SEGURANÇA CIBERFÍSICA NAS EMPRESAS DE ENERGIA

Desafios e oportunidades na proteção das infraestruturas críticas do setor elétrico brasileiro

Tácito Augusto Silva Leite, DSE, ASE, C31000

Download

O download desse eBook pode ser feito no seguinte endereço: http://www.bibliotecadeseguranca.com.br/livros/seguranca-ciberfisica-nas-empresas-de-energia/

Licença

SUMÁRIO

RESUMO
ABSTRACT

Resumo

O presente *paper* tem por objetivo geral observar o cenário global da segurança de infraestruturas críticas (que são organizações provedoras de serviços essenciais, como energia, água, telecomunicações e outros), demonstrando o que tem sido feito e quais as perspectivas de futuro na área da segurança corporativa.

Especificamente, o trabalho destaca os principais desafios do setor de energia elétrica no Brasil. Oferece reflexões e orientações a partir de soluções, erros e acertos encontrados por países experientes na proteção de suas infraestruturas críticas, como Estados Unidos e Espanha. Discorre sobre o conceito de segurança ciberfísica.

Palavras-chave

Infraestruturas críticas; segurança corporativa; setor de energia elétrica; serviços essenciais; segurança ciberfísica.

Abstract

This paper's main objective is to sketch a global security scenario for critical infrastructures, which are essential service provider organizations (companies that deal with energy, water, telecommunications and others), showing what have been done and future prospects in corporate security. Specifically, this work highlights the electric energy sector's main challenges in Brazil. This paper offers reflections and guidance from solutions, mistakes and successes found by experienced countries in protecting their critical infrastructures, as United States and Spain. In addition, it discusses on cyberphysical security.

Keywords

Critical infrastructures; corporate security; electric energy sector; essential services; cyberphysical security.

INTRODUÇÃO

Introdução

Este trabalho tem por objetivo mostrar o que tem sido feito e quais as perspectivas futuras na segurança de infraestruturas críticas, no Brasil e no mundo. Descreve em linhas gerais o que é gestão de riscos e oferece um cenário da segurança nessa área, especialmente no setor elétrico. Entendemos que a área de segurança corporativa dessas infraestruturas é a responsável por garantir a proteção e a resiliência da organização. Entretanto, deve ser complementada pelo Estado, que tem a obrigação de garantir os serviços à população.

O cenário desenhado pelos relatórios internacionais aqui apresentados exige atenção: conforme aumenta globalmente o desenvolvimento tecnológico, surgem novos riscos, e os setores encarregados da proteção, tanto os públicos quanto os privados, nem sempre estão preparados ou, então, preparam-se em ritmo mais lento do que o aparecimento de novos riscos. As tecnologias modernas demandam uma segurança que integre a proteção dos ativos físicos e lógicos das empresas – a segurança ciberfísica.

Cabe às empresas do setor elétrico desenvolver e preservar sistemas e processos eficientes para detectar ameaças, controlar vulnerabilidades e garantir a proteção em níveis aceitáveis. Cabe também a elas estar constantemente preparadas para situações adversas, mantendo planos de continuidade de negócios e contingência bem estruturados, com pessoal treinado para agir rapidamente a fim de minimizar perdas, caso os riscos ocorram. Assim elas asseguram um nível adequado de resiliência, garantindo capacidade para se reestabelecer de ocorrências indesejadas.

Nós brasileiros ainda temos muito a aprender com a Espanha e os Estados Unidos, que historicamente investem de forma intensa na segurança da população. Nesses países são tomadas ações governamentais vigorosas que fomentam a criação de uma cultura de segurança nas organizações, em especial aquelas que compõem suas infraestruturas críticas.

No Brasil, estão sendo implantados sistemas de energia elétrica cada vez mais sofisticados e inteligentes, em todo o território, o que gera novas ameaças e vulnerabilidades. As empresas concessionárias deveriam praticar uma gestão de riscos avançada, uma vez que a interrupção do abastecimento de energia pode gerar sérios prejuízos para elas mesmas e para a população, qualquer que seja a causa. No governo, estão sendo tomadas ações de proteção, como o projeto Proteger, do Exército, ainda em implantação.

Enquanto isso, em nosso país, segundo os últimos relatórios sobre o tema citados ao longo deste estudo, até mesmo companhias de grande porte deixam a desejar no quesito gerenciamento de riscos. Muitas investem em processos e equipamentos, mas negligenciam o treinamento dos colaboradores e a orientação do público quanto à segurança ciberfísica. Poucas dessas companhias estão preparadas para contratar e manter talentos para os cargos executivos de gestão de riscos de segurança ciberfísica.

Capítulo 1

DOIS CASOS REAIS

Capítulo 1 ||| Dois casos reais

No Natal de 2015, no auge do inverno europeu, o oeste da Ucrânia ficou sem energia elétrica por três horas devido a um malware nos sistemas de suas centrais elétricas, inserido a partir do exterior. Simultaneamente, foram também atacados os computadores de empresas de telefonia, além dos sistemas de comunicação das concessionárias de energia, impedindo-as de receber as reclamações dos usuários. Esse caso, ocorrido na tarde de 23 de dezembro 2015, teve grande repercussão na área de segurança. O caso, amplamente divulgado pela mídia na época, está relatado no website da WisePlan[1].

Apesar de fazer fortes investimentos em infraestrutura crítica e de contar com sistemas de controle reconhecidamente seguros, a Ucrânia sofreu um ataque cibernético de grandes proporções e consequências graves, que atingiu uma grande área, incluindo a cidade de Ivano-Frankivsk, com mais de 700 mil habitantes e 200 mil indústrias. Foi uma ação bem planejada, com alta motivação e conhecimento técnico dos complicados sistemas de controle. Os invasores sabiam exatamente onde clicar e o faziam com desenvoltura – reportaram depois os operadores que, atônitos, foram obrigados a assistir em seus monitores o desligamento "autônomo" de um grande número de subestações em poucos minutos.

Nessa região, atendida por diversas empresas privadas de transmissão e distribuição, as fontes de eletricidade são principalmente térmicas. A queda do abastecimento começou um pouco antes das 16 horas e somente às 19 horas começou o reestabelecimento. As equipes de resposta souberam reagir em tempo curto e, além disso, algumas das proteções instaladas no sistema para barrar invasões funcionaram bem, o que evitou prejuízos ainda maiores. O incidente passou a figurar entre os casos clássicos de vulnerabilidade de infraestruturas críticas.

1 Artigo de título Caso de Estudio: Hackeo de la Red de Distribución Eléctrica en la zona oeste de Ukrania el pasado 23 de Diciembre de 2015. Disponível em http://wiseplant.com/2016/03/27/analisis-del-hackeo-de-la-red-electrica-de-ukrania-el-pasado-23-de-diciembre-de-2015. Acesso em setembro de 2017.

acesse aqui

Atiradores passaram 20 minutos alvejando a subestação de Metcalf, San José, inutilizando 17 transformadores que conduziam energia elétrica para o Vale do Silício. O prejuízo de US$ 15 milhões poderia ter sido maior.

No evento, vários computadores das empresas de energia foram infectados. O vetor de ataque foi um malware denominado BlackEnergy (também chamado DarkEnergy). Os acessos remotos foram vulnerados e hackers dominaram a operação. Entre as vulnerabilidades constatadas depois, estava o fato de que o acesso remoto por VPN dos Sistemas SCADA -- Supervisory Control and Data Acquisition --, de supervisão de sistemas conectados, tinha apenas um fator de autenticação, quando deveria ter no mínimo dois.

A recuperação dos sistemas foi longa e trabalhosa, pois eles precisaram ser modificados para não voltarem às mesmas vulnerabilidades. Enquanto isso, o abastecimento foi restituído de forma manual em quase sua totalidade. A restituição manual só foi possível porque a rede ucraniana é razoavelmente antiga, as redes modernas não permitem a volta ao abastecimento sem os sistemas de controle.

Evento igualmente traumático, dessa vez envolvendo a segurança física, já havia deixado o setor elétrico em alerta: em abril de 2013, na Califórnia, uma pessoa infiltrou-se em uma caixa-forte subterrânea nos arredores de San José e cortou vários cabos telefônicos. Meia hora depois, atiradores passaram 20 minutos alvejando a subestação de Metcalf, San José, inutilizando 17 transformadores que conduziam energia elétrica para o Vale do Silício. O prejuízo de US$ 15 milhões só não foi maior porque os técnicos impediram o blecaute redirecionando logo a energia em torno da subestação atacada. O caso é relatado por Megan Gates em artigo publicado em maio de 2015 para a revista Security Management, uma publicação da Asis Internacional[2].

Além dos fios de transmissão, as redes elétricas contam basicamente com: uma fonte geradora (hidrelétrica, termoelétrica, usina de biomassa, usina eólica etc.); subestações de transmissão, que diminuem a voltagem original de 500 kV[3] para 230 kV (valores aproximados); e subestações de distribuição, nas quais a voltagem cai para 115 kV antes de chegar aos consumidores. No caso da Califórnia, os criminosos não atacaram a central elétrica, porém conseguiram prejudicar a distribuição ao agir em uma subestação.

2 Disponível em https://sm.asisonline.org/Pages/The-Power-of-Physical-Security.aspx. Acesso em setembro de 2017 **acesse aqui**

3 Quilovolts

Pouco tempo após o evento de San José, foi elaborado nos Estados Unidos um protocolo específico, o CIP-014, exigindo que estações e subestações de transmissão sejam submetidas a avaliação de riscos detalhada para identificar vulnerabilidades que, se forem exploradas por criminosos, terão forte impacto.

Ataques como os da Califórnia e da Ucrânia podem causar grandes danos às organizações e à sociedade. Entre as lições que trouxeram, mostraram que não basta proteger os dados ou a central de controle, é necessário um sistema abrangente de defesa, que envolva as áreas de segurança física e segurança cibernética, ambas conduzidas estrategicamente por um planejamento baseado na gestão de riscos integrados. A participação de toda a empresa é essencial para haver eficiência na detecção e na proteção em todos os níveis da atividade. Nenhum deles pode se considerar invulnerável. O grau de resiliência exigido por uma infraestrutura crítica só pode ser obtido por ações coordenadas de segurança ciberfísica.

