativos que contribuem para aumentar o grau de inteligência e de automação do sistema, embora fiquem

mais expostos aos atores desse ambiente (ANSI, 2009; BODEAU et al., 2010; MIT, 2011; NIST, 2010; SOREBO; ECHOLS, 2012).

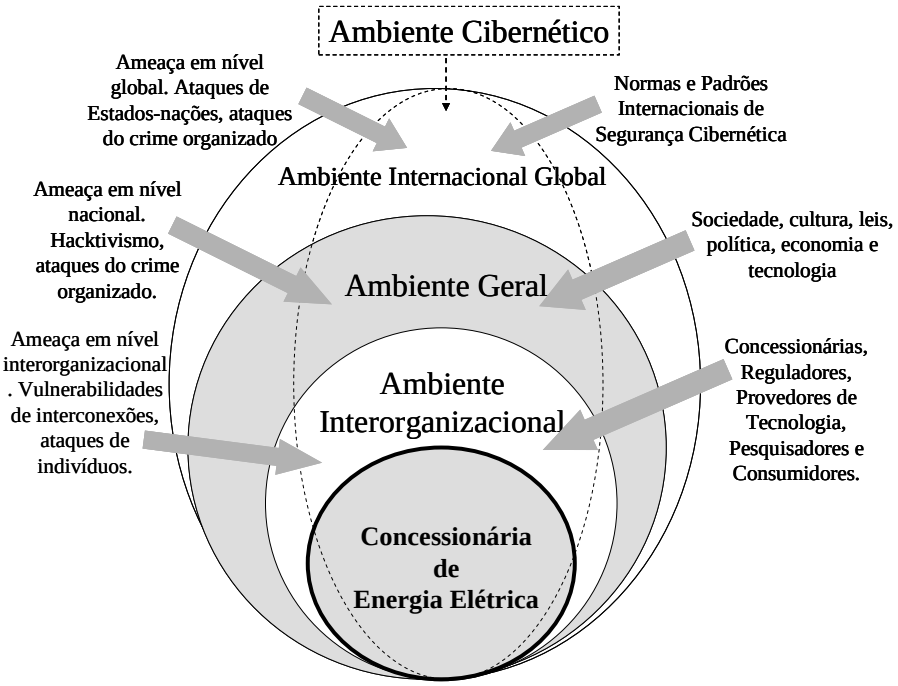

Figura 1 – Ambiente cibernético no contexto do ambiente organizacional
Fonte: Elaborado pelos autores.

Ao integrar sua infraestrutura ao ambiente cibernético, as organizações criam uma área de interesecção do ambiente organizacional com o ambiente cibernético e passam a estar sujeitas às ameaças externas. Ameaças que se diferem nas diversas perspectivas de abordagem do ambiente organizacional. O Quadro 1 apresenta uma taxonomia de riscos que podem vir a afetar o espaço cibernético.

Os invasores do ambiente cibernético são categorizados com base na motivação dos ataques (um *hacker* individual ou um grupo). O invasor pode ser uma nação, um grupo ativista, um grupo criminoso, ou uma pessoa comum individualmente motivada. Os objetivos também diferem sejam, entre outros: a) interromper e destruir as infraestruturas de tecnologia, b) obter informações de operações, projetos, planos de negócios e propriedade intelectual, c) angariar recursos financeiros, d) ganhar publicidade, e) vingar ou simplesmente provar que pode retalhar uma empresa em particular. Assim, os meios de ataque envolvem obter acesso físico local ao sistema de controle, violar a rede interna de computadores do operador e mapear os dados e conexões do sistema com a finalidade de publicá-los ou vendê-los para que outros usem. (AITEL, 2013)

Quadro 1 – Taxonomia do risco operacional cibernético

Ações de pessoas	Falhas de tecnologias e sistemas	Falhas de processos internos	Eventos externos
Inadvertidas	**HW**	**Projeto e execução de processos**	**Desastres**
Equívoco	Capacidade	Fluxo de processo	Eventos climáticos
Erros	Desempenho	Documentação de processo	Fogo
Omissões	Manutenção	Papéis e responsabilidades	Inundação
		Notificações e alertas	Terremoto
Deliberadas	**SW**	Fluxo de informação	Tremor
Fraude	Compatibilidade	Escalamento de questões	Pandemia
Sabotagem	Gerência de configuração	Acordos de nível de serviço	
Roubo	Controle de mudança	Não interferência de tarefas	**Questões legais**
Vandalismo	Configuração de segurança		Observância regulatória
	Práticas de codificação	**Controle de processo**	Legislação
Falta de ação	Testes	Monitoramento de status	Processo
Perfil		Métricas	
Conhecimento	**Sistemas**	Revisão periódica	**Questões de negócio**
Orientação	Projeto	Propriedade do processo	Falha de fornecedor
Disponibilidade	Especificações		Condições de mercado
	Integração	**Suporte a processos**	Condições econômicas
	Complexidade	Pessoal (*staffing*)	
		Financiamento	**Dependência de serviço**
		Treinamento e Desenvolvimento	Concessionárias (*utilities*)
		Aquisição	Serviços de emergência
			Combustível
			Transporte

Fonte: Adaptado de CEBULA; YOUNG (2010, p. 3).

