ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO

ESCOLA MARECHAL CASTELLO BRANCO

ANDRÉ LUIZ NERY DE SÁ

SEGURANÇA CIBERNÉTICA DE USINAS NUCLEARES: UMA ANÁLISE SOBRE MEDIDAS DE MITIGAÇÃO DE ATAQUES DE ENGENHARIA SOCIAL NA CENTRAL NUCLEAR ALMIRANTE ÁLVARO ALBERTO

Rio de Janeiro

2020

André Luiz Nery de Sá

SEGURANÇA CIBERNÉTICA DE USINAS NUCLEARES: UMA ANÁLISE SOBRE MEDIDAS DE MITIGAÇÃO DE ATAQUES DE ENGENHARIA SOCIAL NA CENTRAL NUCLEAR ALMIRANTE ÁLVARO ALBERTO

Texto apresentado como Dissertação de Mestrado do Programa de Pós-Graduação em Ciências Militares do Instituto Meira Mattos da Escola de Comando e Estado-Maior do Exército, como requisito para a obtenção do título de Mestre em Ciências Militares

Orientador: Prof. Dr. RUBENS DE SIQUEIRA DUARTE

Rio de Janeiro
2020

S111s Sá, André Luiz Nery de

Segurança Cibernética de Usinas Nucleares: uma Análise sobre Medidas de Mitigação de Ataques de Engenharia Social na Central Nuclear Almirante Álvaro Alberto. / André Luiz Nery de Sá. —2020.
109 f. : il. ; 30 cm.

Orientação: Rubens de Siqueira Duarte.
Dissertação (Mestrado em Ciências Militares) — Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2020.
Bibliografia: f. 96-106

1. SEGURANÇA CIBERNÉTICA. 2. ENGENHARIA SOCIAL. 3. USINAS NUCLEARES BRASILEIRAS. I. Título.

CDD 352.38

ANDRÉ LUIZ NERY DE SÁ

SEGURANÇA CIBERNÉTICA DE USINAS NUCLEARES: UMA ANÁLISE SOBRE MEDIDAS DE MITIGAÇÃO DE ATAQUES DE ENGENHARIA SOCIAL NA CENTRAL NUCLEAR ALMIRANTE ÁLVARO ALBERTO

Dissertação apresentada à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Mestre em Ciências Militares.

Aprovada em 14 de outubro de 2020.

BANCA EXAMINADORA

RUBENS DE SIQUEIRA DUARTE – Prof Dr – Presidente
Escola de Comando e Estado-Maior do Exército

LUIZ ROGÉRIO FRANCO GOLDONI – Prof Dr – Membro
Escola de Comando e Estado-Maior do Exército

HENRIQUE DE SOUZA ROCHA – Prof Dr – Membro
Universidade da Força Aérea

Ciente

ANDRÉ LUIZ NERY DE SÁ – Postulante
Escola de Comando e Estado-Maior do Exército

À Ciência

AGRADECIMENTOS

Aos meus pais, pelo apoio incondicional ao longo da trajetória, sem os quais minha existência nesse mundo seria apenas uma abstração.

À Juliana, por sua força interior, que a faz vencer as intempéries da vida, o que reflete em amor e companheirismo ao longo desses anos.

Ao meu orientador, pela dedicação e paciência; por acreditar que posso melhorar a cada passo; por constantemente me dar o Norte, mesmo sabendo das dificuldades de orientar alguém natural de uma área tão díspar.

Aos amigos, que não retiram as pedras do caminho, pois elas são importantes, mas que me ajudam a ultrapassá-las.

Ao Departamento de Pesquisa e Pós-Graduação em Ciências Militares/Instituto Meira Mattos da Escola de Comando e Estado-Maior do Exército, na figura de seu chefe, Coronel De Franciscis, aos professores e colegas da ECEME, pela oportunidade, incentivo e amizade.

Aos professores Luiz Rogério Franco Goldoni (ECEME) e Henrique de Souza Rocha (UNIFA), da banca de qualificação, pelas importantes contribuições.

A todos que olham para o céu noturno pontilhado de estrelas e percebem que podem fazer algo mais do que simplesmente existir.

A essa pequena esfera, essencialmente azul, pairando no entorno de uma estrela qualquer dentre as infinitas existentes, que teve a ousadia de desafiar as probabilidades e que hoje cultiva toda sorte de vida.

“Constroem baixo demais aqueles que constroem abaixo das estrelas” - Edward Young

RESUMO

Esta pesquisa tem por objetivo analisar de que modo as medidas de segurança cibernética adotadas pela Central Nuclear Almirante Álvaro Alberto (CNAAA) podem mitigar ataques de engenharia social direcionados aos seus funcionários. Visto que a engenharia social explora a dimensão humana, observa-se que apenas medidas de segurança de ordem técnica não são suficientes para assegurar a proteção das instalações nucleares. A fim de burlar camadas tecnológicas de proteção e explorar vulnerabilidades, a engenharia social tem sido utilizada para apoiar ataques cibernéticos em ambientes nucleares. Nesse contexto, torna-se relevante que sejam adotados procedimentos que contemplem o uso de normas, auditorias periódicas, programas de conscientização e de capacitação para os funcionários e prestadores de serviço. Sustenta-se a hipótese de que as medidas de segurança cibernética adotadas pela CNAAA são adequadas para a mitigação de ataques de engenharia social. Para verificar essa hipótese, adotou-se a metodologia de estudo de caso, utilizando-se entrevistas com profissionais dos setores nuclear e cibernético, pesquisa na literatura especializada e consulta à Eletronuclear por meio da Lei de Acesso à Informação. A fim de prover base para reflexões analíticas para explorar o caso brasileiro, realizou-se estudo sobre ataques de engenharia social em instalações nucleares de outros países em desenvolvimento. Conclui-se que a CNAAA adota diversas medidas de segurança cibernética adequadas para mitigar ataques de engenharia social.

Palavras-chave: Segurança Cibernética; Engenharia Social; Usinas Nucleares Brasileiras.

ABSTRACT

This research aims to analyze how the cyber security measures adopted by the Central Nuclear Almirante Álvaro Alberto (CNAAA) can mitigate social engineering attacks targeted at its employees. Since social engineering explores the human dimension, one can observe that only technical security measures are not sufficient to ensure the protection of nuclear facilities. To circumvent technological layers of protection and exploit vulnerabilities, social engineering has been used to support cyber attacks on nuclear environments. In this context, it is relevant to adopt procedures that contemplate the use of standards, periodic audits, awareness and training programs for employees and service providers. The hypothesis sustained is that the cyber security measures adopted by CNAAA are adequate to mitigate social engineering attacks. To verify the hypothesis, the case study methodology was adopted, using interviews with professionals from the nuclear and cyber sectors, research in the specialized literature and consultation with Eletronuclear through the Access to Information Law. In order to provide a basis for analytical reflections to explore the Brazilian case, a study was conducted on social engineering attacks on nuclear facilities in other developing countries. It is concluded that the CNAAA adopts several cyber security measures appropriate to mitigate social engineering attacks.

Keywords: Cybersecurity; Social Engineering; Brazilian Nuclear Power Plants.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

AIEA	Agência Internacional de Energia Atômica
CERT-BR	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança do Brasil
CNAAA	Central Nuclear Almirante Álvaro Alberto
CNEN	Comissão Nacional de Energia Nuclear
DSIC	Departamento de Segurança da Informação e Comunicações
END	Estratégia Nacional de Defesa
e-SIC	Sistema Eletrônico do Serviço de Informações ao Cidadão
GSI-PR	Gabinete de Segurança Institucional da Presidência da República
IAEA	International Atomic Energy Agency
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IEEE	Institute of Electronics and Electronics Engineers
ISO	International Organization for Standardization
ITU	International Telecommunication Union
LAI	Lei de Acesso à Informação
LBDN	Livro Branco de Defesa Nacional
NEI	Nuclear Energy Institute
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
NTI	Nuclear Threat Initiative
PMBOK	Project Management Body of Knowledge
PMI	Project Management Institute
PND	Política Nacional de Defesa
RAT	Remote Administration Tool
SCADA	Supervisory Control and Data Acquisition
SICI	Segurança das Infraestruturas Críticas da Informação
SMS	Short Message Service
TIC	Tecnologia da Informação e Comunicações
USB	Universal Serial Bus
WANO	World Association of Nuclear Operators
WINS	Institute for Nuclear Security

SUMÁRIO

INTRODUÇÃO

De que modo as medidas de segurança cibernética adotadas pela Central Nuclear Almirante Álvaro Alberto podem mitigar ataques de engenharia social direcionados aos seus funcionários? Ao longo dos anos, a evolução do setor nuclear promoveu o uso de dispositivos digitais para controle e monitoração do ambiente operacional, em complemento ou substituição aos dispositivos analógicos existentes. Mesmo nas usinas com controles predominantemente analógicos, recursos de informática estão atualmente presentes nas áreas de engenharia e recursos humanos, que armazenam dados sensíveis das usinas. Como consequência da adoção de tecnologias digitais, essas instalações se tornaram suscetíveis a vulnerabilidades presentes no ambiente cibernético. Nesse contexto, os funcionários que operam dispositivos digitais podem ser vítimas de ataques de engenharia social, o que eventualmente pode comprometer a segurança do ambiente nuclear.

A segurança cibernética está estreitamente relacionada com a dimensão humana. Em última análise, são os indivíduos que desenvolvem, criam e utilizam a tecnologia dentro do ambiente de trabalho. São eles que interagem com os recursos tecnológicos e são passiveis de erros, percepções equivocadas e manipulações externas, capazes de aumentar o risco de incidentes no ambiente corporativo. Ataques de engenharia social se aproveitam de características da natureza humana e de reações emocionais para burlar as camadas de segurança. Por esse motivo, revela-se importante a adoção de métodos para mitigação de ataques de engenharia social. Nos próximos capítulos será percorrida uma trilha de conhecimento que inclui a compreensão de temas de âmbito técnico, normativo e de recursos humanos, relevantes para o desenvolvimento desta dissertação. Apesar de as análises contidas nesta pesquisa serem orientadas à Central Nuclear Almirante Álvaro Alberto (CNAAA), o estudo pode ser aplicado a outras infraestruturas críticas.

O trabalho inicia com um breve panorama sobre a operação de uma usina nuclear, onde são observados os processos de monitoração e controle existentes. Avança-se para o entendimento sobre a engenharia social e os mecanismos psicológicos por ela empregados, assim como as possíveis consequências de seu uso em usinas nucleares. Com base em entrevistas e análises da literatura, serão

identificados procedimentos de segurança cibernética que podem ser usados para a mitigação de ataques de engenharia social. Com a análise desenvolvida será verificada a hipótese de que as medidas de segurança cibernética adotadas pela CNAAA são adequadas para a mitigação de ataques de engenharia social.

Por ser um tema escasso em pesquisas acadêmicas no Brasil, estudos sobre a interação entre os setores cibernético e nuclear têm importância direta na proteção das usinas nucleares nacionais. Nesse sentido, o uso de medidas de segurança cibernética pode auxiliar a CNAAA na proteção de seus funcionários contra ações de engenharia social e, por conseguinte, assegurar a salvaguarda de suas operações. A partir da pesquisa, observa-se que a Central Nuclear Almirante Álvaro Alberto adota procedimentos técnicos, capacitação, campanhas de conscientização, referencial normativo e auditoria periódica, adequados para a mitigação de ataques de engenharia social.

OBJETIVOS

Este estudo parte da premissa de que os funcionários da CNAAA podem ser alvo de ataques de engenharia social. Além disso, considera-se que a Central Nuclear emprega medidas de segurança cibernética em seus ambientes operacional e administrativo. Nessa linha, o objetivo central deste trabalho consiste em verificar como as medidas de segurança cibernética adotadas na CNAAA podem mitigar ataques de engenharia social direcionados aos seus funcionários.

Em vista de atingir esse objetivo, etapas prévias devem ser cumpridas. Primeiramente, a partir da literatura, obtém-se o histórico de incidentes de segurança relacionados à engenharia social no mundo, permitindo a análise das possíveis consequências que incidentes dessa natureza podem ocasionar. O segundo objetivo específico trata sobre a identificação de normas, orientações e boas práticas de mercado para a mitigação de ataques de engenharia social, apontadas na literatura e por especialistas. Por fim, o terceiro objetivo específico aborda os procedimentos de segurança cibernética adotados na CNAAA. A gama de informações coletada servirá como subsídio para a verificação da hipótese formulada nesta dissertação.

JUSTIFICATIVA: CONTRIBUIÇÕES PARA A LITERATURA CIENTÍFICA E INCIDÊNCIA POLÍTICA

As ameaças cibernéticas perpassam por todas as atividades da sociedade, e podem afetar as esferas social, política, econômica e militar (NUNES, 2015). No mundo moderno, a maior parte das organizações utiliza o espaço cibernético, seja para comunicação com clientes e fornecedores, seja para otimizar seus processos administrativos e operacionais. Conforme afirma Nunes (2015), “a construção de um futuro digital passa inevitavelmente por assumir o espaço cibernético como um novo domínio estratégico” (NUNES, 2015, p. 215). Nesse contexto, convém que a segurança cibernética faça parte do cotidiano das organizações. Mais ainda, as empresas precisam estar cientes das vulnerabilidades e dos riscos a que estão sujeitas no espaço cibernético. Conforme argumentam Medeiros, Carvalho e Goldoni (2019, p.46), “nesse novo ambiente – marcado pela flexibilização de fronteiras e territórios, multiplicidade e anonimato de atores – novas e velhas ameaças desafiam as concepções tradicionais de segurança e defesa”.

Dentre os diversos setores fundamentais para o Brasil, o setor nuclear se apresenta como relevante caso de estudo. Em linhas gerais, ataques cibernéticos direcionados às usinas nucleares de produção de energia elétrica [1] têm o potencial de provocar perturbações no fornecimento energético de um país. Corrobora para a motivação da pesquisa o fato de as empresas do setor energético serem os alvos preferenciais de ataques cibernéticos (ONYEJI; BAZILIAN; BRONK, 2014). Como exemplo, cita-se os ataques cibernéticos ocorridos no Brasil em empresas do setor, como a Enel, Energisa, Light e EDP (COSTA, 2020). Embora não tenham provocados danos direto às operações, esses ataques apontam para a importância de aprofundar o estudo da segurança cibernética em infraestruturas críticas nacionais.

As usinas nucleares nacionais atualmente em operação na CNAAA, denominadas de Angra I e II, desempenham um papel relevante para o setor elétrico nacional, em especial por razão da capacidade de geração, alta disponibilidade e elevada confiabilidade (ONS, 2017). Assegurar a operabilidade dessas usinas, portanto, é fator importante para a estabilidade do sistema elétrico

[1] As usinas nucleares também são denominadas de usinas termonucleares.

nacional. Nessa linha, o ambiente cibernético apresenta-se como importante elemento a ser considerado na gestão da segurança de usinas nucleares. De acordo com Kim (2014), o setor nuclear deve tratar claramente a segurança cibernética, observando questões de regulação e padronização do setor. Além disso, o Brasil tem a responsabilidade com a sociedade brasileira de manter um alto nível de segurança de suas instalações nucleares, assim como um compromisso internacional, pois é membro Agência Internacional de Energia Atômica (IAEA, 1994). Por razão da criticidade do tema, a segurança cibernética tem se tornado essencial para a proteção de instalações nucleares, e diversos países têm desenvolvido abordagens próprias para proteger as instalações de ataques cibernéticos (BRANDENBURG UNIVERSITY, 2015).