Capítulo 2

INFRA-ESTRUTURAS CRÍTICAS NO SETOR ELÉTRICO BRASILEIRO

Capítulo 2 ||| Infraestruturas críticas no setor elétrico brasileiro

Em alusão ao livro *Gestão de riscos na segurança patrimonial* [4], a gestão de riscos é a forma moderna de proporcionar segurança integral às organizações. Sempre que exista algum empreendimento humano, existem riscos, que podem ser quantificados para fins de gerenciamento. Uma excelente ferramenta de quantificação é a equação do risco:

$$\text{RISCO} = \frac{\text{AMEAÇA X VULNERABILIDADE X IMPACTO X PROBABILIDADE}}{\text{RECURSOS DE SEGURANÇA EFICIENTES}}$$

Vê-se que no numerador estão presentes elementos agravantes e, no denominador, o elemento de mitigação. Dessa forma, analisar isoladamente ameaça e vulnerabilidade é apenas uma parte da questão. Se um risco, por exemplo, tiver pouca probabilidade de acontecer, se o sistema tiver pouca vulnerabilidade e se for remota a existência de ameaça, mas se o impacto for enorme, necessita ser protegido com recursos de segurança eficientes.

A partir de uma boa avaliação de riscos, que siga os passos da norma ABNT NBR ISO 31000 [5] ou outra norma equivalente, pode-se determinar quais barreiras serão necessárias para enfrentar as ameaças e controlar as vulnerabilidades. Os investimentos em recursos de segurança precisam englobar pessoas, processos e tecnologia (PPT). Partindo do princípio de que toda atividade humana pressupõe riscos, mesmo aplicando medidas de controle para os riscos inaceitáveis, eles poderão se concretizar e a organização precisa estar preparada. Por isso, um adequado planejamento de segurança, com foco não só na proteção, mas também na resiliência, contempla também programas de continuidade de negócios (BCP), de recuperação de desastres (DRP) e programas de gerenciamento de emergências.

Em geral, são consideradas críticas as infraestruturas que envolvem energia, transporte, água, telecomunicações e finanças. A palavra

4 Mais referências em http://consultoriadeseguranca.com.br/. Acesso em agosto de 2017 **acesse aqui**

5 Acesso em setembro de 2017. Disponível em http://www.abntcatalogo.com.br/curs.aspx?ID=30. **acesse aqui**

"críticas" diz respeito à população que atendem, uma vez que a forma de vida das pessoas depende do bom funcionamento dessas estruturas. As infraestruturas críticas são, na grande maioria, concessões dos governos e os riscos inerentes às suas atividades podem afetar milhões de habitantes.

Sendo o fornecimento de energia uma infraestrutura crítica, a segurança energética transcende a gestão das concessionárias, configurando uma questão governamental. Se uma concessionária de energia elétrica deixar de abastecer as residências, sofrerá reveses comerciais, regulatórios, de imagem, entre outros. Tecnologia da informação e recursos avançados de segurança favorecem o fornecimento ininterrupto de eletricidade.

As concessionárias reveem periodicamente seus planos e procedimentos para prevenir e minimizar os efeitos de possíveis ameaças, e contam com pessoal preparado para responder em uma eventual situação de emergência, seja ela de ordem física ou virtual. Investir preventivamente em segurança é uma forma eficiente para mitigar as ocorrências físicas e cibernéticas, o que se reflete na diminuição das perdas e consequente aumento da lucratividade e competitividade das concessionárias.

Ao redor do mundo, as tecnologias mais avançadas atualmente permitem soluções de segurança centralizadas, que integram múltiplos sensores e alarmes com localização georreferenciada, além de verificação visual regular. As soluções de apoio combinam sistemas tradicionais de segurança com soluções avançadas de simulação, utilizando câmeras em ambientes virtuais 3D e refinando o gerenciamento dos operadores de segurança. No artigo *Tecnologia torna mais inteligentes e seguras as infraestruturas elétricas*, para a revista Smart Energy[6], o autor expõe em linhas gerais como o encontro da tecnologia da informação com os avanços em recursos de segurança promoveram um salto para assegurar a ininterrupção do fornecimento de energia.

Um marco no avanço tecnológico são as smart grids (redes inteligentes), que vêm se expandindo nos últimos anos. Trata-se, em essência, da substituição dos medidores convencionais por medidores eletrônicos inteligentes, que permitem aferição remota, entre outras aplicações. As redes inteligentes, bastante automatizadas, utilizam recursos avançados de TI e potencializam a eficiência das concessionárias.

---

6 Revista Smart Energy set/outubro 2013 p. 42-43 por Tácito Leite. Disponível em http://pt.calameo.com/read/002590700830a78e574d9 **acesse aqui**

Evolução tecnológica da operação implica gestão dos riscos mais eficiente e integrada. O documento *Guidelines for Smart Grid Cybersecurity (NISTIR 7628 Revision 1), Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements* [7], elaborado pelo National Institute of Standards and Technology, EUA, tem foco principal na proteção cibernética, porém é enfático ao incluir a necessidade de proteção física das infraestruturas críticas. Esse documento define requisitos específicos para ajudar as organizações de energia a protegerem suas estruturas físicas, além das cibernéticas.

As concessionárias de eletricidade têm sempre em conta que alguém pode acessar fisicamente seus equipamentos, em qualquer nível, e interferir na entrega de energia – como aconteceu no caso já relatado da Califórnia. A indústria das companhias elétricas, especialmente com o advento das smart grids, é um exemplo claro de organizações que demandam segurança ciberfísica.

Já o relatório *The cost of incidents affecting CIIs* [8], que faz a revisão sistemática de estudos de impacto econômico de incidentes ocorridos com cibersegurança em infraestruturas críticas de informação, *CII (critical information infrastructures)*, realizado pela *European Union Agency For Network And Information Security*, indica que o Brasil é o quinto país, com custo médio por empresa, relacionado a ataques cibernéticos entre as companhias consideradas infraestruturas críticas. O estudo aponta os dados nos gráficos a seguir.

O Brasil é o quinto país, com custo médio por empresa, relacionado a ataques cibernéticos entre as companhias consideradas infraestruturas críticas.

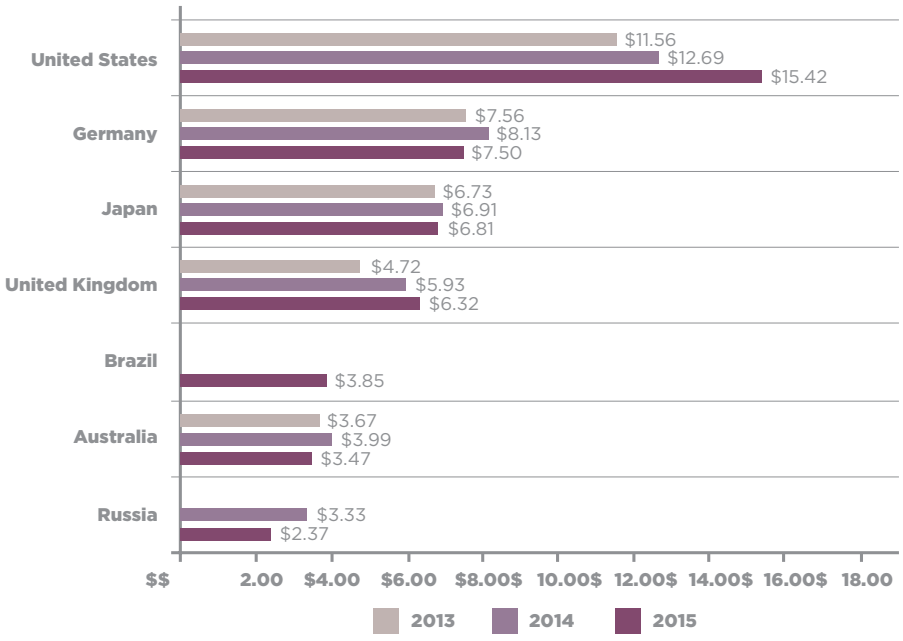


Figura 1 – Impacto econômico médio do cibercrime por organização (milhões)
Reproduzido de The ost of incidents affecting CIIs.

7 Disponível em http://dx.doi.org/10.6028/NIST.IR.7628r1. Acesso em setembro de 2017 **acesse aqui**

8 Disponível em https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis. Acesso em setembro de 2017 **acesse aqui**

E entre as empresas de infraestrutura crítica, os estudos indicam que o setor energético figura entre os mais afetados.

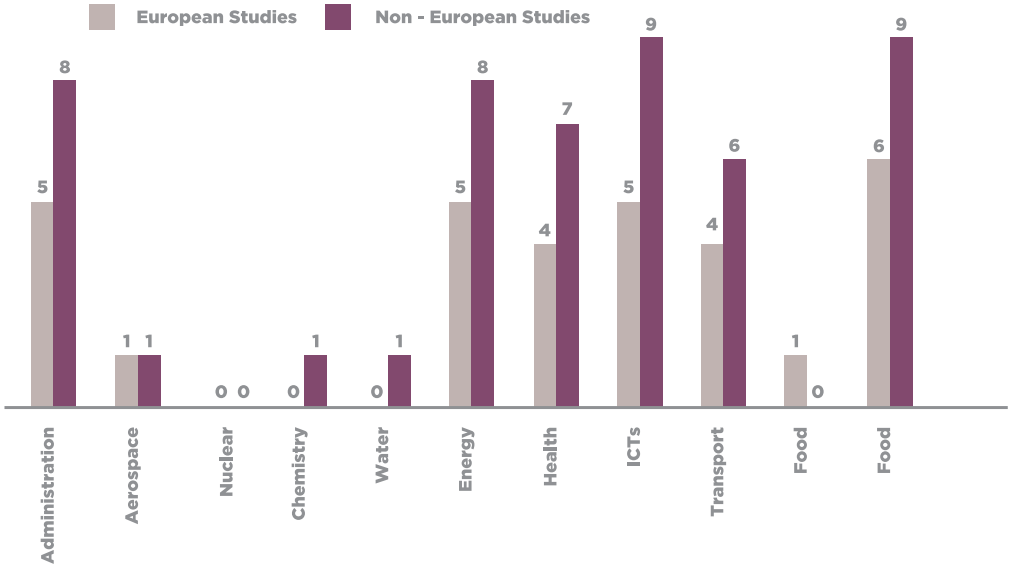


Figura 2 – Setores de CII (critical information infrastructures) mais afetados Reproduzido de The cost of incidents affecting CIIs.