Governança, gestão e modelos normativos da segurança cibernética

A segurança cibernética se refere a toda abordagem voltada a proteger dados, sistemas e redes de ataques deliberados e acidentais e, ainda, da falta de preparo na recuperação dessas infraestruturas em caso de necessidade (MIT, 2011). Trata-se de uma coleção de ferramentas, políticas, conceitos de segurança, salvaguardas, diretrizes, abordagens de gerenciamento de risco, ações, treinamento, melhores práticas e tecnologias, que podem ser usadas para proteger o ambiente cibernético e os ativos de usuários e das organizações (ITU-T, 2008). Diferentemente dos modelos convencionais de segurança de tecnologia da informação, o objetivo da segurança cibernética é reduzir os riscos relacionados à dependência do espaço cibernético e à presença de ameaças externas de adversários (BODEAU et al., 2010).

Dois construtos da segurança cibernética são centrais neste estudo: governança e gestão. O termo governança é usado para descrever um sistema de controle ou de regulação que inclui o processo de nomeação de controladores e reguladores. Já a expressão gestão é adotada para se referir à comunicação da responsabilidade de controladores e reguladores, por meio de ações executivas (TURNBULL, 1997). A governança, segundo Roth e colegas (2012), consiste na definição de critérios para a tomada de decisão, regras, responsabilidades, limites de autonomia e ação das partes envolvidas. O papel da governança não é gerir, mas delimitar a gestão (ROTH *et al*., 2012).

No caso da segurança cibernética, a governança é focada no que as organizações devem fazer de diferente ou a mais do que é aceito nas práticas de governança da segurança da informação. Por esta metodologia, o nível de preparo da organização para a segurança cibernética é analisado sob a perspectiva das seguintes abordagens (BODEAU *et al.*, 2010):

integração estratégica, extensão da estratégia de segurança cibernética para além do ambiente organizacional, mitigação de riscos cibernéticos, adaptabilidade e agilidade na tomada de decisão para fazer frente a ataques cibernéticos à empresa, compromisso dos acionistas e da alta administração e análise dos riscos cibernéticos.

Quanto à dimensão integração estratégica, questiona-se até que ponto a estratégia de segurança cibernética está integrada com outras estratégias, a missão e o gerenciamento de riscos da organização. A perspectiva de adotar estratégias que utilizam recursos advindos do ambiente externo remete ao compromisso da empresa com parceiros, fornecedores e clientes para compartilhar conhecimentos sobre ameaças que podem vir a afetar as atividades organizacionais. Na abordagem de mitigação do risco cibernético, a referência é a estruturação de ações de impedimento de ameaças sob a luz normativa das boas práticas para evitar ataques imprevistos. Em relação a variável agilidade na tomada de decisão, examinam-se as condições proporcionadas pela organização para delegar reponsabilidades no combate aos interesses de adversários de violarem o espaço cibernético da organização. A dimensão compromisso da alta administração indica o engajamento de acionistas, conselheiros e executivos no acompanhamento da execução de ações de segurança cibernética. Finalmente, na análise dos riscos cibernéticos, aborda-se como devem ser gerenciados e atualizados os modelos de ameaças ao ambiente da organização. (ALLEN, 2005; BODEAU *et al*., 2010).

Nesta conjuntura da governança da segurança cibernética é possível, ainda, elencar as recomendações de governança corporativa da Organização para a Cooperação e o Desenvolvimento Econômico (OCDE, 2004). O documento expressa a importância de se respeitar os interesses e o tratamento equitativo dos acionistas; a transparência, qualidade e integridade na divulgação de informações; o exercício das responsabilidades do conselho de administração; a melhoria no cumprimento da leis e; a eficácia dos órgãos reguladores e de supervisão no monitoramento das atividades do setor.

Por meio das recomendações e diretrizes da OCDE é possível elaborar um conjunto de dimensões da governança corporativa aplicados à governança da segurança cibernética no contexto de *Smart Grid*, são elas:

- A base jurídica e regulatória efetiva na governança da segurança cibernética no contexto dos *Smart Grids*;
- As relações com os *stakeholders* de *Smart Grids* na governança da segurança cibernética;
- Os elevados padrões de transparência que atentem a conformidade com os princípios de governança corporativa na gestão da segurança cibernética no contexto de *Smart Grids*;
- O tratamento equitativo dos acionistas;
- As responsabilidades do Conselho de Administração das concessionárias na governança da segurança cibernética de *Smart Grids*.

No esboço da governança, o gerenciamento da segurança cibernética tem seus pilares normativos na ANSI/ISA99 (America National Standard Institute) que trata da segurança em automação industrial e que nos últimos anos vêm se tornando normas internacionais centrais para a proteção de infraestruturas industriais críticas. São instrumentos gerenciais normativos que impactam diretamente a segurança das pessoas, a saúde e o ambiente e, provavelmente, em um futuro próximo, se estenderão a outras áreas de aplicação, mais amplas que as voltadas à automação industrial (ISA99 COMMITTEE ON INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS SECURITY, 2012).

Para a gestão da segurança cibernética operativa, requerem-se das organizações ações que vão além de projetos capazes de elevar o nível de segurança de seus processos. Exige-se a gestão contínua das questões da segurança, de forma a manter o nível desejado. Projetos são

capazes de elevar o nível de segurança, mas mantê-lo não é possível por meio de iniciativas pontuais e, muitas vezes, desalinhadas com a estratégia da empresa. A implementação efetiva de um programa de segurança cibernética engloba o gerenciamento efetivo do risco, o desenvolvimento do sistema e sua manutenção, o gerenciamento da informação e de documentação, o planejamento e a resposta a incidentes crítcos (AMERICAN NATIONAL STANDARDS INSTITUTE, 2009), cabendo acrescentar a preparação e qualificação dos recursos humanos envolvidos.

Com base nas dimensões de governança e de gestão da segurança cibernética, identificadas a partir dos modelos abordados no referencial teórico, elaborou-se o modelo teórico metodológico (Figura 2), a ser adotado no processo de investigação e pesquisa de campo.