As usinas nucleares possuem diversas proteções em seu ambiente, inclusive o isolamento entre os ambientes administrativo e operacional, a fim de dificultar ataques cibernéticos. Via de regra, os sistemas de supervisão, responsáveis pela operação e monitoração das usinas, são separados da rede administrativa. O fato de um ambiente ser isolado, todavia, não significa que não sofrerá manutenções e atualizações periódicas por funcionários externos. Além disso, de acordo com o guia de boas práticas elaborado pelo departamento norte americano *Homeland Security*, várias infraestruturas críticas estão migrando para tecnologias modernas e interconectadas (ZIEME; TURCOTTE, 2016). Embora essa mudança proporcione acesso a tecnologias mais recentes, a integração resultante aumenta o risco de novas vulnerabilidades, uma vez que os sistemas deixam de ser isolados como no passado (KNOWLES, 2015). Essa situação é reforçada por Cho, Chung e Kuo (2016), que argumentam que a transição no uso de equipamentos analógicos para equipamentos digitais nas infraestruturas nucleares fez com que a segurança cibernética se tornasse um fator crítico para essas instalações.

A necessidade de garantir a segurança cibernética das instalações nucleares pode ser evidenciada por um incidente ocorrido no Irã em 2010. Nesse ano, diversas centrífugas utilizadas para enriquecimento de urânio foram danificadas em uma planta industrial na cidade de Natanz. O número exato de equipamentos comprometidos não foi oficialmente divulgado, embora estime-se que tenha sido próximo de mil unidades (ZETTER, 2014). Um dispositivo móvel

de armazenamento do padrão *pendrive*[2], conectado a um computador dentro da usina iraniana, disseminou um sofisticado programa de computador[3] capaz de se aproveitar de vulnerabilidades do ambiente digital para infectar outros sistemas digitais (ZETTER, 2014). Observa-se que o ataque não foi apenas cibernético, mas uma investida que explorou vulnerabilidades humanas com o intuito de transpor as barreiras tecnológicas e o isolamento do ambiente. Conforme argumenta Mann (2008), muitos dos ataques não precisam de vulnerabilidades técnicas para terem sucesso, basta atacar o indivíduo.

Ao longo deste trabalho, será possível identificar os ataques mais utilizados pelos engenheiros sociais e as consequências derivadas. Sob o prisma da engenharia social, a análise se dará pelo exame de instrumentos normativos e procedimentos adotados na segurança cibernética de usinas nucleares. De modo complementar, entrevistas realizadas com especialistas fornecerão subsídios para melhor compreensão sobre o tema. Oportuno, também, será a observação das boas práticas de mercado utilizadas para mitigar ataques de engenharia social.

A importância deste estudo está em tratar a segurança não apenas sob o ponto de vista técnico, mas de abordar a interação das pessoas com o espaço cibernético. Assim, será verificado como a engenharia social pode ser utilizada para manipular os indivíduos. No caso dos funcionários do CNAAA, a engenharia social pode ser usada para apoiar ataques cibernéticos capazes de provocar potenciais prejuízos às instalações. O problema, contudo, não se restringe às questões de ordem técnica, como falhas de operação de equipamentos. O vazamento de informações e a adulteração de dados corporativos podem comprometer a imagem da CNAAA e, por conseguinte, a confiança da população na segurança das usinas nucleares.

Embora esta pesquisa tenha por base a Central Nuclear Almirante Álvaro Alberto, o estudo desenvolvido pode ser aplicado em outros setores estratégicos no Brasil. Enquanto em uma usina nuclear a engenharia social pode facilitar ataques cibernéticos capazes de provocar danos em equipamentos, ataques a uma instituição de estudos em biossegurança podem comprometer dados

[2] Pendrive: sinônimo de dispositivo USB de memória *flash*, podendo ser denominado em outros países de USB *key* ou USB *flash drive*.
[3] O programa tratava-se de um *worm*, *software* capaz de se disseminar de forma autônoma pela rede de computadores. Denominado de *Stuxnet*, foi considerado o primeiro *worm* capaz de atacar sistemas industriais.

sensíveis de pesquisa. No ambiente militar, um ataque de engenharia social pode revelar estratégias de manobras de combate. Neste contexto, o relatório *Cyber Threat Report* aponta que à medida que as empresas constroem defesas cibernéticas mais robustas, os atacantes se adaptam as novas defesas e criam ferramentas mais sofisticadas, capazes de burlar as defesas modernas (SONICWALL, 2019). A título de ilustração, dados publicados pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança do Brasil (CERT-BR) revelam que, em 2019, 39.389 notificações referiam-se a tentativas de fraude cibernética, utilizando a engenharia social (CERT.BR, 2019).

No que tange as infraestruturas críticas, como a CNAAA, não apenas investimentos em tecnologia são adequados para garantir a segurança da instalação. A capacitação dos funcionários, a gestão de contratos orientados à segurança, e a consciência institucional sobre as ameaças cibernéticas podem complementar a gestão da segurança corporativa. Como relatado pela empresa *Verizon*, um terço dos ataques cibernéticos executados no mundo em 2018 utilizaram a engenharia social (VERIZON, 2019).

Embora existam documentos que abordem a segurança cibernética de instalações críticas, pouca literatura nacional é encontrada no que se refere a ataques de engenharia social, em especial os associados ao ambiente nuclear. Por razão dessa lacuna, nesta pesquisa foi necessário recorrer à produção científica internacional. Documentos relacionados aos setores cibernético e nuclear foram analisados, como as normas elaboradas pela Agência Internacional de Energia Atômica (IAEA), pelo *National Institute of Standards and Technology* (NIST) e pelo *Institute of Electronics and Electronics Engineers* (IEEE). Durante o estudo também foram consultados relatórios produzidos por empresas especializadas em segurança cibernética.

A análise desenvolvida avança em uma seara pouco explorada em âmbito nacional. Estudar de modo multidisciplinar a segurança cibernética, a engenharia social e o setor nuclear permite abrir caminhos para futuras pesquisas, além de poder contribuir para a criação de normas brasileiras especificas para segurança cibernética no ambiente nuclear. Uma expansão do assunto pode ser conduzida ao se projetar a pesquisa para além desse setor, englobando-se o setor elétrico e financeiro, ambos considerados áreas críticas para a segurança nacional. O estudo pode, ainda, colaborar para reduzir a lacuna existente na literatura nacional

sobre o tema, além de fomentar o diálogo entre a academia, governo e setor privado. O resultado do trabalho pode ser utilizado em programas corporativos de capacitação, e o material resultante ser aplicado como insumo para o treinamento e capacitação de pessoal.

CONCEITOS E DEFINIÇÕES RELATIVOS À PESQUISA

A fim padronizar o entendimento e prover maior clareza a pesquisa, alguns conceitos chave seguem alinhados à Portaria nº 93, de 26 de setembro de 2019, do Gabinete de Segurança Institucional da Presidência da República, que aprova o Glossário de Segurança da Informação. Nesse documento, infraestruturas críticas são definidas como "instalações, serviços, bens e sistemas, (...) que se forem incapacitados, destruídos ou tiverem desempenho extremamente degradado, provocarão sério impacto social, econômico, político, internacional ou à segurança" (BRASIL, 2019). Em virtude dessa definição, a CNAAA enquadra-se como infraestrutura crítica. Outro conceito se refere à segurança cibernética, cujo documento a define como:

> Ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis. (BRASIL, 2019).

Observa-se que o conceito de segurança cibernética não se restringe a questões de ordem técnica, sendo, portanto, mais amplo. Esse entendimento é corroborado pelo *International Telecommunication Union* (ITU):

> A cibersegurança é a coleção de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, diretrizes, abordagens de gerenciamento de riscos, ações, treinamento, melhores práticas, garantia e tecnologias, que podem ser usadas para proteger o ambiente cibernético, a organização e os ativos do usuário (...). (ITU, 2008, p.2, tradução nossa)[4].

[4] *Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets*

Por vezes mencionado neste trabalho, o ambiente cibernético é classificado como uma gama de elementos que inclui “usuários, redes, dispositivos, software, processos, informação armazenada ou em trânsito, serviços e sistemas que possam ser conectados direta ou indiretamente a redes de computadores” (BRASIL, 2019). Por sua vez, o conceito de ameaça é compreendido como um “conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização” (BRASIL, 2019). O *malware* foi estabelecido como “software malicioso projetado para infiltrar um sistema computacional (...)” (BRASIL, 2019). Por fim, o espaço cibernético é classificado no Glossário de Segurança como:

> Espaço virtual composto por um conjunto de canais de comunicação da internet e outras redes de comunicação que garantem a interconexão de dispositivos de TIC e que engloba todas as formas de atividades digitais em rede, incluindo o armazenamento, processamento e compartilhamento de conteúdo além de todas as ações, humanas ou automatizadas, conduzidas através desse ambiente. (BRASIL, 2019).

Nesta pesquisa, usa-se o conceito de mitigação de ataque de engenharia social, em vez do conceito de prevenção. De acordo com o *Project Management Body of Knowledge* (PMBOK) do *Project Management Institute* (PMI), existe diferença quanto a prevenir e a mitigar um risco. Enquanto prevenir tem por objetivo tentar eliminar a causa raiz do risco, a mitigação busca reduzir a probabilidade de ocorrência ou a posicionar o impacto em um nível aceitável. Assim, por ser difícil eliminar por completo os ataques de engenharia social, a mitigação torna-se um conceito mais alinhado com proposta deste trabalho.

METODOLOGIA DE ESTUDO DE CASO APLICADA À CNAAA

Uma vez que se pretende um estudo aprofundado e particular do objeto de pesquisa, o método de investigação será o estudo de caso único, cuja análise se concentra na Central Nuclear Almirante Álvaro Alberto. Como argumenta Siggelkow (2007), em certos casos é desejável a escolha de uma organização específica para análise, pois por meio dela se obtém percepções diferenciadas, que não seriam fornecidas por outras organizações.

Inicialmente o estudo adotou uma pesquisa bibliográfica, onde verificou-se a literatura orientada à segurança cibernética, em especial artigos e livros que abordassem a temática de ataques de engenharia social. Na sequência, a pesquisa avançou para o setor nuclear, procurando compreender a segurança no setor nuclear brasileiro. A partir dessas duas linhas, buscou-se a interseção entre os dois temas, de modo a compreender como a CNAAA trata as questões relacionadas à segurança cibernética como meio de mitigar ataques de engenharia social. Contudo, diante da escassez de literatura nacional sobre o assunto, foi necessário analisar casos internacionais que pudessem auxiliar na reflexão sobre a CNAAA.

Além da pesquisa bibliográfica, realizou-se consulta à Eletronuclear por meio da Lei de Acesso à Informação (LAI), utilizando-se o Sistema Eletrônico do Serviço de Informação ao Cidadão (e-SIC) para obter informações para o embasamento empírico da pesquisa. Alguns questionamentos, contudo, não foram respondidos, pois a empresa argumentou que, de acordo com o artigo 22 da LAI, tratava-se de assunto sensível, sujeito à proteção da informação nas “hipóteses legais de sigilo, segredo de justiça e segredo industrial decorrentes de atividade econômica pelo Estado” (BRASIL, 2011).

Complementando o estudo, realizou-se entrevistas com profissionais atuantes nos setores cibernético e nuclear, a fim de proporcionar maior coesão das informações e melhor esclarecimento de pontos relevantes da pesquisa. Conforme apresentado no quadro 1, as entrevistas foram conduzidas com um funcionário aposentado da Eletronuclear, dois diretores executivos de empresas de segurança cibernética, um professor em pesquisas nucleares na Universidade Federal do Rio de Janeiro (UFRJ), um mestrando de Relações Internacionais na Universidade de Brasília (UnB), pesquisador do setor cibernético, e um servidor da Comissão Nacional de Energia Nuclear (CNEN). Ressalta-se que todas as informações contidas neste trabalho foram obtidas por meio de documentos ostensivos, de entrevistas e por consulta à Eletronuclear. Não há, portanto, informações que comprometam a segurança do ambiente nuclear ou das empresas citadas neste estudo. Além disso, as medidas de segurança cibernética relatadas na pesquisa são padrões nos setores nucleares e industrial.

Quadro 1 - Relação de entrevistados

Entrevistado	Instituição	Cargo	Modo de entrevista	Data da entrevista
Alan Lima	UFRJ	Professor e Pesquisador	Pessoalmente	outubro/2019
Eduardo Izycki	UnB	Mestrando em Relações Internacionais	Correio eletrônico	março/2020
Olivio Napolitano	Eletronuclear	Ex-Diretor de Manutenção	Pessoalmente e por correio eletrônico	novembro/2019
Renato Tavares	CNEN	Tecnologista Pleno	Correio eletrônico	março/2020
Marcelo Branquinho	ITSafe	Diretor Executivo	Correio eletrônico	novembro/2019
Ricardo Gonzaga	DLMaster	Diretor Executivo	Pessoalmente e por correio eletrônico	fevereiro/2020

Fonte: o autor

A fim de prover melhor clareza ao desenvolvimento do trabalho, foram estruturados três capítulos. O primeiro apresenta o ambiente cibernético de usinas nucleares, as vulnerabilidades associadas às instalações e os atores que representam ameaçam no espaço cibernético. A apresentação do funcionamento dos sistemas digitais de controle e monitoração, que podem ser comprometidos por ataques cibernéticos derivados de engenharia social, conferem um embasamento teórico ao tema. O histórico de incidentes de segurança em ambientes nucleares é apresentado com o intuído de auxiliar na identificação dos métodos de ataques. A compreensão de como se desenvolve um ataque de engenharia social e os comportamentos sociais explorados pelos atacantes são retratados no segundo capítulo. Nele são revelados os modos de ataques de engenharia social. Reforçando a análise, um histórico sucinto sobre ataques de engenharia social é utilizado com o propósito de verificar como a engenharia social é empregada. O terceiro capítulo apresenta as medidas de segurança cibernética para mitigação de ataques de engenharia social. Na sequência, desenvolve-se uma análise sobre as medidas de segurança cibernética adotadas pela CNAAA. Por fim, a estudo verifica se essas medidas são adequadas para a mitigação de ataques de engenharia social.

CAPÍTULO 1 - A SEGURANÇA CIBERNÉTICA NAS USINAS NUCLEARES

> A segurança cibernética é como trancar sua casa ou carro; não afasta os bandidos, mas se a segurança for boa o suficiente, eles podem escolher um alvo mais fácil. (Paul Herbka).

Atualmente, centenas de reatores nucleares estão em operação no mundo, de acordo com Agência Internacional de Energia Atômica[6]. O Brasil, a despeito das oscilações de investimentos no setor, detém tecnologias expressivas, como a capacidade de enriquecimento de urânio, dominada por poucos países (HARTIGAN, 2015). Em operação, encontram-se duas usinas termonucleares na CNAAA, Angra 1 e Angra 2, que têm papel relevante na matriz energética nacional (ONS, 2017). Quando comparado as demais fontes energéticas, o percentual de geração nuclear nacional é considerado baixo. Contudo, as usinas têm seu valor principalmente pela capacidade de gerarem energia elétrica de modo constante e com baixas taxas de interrupção, o que contribui para a estabilidade do fornecimento no Brasil (FGV, 2019).