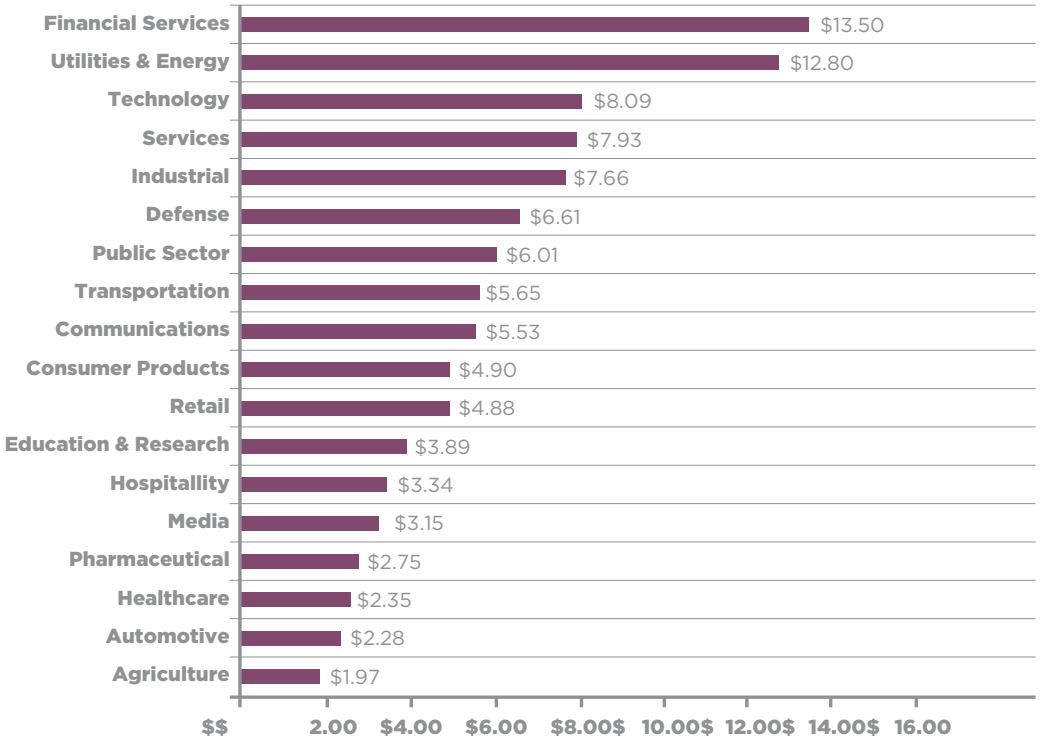


Figura 3 – Custo médio atualizado por setor de indústria (milhões). Reproduzido de The cost of incidents affecting CIIs.

O relatório indica ainda que o impacto econômico mais alto é produzido por pessoas mal-intencionadas, ataques de negação de serviço (também denominados DoS ou DDoS -- distributed denial-of-service attack) e ataques baseados na web. O primeiro vetor relacionado aos impactos financeiros (pessoas mal-intencionadas) tem relação direta com a segurança física. Tudo

isso reforça a necessidade de que a gestão de riscos abarque não apenas a parte física, e não apenas a parte de TI, mas ambas, de maneira integrada.

Ainda no âmbito de segurança ciberfísica, o documento Critical Infrastructure Protection: Security Dependencies and Trends, de 2013 [9], um resumo publicado pela Asis International sobre proteção de infraestruturas críticas, salienta que a segurança física é uma faceta importante da segurança cibernética porque proteger um computador, ou outros equipamentos do sistema de controle, fica quase impossível se o atacante tiver acesso físico a eles. Da mesma forma, não se pode negligenciar a proteção contra inundações, incêndios, vandalismo e muitas outras ameaças físicas.

O documento enfatiza a necessidade de que a segurança tenha foco também na resiliência, não apenas na prevenção. Isso significa aceitar que as ameaças não irão desaparecer e alguns ataques serão efetivamente realizados e bem-sucedidos, além de serem possíveis os eventos naturais. O objetivo é que o sistema e os subsistemas associados sejam projetados e operados de tal forma que as funções críticas continuem durante e após eventos indesejados, apesar de sofrerem, eventualmente, perda de recursos-chave para o negócio e para clientes.

É necessário que a segurança tenha foco também na resiliência, não apenas na prevenção.

As soluções devem levar em consideração o equilíbrio entre os riscos que uma entidade está disposta a aceitar e os riscos reais existentes. Isso só será possível se a segurança ciberfísica for conduzida por uma gestão de riscos integrados. Dentro desse ambiente complexo, a resiliência do sistema será influenciada pelas relações custo versus benefício associadas às soluções e controles particulares que a organização está disposta a adotar.

9 Disponível em https://www.asisonline.org/About-ASIS/Pages/CIP.aspx. **acesse aqui** Acesso em agosto de 2017.

Os ataques físicos a sistemas elétricos não são novos, e alguns países tiveram de suportá-los por anos. Embora antiga, uma análise realizada entre 1994-2004 mostra que dos ataques à infraestrutura elétrica em todo o mundo, o alvo mais comum foi a transmissão, conforme indicado na figura a seguir. Em 2013, o assalto à subestação Metcalf, como já foi visto, resultou em danos de US$15 milhões. Embora nenhum consumidor tenha perdido o fornecimento, a empresa comprometeu-se a investir US$100 milhões ao longo de três anos para melhorar a segurança de suas instalações críticas.

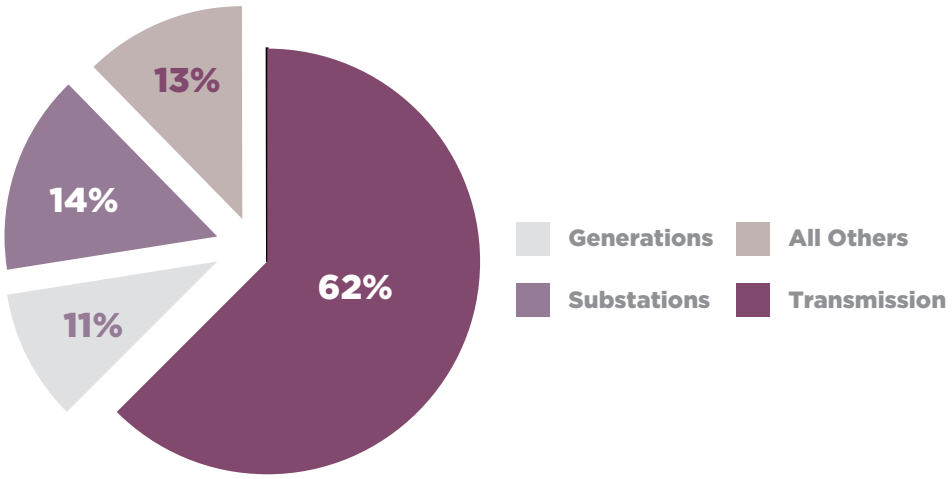


Figura 4 – Ataques terroristas internacionais de 1994 a 2004. Reproduzido de Memorial Institute for the Prevention of Terrorism.

Capítulo 3

RISCOS IDENTIFICADOS EM RELATÓRIOS INTERNACIONAIS

Capítulo 3 ||| Riscos identificados em Relatórios Internacionais

Neste capítulo, são abordados os conteúdos de três grandes relatórios internacionais, produzidos por instituições relevantes: Asis Internacional, Aon e Fórum Econômico Mundial. Esses documentos são referências importantes pois representam o resultado de pesquisas amplas e abrangentes. Mostrando as circunstâncias atuais, sugerem perspectivas de futuro, essenciais para que sejam feitos bons planos estratégicos de segurança.

Seguradora Aon

O relatório Global Risk Management Survey[10], publicado bianualmente pela companhia seguradora Aon, retrata a maneira como as instituições têm lidado com a questão da segurança. A edição de 2017 traz uma extensa pesquisa realizada no último trimestre de 2016, com 2.000 respondentes de 33 diferentes setores de atividade, em 64 países, contemplando companhias públicas e privadas, de todos os tamanhos, configurando assim uma das maiores pesquisas globais, pela abrangência de temas e pela quantidade de dados.

Nesse relatório, são mostrados os dez principais riscos às companhias, do ponto de vista dos entrevistados, sendo o quinto deles: cibercrime, ação de hackers, vírus, códigos maliciosos e o sétimo, falha em atrair e manter talentos.

Na pesquisa anterior da Aon, cibercrime era o nono colocado, enquanto na pesquisa de 2017 passou à quinta posição. Isso mostra que está em curso uma escalada dessa modalidade de crime.

10 Disponível em http://www.aon.com/2017-global-risk-management-survey/. Acesso em agosto de 2017. acesse aqui

Em resposta, as empresas têm investido em novas formas de mitigação. A pesquisa aponta, entretanto, que ainda é pouca a colaboração multifuncional na gestão de riscos cibernéticos.

As boas práticas indicam que a área de gestão de riscos deve ser independente das demais áreas da organização, geralmente respondendo para o conselho ou para o diretor-presidente (CEO). O contrassenso de deixar a área de riscos abaixo de alguma caixa do organograma está nos possíveis conflitos de interesse. Isso fica mais evidente nos riscos, relacionados à área de subordinação, que requeiram investimentos específicos.