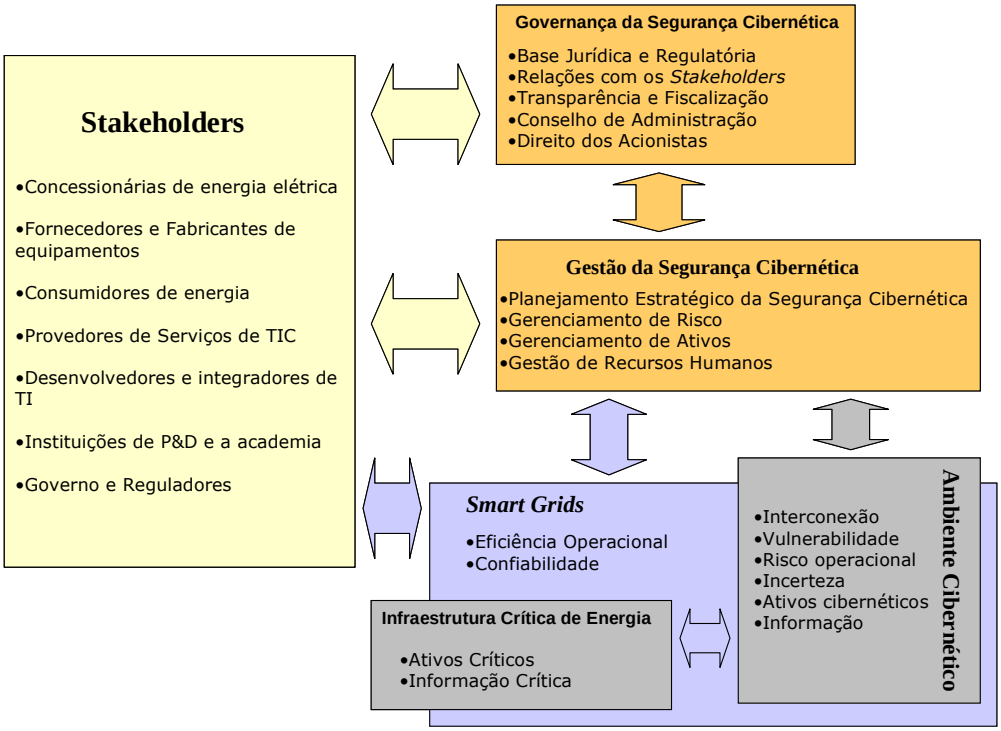

Figura 2 – Modelo teórico-metodológico
Fonte: Elaborado pelos autores.

Metodologia

Esta pesquisa é de natureza exploratória pela incipiência teórica da área de investigação e da necessidade de se explorar o fenômeno empírico no sentido de se contruir e sistematizar conceitos sobre o tema (COOPER; SCHINDLER, 2003). O caminho metodológico foi trilhado em duas etapas. No primeiro momento resgatou-se na literatura estudada as variáveis que compõem as dimensões do modelo teórico-metodológico proposto para a estruturação do questionário. O método utilizado foi a pesquisa bibliográfica.

Na sequência validou-se e testou-se o instrumento de mensuração junto a especialistas do setor elétrico tendo como referência as concessionárias brasileiras de energia elétrica. Aqui utilizou-se o método Delphi realizado com especialistas (acadêmicos, pesquisadores e profissionais) e os testes estatísticos (análise fatorial, esfericidade, *t* de *Student*, Levene, Mann-Whithney e análise de variância) para a estruturação e validação do questionário. A opção pela técnica Delphi advém da potencialidade do instrumento em convergir para o

consenso (ou quase consenso) das opiniões dos especialistas sobre o objeto de pesquisa em foco (WRIGHT; GIOVANAZZO, 2000; DALLA, 2008)

Coleta de dados

A identificação e descrição das dimensões que compõem a governança e a gestão da segurança cibernética foram evidenciadas tendo como base as orientações da OECD (2004), no que concerne a governança corporativa e, as pesquisas de instituições internacionais e acadêmicos, no que se refere à gestão da segurança cibernética (AMERICAN NATIONAL STANDARDS INSTITUTE, 2009; BODEAU *et al*., 2010; US DEPARTMENT OF ENERGY; US DEPARTMENT OF HOMELAND SECURITY, 2012).

Assim, foram identificadas 9 dimensões de análise refletidas em 38 variáveis, sendo, 5 dimensões de governança da segurança cibernética : 1) base jurídica e regulatória (dimensão normativa); 2) interacionista-relacional; 3) transparência e fiscalização (*stakeholders*); 4) conselho de administração; e 5) direito dos acionistas (OCDE, 2004; OCDE, 2005; BODEAU *et al*., 2010; US DEPARTMENT OF ENERGY; US DEPARTMENT OF HOMELAND SECURITY, 2012) e 4 do gerenciamento da segurança cibernética: 1) planejamento estratégico da segurança cibernética; 2) gerenciamento de risco; 3) gerenciamento de ativos; e 4) gestão de recursos humanos (AMERICAN NATIONAL STANDARDS INSTITUTE, 2009; BODEAU *et al*., 2010; US DEPARTMENT OF ENERGY; US DEPARTMENT OF HOMELAND SECURITY, 2012).

Uma versão preliminar do questionário foi elaborada e submetida à análise de quatro especialistas (profissionais envolvidos em projetos de programa de P&D aplicados à área de segurança cibernética em *Smart Grid*, desenvolvidos em parceria com concessionárias de energia elétrica) selecionados por conveniência para a validação das dimensões e variáveis identificadas. Uma primeira versão do questionário foi finalizada e estruturada em formulário eletrônico no *site* Google Docs para a primeira rodadada de respostas. Foram contatados inicialmente 35 especialistas, dos quais 24 se mostraram dispostos a participar da pesquisa.