As usinas nucleares requerem um nível de segurança compatível com a sua relevância. Todavia, apenas a segurança física pode não ser suficiente. Incidentes ocorridos em instalações nucleares apontam para a necessidade de assegurar a proteção desses ambientes também no mundo virtual. Se no passado os equipamentos utilizados nas usinas nucleares eram majoritariamente analógicos, gradativamente os dispositivos foram migrados para equipamentos modernos, que utilizam sistemas de controle digitais (BAYLON; BRUNT; LIVINGSTONE, 2016). Diversos fatores contribuíram para essa migração, como a necessidade de monitoração remota do ambiente de produção e a necessidade de maior conectividade com outras instâncias da empresa. Além da digitalização, destaca-se que as usinas nucleares adotam conexões com o mundo exterior via Internet, a fim de obter interação com prestadores de serviço, consultorias e suporte remoto, em especial no seu ambiente administrativo. Essas conexões expandem o perímetro da organização, ampliando os riscos de ataques originários do espaço cibernético (POLLACK; RANGANATHAN, 2018).

[6] A base de dados do *The Power Reactor Information System* (PRIS), da Agência Internacional de Energia Atômica, informa que 442 reatores nucleares estavam em operação no mundo em setembro de 2020.

Ataques cibernéticos têm o potencial de causar impactos nas infraestruturas críticas, e representam um importante alvo para indivíduos, grupos ou Estados que queiram roubar informações ou causar danos às instalações (HURST, 2015). Além disso, a sofisticação dos ataques cibernéticos dificulta a identificação da autoria e suas motivações (MEDEIROS; CARVALHO; GOLDONI, 2019). Diante desse cenário, o espaço cibernético apresenta-se como importante dimensão a ser considerada na gestão da segurança das usinas nucleares. Para mitigação de ameaças cibernéticas, contudo, é necessário aliar tecnologia com outras medidas não técnicas (LUIIJF, 2016). A adoção de uma cultura de segurança corporativa, que compreenda aspectos de gestão de pessoas e políticas de segurança, é importante para assegurar a proteção do ambiente. Nesse contexto, o Operador Nacional do Sistema Elétrico tem conduzido um trabalho propositivo para estabelecer controles de segurança cibernética na operação do Sistema Interligado Nacional (ONS, 2020).

Em todos os níveis da organização faz-se necessário observar a segurança cibernética, mas a proliferação de dispositivos digitais nas usinas pode ser um vetor de entrada de *malware*s[7] (POLLACK; RANGANATHAN, 2018). Nesse ponto, a engenharia social configura-se como potencial risco às usinas nucleares. Os dispositivos e sistemas digitais responsáveis pelo monitoramento e controle de funções críticas nas infraestruturas nucleares são operados por funcionários, que estão expostos a eventuais ataques de engenharia social. Ataques dessa natureza podem ser utilizados para facilitar ataques cibernéticos. Por esse motivo, para o desenvolvimento desta pesquisa, torna-se relevante uma breve apresentação sobre questões acerca do ambiente nuclear. Como os funcionários da CNAAA podem ser alvo de ataques de engenharia social, é importante observar quais são os atores presentes no espaço cibernético que representam ameaça. No âmbito normativo, é realizada uma análise sucinta dos documentos nacionais e internacionais orientados à segurança cibernética em infraestruturas nucleares. O exame dos instrumentos normativos é importante para se verificar em que grau o tema é tratado.

[7] *Malware* é um software malicioso projetado para infiltrar um sistema computacional com a intenção de roubar dados ou danificar aplicativos ou o sistema operacional (BRASIL, 2019).

1.1 Desafios e ameaças para a segurança cibernética de usinas nucleares

Concepções sobre a segurança do espaço cibernético foram moldadas nos últimos anos a fim de captar a realidade contemporânea dessa dimensão, uma vez que as ameaças cibernéticas se tornaram transversais a todas as atividades das sociedades modernas (NUNES, 2016). Essas ameaças exercem sua força principalmente por razão da extensa conectividade proporcionada pela Internet, que foi concebida para ser uma rede de fácil uso, mas sem altos requisitos de segurança (NYE, 2011). A prática de atos ilícitos, de terrorismo e de conflito entre nações encontra amplo terreno no mundo virtual, principalmente pela dificuldade de atribuição de responsabilidades e pela assimetria do espaço cibernético (CARVALHO, 2011). Nesse ambiente, o ataque tem vantagem sobre a defesa, e os atores podem ser anônimos (NYE, 2011).

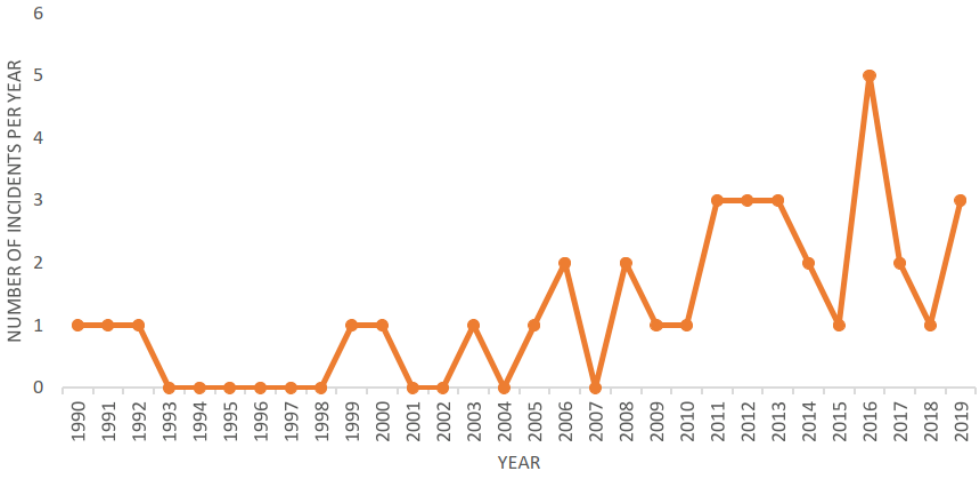
Com uma abordagem orientada à riscos e aos desafios atuais, o Fórum Econômico Mundial publicou, em 2019, o relatório *The Global Risk Report*. O documento classifica os ataques cibernéticos como eventos de alta probabilidade de ocorrência e de alto impacto, em nível de risco comparável às crises hídricas, desastres naturais e colapsos de ecossistemas. Sendo assim, os ataques cibernéticos representam riscos para infraestruturas críticas (WORLD ECONOMIC FORUM, 2019). Dentre as diversas infraestruturas conectadas ao espaço cibernético, as pertencentes ao setor elétrico destacam-se como atrativas para ataques dessa natureza (ONYEJI, BAZILIAN, BRONK, 2014). Incluídas nesse setor estão as infraestruturas do setor nuclear, que por muito tempo enfatizaram a proteção física de suas instalações, pois a dimensão cibernética era pouco difundida nesses ambientes (BAYLON; BRUNT; LIVINGSTONE, 2015).

Por ser altamente regulamentado, o setor nuclear conduz os desenvolvimentos técnicos em velocidade diferente dos aplicados em outros campos da indústria. Assim, tecnologias comuns em outros setores, como serviços baseados em nuvem ou o uso de dispositivos móveis, tornam-se um desafio no setor nuclear, pois os controles de segurança aplicados a essas tecnologias tendem a ser mais complexos em um ambiente crítico (GLUSCHKE, 2017). Em linhas gerais, as instalações nucleares utilizam sistemas de controle industrial para diversos processos, como no acesso, monitoramento, operação e controle da instalação (KNOWLES, 2015). De acordo com Varutamaseni, Bari e

Youngblood (2017), frequentemente os responsáveis pelas usinas acreditam que, por razão de os equipamentos e sistemas críticos serem isolados do mundo externo, o ambiente de produção está totalmente protegido. Para Campell e Singh (2019), o isolamento completo do ambiente de produção de usinas nucleares é um antigo mito. Incidentes podem ocorrer, por exemplo, devido ao acesso de prestadores de serviço durante manutenção de rotina em um equipamento, ou por ataques de engenharia social contra os funcionários.

Em um estudo sobre incidentes cibernéticos em instalações nucleares, Stoutland, Dumbacher e Miller (2020) identificaram trinta e seis incidentes entre os anos de 1990 e 2019, conforme gráfico 1. Esse número inclui desde incidentes menores, como problemas em software e atualizações não testadas adequadamente, até casos de intrusões reais, o que mostra que o setor nuclear não está imune aos incidentes cibernéticos.

Gráfico 1 - Incidentes cibernéticos em infraestruturas nucleares



Fonte: Stoutland, Dumbacher e Miller (2020)

A complexidade de uma instalação nuclear típica, que pode mais de mil componentes digitais, impõe dificuldades para sua proteção, pois aumenta a diversidade de possíveis modos de ataques cibernéticos (STOUTLAND; DUMBACHER; MILLER, 2020). A fim de proteger essas instalações das ameaças cibernéticas, passou-se a adotar uma abordagem de proteção dos sistemas críticos por meio de soluções tecnológicas. Contudo, essa abordagem é efetiva para ataques cibernéticos efetuados contra os ambientes tradicionais de tecnologia da informação, mas não são suficientes para proteger uma instalação

nuclear contra os novos métodos de ataques (VAN DINE; ASSANTE; STOUTLAND, 2016). Como argumenta Decker et al (2018), apenas a tecnologia não é capaz de fornecer a segurança do ambiente cibernético, portanto uma análise das ameaças decorrentes de fatores humanos faz-se necessária (GLUSCHKE, 2017). Diante disso, o estudo sobre ataques de engenharia social torna-se relevante, sendo necessário compreender os mecanismos de ação desses ataques contra os funcionários da CNAAA, assim com identificar os atores que representam ameaças. Nesse sentido, a Agência Internacional de Energia Atômica classifica os atores como os ladrões de tecnologia, funcionários insatisfeitos, hacker recreativo, ativista cibernético, crime organizado, Estados e terroristas (IAEA, 2016). Branquinho et al (2014) elencam os espiões cibernéticos, indivíduos que possuem interesse no roubo de informações confidenciais por meio de *softwares* instalados em computadores alvo, e os hacktivistas, que são indivíduos que, por motivos políticos ou sociais, invadem sistemas de computação. Branquinho et al (2014) apontam também os terroristas cibernéticos, que são grupos organizados patrocinados por um país ou por organizações terroristas, e os guerreiros cibernéticos, que realizam ataques cibernéticos por motivos pessoais, patriotismo ou crenças religiosas, por vezes contratados por governos ou organizações militares. Branquinho et al (2014) assinalam, ainda, os atacantes internos, que são funcionários ou ex-funcionários das organizações, que podem facilitar o roubo, a espionagem ou a sabotagem.

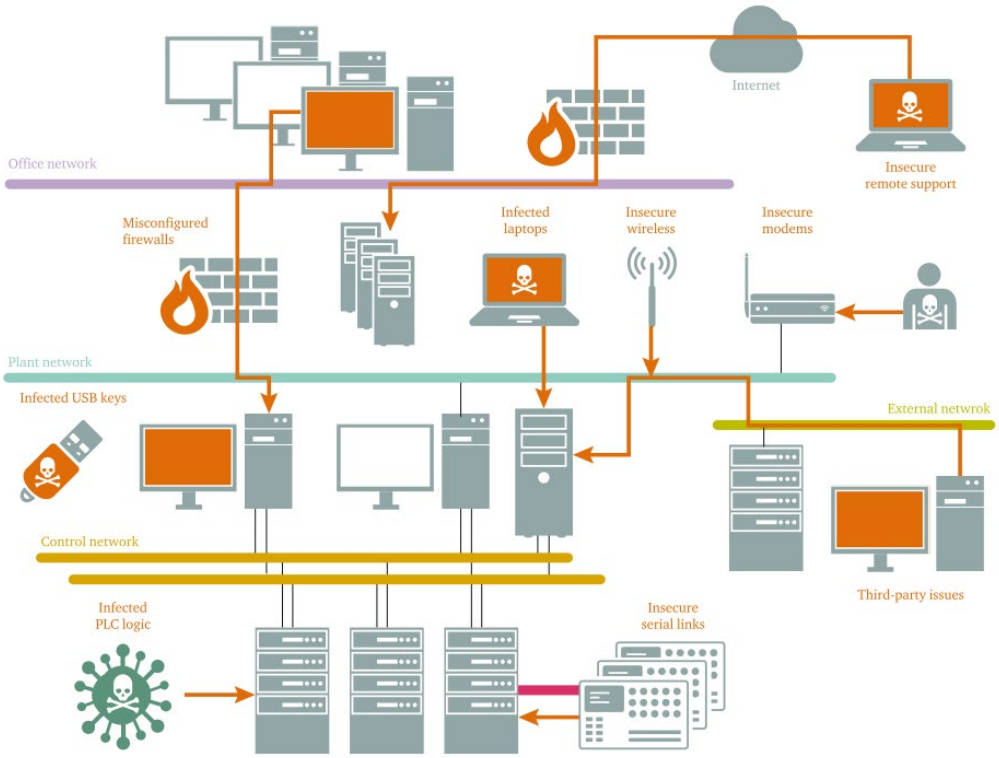
1.2 As consequências potenciais do comprometimento de sistemas supervisórios

A possibilidade de ataques cibernéticos contra usinas nucleares levanta preocupações sobre riscos atuais e futuros, que incluem potenciais perturbações na operação, danos físicos nas instalações, espionagem, incidente radiológico e perda da confiança da opinião pública em relação à energia nuclear (GIAUROV, 2017). A implementação de controles de segurança torna-se complexa pelo fato de ser difícil mensurar a extensão de um incidente em instalações nucleares (IAEA, 2016).

Nas usinas nucleares, assim como em outros ambientes industriais, são utilizados os sistemas supervisórios, também denominados pela indústria de Sistemas de Supervisão e Aquisição de Dados (SCADA) ou Sistemas de Controle

Industrial (ICS). Tais sistemas são responsáveis pelo controle e monitoração de diversos equipamentos, sendo considerados componentes críticos (MASSOD, 2016). Demiroz (2014) afirma que as vulnerabilidades de segurança de ordem técnica existentes em sistemas ICS incluem as falhas no design de sistemas, os erros de configuração de rede e sistemas, o monitoramento deficiente e a fragilidade no controle de acesso. Segundo o referido autor, quando essas vulnerabilidades são exploradas, os componentes dos ICS se tornam suscetíveis a ataques cibernéticos. Além disso, de acordo com a IAEA (2016), fatores humanos podem afetar a habilidade de uma organização em reconhecer e resistir a um ataque cibernético. Baylon, Brunt e Livingstone (2016) apresentam exemplos de potenciais vulnerabilidades de ICS, conforme figura 1. Os autores elencam diversas vulnerabilidades, como as decorrentes de conexões com provedores de serviço, serviços de suporte remoto pela Internet e *firewalls* mal configurados. Além disso, dispositivos USB e *laptops* infectados são potenciais propagadores de *malware*, tal qual redes sem fio mal configuradas. No nível da sala de controle das usinas, equipamentos infectados podem alterar o comportamento padrão de sistemas supervisórios.

Figura 1 - Potenciais vulnerabilidades em sistemas SCADA/ICS



Fonte: Baylon, Brunt e Livingstone (2016)

No que tange os impactos de ataques cibernéticos aos sistemas SCADA/ICS, o documento 800-82-R2, *Guide to Industrial Control Systems Security*, do *National Institute of Standards and Technology* (NIST), elenca impacto físicos, econômicos e sociais. As consequências potenciais associadas ao comprometimento de sistemas supervisórios também são apresentadas no documento, e incluem: redução ou perda de produção em uma instalação ou em várias simultaneamente; ferimento ou morte de funcionários; ferimento ou morte de pessoas na comunidade; danos aos equipamentos; desvio ou roubo materiais perigosos, dano ambiental; violação de requisitos regulamentares; contaminação; questões legais ou criminais; perda de informações proprietárias ou confidenciais; danos à imagem da empresa e perda da confiança do cliente e da população. Portanto, diante da gravidade das consequências mencionadas no documento, observa-se a necessidade de se proteger o ambiente nuclear de ataques de engenharia social, que podem facilitar ataques cibernéticos capazes de comprometer os sistemas supervisórios.