A quem reportar é uma questão sensível em gestão de riscos. Nessa pesquisa, a grande maioria dos respondentes, 86%, relatou que tais decisões estavam a cargo de TI; quase 38% apontaram o departamento de riscos de suas empresas como responsável por esse controle; 13% estavam a cargo do departamento jurídico; e 5%, a cargo de RH. Mais da metade das empresas não contavam com um setor específico para a gestão de riscos em geral.

Essa situação aumenta a vulnerabilidade a uma das formas mais efetivas de ataque contra as organizações, a chamada engenharia social (social engeenering). Nela, o acesso a informações sensíveis é obtido por meio de chamadas telefônicas, e-mails, mídias sociais e outros dispositivos.

As pessoas podem se tornar o ponto mais fraco de qualquer sistema de segurança por não atenderem a políticas e padrões -- se as qualificações e o treinamento não forem bem definidos e mantidos. Além disso, o elemento humano está sempre sujeito a coerção, extorsão e outras formas de indução. Todos os incidentes de segurança de natureza criminal são causados por pessoas. Alguns não são intencionais, mas todos são cometidos por pessoas. Nem todos os perigos são causados por pessoas, mas o crime o é. Muitas vezes um colaborador é o melhor meio para atingir um alvo crítico bem protegido. Por mais avançada que seja a tecnologia de proteção, ela não funcionará como deve se não for considerado o preparo do ser humano para lidar com ela.

A falha em avaliar os riscos, outro ponto abordado pelo documento, resulta em falta de estratégias efetivas para a mitigação. O relatório aponta que a prontidão organizacional para enfrentar o cibercrime está decaindo -- 82% no relatório de 2015 e 79% em 2017. Duas hipóteses para explicar essa situação

seriam: (1) as companhias geraram programas mais sofisticados de análise e por isso estão identificando mais fatores de risco; e (2) as empresas não conseguem avaliar os riscos cibernéticos em ritmo mais rápido do que o surgimento de novas tecnologias.

Geograficamente, a preparação reportada pelos entrevistados para enfrentar os dez maiores riscos aumentou no leste da Ásia e diminuiu nas demais regiões, sendo a América Latina a mais despreparada. É a região com maior defasagem para implantar avaliação de risco, mitigação e estratégias eficazes. Com relação à avaliação de riscos cibernéticos especificamente, as companhias norte-americanas lideram com 76% (19% a mais do que na pesquisa anterior) e as latino-americanas são as últimas, com 38% (também 19% a mais do que na pesquisa anterior).

Relacionando riscos por indústria, o relatório traz cibercrimes como maior risco para a área de energia nos últimos anos e nos próximos três. Dos entrevistados, 35% compram seguro contra cibercrimes. Apesar de não consignarem perdas altas, pois em geral as áreas de TI têm já uma boa proteção e cultura de segurança, o cibercrime é o crime contra o qual há mais proteção, dentre os dez maiores riscos, devido à crescente conscientização nos últimos anos. Na América Latina, enquanto aumenta a previsão desse risco (ataques cibernéticos), o risco de não atrair talentos (um entre os dez maiores) está listado como sétimo. Ou seja, a área de segurança sente carência de recursos no nível executivo, configurando uma pirâmide com o topo muito pequeno. Mesmo grandes organizações gerenciam riscos de forma incipiente e amadora, aponta o relatório.

Relacionando riscos por indústria, o relatório traz cibercrimes como maior risco para a área de energia nos últimos anos e nos próximos três.

Esse cenário é tenebroso porque há baixa maturidade nessa área, em contraposição com o quadro de necessidades. A atividade de segurança não está no nível estratégico, mas sim no nível tático-operacional. Não há conscientização dos riscos em nível suficiente, e não é visto o benefício de se dar mais status à segurança no organograma das instituições. Entendamos segurança como área responsável por garantir a proteção e a resiliência da organização, diminuindo, assim, algumas incertezas relacionadas aos objetivos do negócio.

Na América Latina, a maior parte das empresas não usa qualquer método para avaliar riscos quando só a norma ISO 31010, por exemplo, lista 31 métodos aplicáveis para essa avaliação. [11]

11 Há inclusive métodos que podem ser usados diretamente no website, no modelo SaaS (Software as a Service), como o t-Risk, disponível em www.totalrisk.com.br. acesse aqui

Asis International[12]

As ameaças cibernéticas também são foco de estudo no relatório *Critical Infrastructure Protection: Security Dependencies and Trends,* de 2013, publicação da Asis Internacional já citada no capítulo anterior. O estudo prevê novas ameaças que poderão rondar, no futuro, os sistemas da indústria de energia. São elas:

1. Haverá crescimento das mídias sociais, com novas ferramentas e, ao mesmo tempo, novos vetores de ataque, novas vulnerabilidades e novas formas de explorá-las.

2. Será intensificado o uso da nuvem e das redes de clientes para acessar informações corporativas. Assim, clientes e parceiros precisarão ter o mesmo nível de proteção que as empresas.

3. A prática denominada BYOD (*bring your own device*, ou "traga seu próprio dispositivo"), juntamente com a internet das coisas (IoT), exigirá que as empresas reescrevam suas práticas de TI, considerando que os dispositivos individuais podem ter proteção inadequada, e será necessário registrar, rastrear e controlar mais dados, acompanhar a conformidade dos padrões e garantir auditoria.

4. A maior possibilidade de trabalho remoto aumenta as preocupações sobre quem tem acesso aos dados, sobre baixo nível de segurança, maior vulnerabilidade a furtos, perda de ativos e de informações.

Trabalho remoto aumenta as preocupações sobre quem tem acesso aos dados, sobre baixo nível de segurança, maior vulnerabilidade a furtos, perda de ativos e de informações.

5. As empresas de energia precisarão atuar estrategicamente na gestão de riscos, uma vez que haverá um limbo de problemas de segurança cibernética criado pela combinação de dispositivos móveis para uso pessoal e para trabalho, redes sociais, tecnologia sem fio, trabalho remoto, smart grid, serviços em nuvem, entre outros riscos operacionais com desdobramentos na estratégia da organização.

12 Disponível em https://www.asisonline.org/About-ASIS/Pages/CIP.aspx. **acesse aqui** Acesso pode exigir cadastro

6. O malware do futuro será lançado mais rapidamente do que as soluções de segurança, e continuarão ocorrendo extorsão, sequestro de dados e ataques de negação de serviço (DoS, DDoS). O relatório afirma não haver indicação de que as empresas médias estejam investindo em segurança. A falta de conscientização, a complacência e a falta de políticas efetivas contribuem para um cenário obscuro.

7. Visualização geoespacial com base no SIG (sistema de informação geográfica) permite identificar e mapear uma infraestrutura crítica de maneira muito detalhada e nem todos os profissionais de segurança estão cientes disso. Somente uma gestão de riscos permanente capacitará as organizações a terem níveis adequados de proteção.

Além do Critical Infrastructure Protection, a Asis Internacional publicou no ano de 2013 dois white papers de grande interesse para o setor elétrico. Um deles, de número 03, sob o título *Utility Security Risk Management – Security Program Fundamentals* [13], afirma que a geração e distribuição de utilities (serviços essenciais) demanda ambientes de alto risco, como barragens, usinas nucleares etc. Toda essa infraestrutura crítica é responsabilidade das companhias envolvidas e também dos governos. Para fazer frente a tal responsabilidade, são necessárias barreiras e controles de segurança de alta sofisticação, que abranjam uma grande gama de ameaças, inclusive fenômenos naturais. Quanto mais crítico for um ativo, segundo a Asis, menor deve ser o tempo de paralização previsto nos planos.

A expansão das utilities aumenta as ameaças e torna mais complexa a gestão do risco, pois novas tecnologias trazem também novas vulnerabilidades e novos vetores de ataque. Uma vez que os riscos não estão isolados e têm impacto em diferentes níveis das companhias, devem ser tratados em vários níveis, de forma cruzada (levando em consideração a possibilidade de um risco impulsionar ou ser impulsionado por outro risco) e por equipes com competências apropriadas.

A abordagem de gerenciamento de riscos na indústria de energia precisa ser muito mais abrangente do que tem sido. Deveria ser contemplada e aplicada a partir de uma perspectiva de governança, risco e conformidade (GRC). Da mesma forma que

13 O arquivo pode ser acessado neste endereço. Pode exigir cadastro: **acesse aqui** https://www.asisonline.org/About-ASIS/Pages/CIP.aspx .

a segurança se assenta no tripé pessoas, processos e tecnologia (PPT), o GRC não deveria ser dividido em partes independentes.

Uma infraestrutura crítica demanda proteção cibernética, proteção física e gestão de emergências.

O outro white paper da Asis Internacional, de número 05, recebeu o título de *Critical Infraestructure Protection – Security dependencies and trends*[14]. O documento define como infraestrutura crítica o conjunto de ativos, sistemas e networks, físicos ou virtuais, que são vitais à sociedade. Uma infraestrutura crítica demanda proteção cibernética, proteção física e gestão de emergências. As smart grids representam uma proliferação de tecnologias de operação. Demandam complexos sistemas de informação que incorporam muitos dos sistemas de comunicação púbicos e privados, além de tecnologias prontas (off-the-shelf), compondo os dados de network mais interconectados que a humanidade já viu – afirma a publicação. As smart grids podem, entretanto, ter conexão com estruturas pré-existentes obsoletas, como redes telefônicas e outros equipamentos pré-existentes à instalação da smart grid.

Para fazer frente a todos esses desafios, é preciso engajamento, inteligência, colaboração e participação abrangente. E com a participação vem conhecimento, tanto para saber para onde ir quanto para saber a quem perguntar a fim de obter mais conhecimento – conclui a matéria.