A partir das respostas obtidas na primeira rodada, foi possível levantar uma opinião preliminar dos especialistas sobre as práticas de governança e gestão de segurança cibernética nas concessionárias de energia elétrica, embora os resultados gerados pela ferramenta Google Docs já apontassem para uma falta de consenso bastante significativa dos especialistas na maioria das afirmativas. Os resultados da primeira rodada serviram então de subsídios para a elaboração de um novo formulário empregado na segunda rodada de pesquisa com os especialistas respondentes da primeira etapa.

Tratamento dos dados

Os formulários preenchidos pelos especialistas na segunda rodada foram armazenados em uma planilha, agrupando as respostas e os comentários relacionados a cada afirmativa. Por meio da ferramenta Survey Monkey trabalhou-se estatisticamente os resultados, de forma a possibilitar uma análise de consenso das opiniões em relação a cada variável.

A análise do consenso procedeu-se a partir do cálculo da mediana e dos quartis. O encaminhamento ao consenso foi medido pela distância entre o primeiro e o terceiro quartis das respostas e o valor da mediana (WRIGHT; GIOVANAZZO, 2000). Neste trabalho, buscou-se, para cada uma das afirmativas apresentadas no formulário da segunda rodada da pesquisa, obter uma distância de no máximo uma unidade da escala entre o primeiro quartil e a mediana e o terceiro quartil e a mediana.

Em um segundo momento, por meio da análise fatorial confirmatória, verificou-se a adequação do agrupamento proposto das diversas variáveis nas respectivas dimensões de

governança e gestão da segurança cibernética. Antes porém, procedeu-se os testes KMO (Kaiser-Meyer-Olkin) e Bartlett de adequacidade dos dados. Adidionalmente, utilizou-se o teste *t* de *Student* para verificar as diferenças de opiniões quanto às dimensões de governança e gestão entre os grupos de respondentes e o teste de Levene para avaliar as variâncias apuradas. Adotou-se ainda o teste de Mann-Whitney, usado para comparar dois grupos independentes e o teste de normalidade de Shapiro-Wilk (MESQUITA, 2010).

Validado o instrumento de avaliação, descreveu-se a análise da governança e gestão da segurança cibernética em concessionárias de energia elétrica brasileiras. Esse diagnóstico analítico foi realizado, a partir de indicadores qualitativos que tipificam a prática, a relevância, o desempenho e o risco de cada variável que compões as dimensões dos contrutos governança e gestão. O tópico seguinte aborda os resultados da pesquisa.

Análise das dimensões de governança e gestão da segurança cibernética de *smart grids* no contexto das concessionárias de energia elétrica brasileiras

Os resultados do estudo são apresentados em duas etapas. A primeira refere-se a validação do modelo teórico-metodológico e do instrumento de mensuração dos dois construtos – governança e gestão da segurança cibernética de smart grids e suas respectivas dimensões e variáveis. Na sequência, por meio das opiniões dos especialistas evidenciadas na aplicação do método Delphi são analisadas a situação do parque energético brasileiro no que concerne à proteção do espaço cibernético dos *smart grids*.

Validação do instrumento de avaliação das dimensões e variáveis do modelo teórico metodológico

Para a verificação da adequação do agrupamento das variáveis nas nove dimensões extraídas dos contrutos gestão e governança utilizou-se a análise fatorial confirmatória. No cálculo das análises fatoriais de cada dimensão, foram calculadas as médias simples das quatro perguntas referentes a cada afirmativa do instrumento de avaliação: prática, relevância, desempenho e diminuição de risco da variável para as concessionárias de energia elétrica. Procedeu-se aos testes de adequacidades de dados de KMO (Kaiser-Meyer-Olkin) e Bartlett. A Tabela 1 apresenta os resultados dos testes e da análise fatorial para as nove dimensões, indicadores que certificam a validação do modelo.

Tabela 1 – Indicadores de validação do modelo teórico-metodológico

Dimensões de Governança e Gestão	KMO	Bartlett	Pvalor	Variância	Variância (%)
1) Base jurídica e regulatória (dimensão normativa)	0,838	44,241	0	3,197	79,92%
2) Dimensão interacionista	0,683	20,065	0	2,263	75,42%
3) Transparência e fiscalização (dimensão *stakeholders*)	0,419	23,941	0	2,091	70%
4) Dimensão Conselho de Administração	0,675	14,287	0,003	2,11	70%
5) Direito dos acionistas	0,5	5,19	0,023	1,533	76,67%
6) Planejamento estratégico da segurança cibernética	0,666	95,473	0	5,053	63%
7) Gerenciamento de risco	0,801	111,246	0	5,503	68,79%
8) Gerenciamento de ativos	0,705	24,029	0	2,373	79,095
9) Gestão de recursos humanos	0,763	44,928	0	3,109	77,73%

Fontes: Dados de pesquisa

Realizada a análise de consenso após a aplicação das duas rodadas da técnica *Delphi* com os especialistas foi possível identificar aquelas variáveis das dimensões validadas que indicavam: a) a prática ou não da variavel pela concessionária, b) importância da variável para a concessionária, c) as implicações da variável no desempenho e d) na diminuição do risco.
A análise qualitativa das dimensões e suas respectivas variáveis são tratadas no item que se segue.