1.3 O processo de digitalização das usinas nucleares e os riscos resultantes no espaço cibernético

A maior exposição das usinas nucleares a ameaças cibernéticas se deve, em parte, ao processo de digitalização, uma vez que os vetores de ameaça deixaram de ser restritos ao plano físico, para serem conduzidos também no ambiente digital (PWC, 2019). Por esse motivo, torna-se relevante estudar a CNAAA. A partir de documento da Eletronuclear, verifica-se que a usina de Angra 3 terá sistemas de controle digitais.

> Angra 3 terá equipamentos de Instrumentação e Controle digitais no mesmo padrão dos projetos mais recentes de usinas nucleares, que deve contribuir para um melhor desempenho e segurança da planta. A sala de controle de Angra 3 é projetada com tecnologia digital e reflete o estado da arte em projetos de sala de controle. As atuações de componentes e monitoração de processos e alarmes são realizadas através de telas digitais em computadores. (ELETRONUCLEAR, 2017, p. 3).

Cita-se, ainda:

> Em uma tendência mundial, onde, cada vez mais, a tecnologia analógica para sistemas de controle tem se tornado obsoleta e a reposição de peças tem se tornado cada vez mais difícil, a atualização destes sistemas para os modernos sistemas de controle digital tem se tornado cada vez mais necessária. (ELETRONUCLEAR, 2017, p. 33).

Sobre Angra 2, a Eletronuclear afirma que a usina "mudou recentemente um dos sistemas de I&C (Sistema de Controle do Reator) para equipamento digital igual ao que está sendo projetado para Angra 3" (ELETRONUCLEAR, 2017, p.33). Nota-se, portanto, que Angra 2 já tem equipamentos digitais no ambiente de produção, e que Angra 3 terá um ambiente majoritariamente digitalizado, incorporando a evolução de base normativa e tecnológica nacional e internacional das últimas décadas (ELETRONUCLEAR, 2017). Esse fato reforça a necessidade de ser estudar as medidas de segurança cibernética adotadas pela CNAAA e de como a engenharia social pode facilitar ataques cibernéticos. Contudo, não apenas a digitalização na operação das usinas pode ocasionar vulnerabilidades no ambiente. O uso de computadores no ambiente administrativo pode aumentar o risco de ataques cibernéticos, como o incidente ocorrido na usina nuclear indiana de Kudankulam.

A usina indiana pode ser utilizada como contraste com Angra I e II, a fim de agregar elementos empíricos para auxiliar na análise do ambiente cibernético das usinas brasileiras. As capacidades produtivas das usinas de Kudankulam e da CNAAA são semelhantes. Enquanto a usina indiana tem dois reatores nucleares de 1000MW cada (CAMPBELL, 2019), as usinas de Angra 1 e 2 dispõe de uma capacidade somada de 2000MW (ELETRONUCLEAR, 2019a). Outra questão se refere à tecnologia empregada, pois as usinas indianas e brasileiras utilizam a mesma categoria de reator nuclear, baseado em água pressurizada – PWR (Power Technology, 2019). Além disso, ambos os países utilizaram tecnologia estrangeira para a construção dos reatores: o Brasil importou tecnologia dos EUA e da Alemanha (ELETRONUCLEAR, 2019a) e a Índia obteve os equipamentos da Rússia (SAMUEL; SHARMA, 2019).

O incidente cibernético na usina nuclear de Kudankulam ocorreu em setembro de 2019, após um funcionário ter conectado um computador pessoal na rede interna e na Internet, disseminando um *malware* que contaminou o ambiente de tecnologia da informação da instalação (NPCIL, 2019). O governo indiano confirmou o incidente, e assegurou que a área de controle do reator não fora

atingida, apenas o ambiente administrativo (PIB, 2019). De acordo com o Departamento de Energia Atômica da Índia, algumas medidas foram tomadas para fortalecer a segurança da usina após o incidente, dentre as quais o aumento das proteções no acesso à Internet, a restrição de mídias removíveis e o bloqueio de endereços que apresentavam atividade maliciosa (PIB, 2019). A CyberBIT, empresa especializada em segurança cibernética, analisou o *malware* e verificou que se tratava de um RAT[8] denominado *Dtrack*, capaz de roubar informações de histórico de navegação de usuários, informações sobre a rede de dados e arquivos corporativos (CYBERBIT, 2019). A empresa de segurança cibernética Dragos identificou que o *malware* continha em seu código endereços de rede e credenciais de acesso pertencentes à usina indiana, o que indicaria um ataque direcionado à instalação de Kudankulam (DRAGOS, 2019). Anteriormente, em setembro de 2019, a empresa Kaspersky já havia reportado a existência de variantes do *malware* em instituições financeiras e em centros de pesquisa indianos (KASPERSKY, 2019a).

O governo indiano realizou ações de contenção de danos e medidas para mitigar novos ataques, porém, alguns procedimentos de segurança cibernética já eram praticados na usina antes do ataque. As portas USB dos equipamentos da usina indiana estavam desabilitadas em todo o ambiente de operação, o que impedia o uso de *pendrive* e outros dispositivos externos (SUDHAKAR, 2019). O ambiente de produção estava isolado, de modo a não poder ser acessado a partir de nenhuma rede externa. Os sistemas eram protegidos por *firewalls*[9], capazes de filtrar as conexões entre as redes internas e externas da instalação nuclear. Os funcionários e terceirizados não podiam utilizar celulares. Equipamentos eletrônicos identificavam e desativavam dispositivos que porventura fossem utilizados no ambiente cibernético interno. Além disso, uma auditoria de segurança cibernética fora realizada, após uma tentativa anterior de ataque ao ambiente de produção da usina (SUDHAKAR, 2019).

A partir desse incidente, observa-se que, apesar da adoção de medidas de proteção tecnológica, a ação de um único funcionário comprometeu a segurança cibernética da instalação nuclear. O fato aponta para a importância de se observar

[8] RAT: acrônimo de *Remote Administration Tool*. Trata-se de um *malware* que permite a administração remota de um computador infectado.
[9] *Firewall*: recurso destinado a evitar acesso não autorizado a uma determinada rede, ou a um conjunto de redes, ou a partir dela. Podem ser implementados em *hardware* ou *software*, ou em ambos. (BRASIL, 2019)

a dimensão humana na gestão da segurança cibernética das instalações nucleares. Para Campbell e Singh (2019), o incidente ocorrido na usina indiana, um país que tem um programa nuclear desde a década de 50, revela que países com anos de experiência na área nuclear não estão imunes a incidentes cibernéticos. Diante desse incidente, pode-se notar que, mesmo com a utilização de mecanismos tecnológicos para proteção do ambiente cibernético, a proteção do ambiente nuclear não estará completamente assegurada se os funcionários estiverem vulneráveis às ameaças externas e internas (CAMPBELL; SINGH, 2019). Em tais circunstâncias, ainda que o ambiente operacional, diretamente relacionado ao reator nuclear, seja protegido de ameaças cibernéticas, os funcionários estarão vulneráveis aos ataques de engenharia social. Isso pode acarretar, por exemplo, no vazamento de informações pessoais e corporativas (CAMPBELL; SINGH, 2019). O incidente ocorrido na usina de Kudankulam revela a importância de se estudar o ambiente cibernético da CNAAA, em especial no que tange a dimensão humana. O fato de as usinas indiana e brasileiras possuírem característica semelhantes, reforça a necessidade de pesquisas científicas que possam auxiliar na segurança cibernética das usinas nacionais.

1.4 Incidentes de segurança cibernética em usinas nucleares

O incidente na usina de Kudankulam não foi o único ocorrido em infraestruturas nucleares. Verificar o histórico de incidentes de segurança cibernética é um importante meio de se compreender como são realizados os ataques, o que pode facilitar a adoção de mecanismos de mitigação. Nesse aspecto, Eduardo Izycki [10], em entrevista para esta pesquisa, afirma que diversas campanhas de ataques cibernéticos provocaram, ou almejaram provocar, resultados cinéticos em ambientes industriais. Ele cita as campanhas *Dragonfly* 2.0, *Shamoon*, *BlackEnergy*, *NotPetya*, *Industroyer* e *Triton/Trisis*. Eduardo Izycki menciona, ainda, que duas operações, *Cleaver* e *Sharpshooter*, foram desmanteladas antes de alcançarem resultados concretos, e tinham como objetivo campanhas de engenharia social contra alvos de infraestruturas críticas.

[10] Entrevista realizada em março de 2020

Em 2003, a usina *Davis-Besse Nuclear Power Station*, nos EUA, foi infectada pelo *malware Slammer*. O incidente foi causado por um consultor de uma empresa prestadora de serviços que inadvertidamente conectou um equipamento contaminado na rede de dados da usina. Embora o *malware* não tenha sido criado especificamente para ambientes industriais, ele sobrecarregou um computador importante para a operação da instalação. Como a rede estava conectada sem proteção ao sistema de controle da usina, o *malware* conseguiu infectar o ambiente de operação. Esse fato provocou indisponibilidade nos sistemas de exibição de parâmetros de segurança durante cinco horas. Por essa razão, os operadores não puderam acompanhar informações críticas, como os indicadores de parâmetros relativos ao núcleo do reator. Contudo, a usina não estava operacional no período da infecção, caso contrário, poderiam ter ocorrido problemas significativos (VAN DINE; ASSANTE; STOUTLAND, 2016).

Aproximadamente mil centrifugas de enriquecimento de urânio foram danificadas após um *malware* ter sido introduzindo no sistema de controle das centrifugas de enriquecimento de urânio das instalações nucleares de Natanz, no Irã, em 2010 (SPRINGER, 2017). Denominado de *Stuxnet*, o *malware* foi criado especificamente para infectar controladores lógicos da empresa Siemens, e foi considerado a primeira arma cibernética a explorar sistemas SCADA (CARVALHO, 2014). Por razão do incidente, os equipamentos passaram a operar em regime fora do padrão de segurança especificado, provocando a fadiga das centrífugas e, por conseguinte, a fratura do material (LENDVAY, 2016). O *malware* infectou computadores em diversos países, inclusive no Brasil (ZETTER, 2014), o que poderia ter causado incidentes em infraestruturas críticas no país.

A usina nuclear de Gundremmingen, na Alemanha, foi alvo de *malware*s em 2016, durante a atualização de um sistema instalado em um computador. O vírus infectou dezoito dispositivos externos de armazenamento, que não estavam conectados aos sistemas de produção. Duas variantes de vírus foram encontradas, sendo o primeira especializada em roubar arquivos e permitir o controle remoto do computador infectado. A outra era capaz se espalhar pela rede, obtendo *logins* e dados sensíveis (VAN DINE; ASSANTE; STOUTLAND, 2016).

Os ataques cibernéticos nem sempre acarretam danos físicos às instalações. Informações sensíveis, incluindo dados pessoais e de pesquisa,

podem ser roubados para diversos fins. O uso dessas informações pode facilitar ataques de grupos terroristas, servir como insumos em caso de guerra cibernética ou utilizado para espionagem industrial. O ataque à usina indiana mostrou que a ação de um único funcionário pode burlar toda a infraestrutura tecnológica de segurança. O ataque à usina de *Davis-Besse* revelou a necessidade de se observar como as empresas prestadoras de serviço praticam a segurança cibernética. Por outro lado, o ataque do *Stuxnet* apontou como a inserção de dispositivos não autorizados na rede pode provocar danos físicos à infraestrutura, enquanto a infecção na usina alemã expos a importância de se ter processos bem definidos para a atualização de sistemas críticos. Observa-se que em nenhum dos casos citados houve falha relativa à tecnologia. Os equipamentos físicos de segurança não foram atacados diretamente. O ponto nefrálgico, que possibilitou os ataques, se originou da ação de funcionários durante o uso do ambiente cibernético, o que aponta para a importância da dimensão humana na segurança cibernética.

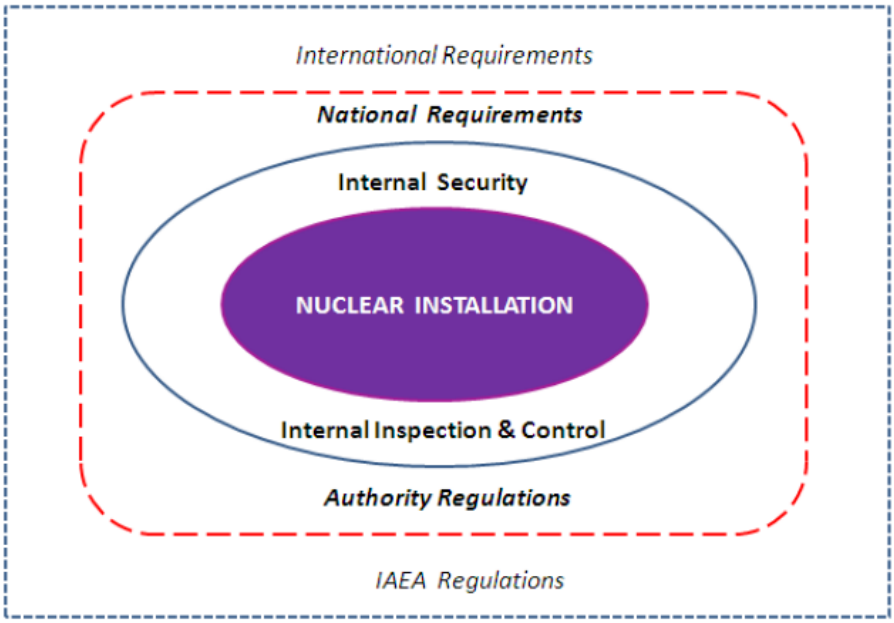
1.5 Instrumentos normativos internacionais orientados à segurança cibernética de instalações nucleares

A segurança cibernética envolve, além de questões técnicas, aspectos de ordem regimentar. Por meio de políticas, normas e diretrizes, os gestores responsáveis pela gestão da segurança podem obter a orientação necessária para conduzir atividades de proteção dos ambientes cibernéticos sob sua responsabilidade. Do mesmo modo que existem normas especificas para a proteção do ambiente físico de usinas nucleares, há normas que estabelecem padrões em nível institucional, nacional e internacional para a proteção do ambiente cibernético de instalações nucleares. A análise dessas normas é pertinente para esta pesquisa na medida que os documentos fornecem orientações sobre métodos e procedimentos de segurança cibernética, que podem ser usados para a mitigação de ataques de engenharia social.

O arcabouço normativo do setor cibernético é estratificado, e abrange desde políticas no nível estratégico, até procedimentos operacionais. No primeiro nível, encontram-se as questões internas de operação e controle da instalação nuclear, como os procedimentos, especificações técnicas e diretrizes

corporativas, conforme apresentado na figura 2. No nível seguinte estão os instrumentos normativos nacionais, que se materializam em políticas domésticas mais abrangentes. Por fim, em nível internacional, existem as regulamentações elaboradas pela Agência Internacional de Energia Atômica (VAN DINE; ASSANTE; STOUTLAND, 2016).