Atualmente, para gerenciar a segurança de forma efetiva, são necessários vários aplicativos, geralmente executados independentemente uns dos outros, com administradores separados. Em um modelo de segurança integrado, se considerarmos um centro de monitoramento de segurança para todos os sistemas físicos e cibernéticos (CFTV, acesso, rede SIEM etc.), com monitoramento dos sistemas de segurança, além dos requisitos tradicionais e aprimorados de monitoramento de segurança para uma smart grid ou equivalentes, parece improvável que exista qualquer tecnologia que possa combinar todos os sinais, todos os dados e todas as análises desses diversos sistemas para criar um centro de operações de rede eficiente para as empresas do setor elétrico.

14 O arquivo pode ser acessado neste endereço após cadastro: https://www.asisonline.org/About-ASIS/Pages/CIP.aspx. **acesse aqui**

Isso deixa a organização com o desafio de monitorar e avaliar eventos de segurança em toda a empresa e responder de forma efetiva, informando as partes interessadas de forma significativa quando ocorrer algum evento indesejado. O tempo de resposta, diante de um evento de segurança física, pode ser eficiente mesmo que leve alguns ou vários minutos. Já para os eventos de segurança lógica, o mesmo não ocorre. Fazer frente à necessidade de resposta imediata só será possível se houver processos bem definidos, além de equipe capacitada e permanentemente treinada.

Fórum Econômico Mundial – Genebra [15]

Outra peça de grande relevância em segurança, por sua profundidade e abrangência, é o relatório The Global Risks Report 2017 - 12th Edition, publicação da equipe denominada The Global Competitiveness and Risks Team, ligada ao Fórum Econômico Mundial. O documento destaca que estamos em plena Quarta Revolução Industrial, marcada pela convergência entre tecnologias digitais, biológicas e físicas, que traz novos riscos globais e exacerba riscos já existentes. Uma governança cuidadosa pode guiar tanto a distribuição de benefícios quanto o impacto de riscos globais. Afirma o relatório que toda essa evolução tecnológica deverá ser influenciada por normas sociais, políticas corporativas, padrões industriais e princípios regulatórios. Porém, as instituições legais, policiais e de regulação tendem a se mover mais lentamente do que a tecnologia.

Em relação aos sistemas de energia elétrica, seu papel cada vez mais central em várias áreas da vida vai exigindo mais pontos de abastecimento. Com isso, o sistema se aperfeiçoa ao mesmo tempo em que multiplica os aspectos vulneráveis, em diferentes redes de infraestrutura que se tornam mais interdependentes. Os riscos sistêmicos vêm, então, de diversas direções: ciberataques de larga escala, furto de dados, problemas técnicos em softwares, eventos naturais, ataques a estruturas físicas, fraudes, furtos de cabos e baterias, vandalismo etc. Os ataques terroristas de larga escala - quarto lugar na lista dos principais riscos em 2017 - e conflitos entre países, indicados no documento, que antes tinham pouca relevância no Brasil (historicamente não sofremos ataques, e não ocorreram ataques internacionais nas últimas décadas) agora ganha outra conotação, uma vez que a indústria de energia brasileira está sendo controlada por grandes grupos internacionais.

Atenção especial deve ser dada para o risco de ataques cibernéticos em larga escala, o relatório aponta esse risco como o sexto na lista de riscos mais susceptíveis de ocorrer nos próximos dez anos.

---

15 Disponível em http://www3.weforum.org/docs/GRR17_Report_web.pdf. **acesse aqui**
Acesso em agosto de 2017.

Capítulo 4

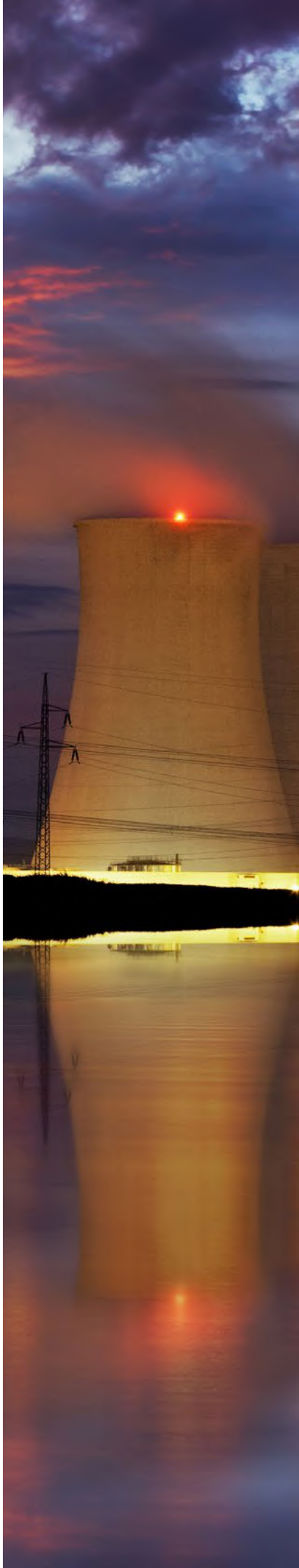
ESPANHA E ESTADOS UNIDOS – DUAS REFERÊNCIAS EM SEGURANÇA DE INFRAESTRUTURA CRÍTICA

Capítulo 4 ||| Espanha e Estados Unidos – duas referências em segurança de infraestrutura crítica

A longa tradição em cuidar da segurança patrimonial coloca dois países na posição de referência internacional na área. Neste capítulo, são abordados alguns aspectos da segurança ciberfísica na Espanha e nos Estados Unidos. Como grandes centros de desenvolvimento da segurança pública e privada, os dois têm muito a ensinar ao mercado brasileiro de segurança (ainda em amadurecimento) e, principalmente, às infraestruturas críticas de nosso país.

Espanha

A Espanha é um dos países com mais investimento em segurança. Em documento intitulado *Estrategia de Seguridad Energética Nacional* [16], publicado em 2015, o governo espanhol recomenda proteger as infraestruturas energéticas, especialmente as consideradas críticas, sob o ponto de vista da segurança integral, impulsionando e melhorando os canais e procedimentos de comunicação de incidentes para garantir e, quando necessário, restabelecer a continuidade do abastecimento. A publicação é enfática ao dizer que a cooperação da indústria energética com a cibersegurança só faz aumentar e requintar a detecção, prevenção, resposta e capacidade de recuperação (resiliência) da infraestrutura diante das ameaças. O documento destaca ser essencial fomentar uma cultura de segurança energética nacional nas gerações atuais e futuras, a partir da tomada de consciência, com inclusão do tema no sistema escolar desde as primeiras séries.



16 Disponível em http://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-energética-nacional. Acesso em setembro de 2017. acesse aqui

A segurança ciberfísica

O documento Estrategia de Seguridad Energética Nacional foi emitido pelo Departamento de Seguridad Nacional do governo da Espanha e atribui prioridade absoluta para a proteção dos sistemas de energia do país, pois entende que zelar pela proteção do patrimônio energético atual e futuro é zelar pelos demais interesses vitais do país.

Ganha destaque, no documento, uma visão integral para garantir proteção adequada das infraestruturas críticas frente às ameaças físicas e cibernéticas às suas instalações, suas redes, sistemas e equipamentos físicos e lógicos. São também destacadas as ameaças técnicas e físicas, além de sua mitigação. A visão integral da segurança é resumida, no documento, por uma figura mostrando o posicionamento da segurança ciberfísica das infraestruturas críticas e ilustrando como a segurança corporativa se posiciona dentro da estratégia nacional de defesa. A Figura 5 reproduz a ilustração do documento.

Figura 5 – Visão integral da segurança.
Reproduzido de Estrategia de Seguridad Energética Nacional.

O Estado espanhol assume um papel de copartícipe e orientador, tendo presença muito forte nessa estratégia, bem mais do que os Estados Unidos e o Brasil -- que quer assumir o controle, mas não tem demonstrado capacidade suficiente para tal.

O Sistema de Seguridad Nacional da Espanha é dirigido pelo primeiro ministro (presidente del gobierno), assessorado pelo Conselho de Segurança Nacional, no qual o Departamento de Segurança Nacional exerce as funções de secretaria técnica e órgão de trabalho permanente. O organograma a seguir (Figura 6) ilustra o relacionamento entre esses órgãos.

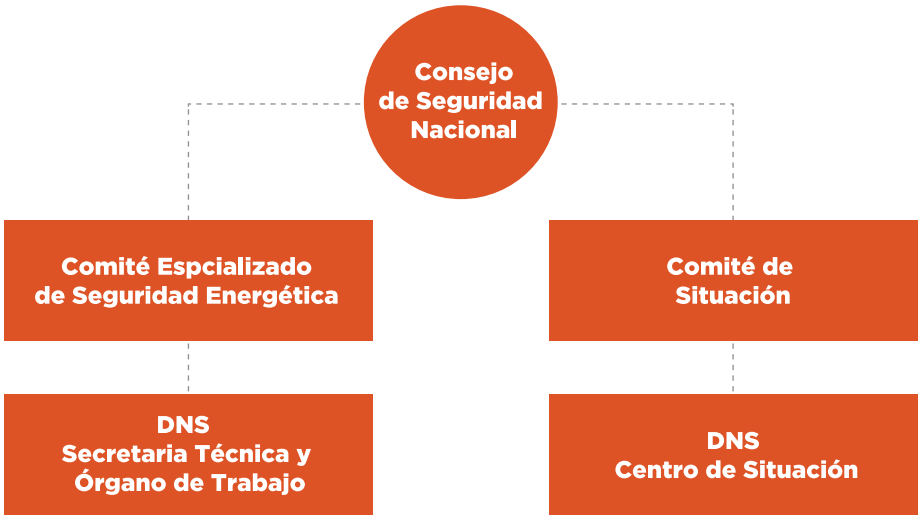


Figura 6 – Estrutura da segurança energética na Espanha. Reproduzido de Estrategia de Seguridad Energética Nacional.

Para encerrar, é espanhol um dos mais abrangentes projetos de segurança de centrais geradoras, subestações e torres elétricas. Trata-se do projeto *Pelgrin – Protetion of Electrical Grid Infraestructures*[17], em que as redes elétricas, tanto as torres como suas estações e subestações, são protegidas contra possíveis ataques terroristas e outras ameaças. O projeto compreende diferentes alarmes acionados por diferentes sensores, utilizando-se de câmeras instaladas nas torres e sensores sísmicos enterrados, entre outros. São cobertos mesmo equipamentos localizados em regiões de difícil acesso, sem sinal de comunicação e sem energia elétrica de baixa tensão.