Análise das dimensões da governança da segurança cibernética em concessionárias de energia elétrica

As análises de consenso dos especialistas sobre as dimensões de governança praticadas por concessionárias de energia elétrica brasileiras são realizadas na sequência.

Dimensão base jurídica e regulatória

Duas variáveis desta dimensão apresentaram consenso dos especialistas sobre a relevância dessa perspectiva normativa: a necessidade das concessionárias atenderem às normas internacionais da segurança cibernética paras as infraestruturas críticas no Brasil e a importância do papel que os órgãos reguladores devem desempenhar na segurança do sistema elétrico. Há o reconhecimento que essas duas variáveis reduzem os riscos operacionais das concessionárias no contexto dos *smart grids*.

Alguns comentários evidenciam a distância qua ainda perdura em relação às normas internacionais para a seguraça cibernética de estruturas críticas, seja pela novidade do assunto, desconhecimento, foco em áreas operacionais que não a de segurança ou ausência de exigências dos órgãos regulaores:
"*a maioria das empresas ainda não adotam práticas totalmente aderentes às normas internacionais, apesar do conhecimento sobre o assunto*", muito em função ao "*tema ser recente no Brasil e os estudos na área serem incipentes*"
"Existem infinitos procedimentos de segurança na empresa" porém desconhece-se *"aqueles que teriam sido desenvolvidos especificamente para atendimento legal, regulamentar ou contratual no que se refere aos sistemas críticos da operação*."
"*No que tange a Smart Grid as concessionárias estão se preocupando em um primeiro momento mas nas questões técnicas de implantação, aplicações, custos e impactos nos negócios e não tanto nas questões envolvendo segurança*."
"[..] *a ANEEL não aplica, na prática, nenhuma política governamental que obrigue as concessionárias a aplicarem metodologias mais adequadas com relação à segurança cibernética de suas áreas críticas*."

Dimensão interacionista relacional

No que concerne as interações constantes que devem prevalecer nas relações da segurança cibernética de infraestruturas de energia entre governo e empresas concessionárias, os especialistas, apesar de concordarem sobre a relevância desta prática, convergem que no sistema de governança brasileiro não prevalece esses relacionamentos. Os entrevistados consensualizam ainda sobre a relevância da Livre comunicação a ser exercida sobre as práticas ilegais relacionadas à segurança cibernética das concessionárias de energia elétrica.

A questão da segurança cibernética deve se extender para além da concessionária (BODEAU; et al. 2010). Assim que as ameaças são respondidas e as vulnerabilidades descobertas, as concessionárias devem assegurar que os dados relevantes sejam

compartilhados de maneira eficaz e adequada de forma que os *stakeholders* também possam reduzir o risco e melhorar a resiliência da rede e vice-versa. Fóruns do setor, podem facilitar esse compartilhamento (DOE; DHS, 2012) ainda não observado pelas concessionárias brasileiras.

Dimensão transparência e fiscalização (*stakeholders*)

Os especialistas concordam sobre a importância do acesso a informações precisas, relevantes e oportunas sobre a segurança cibernética, no entanto, caminham para a unanimidade que no contexto das concessionárias brasileiras acionistas, consumidores, diretores, auditores, funcionários e demais *stakeholders* (mídia, fornecedores, credores etc.) não têm acesso a informações precisas, relevantes e oportunas sobre a segurança cibernética. Referem-se também a importância de se praticar de maneira constante auditorias periódicas da segurança cibernética executadas por auditores independentes, mecanismo que aumentaria o desempenho operacional das concessionárias.

Algumas opiniões dos especialistas revelam as condições em que a tansparência e a fiscalização são observadas: *"apenas quando solicitado". "As empresas ainda não sabem como tratar o tema do ponto de vista de suas relações públicas". "Na parte corporativa já funciona, mas não na parte operativa*."

Dimensão conselho de administração

Há uma convergência de opiniões para a unanimidade dos especialistas sobre a relevância do Conselho de Administração estar bem informado sobre a gestão dos riscos cibernéticos operacionais. O mesmo consenso vale para a importância do Conselho em definir os investimentos a serem realizados na proteção dos ativos cibernéticos críticos. Por outro lado, há um consenso, no sistema de governança brasileiro não prevalece uma interação constante nas relações da segurança cibernética de infraestruturas de energia entre governo e empresas concessionárias.

O conselho de administração das consecionárias de energia elétrica ainda não acompanha a gestão da segurança cibernética operacional, uma vez que apenas as questões da segurança cibernética corporativa/administrativa. As justificativas são: *"talvez ainda de forma indireta, sem a formalização do tema como um indicador (informações apenas por eventos). "O conselho de adminitração pode não estar sendo bem informado uma vez que este fluxo de informação só ocorre por demanda, em função de não existir um plano de comunicação específico para esse fim"*.

Dimensão direito de acionistas

Os especialistas consensualizam quanto aos direitos de acionistas que, assuntos relacionados à segurança cibernética não são temas das assembléias gerais de acionistas das concessionárias de energia elétrica. Curiosamente e ambíguo, os entrevistados convergem que os assuntos de segurança cibernética ao serem tratados nas assembleias de acionistas podem vir a aumentar o desempenho operacional das empresas do setor energético.

As análises subsequentes referem-se a dimensão gestão da segurança cibernética dos smart grids nas empresas de energia elétrica.

Dimensões da gestão da segurança cibernética em concessionárias de energia elétrica

Dimensão planejamento estratégico

Se por um lados os especialistas concordam que as concessionárias de energia elétrica realizam algum tipo de planejamento prévio para o estabelecimento de ações voltadas à segurança cibernética e o devido monitoramento destas ações, por outro, de maneira consensual, não concordam que os acionistas e que a alta administração estejam engajados ativamente nas decisões de segurança cibernética.