Figura 2 - Estrutura normativa do setor nuclear



Fonte: Tugrul (2018)

Dentre as publicações utilizada no setor nuclear, a Agência Internacional de Energia Atômica (IAEA) elabora a coletânea *Nuclear Security Series*, que provê orientações sobre diversos aspectos da segurança nuclear. São abordados tópicos sobre operações de instalações nucleares, transporte e produção de material nuclear, entre outros. Para esta pesquisa, quatro documentos da AIEA, dedicados especificamente à segurança, são relevantes. O primeiro documento, *Conducting Computer Security Assessments at Nuclear Facilities,* foi elaborado para servir como guia, e trata de práticas de segurança computacional em instalações nucleares. Ele propõe uma avaliação de segurança para mapear os sistemas computacionais de uma instalação nuclear. O segundo documento, denominado *Computer Security Incident Response Planning at Nuclear Facilities,* categoriza os incidentes de segurança em ambientes computacionais, e sugere um processo estruturado de tratamento de incidentes de segurança cibernética. Nessa linha, o documento *Computer Security at Nuclear Facilities* apresenta

programas para proteger sistemas computacionais, redes e sistemas digitais que sejam críticos para o funcionamento de instalações nucleares. A intenção é auxiliar na prevenção de roubo e sabotagem, além de outros atos que comprometam a segurança. Por fim, o *Computer Security of Instrumentation and Control System at Nuclear Facilities* serve como guia para proteger sistemas computacionais, porém orientado para proteção de sistemas de controle. Os quatro documentos são complementares, e proveem orientações relevantes para a gestão da segurança das usinas nucleares.

Além dos documentos elaborados pela IAEA, outras normas são utilizadas pelo setor nuclear para a segurança cibernética. A *International Organization for Standardization* (ISO) publica a família de normas ISO/IEC 27000, utilizada no setor de tecnologia da informação, mas também empregada em infraestruturas nucleares. Segundo Piggin (2012), as organizações geralmente se baseiam nas normas ISO/IEC 27001 e 27002 para o gerenciamento de risco de informação. Essas normas consistem em guias para gerenciamento de políticas de segurança, governança, controle de acesso, gerenciamento de incidentes, entre outros (KNAPP, 2011). No ambiente industrial, a ISA-99 é igualmente utilizada, e consiste de uma coletânea de normas e relatórios técnicos elaborados pela *International Society of Automation* (ISA), com a finalidade de estabelecer a segurança da informação em redes industriais e de minimizar o risco de ataques cibernéticos (BRANQUINHO et al, 2014).

O uso de diversas camadas de proteção para reduzir o impacto de uma falha de segurança é citado no NIST SP 800-8 *Nuclear Regulatory* Commission, enquanto o NIST 800-30 apresenta um framework de gerenciamento de risco. Da mesma família, o guia NIST SP 800-82 *Industrial Control Systems Security* fornece orientação para a segurança de ambientes SCACA/ICS. Esse documento apresenta a topologia típica de sistemas de controle, a identificação de ameaças e vulnerabilidades, além de recomendações de contramedidas de segurança. De acordo com o guia, os principais objetivos na implementação de segurança em sistemas de controle contempla: restringir o acesso lógico a redes; restringir acesso físico aos equipamentos e redes de controle; proteger os componentes dos sistemas de controle com a remoção de funcionalidades não utilizadas; restringir modificações não autorizadas; detectar eventos de segurança e incidentes; manter o funcionamento dos sistemas durante um incidente; restaurar

o sistema após um incidente. Assim, algumas ações importantes são elencadas: desenvolvimento de políticas de segurança; diretrizes e capacitação de pessoal; implementação de redes de comunicação separadas para ICS; separação lógica entre a rede corporativa e a rede de controle ICS; redundância de redes e ICS; retirada de serviços não utilizados; restrição de acesso físico ao ambiente de ICS; utilização de mecanismos de autenticação e credenciais de usuários para acesso em redes de ICS e corporativas; aplicação de criptografia no ambiente de ICS e o monitoramento dos sistemas ICS e das áreas críticas.

1.6 Documentos nacionais orientados à segurança cibernética de instalações nucleares

A interdisciplinaridade entre os setores cibernético e nuclear é pouco abordada nos documentos nacionais. A Estratégia Nacional de Defesa (END), na versão publicada em 2020, indica a necessidade de se desenvolver os setores estratégicos de defesa nuclear e cibernético, assim como de aumentar a capacidade de prover a defesa nuclear. A END também menciona o setor nuclear como de importância estratégica, em especial para garantir o equilíbrio e versatilidade da matriz energética, e para capacitar o país na produção de tecnologia, como na construção do submarino nuclear. Segundo o documento, existe a necessidade de se aprimorar a segurança cibernética, em especial na proteção das infraestruturas críticas (BRASIL, 2020a). Nessa linha, a Política Nacional de Defesa (PND) afirma que a segurança e a defesa do espaço cibernético são “essenciais para garantir o funcionamento dos sistemas de informação, gerenciamento e de comunicações de interesse nacional” (BRASIL, 2020b, p. 14). Ainda em 2010, o Guia de Referência para a Segurança das Infraestruturas Críticas da Informação (SICI), elaborado pelo Gabinete de Segurança Institucional da Presidência da República (GSI-PR), apresentava os requisitos mínimos para a segurança das infraestruturas críticas (BRASIL, 2010).

Passo importante foi dado ao final de 2018 com a publicação da Política Nacional de Segurança de Infraestruturas Críticas. O documento esclarece que o GSI-PR é o responsável por assuntos relativos às infraestruturas críticas (IC) no âmbito da Administração Pública Federal (APF). Embora a Política deva ser seguida apenas pela APF direta, autárquica, fundacional e por empresas estatais

que dependam do Tesouro Nacional, o documento é importante para orientar todos os entes envolvidos. O documento foi o ponto de partida para uma discussão mais ampla, que pretende abranger outros instrumentos, como o Plano Nacional de Segurança de IC e o Sistema Integrado de Dados de Segurança de IC.

Em fevereiro de 2020 foi publicado o decreto n° 10.222, a Estratégia Nacional de Segurança Cibernética (E-Ciber). Embora o documento não seja específico sobre infraestruturas críticas, tampouco aborde o ambiente nuclear, ele cita pontos pertinentes sobre tema. Nele é mencionado que ataques às infraestruturas críticas estão entre as maiores ameaças à segurança nacional, e que um ponto crítico para o governo brasileiro é a proteção das empresas que operam essas infraestruturas críticas:

> Um ataque cibernético de grande envergadura, caso não seja adequadamente tratado, pode afetar profundamente a reputação da organização, ocasionar perda de receitas, levar a prejuízos operacionais com a paralização dos serviços, resultar em perda de informações e ainda levar à aplicação de sanções legais e administrativas. (BRASIL, 2020c).

O documento avança:

> (...) é importante que as organizações, públicas ou privadas, estabeleçam política se procedimentos de segurança cibernética que sejam periodicamente revisados, atendam à evolução tecnológica, ao aperfeiçoamento de processos e à necessidade de capacitação contínua e estruturada para todos os colaboradores, por meio de programas de capacitação e de treinamento. (BRASIL, 2020c).

Dentre as diversas ações estratégicas elencadas no E-Ciber, ressalta-se o objetivo de aumentar o nível de proteção das infraestruturas críticas nacionais. Tal objetivo tem por princípio proporcionar maior resiliência a essas instalações, incentivar a implementação de políticas de segurança cibernética, e estimular a participação das infraestruturas críticas em exercícios cibernéticos.

Em relação ao documento intitulado Política Nuclear Brasileira (BRASIL, 2018), não há referência explícita à cibernética, apenas à segurança nuclear e à proteção física. Contudo, fato relevante é a ratificação sobre as convenções, acordos e tratados dos quais o Brasil é signatário, o que reforça a possibilidade

de uso de instrumentos normativos internacionais como fonte de orientação para ações de proteção cibernética em instalações nucleares nacionais. Intitulado de Programa Política Nuclear PPA 2016-2019, o documento foi elaborado pela Comissão Nacional de Energia Nuclear (CNEN), e afirma que as atividades nucleares brasileiras têm como objetivo assegurar o uso pacífico e seguro da energia nuclear e desenvolver a ciência e tecnologia, além de fornecer insumos e equipamentos ao mercado (CNEN, 2016). Em entrevista para esta pesquisa, Renato Tavares[11] informa que tanto no Brasil, quanto em âmbito internacional, os aspectos de segurança cibernética têm assumindo um papel de destaque, sendo bastante discutidos no espectro da segurança nuclear. De acordo com o entrevistado, a norma CNEN NN 2.01 já menciona requisitos relacionados aos princípios de segurança cibernética, orientados para os sistemas de proteção física. Renato Tavares afirma, ainda, que a CNEN tem competência legal para expedir normas, regulamentos e para fiscalizar assuntos referentes à segurança nuclear, proteção física e salvaguardas. Embora a instituição não tenha uma norma específica sobre segurança cibernética em ambiente nuclear, Renato Tavares informa que a CNEN instituiu um grupo de trabalho com o objetivo de conduzir estudos para a elaboração de uma norma nuclear nacional, que contemplará questões de segurança cibernética, em especial no que se refere aos aspectos relacionados à segurança nuclear. Além disso, o entrevistado menciona que a CNEN, por meio do Centro de Apoio à Segurança Física Nuclear (CENASF), realiza o treinamento de profissionais que atuam nas organizações operadoras do setor nuclear e radiológico brasileiro, incluindo as usinas nucleares. Contudo, o CENASF tem foco em treinamentos orientados à segurança física nuclear.

1.7 Riscos inerentes da digitalização e a lacuna de documentos no setor nuclear brasileiro

A gradativa mudança de dispositivos analógicos para digitais nas usinas nucleares resultou em maior vulnerabilidade para essas instalações. Visto que os funcionários que operam os sistemas digitais críticos podem ser alvo de ataques de engenharia social, a dimensão humana se apresenta como fator fundamental

[11] Entrevista realizada em março de 2020

para a segurança do ambiente cibernético das usinas nucleares. Os incidentes cibernéticos apresentados nesse capítulo reforçam a relevância de se realizar estudos sobre o tema na CNAAA.

Com a intenção de proporcionar embasamento teórico, apresentou-se uma breve descrição sobre os sistemas supervisórios, útil para o estudo das medidas de segurança capazes de mitigar ataques de engenharia social. A análise de documentos nacionais e internacionais revelou que, enquanto no exterior existem documentos que promovem a interdisciplinaridade entre os setores cibernético e nuclear, no Brasil há uma lacuna de instrumentos normativos sobre a questão. Apenas documentos da CNEN apontam princípios de segurança cibernética, contudo de modo não dedicado, e sem apresentar orientações de como o setor deve tratar a questão cibernética nas instalações nucleares brasileiras. Esse fato remete à necessidade de criação de novos instrumentos normativos específicos para essa finalidade. Embora existam grupos de pesquisa no país que realizam a discussão sobre o tema, é relevante que o Brasil promova o contínuo diálogo entre os setores nuclear e cibernético, e avance na elaboração de instrumentos normativos específicos que contemplem a integração entre esses setores. Importante, ainda, que o diálogo considere a dimensão humana, uma vez que o indivíduo é considerado peça-chave para a segurança cibernética e nuclear. Por esse motivo, o próximo capítulo aborda o modo como a engenharia social é capaz de influenciar os funcionários da CNAAA.

CAPÍTULO 2 – A ENGENHARIA SOCIAL NO CONTEXTO DO ESPAÇO CIBERNÉTICO.

> Seja um pouco desconfiado. Um número muito grande de ataques depende de engenharia social simples. Pergunte a si mesmo na próxima vez em que receber um e-mail dizendo que ganhou um iPad ou recebeu um pacote da FedEx - isso é real? Isso aconteceria comigo ao andar na rua? (James Lyne).

Coube ao capítulo anterior apresentar um panorama sobre a segurança cibernética no setor nuclear, a qual não se restringe apenas a questões de ordem técnica, mas está estreitamente relacionada à dimensão humana. Decisões e ações equivocadas executadas pelos indivíduos, decorrentes do uso da engenharia social, podem desencadear incidentes de segurança em instalações nucleares. Compreender como a dimensão humana pode ser exposta à engenharia social torna-se fundamental para o estudo de medidas de segurança cibernética aplicadas às instalações nucleares.

A engenharia social é uma das maiores ameaças para organizações que têm operação no ambiente digital (ALDAWOOD; SKINNER, 2019). Em razão da criticidade das usinas nucleares, a condução de práticas seguras de gestão da segurança cibernética, orientadas à mitigação de ataques de engenharia social, torna-se especialmente relevante. Embora o ambiente crítico de uma usina nuclear seja isolado do ambiente externo e, portanto, menos suscetível a ataques cibernéticos, o uso da engenharia social tem o potencial de ultrapassar a barreira física do isolamento, pois é orientada ao indivíduo, o qual, ao contrário das instalações físicas, não está completamente isolado, pois vive em sociedade. Apenas o uso de políticas e soluções tecnológicas, portanto, pode não ser suficiente para garantir uma proteção robusta e resiliente para a Central Nuclear Almirante Álvaro Alberto.

Nesse contexto, este capítulo inicia com o aprofundamento sobre a engenharia social, e expõe de que modo ela pode ser utilizada para ultrapassar as proteções tecnológicas existentes. São apresentados métodos utilizados pelos engenheiros sociais, assim com alguns possíveis modos de mitigar a ação de ataques. A sessão seguinte mostra um breve histórico de incidentes causados por ataques de engenharia social em ambiente nucleares, útil para o entendimento sobre os potenciais riscos aos quais a CNAAA pode estar sujeita.

2.1 A engenharia social como ameaça à segurança no espaço cibernético

A engenharia social não é um conceito recente. No início do século XX, o termo era usado para representar métodos de resolução de problemas sociais no campo das ciências políticas (IVATURI; JANCZEWSKI, 2011). Se no passado representava a ideia de transformação, atualmente o conceito está associado à segurança da informação e aos métodos de persuasão usados para se obter informações sensíveis de uma organização. À medida que cresce o uso da tecnologia no meio digital, mais a engenharia social se torna uma ameaça para a segurança (MUSCANELL, GUADAGNO, 2014). Como argumentam Steinmetz, Pimentel e Goe (2019), a engenharia social é considerada como umas das mais expressivas ameaças à segurança da informação.

A engenharia social não consiste no uso de tecnologia avançada, mas na exploração psicológica, onde os atacantes, denominados engenheiros sociais, utilizam técnicas para obter acesso às informações privadas e confidenciais (LUO et al, 2011). Com ela é possível obter dados sobre as vítimas, de modo a possibilitar a infiltração de softwares maliciosos nos ambientes corporativos (POLLACK, RANGANATHAN, 2018). A engenharia social se aproveita de características humanas, como a tendência das pessoas em confiar e cooperar com outros indivíduos, e de ter curiosidade sobre determinado assunto (CONTEH, SCHMICK, 2016). Um engenheiro social consegue contornar soluções de segurança cibernética avançadas e persuadir um indivíduo, a fim de revelar informações sensíveis, tais como senhas, credenciais de acesso e documentos restritos (POLLACK, RANGANATHAN, 2018). Gupta (2009) argumenta que a natureza humana e as interações sociais são mais fáceis de se manipular do que as modernas proteções tecnológicas encontradas nos ambientes computacionais. Se antes era necessária a presença física do atacante para efetuar um ataque, a ampla gama de dispositivos móveis e de meios de comunicação presentes nas organizações permite a execução remota de ataques. O uso disseminado de *email*, redes sociais e aplicativos de mensagens instantâneas facilitam o ataque do engenheiro social, e abre novas frentes de ataque que antes não existiam. A questão se agrava pelo fato de, no ambiente cibernético, ser difícil a separação entre a dimensão humana e a tecnológica. Quanto a isso, Mitnick (2003) afirma que muito se investe no desenvolvimento de soluções de segurança cibernética,

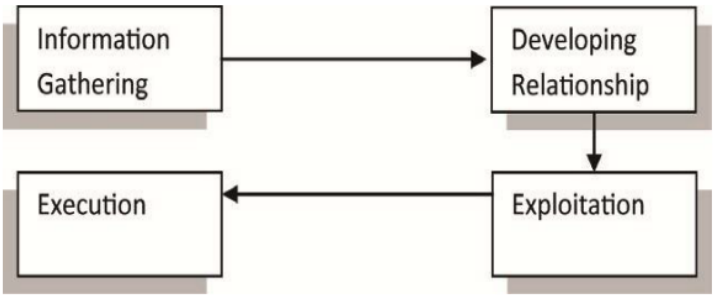
mas pouco na proteção da dimensão humana no espaço cibernético. Segundo Pollack e Ranganathan (2018), o processo de segurança cibernética deve considerar não apenas aspectos técnicos, mas também dimensão humana. Nesse contexto, Rhee, Kim e Ryu (2009) afirmam que no passado a segurança da informação era considerada uma questão essencialmente técnica e, portanto, apenas pessoal técnico era contratado pelas organizações. Esse fato fez com que as empresas subestimassem a dimensão humana em seus processos internos de segurança cibernética (RHEE, KIM; RYU, 2009).