17 Disponível em www.pelgrin.european-project.eu. Acesso em setembro de 2017. acesse aqui

Estados Unidos

São tratadas com muito rigor, nos Estados Unidos, as negligências das empresas quanto às medidas de segurança que visam a proteção de seus clientes contra os crimes e acidentes. Nas ações judiciais, os veredictos de casos de negligência em segurança podem envolver quantias substanciais. É levado muito a sério o dever que têm as empresas de serviços públicos de manter seus clientes e funcionários seguros nas instalações. A energia tem que chegar até os clientes, é dever de honra das concessionárias. Se houver um ato criminoso ou de vandalismo e um hospital ficar sem energia por um período significativo de tempo, os pacientes terão seus quadros piorados e alguns podem, inclusive, morrer em consequência da falta de energia elétrica. Um advogado competente da parte demandante, na fase de coleta de informações para o processo, poderá obter cópias de todas as avaliações de risco e medidas de segurança. Se ficar provado que a avaliação de risco estava inadequada ou desatualizada, a empresa será responsabilizada pelos danos. Além disso, no atual ambiente legal, nos Estados Unidos, mesmo os ataques terroristas são agora considerados previsíveis. Portanto, os gerentes de segurança redobram as atenções às questões de responsabilidade decorrentes de falhas nas avaliações de risco, e devem garantir que a empresa mitigue os riscos conforme indicado na sua avaliação de riscos e nos planos de segurança. Após o bombardeio do World Trade Center de 1993, por exemplo, houve mais de 175 ações judiciais separadas, 400 reivindicações de compensação e um veredicto de US $ 1,8 bilhão. Nesse caso, descobriu-se que, embora a avaliação de risco fosse adequada, a empresa não havia mitigado o risco da forma como afirmou que faria na avaliação. Uma das vulnerabilidades mencionadas na avaliação de risco foi que os World Trade Centers eram vulneráveis a uma bomba. Portanto, um ataque terrorista usando uma bomba foi considerado previsível e assim evitável.

Se ficar provado que a avaliação de risco estava inadequada ou desatualizada, a empresa será responsabilizada pelos danos.

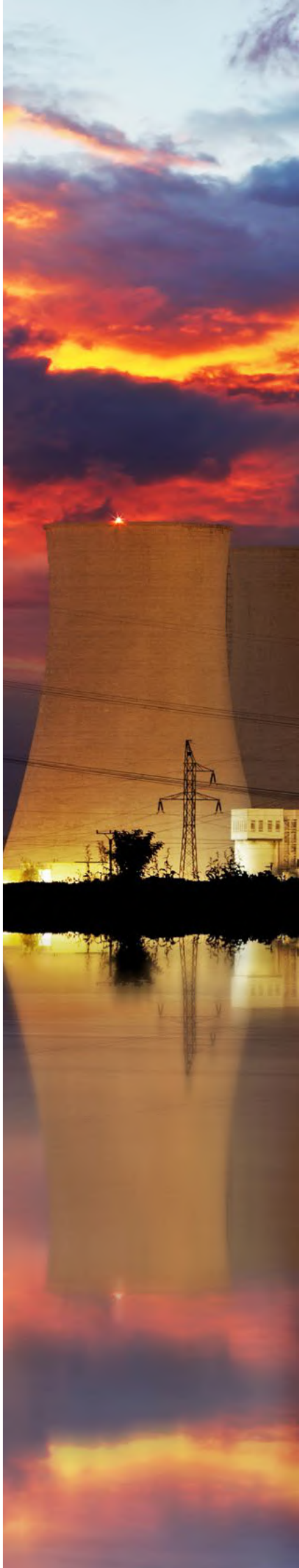
Um excelente estudo que serve de referência para o setor elétrico brasileiro é o *Review of Physical Security Protection of Utility Substations and Control Centers*[18], publicado em 2014 pelo *The Florida Public Service Commission Office of Auditing and Performance Analysis*. Em síntese, esse documento faz uma revisão das medidas

18 Disponível em http://www.psc.state.fl.us/Files/PDF/Publications/Reports/General/Electricgas/Physical_Security_2014.pdf. Acesso em setembro de 2017. acesse aqui

de segurança física que protegem as subestações de transmissão e distribuição, além dos centros de controle do sistema, nas quatro principais empresas de eletricidade da Flórida. Os ensinamentos que esse estudo pode trazer para as empresas de energia do Brasil estão relacionados a documentos, planos, procedimentos e política de segurança física das subestações e dos centros de controle.

Segundo o relatório já mencionado da Asis International, *Critical Infrastructure Protection: Security Dependencies and Trends*, o objetivo da área de proteção de infraestrutura crítica é "criar recursos para fortalecer e suportar a robustez, confiabilidade, resiliência e proteção de instalações, redes, serviços e recursos de tecnologia física e informática (TI), que, se interrompidos ou destruídos teriam um sério impacto na saúde, segurança, bem-estar econômico ou efetivo funcionamento da nação" (tradução livre).

E o relatório *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector* [19], publicado pelo Laboratório Nacional de Idaho em agosto de 2016, compila uma análise de fontes abertas de ameaças cibernéticas e riscos para a rede elétrica, melhores práticas para o setor, além de formas de prevenção e resposta a ameaças cibernéticas. Faz sugestões para o setor elétrico sobre como o governo federal pode auxiliar os serviços públicos na mitigação de riscos. Destaque-se que esse documento, embora tenha como foco o ataque cibernético, vê a segurança física como indissociável da segurança lógica: um criminoso pode acessar fisicamente uma subestação e implantar um malware diretamente em computadores e dispositivos. Além disso, relés de proteção podem ser manipulados e equipamentos, destruídos fisicamente.



19 Disponível em https://info.publicintelligence.net/INL-CyberThreatsElectricSector.pdf. Acesso em setembro de 2017. **acesse aqui**

Capítulo 5

SEGURANÇA DO SETOR ELÉTRICO NO BRASIL

Capítulo 5 ||| Segurança do Setor Elétrico no Brasil

Mais do que os sistemas elétricos tradicionais, as *smart grids* demandam uma gestão de riscos dinâmica, contínua e sustentável. No Brasil, esses sistemas com alto grau de automação e eficiência operacional estão configurando cada vez mais a distribuição e a transmissão de eletricidade. Estará o país preparado para os desafios de segurança que as redes inteligentes trazem?

Tem aumentado o número de multinacionais que estão assumindo a matriz energética brasileira e esse é mais um motivo para se aumentar a segurança, uma vez que traz riscos novos, inerentes aos países de origem das multinacionais que estão vindo para cá (ciber-ativistas; ciberterroristas; cibercriminosos daqueles países). É o que apontam os autores de *As oito grandes tendências de crescimento até 2020,* Giovanni Fiorentino, Lucas Brossi, Ivan Amelong e Ciro Campanatti em e-book disponibilizado no site da empresa Bain & Company[20].

A ampliação que se tem observado dos ramos de atividade explorados por organizações criminosas deverá continuar. É o que consideram Helder Rogério Sant'Ana Ferreira e Elaine Coutinho Marcial, autores do excelente livro *Violência e segurança pública em 2023* – cenários exploratórios e planejamento prospectivo.[21] Como o livro trata de cenários prospectivos da segurança pública no Brasil até 2023, vem ratificar os relatórios da AON e o do Fórum Mundial sobre riscos no setor de energia e mostra perspectivas ainda mais graves. Esses riscos estão no mundo físico e não no cibernético, as concessionárias já enfrentam fraudes físicas, como o furto "formiguinha" que, apesar de apresentar valores individuais pequenos, na soma causam grande prejuízo. No Brasil, as facções criminosas estão aumentando cada vez mais sua intenção e suas tentativas de ataque ao setor elétrico. Em nossa visão, as organizações criminosas no Brasil, embora tenham

20 Disponível em http://www.bain.com/offices/saopaulo/pt/Images/The_great_eight_POR.PDF Acesso em setembro de 2017. acesse aqui

21 Publicado pelo Ipea, RJ, em 2015. Disponível em http://www.ipea.gov.br/portal/index.php?option=com_content&view=article&id=26752&catid=345&Itemid=383. acesse aqui

limitada capacidade técnica hoje, estão investindo fortemente contra o nosso setor financeiro, que está se protegendo muito bem, chegando a figurar entre os mais protegidos do mundo. Como as organizações criminosas buscam sempre uma excelente relação de custo versus benefício, pode-se deduzir que as demais infraestruturas críticas serão atacadas com mais ênfase nos próximos anos, sobretudo o setor elétrico.

A proteção de infraestruturas críticas entrou em pauta no Brasil em 2006, no GSI (Gabinete de Segurança Nacional).

Já em uma monografia de título *Segurança das infraestruturas críticas de óleo e gás no Brasil: proposta para um programa de Estado*[22], o capitão (na época) Fábio Evangelho de Araújo afirma que a proteção de infraestruturas críticas entrou em pauta no Brasil em 2006, no GSI (Gabinete de Segurança Nacional). Em maio de 2007, relata o autor, o Movimento dos Atingidos por Barragem (MAB) invadiu a usina de Tucuruí (PA), da Eletronorte. Esse fato patenteou a importância da gestão de riscos para as infraestruturas críticas. Os manifestantes obtiveram detalhes das vulnerabilidades da usina durante visita turística à hidrelétrica, "ocasião em que se permitia o acesso de pessoas a locais que deveriam ser negados a visitantes devido à sensibilidade", destaca o autor.

Com um parque de infraestruturas críticas de dimensões continentais, o Brasil se beneficiaria mais da gestão de riscos realizada pelas empresas concessionárias se fossem feitas abordagens de forma integral, sistemática e seguindo métodos compatíveis com a complexidade das atividades da organização. Existem ações significativas no âmbito governamental, porém esses projetos importantes de segurança ciberfísica ainda estão se estabelecendo.