Prevalece também o consenso de todos os especialistas que:

- ✓Devem ser realizados planejamentos prévios para o estabelecimento de ações voltadas à segurança cibernética e o devido monitoramento dessas ações.
- ✓Faz-se importante consultar as organizações parceiras, os fornecedores e os clientes das concessionárias de energia elétrica, na definição das estratégias de segurança cibernética.
- ✓É necessária a integração das estratégias de segurança cibernética às outras estratégias da organização, entre elas a de *Smart Grid*.
- ✓Precisa-se manter o plano de continuidade do serviço para os casos de incidentes de segurança cibernética.

Essas mesmas variáveis são indicadas, de forma consensual, como mecanismos que aumentam o desempenho e reduzem os riscos operacionais das concessionárias de energia no contexto dos smart grids. Alguns depoimentos indicam o descaso da prática do planejamento estratégico para a segurança cibernética:

"A questão da segurança cibernética para os sistemas críticos da operação estão apenas em fase embrionária na concessionária. Os demais temas relacionados com segurança sempre foram tratados de forma independente."

"Existem planos de contingência que são elaborados periodicamente e ainda em função da ocorrência de eventos importantes." e,

"em pouquíssimas ocasiões elabora-se um planejemanto estratégico operacional, assim mesmo. não um planejamento de longo prazo, exceto para as questões administrativas."

Dimensão gerenciamento de risco

Os entrevistados consensualizam que na análise de risco do negócio das concessionárias ainda não são considerados aqueles riscos cibernéticos operacionais advindos da adoção de tecnologia de informação e comunicação (TIC) em processos de controle e automação do sistema elétrico. Concordam também que os controles de segurança cibernética operacional das concessionárias de energia não são aplicados de forma compatível com os riscos previstos e regularmente testados, monitorados e revisados.

A relevância de algumas ações de gestão do risco cibernético têm a aprovação dos especialistas. São ações que na opinião dos depoentes aumentam o desempenho e reduzem o risco operacional das concessionárias:

- ✓Observar os riscos associados às vulnerabilidades, invasões do sistema elétrico e desastres naturais na estruturação dos processos das concessionárias de energia elétrica.
- ✓Monitorar o ambiente cibernético considerando os riscos das relações entre a concessionária e as partes interessadas (consumidores, fornecedores, concorrentes etc.).
- ✓Observar aos riscos operacionais que podem gerar interrupção ou destruição dos ativos cibernéticos críticos, no estabelecimento de estratégias para a gestão de riscos de segurança cibernética.

Alguns extratos orais reforçam as características da gestão de riscos nas concessionárias:

"Historicamente, os sistemas especializados para a operação do sistema elétrico que os Centros de Operação utilizam são coordenados, implantados e mantidos por áreas de engenharia que deviam se especializar também, e fortemente, em segurança cibernética.".
"Não há nas concessionárias planos de deteção, identificação, análise e resposta às ameaças e vulnerabilidades de segurança cibernéticasão desenvolvidos especificamente para os sistemas críticos da operação do sistema elétrico."
Existe área de gestão de riscos nas concessionárias, entretanto, "ações ou diretrizes, voltadas para os sistemas críticos da operação observando os riscos operacionais que podem gerar interrupção ou destruição dos ativos (instalações, serviços, e sistemas) da rede elétrica, são desconhecidas".
[...] "só existem para os sistemas corporativos, não sendo aplicados aos sistemas críticos da operação (supervisão e controle)".

Dimensão gerenciamento de ativos

Os especialistas consultados consensualizam sobre a importância e seus impactos positivos no desempenho e redução de riscos operacionais sobre as seguintes ações da dimensão de gestão de ativos:

- ✓Monitorar os ativos cibernéticos críticos do sistema elétrico das concessionárias (incluem-se: ativos de comunicação e de automação do sistema elétrico).
- ✓Controlar a permissão e o acesso físico e lógico aos ativos críticos de tecnologia da informação (TI) e tecnologia da operação (TO).
- ✓Gerenciar a configuração e as mudanças nos ativos de tecnologia da informação (TI) e tecnologia da operação (TO) de forma compatível com o risco para a infraestrutura crítica de energia.

Em se tratando da gestão da segurança cibernética no contexto das redes inteligentes de energia elétrica, cabe às concessionárias, monitorar os ativos cibernéticos críticos do sistema elétrico (incluem-se os ativos de comunicação e de automação do sistema elétrico) e controlar a permissão e o acesso físico e lógico a eles; gerenciar a configuração e mudanças nos mesmos, de forma compatível com o risco tolerável para a infraestrutura crítica de energia. Os resultados da pesquisa indicam a existência de controles de acesso pontuais para os sistemas de tecnologia da informação (TI) e tecnologia de operação (TO) aplicados, cujas concepções se acomodam no fato de estarem sob o berço da rede corporativa, protegidos previamente por controles gerais. Os especialistas indicam a necessidade de planejamentos específicos para o controle dos sistemas críticos, com a definição de novos perfis de usuários, acessos (lógico e físico) e domínios, bem como a gerenciamento efetivo desses controles.

Dimensão gestão de recursos humanos

Para os especialistas a um consenso que na descrição de cargos e funções em concessionárias de energia elétrica não são claramente atribuídas responsabilidades de segurança cibernética operacional. Entre as variáveis da dimensão de recursos humanos, apenas os planos de treinamento e educação continuada em segurança cibernética operacional tiveram a unanimidade dos respondentes sobre os impactos positivos no desempenho operacional das concessionárias de energia.