A crescente integração e dependência das novas tecnologias digitais, aliada à evolução dos métodos de ataques de engenharia social, tornam a proteção dos indivíduos um desafio (ALDAWOOD, SKINNER, 2019). Ao passo que avanços são realizados no desenvolvimento de soluções de segurança mais robustas, os atacantes tendem a explorar mais a dimensão humana. Sem a consciência dos indivíduos sobre o quão expostos estão à engenharia social, o combate a esse método de ataque se torna mais difícil (CONTEH, SCHMICK, 2016). Soma-se a isso o fato de os atacantes se adaptarem a cada nova medida de proteção adotada pelas organizações, desenvolvendo técnicas com as quais as empresas não estão familiarizadas.

Em se tratando de segurança cibernética, não há como garantir a completa proteção do ambiente, pois em todas as organizações há pessoas passíveis de iniciar ou facilitar um ataque, mesmo sem intenção (ZULKURNAIN et al, 2015). O foco de diversas organizações é a segurança cibernética orientada à proteção de redes e sistemas digitais, contudo muitos ataques cibernéticos ocorrem pela exploração da dimensão humana (NAUMOVSKI, TANESKI, 2019). Sofisticados sistemas de segurança não podem proteger os ambientes de ataques aparentemente legítimos, que utilizam, por exemplo, credenciais de acesso válidas (CONTEH, SCHMICK, 2016). Independentemente do quão elaborada é a infraestrutura tecnológica baseada em *firewall*, criptografia e sistemas antivírus, a engenharia social é capaz de desafiar a segurança cibernética (SALAHDINE, 2019). Quando se trata de segurança cibernética, o indivíduo é o elo mais fraco de toda organização (ALDAWOOD, SKINNER, 2019).

Como meio de organizar a estrutura de um ataque de engenharia social, Luo et al (2011) realizam uma divisão de quatro fases, geralmente utilizadas por engenheiros sociais em suas ações, conforme figura 3.

Figura 3 - Fases de um ataque de engenharia social



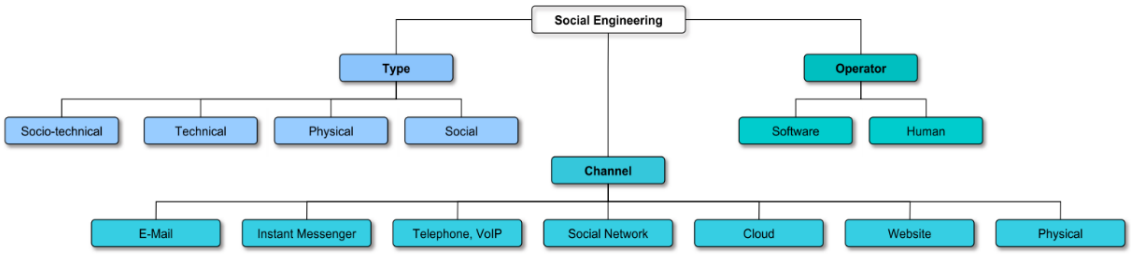
Fonte: Luo e al (2011)

A primeira fase do ataque (*information gathering*) tem por base o estudo e a aquisição de informações sobre o indivíduo alvo, onde uma profunda prospecção é realizada em redes sociais, *sites* corporativos e mecanismos de busca. Em seguida, uma relação de confiança é estabelecida entre o atacante e a vítima, seja por interação direta por voz, email ou pessoalmente (*developing relationship*). O passo seguinte é a exploração, onde ocorre o acesso aos sistemas alvo, infectando um recurso computacional ou obtendo informação sensível da vítima (*exploitation*). Por fim, a última fase se caracteriza pela execução da ação (*execution*). Quando associado com ataques cibernéticos, o uso da engenharia social pode ter consequências diversas, como o roubo de informações confidenciais ou o desligamento de equipamentos e sistemas.

2.2 Taxonomia da engenharia social

A capacidade de perceber e identificar ataques de engenharia social é fator essencial para a segurança de um ambiente crítico. Os ataques incluem aspectos físicos, sociais e técnicos, que podem ser utilizados em diferentes estágios de um ataque cibernético (KROMBHOLK et al, 2015). Partindo desse princípio, Krombholtz et al (2015) elaboraram a taxonomia da engenharia social, a fim de organizar os diversos aspectos relacionados à área. Para os métodos de ataques de engenharia social, três categorias foram definidas: método, operador e canal. A figura 4 exibe a organização idealizada pelos autores.

Figura 4 - Taxonomia da engenharia social



Fonte: Krombholz et al (2015)

A primeira categoria trata do método de emprego da engenharia social, cuja classificação encontra-se dividida em quatro abordagens. A abordagem física está relacionada a alguma ação de coleta de informações sobre o alvo. Para se obter informações como endereços, credenciais de acesso e números de documentos, o atacante pode examinar o lixo produzido por uma organização, onde eventualmente podem ser encontrados manuais, documentos oficiais, fichas de funcionários, cartões, entre outros objetos físicos descartados sem a devido tratamento de segurança da informação (KROMBHOLTZ et al, 2015). Soma-se a isso a possibilidade de prospecção de insumos de informática, como *pendrives*, discos rígidos e demais dispositivos de armazenamento.

Outra abordagem adotada pelos autores se refere ao social, onde o atacante utiliza métodos psicológicos, como a persuasão, para manipular as vítimas. Assim, o engenheiro social procura estabelecer uma relação de confiança e de credibilidade com a vítima alvo, a fim de coletar informações. Na abordagem técnica não há o contato com a vítima. A intenção, nesse caso, é coletar a maior quantidade possível de informações de modo não presencial, especialmente via Internet. Redes sociais, fórum e blogs são campos de pesquisa para o engenheiro social. A fim de analisar a grande quantidade de dados disponíveis, ele pode utilizar ferramentas de *Big Data* para filtrar e extrair informações úteis para o ataque. Por fim, a abordagem sociotécnica combina as abordagens anteriores para tornar os ataques mais efetivos. A coleta de informações pessoais na Internet, por meio da abordagem técnica, pode ser conjugada com as informações coletadas no descarte de material corporativo. Juntas, essas duas abordagens auxiliam o ataque, onde o engenheiro social pode realizar, por exemplo, um contato telefônico com o alvo usando informações previamente adquiridas.

No que tange os canais utilizados em ataques de engenharia social, Krombholtz et al (2019) adotam sete classes: *email*, aplicativos de mensagens

instantâneas, telefone e VOIP[12], redes sociais, nuvem, *sites* e físico. Para os autores, o *email* é o mais comum dos canais utilizados, enquanto os aplicativos de mensagens instantâneas são úteis para envio de *links* maliciosos. Ligações telefônicas, seja pelos meios telefônicos tradicionais, seja por meio de VOIP, tal como o uso de software *Skype* e similares, são adequados para se estabelecer uma relação direta com a vítima. As redes sociais são importantes fontes de informações pessoais, que podem ser vantajosas para se criar uma relação de confiança. Os serviços na nuvem podem servir como repositório de arquivos, utilizados como auxiliar em outros ataques, como no envio de *links* maliciosos para o *email* da vítima, que apontam para documentos infectados na nuvem. O uso de *sites* pode ser usado como coadjuvante de outros ataques, onde um *site* falso é criado com o intuído de simular uma página legítima. Existe, ainda, a possibilidade de o engenheiro social agir de modo presencial, face a face com a vítima (KROMBHOLTZ et al, 2015).

No que se refere a classificação de operador, o ataque pode ser originado de humanos ou de software. No primeiro, o ataque é conduzido diretamente por um indivíduo, todavia, a capacidade de ataques simultâneos se torna limitada. Por outro lado, os ataques podem ser automatizados por *softwares*, o que possibilita ataques a múltiplos alvos em um curto período (KROMBHOLTZ et al, 2015).

2.3 Comportamentos sociais e a influência da engenharia social sobre os indivíduos

A exploração de aspectos comportamentais é processo basilar nos ataques de engenharia social. Mitnick (2003) argumenta que as pessoas têm maior empatia por alguém que se diz colega de trabalho, ou que conheça os procedimentos e a linguagem da organização. Um método simples de ataque consiste no engenheiro social aparentar ser um funcionário da área de suporte de informática. Assim, de posse do papel de especialista, e utilizando um jargão técnico, ele pode recomendar uma atualização de *software* corporativo. Nesse cenário, é possível que o atacante envie um aplicativo para a vítima, com a justificativa de que a instalação trará benefícios, como o aumento da segurança

[12] A transmissão de voz por uma rede de dados como Internet é denominada de VOIP, acrônimo de *Voice Over Internet Protocol*. No setor de tecnologia é também denominada de Telefonia IP.

do computador contra supostos vírus. O *software* disponibilizado à vítima, no entanto, pode ser um *spyware*[13], cuja consequência, em certos casos, se traduz no roubo de senhas, do histórico de *sites* visitados, de conversas em *chats*, mensagens instantâneas e email. Além disso, o *software* malicioso pode ser capaz de capturar o som ambiente por meio do microfone, assim como gravar imagens utilizando uma *webcam*[14]. Podem surgir janelas no navegador, a fim de motivar a vítima a clicar em propagandas maliciosas. *Sites* falsos podem simular a aparência de um serviço legítimo, como um correio eletrônico, fazendo a vítima digitar suas credenciais de acesso por acreditar estar diante do *site* verdadeiro. Dependendo do *malware* utilizado, o atacante pode obter controle dos computadores com o uso de RAT[15].

Outro método adotado pelos engenheiros sociais consiste em ajudar a vítima na resolução de algum problema, possivelmente causado pelo próprio atacante. A vítima, agradecida pelo auxílio, estará mais suscetível a passar alguma informação de alto valor (MITNICK, 2003). Pode ocorrer de o engenheiro social se passar por alguém com autoridade, com nível hierárquico superior dentro da estrutura da organização, e intimidar a vítima para que ela execute alguma ação. Outra possibilidade é deixar propositalmente um *pendrive*, contendo *software* malicioso, em um local onde a vítima possa encontrá-lo e, eventualmente, levá-lo para dentro da organização (MITNICK, 2003). Nesse caso, por não envolver contato direto, o atacante se protege com o anonimato.

Os métodos citados no parágrafo anterior são apenas um subconjunto dentre vários possíveis. Há de se analisar algumas razões pelas quais tais ataques obtêm sucesso. Em um primeiro momento, poder-se-ia considerar difícil manipular os indivíduos em grau suficiente para que ocorresse a colaboração com o atacante. Nesse ponto, cabe compreender alguns comportamentos que facilitam a aplicação da engenharia social. Para Nohlberg (2009), o ato de solicitar algo com gentileza, e de justificar a necessidade da solicitação, pode funcionar como catalizador para que a tarefa seja executada. Um atacante que faça contato de modo educado com a vítima, e diga a razão pelo qual está pedindo determinada ação, terá mais chance de sucesso. Outro comportamento social se refere ao fato

[13] *Spyware*: software especializado em monitorar de modo oculto as atividades realizadas em um computador.
[14] *Webcam*: câmera de vídeo de pequena dimensão utilizada em computadores.
[15] RAT: acrônimo de *Remote Access Trojan*. Trata-se de malware que permite o controle remoto de um dispositivo, tal como computador ou *smartphone*.

de as pessoas pouco demonstrarem suas emoções no ambiente de trabalho (MITNICK, 2003). Por esse fato, o engenheiro social, ao simular fragilidade e dúvida, pode sensibilizar a vítima, tornando-a emocionalmente envolvida com a situação, o que favorece o ataque.

Uma análise mais completa dos comportamentos sociais capazes de influenciar os indivíduos é descrita por Cialdini (2009). O autor relaciona seis técnicas de influência que podem ser adotadas por engenheiros sociais em ataques orientados aos funcionários de uma organização. A primeira técnica se refere à autoridade. De acordo com Cialdini (2009), os indivíduos tendem a obedecer a autoridade, pois geralmente são condicionados a respeitar a hierarquia e as pessoas que detém maior nível de conhecimento. Caso os processos decisórios nas organizações não estejam corretamente mapeados e assimilados pelos funcionários, um atacante pode se passar por um profissional especializado, e demandar uma ação capaz de gerar prejuízos ao ambiente. Soma-se a isso o fato de que, lidando com grande volume de informação e com pouco tempo disponível para refletir, a capacidade do indivíduo de realizar uma avaliação crítica sobre a situação torna-se reduzida. No âmbito da CNAAA, o engenheiro social pode, por exemplo, se apresentar como uma pessoa de hierarquia mais alta, e exigir da vítima uma ação operacional imediata. O fato de o interlocutor conhecer o nome de funcionários ou os procedimentos corporativos não garante que ele seja quem alega ser, assim como não o habilita a receber informações internas ou a acessar equipamentos e sistemas (MITNICK, 2003).

Na técnica da escassez, quando informadas de que algo é escasso, as pessoas tendem a querer ainda mais determinado produto ou serviço (CIALDINI, 2009). Isso se relaciona com o senso de competição, onde a escassez pode significar que bens mais difíceis de se obter são mais valorizados do que aqueles mais fáceis. Historicamente, existe a percepção de que os bons produtos e serviços são exclusivos e em quantidade limitada. Um email malicioso enviado para um funcionário da CNAAA pode apresentar uma promoção de um produto em quantidade limitada. Movido pelo senso de urgência e pela pressão do pouco tempo para tomar a ação, o funcionário pode, sem medir as consequências do ato, clicar em um *link* malicioso e infectar o computador do setor administrativo da usina, possibilitando ataques cibernéticos subsequentes.

A técnica denominada afeição se aproveita do fato de os indivíduos serem propensos a reagir favoravelmente a uma pessoa semelhante a eles (CIALDINI, 2009). Essa semelhança pode ser de várias categorias, incluindo o modo como uma pessoa se veste, seus antecedentes ou interesses. Se houver uma situação em que a semelhança converge para uma cooperação mútua, onde ambos poderão obter benefícios, a identificação entre os indivíduos tende a aumentar. Esses mecanismos são utilizados para criar empatia entre o atacante e a vítima. Um atacante pode, previamente, obter nas redes sociais informações sobre um funcionário da CNAAA, como estilo de música preferido, viagens realizadas e animais de estimação. Essas informações podem ser utilizadas para a elaboração de um *email* malicioso personalizado para a vítima, que tenderá a se identificar com o conteúdo da mensagem, alinhado aos seus gostos pessoais. Em uma interação por telefone, o interlocutor pode direcionar a conversa de acordo com as características físicas e sociais da vítima, tornando-a mais receptiva a tomar ações para as quais não está autorizada a executar no ambiente de uma usina nuclear.