Além dos sistemas de segurança próprios das concessionárias, está em implantação, liderado pelo Exército Brasileiro, o sistema Proteger - Sistema Integrado de Proteção de Estruturas Estratégicas Terrestres. As etapas de implantação começaram em 2012 com previsão de dez anos para a implantação completa. Quando isso acontecer, o sistema terá, entre outros, o objetivo de cobrir hidrelétricas, refinarias de petróleo, termoelétricas, usinas nucleares, portos, aeroportos, ferrovias, linhas de transmissão

22 Monografia apresentada ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do diploma do Curso de Altos Estudos de Política e Estratégia, RJ, 2016. Disponível em http://www.esg.br/images/Monografias/2016/ARAÚJO.pdf. Acesso em setembro de 2017. **acesse aqui**

de energia e telecomunicações, reunindo aproximadamente 664 estruturas, um terço das quais pertencentes ao setor elétrico.

Iniciativa semelhante foi divulgada em um documento de orientação publicado pelo governo dos Estados Unidos, ainda em 2003. Trata-se do *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection.*[23] Essas diretrizes estabeleceram uma política nacional para os departamentos federais e agências dedicados a identificar e priorizar a infraestrutura crítica do país e recursos-chave, com o objetivo de protegê-los contra ataques terroristas. Pouco tempo depois, em 2006, o Department of Homeland Security lançou o plano *National Infrastructure Protection Plan.*[24] O documento salienta ser vital a habilidade de proteger a infraestrutura crítica e recursos-chave para assegurar que as missões governamentais, serviços públicos e funções econômicas sejam mantidos no evento de ataque terrorista, desastre natural, ou outro tipo de incidente e que essas estruturas não sejam utilizadas como armas de destruição em massa contra o povo e instituições do país.

Todas essas políticas indicam os papéis que as agências federais, estaduais e locais devem desempenhar.

Documento intitulado *Segurança das Infraestruturas Críticas*[25], assinado pelo coronel do Exército Fernando Antonio Demeterco, do Gabinete de Segurança Institucional (GSI) da Presidência da República, na gestão de Dilma Rousseff, afirma que, devido às dimensões do país, o desafio de proteger suas infraestruturas críticas é enorme. O documento sugere que sejam feitas parcerias público-privadas (PPP).[26]

As PPPs seriam de grande interesse na proteção de infraestruturas críticas em nosso país, uma vez que os governos carecem de verba para implantar e manter projetos de segurança com a sofisticação que elas demandam. Além disso, as empresas de energia (e demais de infraestrutura crítica) não têm know-how nem recursos para desenvolver uma estrutura de proteção em âmbito de Estado a fim de preservarem a si próprias.

---

23 Disponível em https://www.dhs.gov/homeland-security-presidential-directive-7. Acesso em setembro de 2017. acesse aqui

24 Disponível em https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf. Acesso em setembro de 2017. acesse aqui

25 Disponível em http://portal.eceme.ensino.eb.br/meiramattos/index.php/RMM/article/view/197/166. Acesso em setembro de 2017. acesse aqui

26 Parceria público-privada (PPP) é um contrato de prestação de obras ou de serviços firmado entre uma empresa privada e o governo federal, estadual ou municipal. O valor mínimo do contrato é R$ 20 milhões, e a duração varia entre 5 e 35 anos.

Um exemplo bem-sucedido de PPP nesse setor, acrescente-se, é o projeto InfraGard [27], nos Estados Unidos. Essa organização desempenha papel em parte como "uma parceria entre o FBI e o setor privado. A InfraGard é uma associação de empresas, instituições acadêmicas, agências estatais e locais de aplicação da lei e outros participantes dedicados a compartilhar informação e inteligência para prevenir atos hostis contra os Estados Unidos" (tradução livre). No Brasil, o projeto Proteger do Exército, já citado, poderia ter esse nível de abrangência.

Perfil do Profissional

Em linhas gerais, as grandes organizações costumam ter três níveis hierárquicos: alta administração, gerência e operação. Cada nível tem visão estratégica e visão operacional em proporções diferentes. No primeiro nível, a visão estratégica predomina sobre a operacional -- quantificando, seria aproximadamente visão 80% estratégica e 20% operacional.

Na camada operacional (comumente denominada chão de fábrica), essa proporção se inverte. Um pouco de visão estratégica é sempre bem-vinda, mesmo para a função mais operacional da estrutura, uma vez que dá ao colaborador a confiança de saber como o seu trabalho contribui para a organização.

No nível médio, o equilíbrio entre as duas visões permite aos gerentes darem apoio técnico e operacional ao nível superior, ao mesmo tempo em que orientam e conduzem o nível abaixo dele.

Um diretor de segurança não esquece o conhecimento operacional, adquirido ao longo da carreira. Ele sabe, por exemplo, que se faz necessário configurar uma câmera que esteja fora de foco. Em vez de fazer isso, entretanto, ele dialoga com os níveis correspondentes, sempre atento às questões estratégicas em que o problema do equipamento se insere.

Como ele lida com atores de competências as mais diversas, nos três níveis hierárquicos, em diferentes áreas da organização, necessita de flexibilidade para se adaptar a diferentes situações e obter soluções compartilhadas.

---

27 Disponível em https://www.infragard.org. Acesso mediante cadastro. acesse aqui

Cada vez mais, a demanda por gestão integrada de riscos de diferentes origens (físicos, lógicos, financeiros, operacionais e outros) obriga o diretor de segurança a conciliar diferentes habilidades e ter uma visão holística da empresa. Acompanhar política, finanças e outros domínios também é recomendado. Ele precisa entender os interesses dos agentes internos e externos e construir bom relacionamento com todos eles. Nas infraestruturas críticas, entre os agentes externos se destacam o entorno (sociedade), órgãos regulatórios e fiscalizadores, fornecedores, ONGs etc.

O executivo de segurança precisa, também, acompanhar seus pares no mercado e estar constantemente atualizado sobre o que acontece na área de segurança, participando de associações de classe e outras entidades. Se, por acaso, estiver para entrar em circuito comercial algum equipamento de última geração, o executivo de segurança terá de orientar a empresa sobre possíveis riscos associados à sua compra e implantação e, ainda, sobre as formas de proteção que o novo equipamento irá exigir. É sua atribuição entender como um novo equipamento ou serviço pode criar novos riscos e potencializar ou minimizar riscos já existentes.

Ele tem obrigação de manter seu radar operando em todas as direções ao mesmo tempo, de maneira global, e ter visão ampla para antever problemas que podem surgir no horizonte. Sem isso, não consegue cumprir seu papel de manter a organização protegida e resiliente.

Uma das habilidades requeridas do executivo de segurança é saber motivar e liderar, além de inspirar a interconectividade dentro da organização. Estruturar equipes eficientes, com complementaridade de competências e alto desempenho é um de seus objetivos.

Foi visto neste trabalho que o relatório *Global Risk Management Survey* aponta entre os dez riscos mais importantes a falha em atrair e manter talentos. Esse é um problema concreto no Brasil que somado ao fato de existirem poucos executivos de segurança com visão abrangente, cria um cenário preocupante. Os rápidos avanços tecnológicos da última década não foram acompanhados pelo surgimento de novos cursos, ou de novos currículos em cursos já existentes. Ter uma visão abrangente da segurança não é simples e não está sendo treinado nas escolas. Isso se reflete no mercado.[28]

---

28 Esse e outros assuntos relacionados ao perfil de profissionais de segurança são abordados em detalhes no paper Panorama da Segurança Empresarial, de Tácito Leite. Disponível em https:// www.linkedin.com/pulse/panorama-da-segurança-empresarial-brasil-o-futuro-e-tácito/. Acesso em setembro de 2017. **acesse aqui**

Essa questão das competências do executivo de segurança é esmiuçada também no ótimo relatório publicado pela Asis Foundation em parceria com a University of Phoenix, em 2014, denominado *Security Industry Survey of Risks and Professional Competencies.* [10] O documento é resultado de mesas redondas sobre segurança realizadas no ano anterior pela University of Phoenix, com a participação de executivos e acadêmicos. Entre os maiores desafios do mercado, o relatório cita: limitação de recursos; segmentação da indústria; envelhecimento da força de trabalho; e falta de educação estandardizada e de certificações. E, na lista de competências essenciais de um executivo de segurança, o documento destaca: tomada de decisão, comunicação oral, pensamento crítico, maximização da performance de outros e capacidade de influenciar.

Competências essenciais de um executivo de segurança: tomada de decisão, comunicação oral, pensamento crítico, maximização da performance de outros e capacidade de influenciar.

A carreira em segurança patrimonial, até pouco tempo, estava centrada em competências ligadas à segurança física. Agora, entretanto, as competências precisam ir muito além, especialmente em infraestruturas críticas, como é o setor de energia elétrica. Em futuro próximo, será comum que um único gestor administre toda a segurança corporativa por meio da gestão integrada dos riscos. Alguns profissionais, por necessidade da demanda, estão ampliando os limites desse mercado de trabalho.

29 Disponível em https://foundation.asisonline.org/FoundationResearch/Research/Current-Research-Projects/Documents/UOPX-ASIS_Security%20report_WEB.pdf. Acesso em setembro de 2017. acesse aqui

Conclusão

Neste trabalho, comentamos o conteúdo de relatórios importantes em segurança de infraestruturas críticas, publicados após pesquisas de amplo espectro. Com eles, pudemos ter uma visão geral do cenário da segurança no mundo e no Brasil. Muito há para ser feito a fim de que o futuro seja mais promissor, a fim de que a segurança das infraestruturas críticas atenda às suas necessidades de proteção e resiliência.

O grande e veloz desenvolvimento de novas tecnologias traz novas vulnerabilidades e novos riscos. Em todo o mundo, as instituições responsáveis tendem a criar planos de gestão de riscos mais lentamente do que o exigido pela velocidade da criação de novas tecnologias. E foi relatado que a América Latina é a região menos preparada para fazer frente aos desafios atuais em segurança.