Algumas outras proposições são identificadas nos depoimentos: a) implementar práticas (planos, procedimentos, tecnologias e controles) para criar uma cultura de segurança cibernética e assegurar a adequação contínua e competência do pessoal, compatível com o risco tolerado para a infraestrutura crítica, b) atribuição clara das responsabilidades de segurança cibernética; c) o uso de estratégias de socialização para conscientizar novos e

antigos funcionários e terceirizados, sobre planos procedimentos, tecnologias e controles da segurança cibernética operacional e contar com planos de treinamento e educação continuada sobre a segurança cibernética no contexto das *Smart Grids* d) considerar os antecedentes do funcionário em relação a casos violação da segurança operacional na seleção e contratação de pessoal, e) na descrição de cargos e funções atribuir claramente as responsabilidades do exercício da segurança cibernética operacional.

Conclusão

Por meio deste estudo foi possível estruturar, validar e avaliar as dimensões de governança e de gestão aplicadas às concessionárias brasileiras de energia elétrica diante dos desafios da segurança cibernética apresentados pelas concepções das redes inteligentes de energia elétrica (*Smart Grid*) no Brasil.

Embora a governança e a gestão da segurança cibernética já sejam temas bastante investigados na Administração, quando voltado para a segurança de TI no contexto dos *Smart Grids*, essa abordagem ainda é pouco explorada. Talvez pela própria contemporaneidade da temática, a escassez de pesquisas aumenta quando o foco se limita a segurança cibernética de infraestruturas críticas que fazem uso de sistemas de controle e automação industrial. As características das redes inteligentes de energia elétrica, sistemas acessíveis e interoperáveis que tratam um grande volume informações que transitam em complexas tecnologias de informação e comunicação as tornam assuntos estratégicos, não só para as operadoras de energia elétrica, como também para o Estado, uma vez que o comprometimento do sistema elétrico afeta a sociedade como um todo.

A partir da literatura pesquisada foram identificadas as dimensões normativa, interacionista, transparência e fiscalização, Conselho de Administração e direito dos acionistas para o construto governança corporativa e, planejamento estratégico, gerenciamento de riscos, gerenciamento de ativos e gestão de recursos humanos para o construto gestão. A validação estatística do modelo permitiu sua aplicação no contexto da segurança cibernética dos smart grids em empresas de energia elétrica.

Em relação à dimensão normativa, identificou-se, na opinião dos especialistas, o distanciamento entre as concessionárias de energia elétrica, governo e órgãos reguladores, na busca por uma estrutura reguladora e legal efetiva para a segurança cibernética das infraestruturas críticas no Brasil.

Percebe-se ainda que nas concessionárias brasileiras a segurança cibernética operacional é tratada nos níveis mais baixos da organização, com base em ações isoladas, sem planejamento estratégico de longo prazo e com foco bastante centrado em processos desenvolvidos basicamente por profissionais das áreas de tecnologia da informação e comunicação.

A análise de consenso das respostas extraídas da técnica Delphi permite também inferir que, mesmo os especialistas, desconhecem ainda a representatividade das dimensões de governança. Os resultados indicam um conhecimento maior na relevância da gestão operacional da segurança cibernética do que por variáveis que dizem respeito a relevância das interações entre a alta administração e outros órgãos institucionais envolvidos com a segurança cibernética.

A pesquisa reflete o fato de a alta administração das concessionárias de energia brasileiras ainda não estar ativamente engajada nas decisões de segurança cibernética operacional. Por mais que acionistas e executivos se interessem ou mesmo iniciem os processos de segurança cibernética, o seu planejamento prévio ocorre como iniciativas isoladas e operacionais e não como parte do processo da gestão e da governança corporativa.

De uma forma geral, conclui-se que todas as dimensões descritas como resultado deste estudo, atendem às concessionárias brasileiras de energia elétrica para a governança e a gestão da segurança cibernética no contexto das redes inteligentes de energia (*Smart Grids*).
A dimensão que se mostrou melhor avaliada pelos especialistas, com base nos critérios de adoção pelas concessionárias brasileiras, foi o a dimensão de gestão que comporta o gerenciamento de ativos críticos. A dimensão pior avaliada foi a dimensão de governança que trata do direito dos acionistas.

O presente estudo aponta insights para a teorização deste campo de conhecimento pouco abordado na literatura. As dimensões apresentadas podem auxiliar na aplicação e operação de modelos de governança e de gestão da segurança cibernética para outros setores. Em especial, no contexto dos sistemas críticos de operação do sistema elétrico brasileiro, os resultados demonstram que não há nas concessionárias de energia planos de detecção, identificação, análise e resposta às ameaças e vulnerabilidades de segurança cibernética operacional.

Referências

AITEL, Dave. Cybersecurity Essentials for Electric Operators. **The Electricity Journal**, v. 26, p. 52-58, Jan.-Feb. 2013.

ALLEN, Julia. **Governing for Enterprise Security**. Pittsburgh: Carnegie Mellon University, 2005. Disponível em: <http://www.cert.org/archive/pdf/05tn023.pdf>. Acesso em: 15 abr. 2012.

ANEEL - AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA. **Processo 48500.005714/2009-46**. Brasília: ANEEL, 2012. Disponível em: <http://www.aneel.gov.br/cedoc/aren2012502_1.pdf>. Acesso em: 12 ago. 2012.

ANSI- AMERICAN NATIONAL STANDARDS INSTITUTE. **ISA – 99.00.02-2009**. Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program. USA, 2009.

BANDEIRA, Fausto de Paula Menezes. **Redes de energia elétrica inteligentes (*Smart Grids*)**. Brasília: Câmara dos Deputados, 2012.