A técnica seguinte citada por Cialdini (2009) se refere à reciprocidade. Nesse mecanismo social, ao se fazer um favor a alguém, existe a necessidade de retribuir o favor, mesmo que a pessoa não seja solicitada para tal. Para Cialdini (2009), a necessidade de reciprocidade transcende questões culturais, distâncias físicas e interesses pessoais. Nessa lógica, um atacante pode realizar um pequeno favor à vítima, e em seguida solicitar informações privilegiadas. Um engenheiro social pode causar um problema no computador de um funcionário e, por telefone, se identificar como um especialista do setor técnico da Eletronuclear. Em seguida, o atacante pode resolver o problema, de modo que a vítima, agradecida pela rápida resolução da questão, ficará mais propensa a retribuir o favor. Nesse momento, o atacante pode solicitar alguma informação sensível sobre a CNAAA.

O mecanismo denominado aprovação social ocorre quando as pessoas precisam tomar uma decisão sobre uma situação e, por não terem certeza de como agir, observam e atuam conforme outras pessoas nas proximidades (CIALDINI, 2009). Esse mecanismo pode facilitar a ação dos engenheiros sociais, pois caso os funcionários compartilhem senhas corporativas, em desacordo com normas internas, um atacante poderá conseguir essa informação via engenharia

social. Um novo funcionário na organização observará o comportamento dos colegas mais antigos e, se não houver treinamento adequado sobre a prática da segurança no ambiente de trabalho, poderá adotará as práticas tácitas, ao invés de seguir as orientações formais. Nesse caso, o agravante, segundo o Cialdini (2009), é o fato de as pessoas demonstrarem pouco interesse em questões nas quais não estão diretamente envolvidas.

Denominado de compromisso e coerência, esse método se refere ao desejo de uma pessoa em ser ou parecer coerente com algum compromisso ou ideia assumida. De acordo com Cialdini (2009), após ter escolhido uma opção, ou firmado um compromisso com alguém, a tendência é que a pessoa permaneça com a decisão ou promessa inicial. Portanto, se um funcionário assume um compromisso com alguém, é provável que ele se esforce para cumprir esse compromisso. Os engenheiros sociais utilizam esse mecanismo para criar uma situação em que o funcionário se compromete a realizar algo, como acessar um sistema ou passar alguma informação. Mesmo que, após certo tempo, o funcionário considere a decisão equivocada, o fato de ter assumido o compromisso com alguém dificulta uma ação contrária.

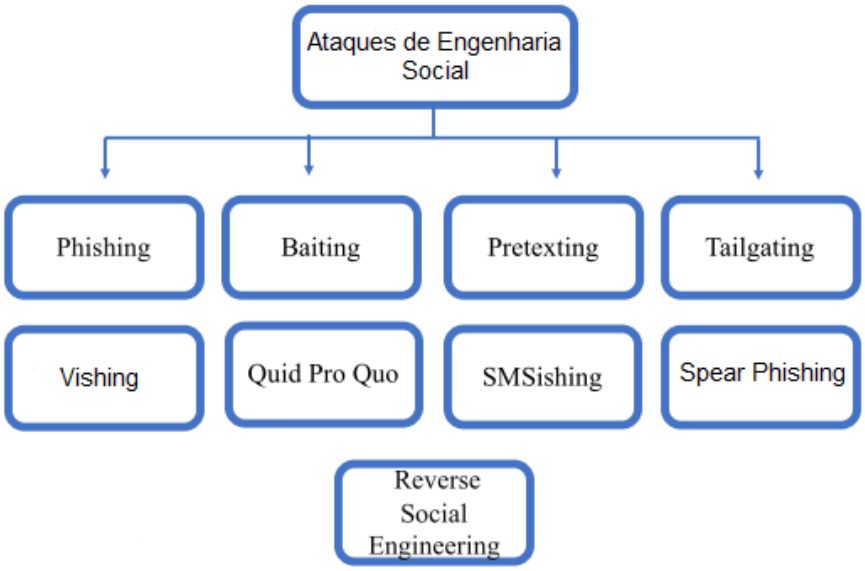
2.4 Métodos de ataques de engenharia social aplicados ao setor nuclear

Ataques de engenharia social podem ocorrer nas mais diversas áreas de uma instalação nuclear. Aproveitando-se das técnicas elencadas por Cialdini (2009), os engenheiros sociais tendem a escolher aquelas mais adequadas à estratégia elaborada. Se a intenção é roubar informações de um banco de dados corporativo, o atacante direcionará o ataque aos indivíduos que possuem permissões administrativas. Se o atacante deseja o controle de um sistema supervisório, ele tentará obter as senhas dos indivíduos responsáveis pela operação dos sistemas na sala de controle.

Os ataques de engenharia social são amplos e com diversos níveis de complexidade. Alguns não se relacionam diretamente com a cibernética, como o *dumpster diving*, que consiste em vascular o lixo produzido pelos funcionários em busca de documentos relevantes, ou o *shoulder surfing,* onde os engenheiros sociais observam discretamente um indivíduo durante a digitação de uma senha. Dentre os diversos ataques de engenharia social existentes, serão apontados

nesta pesquisa nove métodos apresentados por Slahdine (2019), conforme mostra a figura 5. Uma vez que existe a possibilidade de que alguns desses ataques sejam utilizados contra os funcionários da CNAAA, torna-se relevante sua compreensão.

Figura 5 - Métodos de ataques de engenharia social



Fonte: Adaptado de Slahdine (2019)

2.4.1 *Phishing*

Os primeiros ataques de *phishing* datam da década de 1990, quando o método foi utilizado para realizar roubo *online* de contas de cidadãos norte-americanos (KAY, 2014). Pela semelhança com o ato de pescar, onde a isca é jogada na água à espera de que um peixe a fisgue, esse método de ataque foi denominado *phishing*, e permanece como um dos grandes vetores de ataques cibernéticos. O modo tradicional de ataque *phishing* consiste em utilizar o serviço de correio eletrônico para enviar *emails* com *links* ou arquivos maliciosos. Assim, um atacante pode enviar um grande volume de *emails* para endereços eletrônicos de usuários aleatórios na Internet, cuja mensagem pode ser, por exemplo, uma propaganda ou uma promoção.

Embora o ataque use o princípio do SPAM[16], o *phishing* não se propõe a fazer propaganda de um produto ou serviço, mas de induzir a vítima a tomar uma atitude diante do *email* recebido. Esse método de ataque se inicia com uma pesquisa na Internet por dados pessoais de funcionários de determinada organização, de modo a entender o melhor modo de enganá-los (ALI, 2015). A técnica é capaz de criar nos indivíduos um estado psicológico de pouca reflexão, motivando a adoção de uma postura pouco conservadora na análise da veracidade das informações contidas na mensagem (GAO et al, 2010). Um funcionário pode, sem perceber a intenção do atacante, clicar em um *link* que o levará a acessar um *site* infectado, ou a realizar o *download* de arquivos que supostamente contém fotos ou informações confidenciais, mas que, na realidade, possuem *malware*s tais como *ransomware*[17] e vírus. De acordo com Abraham e Chegalur (2010), o *phishing* é o ataque predominante quando se trata de engenharia social. Ao receber um *email* semelhante ao do suporte técnico da empresa, onde seja solicitado acesso remoto, é provável que esse usuário considere o procedimento verídico (OWEN-JACKSON; CASEY, 2020).

O *phishing*, portanto, não se restringe a mensagens inoportunas. Trata-se de um vetor de ataque eficiente, cuja função é facilitar ataques cibernéticos (DAS et al, 2019). Para Das (2019), o sucesso do ataque é diretamente proporcional ao quão estruturada e verossímil é construída a interação entre o atacante e a vítima. Essa interação pode ocorrer tanto no meio digital, quanto por uma interação presencial. O *phishing* também pode ser usado para simular o acesso à serviços legítimos, como ocorre no “Dropbox/Google *phishing*”, onde a vítima recebe um *email* forjado do serviço Dropbox ou do Google, alertando para mudanças na política de segurança, ou relatando haver pouco espaço disponível para armazenamento (VARVARA, 2018). Ao clicar no *email*, a vítima é direcionada para uma página falsa, com as características de layout semelhante à página original. Ao informar *login* e senha, essas informações são capturadas e o indivíduo é imediatamente redirecionado para a página verdadeira do serviço. Pode ocorrer de o indivíduo não perceber que utilizou um *site* falso, e considerar

[16] SPAM se refere a emails não solicitados enviados para muitos destinatários.
[17] *Ransomware* são softwares maliciosos capazes de criptografar dados da vítima, de modo a torná-los inacessíveis. Geralmente é exigido um pagamento em moeda digital para que os dados sejam desencriptados.

que a requisição subsequente das credenciais se deu por uma digitação errada da senha na primeira tentativa.

2.4.2 *Spear Phishing*

Diferentemente do *phishing*, o ataque de *spear phishing* é mais difícil de ser mitigado e é mais efetivo que o *phishing* tradicional (DAS et al, 2019). Neste ataque, a mensagem contida no *email* é elaborada de modo personalizado, a fim de apresentar maior afinidade com as preferências da vítima. Trata-se, portanto, de um ataque com um alvo específico.

Ao acreditar estar diante de uma fonte confiável, a vítima, em geral, não atesta a veracidade da mensagem. Assim, uma mensagem forjada que contenha dados pessoais e informações de interesse tem maior possibilidade de ser lida e interpretada como legítima. Para elaborar uma mensagem personalizada, o engenheiro social pode coletar informações sobre a vítima em redes sociais, mecanismos de busca e fóruns na Internet. De posse dessas informações, a mensagem é elaborada com um conteúdo com o qual a vítima se identifica. De acordo com Das et al (2019), esse ataque é comumente direcionado para indivíduos que possuam posições chave dentro de organização, seja porque detenham permissões a sistemas relevantes, seja porque pertençam ao quadro de direção executiva, que detém informações privilegiadas. Para Ford (2017), o ataque de *spear phishing* representa a maior ameaça para as usinas nucleares no campo cibernético.

2.4.3 *Vishing*

O *vishing* é uma concatenação das palavras *voice* e *phishing*. A principal característica desse ataque é utilizar o meio telefônico para obter informações da vítima. Uma ligação automatizada, isto é, com uma mensagem previamente gravada, é realizada pelo engenheiro social para um funcionário dentro da organização alvo. O conteúdo da ligação indica uma ação a ser feita, como ligar para um número de telefone (YEABOAH-BOATENG; AMANOR, 2014).

Como exemplo, cita-se um cenário onde um funcionário da CNAAA recebe uma ligação telefônica automática, cuja mensagem informa que o serviço de

atendimento de informática da Eletronuclear tentou entrar em contato sem sucesso, e pede retorno do usuário para resolver problema de conexão. Dependendo do quão bem estruturada e convincente estiver a narrativa, a vítima pode retornar à ligação sem verificar se o número telefônico pertence, de fato, à empresa. Nesse momento, o atacante, ou uma gravação automática, pode interagir com a vítima, solicitando informações específicas, como credenciais de acesso e demais informações sensíveis. Ao utilizar o telefone para realizar a engenharia social, o atacante consegue burlar as possíveis proteções contra *phishing* do serviço de correio eletrônico da organização. Uma vez que diversos sistemas de telefonia utilizam redes de dados para a realização de ligações, o *vishing* pode ser considerado como pertencente ao ambiente cibernético.

2.4.4 *Smishing*

O termo é uma combinação da sigla SMS [18] com a palavra *phishing*. Esse ataque se assemelha ao *phishing*, diferenciando-se apenas no processo de interação. Ao invés de um *email*, o atacante usa como vetor de ataque mensagens SMS. Esse método de ataque é considerado mais perigoso do que o *phishing,* na medida que os indivíduos tendem a acreditar mais em mensagens recebidas em seu telefone celular do que em emails recebidos via correio eletrônico (NORTON, 2019?). Além disso, os indivíduos acreditam que os smartphones são mais seguros do que os computadores (KASPERSKY, 2019). Ao tomar a ação proposta pela mensagem, como clicar em um *link* contido no SMS, o usuário pode expor seu dispositivo à entrada de *malware*s, que poderão se apropriar de funcionalidades do aparelho, como câmera e microfone. Com a disseminação de aplicativos de mensagens, a abrangência desse método de ataque aumentou, estendendo-se para além do SMS. Considera-se, ainda, que o uso de *smartphones* no ambiente de trabalho, denominado BYOD [19], aumenta o risco de danos ao ambiente computacional das organizações (KASPERSKY, 2019). Isso ocorre pois, em certos casos, os funcionários utilizam o dispositivo pessoal na

[18] SMS: acrônimo de Short Message Service
[19] BYOD: acrônimo de *Bring your own Device*. Trata-se de uma política adotada por algumas organizações que permite que os dispositivos pessoais dos funcionários possam acessar informações corporativas no local de trabalho, utilizando a infraestrutura da organização.

rede corporativa para acessar arquivos e *emails*, ou o conectam diretamente no computador da empresa para carregar a bateria do dispositivo.

2.4.5 *Pretexting*

Esse método de ataque pretende criar uma história que possua argumentos bem estruturados, que possam ser confundidos com uma história verídica (BISSON, 2015). Eles são baseados em pretextos, que fazem a vítima acreditar no engenheiro social. A ideia é criar um senso de urgência para se obter informações que, de outro modo, não seriam obtidas. Assim, o atacante pode ligar para o setor de engenharia da CNAAA, se identificar como assessor da diretoria, e solicitar informações específicas sobre um funcionário, argumentando que seu superior hierárquico precisa imediatamente da informação. Considerando, hipoteticamente, que a resposta contenha informações relevantes, o atacante pode posteriormente executar um ataque de *spear phishing* direcionado ao funcionário.

2.4.6 *Baiting*

Nessa categoria de ataque, um dispositivo contaminado por *malware*, como um *pendrive*, é deixado propositalmente em um lugar propício a ser encontrado, tal como o estacionamento ou a entrada da organização alvo. Caso um funcionário encontre o dispositivo, existe a possibilidade de que ele o conecte a um computador da empresa, contaminando o ambiente computacional (WATSON; MASON; ACKROYD, 2014). O fato de as portas USB dos computadores fornecerem energia faz com que os funcionários as utilizem para carregar a bateria dos dispositivos móveis, como celulares. Porém, quando um dispositivo é conectado a uma porta USB, pode ocorrer simultaneamente uma transferência de dados, que pode acarretar na contaminação do computador por *malware*s (BOCK, 2016). Outros dispositivos de uso cotidiano podem ser utilizados para disseminar *malware*s via portas USB, como teclados e mouses, o que dificulta a identificação da fonte de ataque (PEREKALIN, 2019).

2.4.7 *Quid pro quo*

Trata-se de uma variante ao *baiting*, porém, ao invés de oferecer bens, o atacante oferece serviços ou benefícios em troca de informações (PAGANINI, 2019). Um funcionário da CNAAA pode, por exemplo, receber uma ligação telefônica de um falso profissional do setor de informática, induzindo-o a instalar determinado aplicativo com a promessa de que novas funcionalidades serão habilitadas no computador.

2.4.8 *Tailgating*

Conhecido também como *piggybacking*, o *tailgating* utiliza a distração ou a boa vontade dos indivíduos para acessar, sem permissão, áreas restritas (SALAHDINE, 2019). Um exemplo desse ataque ocorre quando o atacante precisa passar por um sistema físico de segurança. O engenheiro social pode aproveitar o momento em que um funcionário abre uma porta para, rapidamente, passar antes do fechamento, tirando vantagem da distração do funcionário. Em um sistema de catracas, o atacante pode se aproximar do dispositivo carregando uma caixa pesada. Ao simular dificuldade para pegar o crachá, ele pode ter o acesso liberado por guardas ou recepcionistas que, ao se solidarizar com o atacante, burlam o procedimento padrão de segurança do local. Mesmo que por meio desse método os atacantes não consigam acesso ao interior das usinas, eles podem conseguir acesso aos setores menos críticos da CNAAA, como o estacionamento e o centro de visitantes, onde podem disseminar dispositivos para realizar ataques *baiting*.