Na área de energia elétrica, as redes inteligentes já são uma realidade no Brasil, com um nível de automação sem precedentes. São necessários planos integrados de segurança ciberfísica que deem conta de todos os desafios da segurança. Os governos têm tomado iniciativas de proteção que deixam a descoberto muitos riscos atuais e futuros. De sua parte, as empresas, em geral, não estão amadurecidas na gestão de riscos integrados, não têm consciência da importância estratégica de suas áreas de segurança e as relegam ao nível gerencial e operacional, quando deveriam elevá-las ao nível estratégico.

Diante disso tudo, criam-se novos desafios e novas oportunidades na proteção das infraestruturas críticas do setor elétrico brasileiro, tanto para as organizações quanto para os profissionais do setor.

REFERÊNCIAS

Referências

As oito grandes tendências de crescimento até 2020. Giovanni Fiorentino, Lucas Brossi, Ivan Amelong e Ciro Campanatti. Bain & Company, 2012.
http://www.bain.com/offices/saopaulo/pt/Images/The_great_eight_POR.PDF Acesso em setembro de 2017 acesse aqui

Caso de Estudio: Hackeo de la Red de Distribución Eléctrica en la zona oeste de Ukrania el pasado 23 de Diciembre de 2015. WisePlan.
http://wiseplant.com/2016/03/27/analisis-del-hackeo-de-la-red-electrica-de-ukrania-el-pasado-23-de-diciembre-de-2015
Acesso em setembro de 2017. acesse aqui

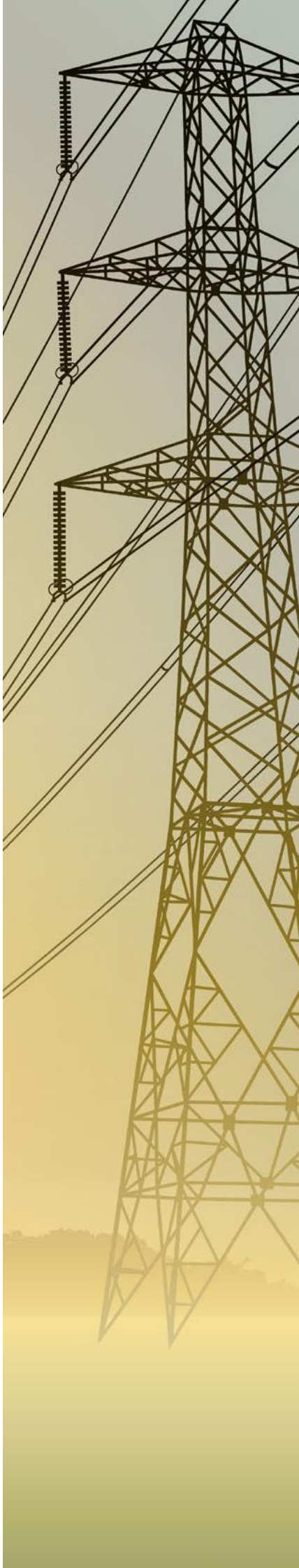
Critical Infraestructure Protection – Security dependencies and trends. Asis Internacional, 2013.
https://www.asisonline.org/About-ASIS/Pages/CIP.aspx acesse aqui

Critical Infrastructure Protection: Security Dependencies and Trends. Asis International, 2013.
https://www.asisonline.org/About-ASIS/Pages/CIP.aspx
Acesso em agosto de 2017. acesse aqui

Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector. Laboratório Nacional de Idaho, 2016.
https://info.publicintelligence.net/INL-CyberThreatsElectricSector.pdf
Acesso em setembro de 2017. acesse aqui

Estrategia de Seguridad Energética Nacional. Departamento de Seguridad Nacional do governo da Espanha.
http://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-energética-nacional
Acesso em setembro de 2017. acesse aqui

Gestão de riscos na segurança patrimonial. Tácito Leite. Editora Qualitymark, 2016.
http://consultoriadeseguranca.com.br/
Acesso em agosto de 2017. acesse aqui



Global Risk Management Survey. Seguradora Aon, 2017.
http://www.aon.com/2017-global-risk-management-survey/
Acesso em setembro de 2017. acesse aqui

Guidelines for Smart Grid Cybersecurity (NISTIR 7628 Revision 1), Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements. Elaborado pelo National Institute of Standards and Technology, EUA.
http://dx.doi.org/10.6028/NIST.IR.7628r1
Acesso em setembro de 2017. acesse aqui

Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection. United States Department of Homeland Security, 2003.
https://www.dhs.gov/homeland-security-presidential-directive-7
Acesso em setembro de 2017. acesse aqui

InfraGard Project
Disponível em https://www.infragard.org
Acesso mediante cadastro. acesse aqui

National Infrastructure Protection Plan. United States Department of Homeland Security, 2006.
https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf
Acesso em setembro de 2017. acesse aqui

Norma ABNT NBR ISO 31000.
http://www.abntcatalogo.com.br/curs.aspx?ID=30
Acesso em setembro de 2017. acesse aqui

Panorama da Segurança Empresarial, de Tácito Leite.
https://www.linkedin.com/pulse/panorama-da-segurança-empresarial-brasil-o-futuro-e-tácito/
Acesso em setembro de 2017. acesse aqui

Pelgrin – Protetion of Electrical Grid Infraestructures.
www.pelgrin.european-project.eu acesse aqui
www.indracompany.com/en/indra/pelgrin-protection-electrical-grid-infrastructures
Acesso em setembro de 2017. acesse aqui

Review of Physical Security Protection of Utility Substations and Control Centers. The Florida Public Service Commission Office of Auditing and Performance Analysis, 2014. http://www.psc.state.fl.us/Files/PDF/Publications/Reports/General/Electricgas/Physical_Security_2014.pdf acesse aqui
Acesso em setembro de 2017.

Security Industry Survey of Risks and Professional Competencies.
Asis Foundation, 2014.
https://foundation.asisonline.org/FoundationResearch/Research/Current-Research-Projects/Documents/UOPX-ASIS_Security%20report_WEB.pdf
Acesso em setembro de 2017. acesse aqui

Segurança das infraestruturas críticas de óleo e gás no Brasil: proposta para um programa de Estado. Fábio Evangelho de Araújo. Monografia apresentada ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do diploma do Curso de Altos Estudos de Política e Estratégia, RJ, 2016.
http://www.esg.br/images/Monografias/2016/ARAÚJO.pdf
Acesso em setembro de 2017 acesse aqui

Segurança das Infraestruturas Críticas. Fernando Antonio Demeterco.
http://portal.eceme.ensino.eb.br/meiramattos/index.php/RMM/article/view/197/166.
Acesso em setembro de 2017. acesse aqui

Tecnologia torna mais inteligentes e seguras as infraestruturas elétricas. Tácito Leite. Revista Smart Energy set/outubro 2013 p. 42-43
http://pt.calameo.com/read/002590700830a78e574d9 acesse aqui

The cost of incidents affecting CIIs. European Union Agency For Network And Information Security.
https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis
Acesso em setembro de 2017. acesse aqui

The Global Risks Report 2017 - 12th Edition. The Global Competitiveness and Risks Team, Fórum Econômico Mundial, Genebra.
http://www3.weforum.org/docs/GRR17_Report_web.pdf
Acesso em agosto de 2017. acesse aqui

The Power of Physical Security. Megan Gates.
https://sm.asisonline.org/Pages/The-Power-of-Physical-Security.aspx.
Acesso em setembro de 2017. acesse aqui

Utility Security Risk Management – Security Program Fundamentals.
Asis Internacional, 2013.
https://www.asisonline.org/About-ASIS/Pages/CIP.aspx acesse aqui

Violência e segurança pública em 2023 – cenários exploratórios e planejamento prospectivo. Helder Rogério Sant'Ana Ferreira e Elaine Coutinho Marcial. Publicado pelo Ipea, RJ, em 2015.
http://www.ipea.gov.br/portal/index.php?option=com_content&view=article&id=26752&catid=345&Itemid=383 acesse aqui

Sobre o Autor

TÁCITO AUGUSTO SILVA LEITE
DSE, ASE, C31000

Executivo com 23 anos de experiência no mercado de segurança corporativa, gestão de riscos em empresas nacionais e multinacionais, atuação em associação de classe e organização militar. Habituado a conciliar visão de negócio e resolução de problemas complexos de segurança corporativa, foi diretor de segurança física & informação. Autor do livro **Gestão de Riscos na Segurança Patrimonial, Editora Qualitymark**. Recebeu os prêmios Profissional de Segurança do Ano (Município de São Paulo, 2010) e Top 50 Most Influential People in Security (IFSEC 2017).

Certificação internacional DSE (director de seguridad empresarial), Universidad Pontificia Comillas, Madrid; certificação internacional C31000 de gestão de riscos, Global Institute for Risk Management, Suíça; certificação nacional ASE (analista de segurança empresarial), Associação Brasileira dos Profissionais de Segurança & Associação dos Diplomados da Escola Superior de Guerra, Brasil.

MBAs em Gestão Estratégica de Segurança Empresarial (Anhembi-Morumbi) e Gestão Avançada de Empresas, com especialização em Segurança da Informação (Universidade Potiguar), pós-graduações em Direção de Segurança em Empresas (Universidad Pontificia Comillas – Madri) e Gestão de Recursos de Defesa (Escola Superior de Guerra). É licenciado e bacharel em História – UFRN e fez curso sobre Terrorismo e Contraterrorismo – Universiteit Leiden, Holanda.

Criador e mantenedor da **Biblioteca de Segurança** e da plataforma **t-Risk**, que disponibiliza seu método de avaliação de riscos **Total Risk**.

www.linkedin.com/in/tacitoleite

www.lattes.cnpq.br/6763601233758573

SEGURANÇA CIBERFÍSICA NAS EMPRESAS DE ENERGIA

Tácito Augusto Silva Leite, DSE, ASE, C31000