BODEAU, Deb *et al*. **Cyber Security Governance**: A Component of *MITRE's Cyber Prep* Methodology. Washington: MITRE Corporation, 2010. Disponível em: <http://www.mitre.org/work/tech_papers/2010/10_3710/10_3710.pdf>. Acesso em: 15 abr. 2012.

CEBULA, James J.; YOUNG, Lisa R. **A Taxonomy of Operational Cyber Security Risks**. Pittsburgh: Carnegie Mellon University, 2010. Disponível em: <http://www.cert.org/archive/pdf/10tn028.pdf>. Acesso em: 15 maio 2012.

COOPER, Donald R.; SCHINDLER, Pamela S. **Métodos de pesquisa em administração**. 7 ed. Porto Alegre: Bookman, 2003.

COUTINHO, Maurílio Pereira. **Detecção de Ataques em infraestruturas críticas de sistemas elétricos de potência usando técnicas inteligentes**. 2007. 260 f. Tese (Doutorado em Ciências em Engenharia Elétrica) – Universidade UNIFEI, Itajubá, 2007.

DALLA, Werner Duarte. **O pensador estrategista**: fatores privilegiados na tomada de decisão estratégica em pequenas e médias empresas. 2008. 183 f. Dissertação (Mestrado em Administração) – Faculdade de Ciências Econômicas, Universidade Federal de Minas Gerais, Belo Horizonte, 2008.

DHS- US DEPARTMENT Of HOMELAND SECURITY. **Cybersecurity:** What Every CEO Should Be Asking. Washington: DHS, 2013.

DOE - US DEPARTMENT OF ENERGY; DHS - US DEPARTMENT Of HOMELAND SECURITY. **Electricity Subsector – Cybersecurity Capability Maturity Model – ES-C2M2**. Washington: DOE/DHS, 2012. Disponível em: <http://energy.gov/sites/prod/files/Electricity%20Subsector%20Cybersecurity%20Capabilities%20Maturity%20Model%20(ES-C2M2)%20-%20May%202012.pdf>. Acesso em: 2 jul. 2012.

GELLINGS, Clark W. **The *Smart Grid***: Enabling Energy Efficiency and Demand Response. Lilburn: TFP/CRC, 2009.

HATCH, Mary Jo. **Organization Theory**: Modern, Symbolic and Postmodern Perspectives. 2 ed. Oxford: Oxford University Press, 1997.

ISA99 COMMITTEE ON INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS SECURITY. Disponível em: <http://isa99.isa.org/ISA99%20Wiki/Home.aspx>. Acesso em: 21 maio 2012.

ITU-T - INTERNATIONAL TELECOMUNICATION UNION. **Recommendation X.1205**: Overview of Cybersecurity. Geneva: ITU-T, 2008.

LOBÃO, Edison. **Panorama energético brasileiro**. Brasília: Ministério de Minas e Energia, 2008.

MESQUITA, José Marcos Carvalho de. **Estatística Multivariada Aplicada à Administração**. Guia Prático para utilização do SPSS. Curitiba: CRV, 2010.

MIT - MASSACHUSETS INSTITUTE OF TECHNOLOGY. **The Future of the Electric Grid**: An Interdisciplinary MIT Study. Cambridge: MIT, 2011.

MOMOH, James. ***Smart Grid***: Fundamentals of Design and Analysis. Piscataway: IEEE Press; Wiley, 2012.

NERC- NORTH AMERICAN ELECTRIC RELIABILITY CONCIL'S. **Critical Infrastructure Protection Standards – CIP 001-009**. Princeton: NERC, 2011.

NEWTON's Telecom Dictionary. 25. ed. New York: Flatiron, 2009.

NATIONAL INSTITUTE OF STANDARDS TECHNOLOGIES – NIST. **NISTIR 7628**: Guidelines for *Smart Grid* Cyber Security National Institute of Standards and Technology Interagency Report 7628. Gaithersburg: Department of Commerce/NIST, 2010. 1 v. 289 p. Disponível em: <http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf>. Acesso em: 4 fev. 2011.

OCDE. Os Princípios da OCDE sobre o Governo das Sociedades. 2004. Disponível em: <http://www.oecd.org> .Acesso em: 25 out. 2012.

OCDE. Diretrizes da OCDE sobre Governança Corporativa para Empresas de Controle Estatal, 2005.

OCDE. Latin American White Paper on Corporate Governance. 2003. Disponível em: <http://www.oecd.org/daf/ca/corporategovernanceprinciples/latinamericanwhitepaperoncorporategovernance.htm> . Acesso em: 25 out. 2012

ROTH, Ana Lúcia *et al*. Diferenças e inter-relações dos conceitos de governança e gestão de redes horizontais de empresas: contribuições para o campo de estudos. **Revista de Administração da Universidade de São Paulo – RAUSP**, v. 47, n. 1, p. 112-123, jan./fev./mar. 2012.

SOREBO, Gilbert N.; ECHOLS, Michael C. ***Smart Grid* Security: An End-to-End View of Security in the New Electrical Grid**. Boca Raton: CRC Press, 2012.

TURNBULL, Shann. Corporate Governance: Its Scope, Concerns and Theories. **Scholarly Research and Theory Papers**, v. 5, n. 4, Oct. 1997.

WRIGHT, James Terence Coulter; GIOVANAZZO, Renata Alves. *Delphi*: uma Ferramenta de Apoio ao Planejamento Prospectivo. **Caderno de Pesquisa em Administração**, São Paulo, FIA/FEA/USP, v. 1, n. 12, p. 54-65, 2000.