2.4.9 *Reverse Social Engineering*

Nesse método de ataque, o indivíduo alvo é convencido de que há um problema em que o atacante é o único capaz de resolvê-lo. Geralmente o ataque consiste em causar dano a um equipamento, convencer a vítima de que o somente o atacante tem a capacidade de resolver rapidamente a situação e, por fim, obter acesso a informações sensíveis (SALAHDINE, 2019).

2.5 Histórico de incidentes decorrentes de ataques de engenharia social

A engenharia social tem sido utilizada na maioria dos ataques cibernéticos (PROOFPOINT, 2019). Em entrevista para esta pesquisa, Ricardo Gonzaga[20] cita que as consequências mais comuns em ataques de engenharia social são o roubo de credenciais de acesso e de dados sensíveis. Para tanto, o entrevistado aponta que os métodos de *phishing*, *spear phishing*, *vishing* e *pretexting* são os mais utilizados pelos engenheiros sociais.

Em 2011, um ataque cibernético à empresa RSA, especializada em segurança da informação, provocou o vazamento de diversos dados sensíveis (WATSON; MASON; ACKROYD, 2014). O vetor de ataque foi um *email* enviado aos funcionários da empresa, contendo um arquivo anexo infectado. O arquivo permitiu aos atacantes acesso ao ambiente computacional interno da empresa. A partir dos dados coletados no ataque, os atacantes conseguiram roubar informações da empresa *Lockheed Martin*, fornecedora de produtos militares para o governo norte-americano.

Dois anos após o ataque à RSA, a empresa Target Corporation foi vítima de ataque cibernético, cujo resultado foi o roubo de 40 milhões de números de cartão de crédito e 70 milhões de registros de informações pessoais. O ataque se originou a partir uma empresa prestadora de serviço, a *Fazio Mechanical Services*, responsável pela manutenção dos sistemas de climatização da Target. Os atacantes, por meio do envio de um *email* infectado, conseguiram acesso à rede interna da empresa terceirizada. Como a empresa *Fazio* estava diretamente conectada à Target por um *link* de dados, os atacantes conseguiram realizar o ataque (SHU et al, 2017).

O *Oak Ridge National Lab*, laboratório de ciência e tecnologia norte-americano, patrocinado pelo Departamento de Energia dos Estados Unidos, foi vítima de um ataque cibernético em 2011. O ataque inicial se deu por meio do método de *spear phishing*, onde um *email* forjado como originário do departamento de recursos humanos foi enviado para um grupo de funcionários. Dos cinco mil funcionários, em torno de 530 receberam o email e 57 abriram o *link* malicioso contido na mensagem, sendo que dois computadores foram infectados.

[20] Entrevista realizada em fevereiro de 2020.

Vários dados foram roubados antes que as equipes e segurança conseguissem desconectar o ambiente da Internet (VAN DINE; ASSANTE; STOUTLAND, 2016).

Em 2014, houve um ataque à empresa sul coreana *Korea Hydro and Nuclear Power Company*, responsável por 23 reatores nucleares. Os atacantes utilizaram estratégia de *phishing* para inserir o *malware* dentro da companhia. A partir da invasão, conseguiram roubar as plantas e manuais de duas usinas nucleares, além de dados sobre a radiação nas áreas adjacentes às usinas e informações pessoais de dez mil funcionários. O grupo publicou algumas informações na rede social Twitter, e exigiu que três reatores nucleares fossem desligados (VAN DINE; ASSANTE; STOUTLAND, 2016).

Um ataque baseado em *spear phishing* ocorreu em 2016, no *Hydrogen Isotope Research Center*, da Universidade de Tayama, no Japão. Em um *email* direcionado aos funcionários do centro de pesquisa, atacantes se passaram por estudantes da Universidade de Tóquio em busca de respostas para algumas questões científicas. O *malware* contido no *email* permitiu o roubo milhares de arquivos, incluindo os resultados de pesquisas sobre a água contaminada da usina nuclear de Fukushima, além de informações pessoais de 1500 pessoas que colaboraram com a universidade (VAN DINE; ASSANTE; STOUTLAND, 2016).

Os casos apresentados revelam que ataques de engenharia social podem transpor barreiras de segurança de diferentes setores de um país. Mesmo que um ataque de engenharia social não impacte diretamente a operação de equipamentos críticos, a perda de informações sensíveis pode resultar em risco para a segurança da organização. Com as informações coletadas, os atacantes passam a dispor de maior conhecimento sobre o ambiente, o que facilita ataques cibernéticos futuros. Além disso, a imagem da organização e a confiança da população também podem ser afetadas se informações críticas forem expostas na Internet ou na mídia.

2.6 A dimensão humana e sua vulnerabilidade à engenharia social

O propósito desse capítulo foi verificar como a dimensão humana pode ser vulnerável à engenharia social. Observou-se que apenas medidas de ordem tecnológicas não são suficientes para proteger o ambiente cibernético das usinas nucleares. Visto que engenheiros sociais são potencialmente capazes de burlar

soluções tecnológicas, cabe às organizações adotar outros métodos para se proteger de ataques de engenharia social. Neste capítulo, também foram estudadas as fases, a taxonomia e os métodos de ataques engenharia social. Com esse entendimento será possível analisar, no próximo capítulo, os procedimentos utilizados contra ataques de engenharia social, e será verificado se as medidas de segurança cibernética adotadas na CNAAA são adequadas para a mitigação de ataques dessa natureza.

CAPÍTULO 3 – A SEGURANÇA CIBERNÉTICA DA CNAAA: MITIGAÇÃO DE ATAQUES DE ENGENHARIA SOCIAL

> As empresas gastam milhões de dólares em firewalls, criptografia e dispositivos de acesso seguro, mas seu dinheiro é desperdiçado porque nenhuma dessas medidas trata do elo mais fraco da cadeia de segurança: as pessoas que usam, administram, operam e respondem por sistemas de computadores que contêm informações protegidas. (Kevin Mitnick).

No âmbito dessa pesquisa, o interesse concentra-se nas usinas da CNAAA, que apresentam características distintas. Angra 1 e 2 entraram em operação na década de 80 e, além de dispositivos digitais, têm um legado de equipamentos analógicos em seu ambiente de produção. Por outro lado, o Brasil aceitou o desafio de retomar a construção de Angra 3, que irá ampliar a segurança energética do país e estimular investimentos no setor nuclear (FIRJAN, 2019). A usina terá equipamentos de instrumentação e controle digital no mesmo padrão dos projetos mais recentes de usinas nucleares do mundo (ELETRONUCLEAR, 2017). O estudo desenvolvido nessa pesquisa, portanto, pode colaborar não apenas para as atuais usinas em operação, mas futuramente para Angra III.

Neste capítulo, será analisado se as medidas de segurança cibernética adotadas pela CNAAA são adequadas para a mitigação de ataques de engenharia social. Contudo, antecedendo essa análise, é necessário examinar os procedimentos de segurança cibernética, encontrados na literatura e indicados por especialistas, que podem mitigar ataques dessa natureza.

3.1 Medidas de segurança cibernética para mitigação de ataques de engenharia social

Procedimentos para a proteção contra ameaças cibernéticas são aplicados em diversas organizações. O setor nuclear, contudo, tende a considerar o risco das ameaças cibernéticas relativamente baixo em comparação a outras ameaças de ordem física (BAYON; BRUNT; LIVINGSTONE, 2015). Soma-se a isso o fato de que os atacantes estão se tornando mais hábeis no uso da engenharia social (CONTEH; SCHMICK,

2016). Como visto no capítulo anterior, a engenharia social pode ser utilizada para adquirir informações sensíveis e explorar sistemas de segurança (ALI, 2015).

Apesar do esforço contínuo das organizações para melhorar a conscientização dos usuários, o número de incidentes causados por ataques de engenharia social tem aumentado, o que configura uma ameaça à segurança nas empresas (ABRAHAM; CHENGALUR, 2010). Nesse sentido, é importante verificar como as organizações podem utilizar medidas para mitigar ataques de engenharia social. Pollack e Ranganathan (2018) argumentam que procedimentos de segurança cibernética podem auxiliar na defesa contra ataques de engenharia social, mitigando alguns dos vetores de ataque padrão utilizados por engenheiros sociais. Nesta lógica, Abraham e Chengalur (2010) apontam que a identificação de estratégias de ataque é essencial para a elaboração de medidas de mitigação. Uma vez que a engenharia social pode facilitar ataques cibernéticos subsequentes, o estudo torna-se relevante no âmbito da CNAAA, pois as consequências de ataques cibernéticos em usinas nucleares podem variar desde a perda de informações confidenciais, ao desligamento do reator nuclear (CAMPBELL; SINGH, 2019). Em entrevista, Marcelo Branquinho[21] aponta que ataques a instalações industriais podem ter consequências imprevisíveis, pois caso o atacante obtenha as credenciais de acesso ao ambiente SCADA, ele poderá ter controle total sobre os sistemas. *Malware*s mais complexos, além de infectar o ambiente, podem tentar estabelecer uma conexão com a Internet, a fim de manterem contato com um computador externo de comando e controle do atacante.

Aliados à tecnologia, processos estruturados de segurança, formalizados em políticas e normas corporativas, podem auxiliar na gestão da segurança cibernética e mitigar ataques de engenharia social, uma vez que esses documentos fornecem orientações aos funcionários no que tange a segurança do ambiente cibernético (MITNIK, 2003). Nos itens a seguir serão elencados procedimentos que podem ser aplicados na mitigação de ataques de engenharia social. Para tanto, será adotada a estrutura organizada por

[21] Entrevista realizada em novembro de 2019.

Conteh e Schmick (2016), que se divide em procedimentos técnicos, educação e treinamento, auditoria, políticas de segurança cibernética e proteção física.

3.1.1 Procedimentos técnicos de segurança cibernética

Procedimentos técnicos são softwares, equipamentos e processos necessários para a construção de camadas de defesa usadas no ambiente cibernético. Ataques cibernéticos tradicionais, como as tentativas de capturar senhas, invasão de sistemas digitais, alteração de banco de dados e desfiguração de *sites*, podem ser mitigados, principalmente, com tecnologia (SLAHDINE, 2019). Em geral, para que os *malware*s utilizados em ataques de engenharia social tenham sucesso, é necessário que uma ação seja executada por um funcionário da organização. O que se tenta com medidas de segurança é evitar que um *malware* alcance os funcionários (ABRAHAM, CHENGALUR, 2010). Surge, assim, a importância em se adotar vária camadas de proteção (BRANQUINHO et al, 2014). Conteh e Schmick (2016) e CISA (2017) argumentam que *softwares* como *Intrusion Prevention System*[22] (IPS) devem ser instalados em todos os dispositivos. Soluções de *firewalls* podem ser implementados para controle do tráfego, tanto da rede administrativa, quanto do ambiente de operação (BRANQUINHO et al, 2014), sendo capazes de bloquear conexões de fontes externas não confiáveis, além de garantir visibilidade e controle sobre toda a organização (CISA, 2017). A adoção de medidas técnicas de segurança cibernética pode mitigar ataques de engenharia social na medida em que são criadas barreiras que dificultam, por exemplo, o uso de *phishing* e *spear phishing*.

Adotar uma política de classificação de dados, que auxilie na implementação de controles adequados para a divulgação de informações corporativas, é uma medida importante citada por Mitnick (2003). O ato de classificar as informações internas evita que elas sejam acessíveis por funcionários que não necessitem do acesso para a execução de suas atividades cotidianas. A técnica de segmentar as informações de acordo com o perfil de trabalho de cada funcionário é conhecido no setor de segurança da

[22] *Intrusion Prevention System* é um sistema de prevenção de intrusão que tem a capacidade de detectar e prevenir vulnerabilidades.

informação pelo termo “necessidade de saber” (MITNICK, 2003). Ao ter acesso apenas às informações relevantes ao seu trabalho, o funcionário tem menor possibilidade de passar informações sensíveis para um engenheiro social, o que mitiga ações de *spear phishing*. Contudo, é relevante que as empresas prestadoras de serviço, colaboradores externos, consultores e as pessoas que, de algum modo, têm acesso a informações corporativas sejam contempladas nas normas de segurança da organização (MITNICK, 2003).

Além do uso da tecnologia e de processos definidos, o papel dos funcionários é essencial para a segurança cibernética da organização. Cabe a eles verificar se os *sites* acessados na Internet, em especial os que exigem *login* e senha, exibem o logotipo https, que indica se tratar de uma conexão criptografada. Do contrário, as credenciais e dados de formulários percorrerão a Internet sem criptografia (MITNICK, 2003). Assim, uma interceptação dos dados entre a origem e o destino poderá capturar as informações e usá-las para futuros ataques, como *quid pro quo, reverse social engineering* e *pretexting*. É de responsabilidade dos funcionários observar se os *softwares* sugeridos por terceiros fazem parte do conjunto de aplicativos utilizados pela organização e se, de fato, a instalação é necessária. Nesse caso, um contato com a área de suporte e segurança da organização pode sanar quaisquer dúvidas e mitigar ações de engenharia social. Ao adotar um comportamento crítico em relação ao uso dos recursos computacionais, os funcionários podem diminuir o risco de serem explorado por métodos de engenharia social.

Quaisquer tentativas de instalação de *softwares* que não sejam contemplados nas listas de aplicativos permitidos pela organização, denominadas *whitelists*, devem monitoradas e bloqueadas (CISA, 2017). Dentre os procedimentos que podem ser implementados em um ambiente cibernético para mitigar ataques de engenharia social, Ricardo Gonzaga cita, em entrevista, a gestão de identidades, ferramentas *antispam*, autenticação de dois fatores[23] e controle de acesso. Segundo o entrevistado, a capacitação dos profissionais é essencial, pois qualquer proteção técnica pode falhar em algum momento. Nessa mesma linha, Marcelo Branquinho ressalta a importância do uso da autenticação de dois fatores para reforçar a segurança contra

[23] Processo de segurança que exige que os usuários forneçam dois meios de identificação antes de acessarem suas contas (BRASIL, 2019)

vazamentos de credenciais de acesso. Relacionado a isso está o uso de senhas no ambiente corporativo. Bayon, Brunt e Livingstone (2015) aconselham que as senhas padrão sejam trocadas no momento da instalação de novos equipamentos e sistemas, pois os fabricantes normalmente utilizam senha simples. A organização pode adotar medidas preventivas de proteção, como a troca periódica de senhas dos funcionários e o uso de filtros de *email* para evitar *phishing* (CONTEH, SCHMICK, 2016).

Uma vez que as unidades de armazenamento portáteis, como *pendrives*, podem ser utilizadas para inserir *malware*s em computadores, é conveniente que as portas USB sejam desabilitadas nos computadores corporativos (ABRAHAM; CHENGALUR, 2010). Assim, caso um funcionário seja vítima do método de *baiting,* e tente usar um dispositivo móvel em um computador, o conteúdo malicioso não contaminará o ambiente (ABRAHAM; CHENGALUR, 2010). Se o uso desses dispositivos for imprescindível, podem ser adotados *softwares* para análise do conteúdo quando o dispositivo for conectado ao computador. Isso pode ser feito com o uso de softwares antivírus, que devem ser periodicamente atualizados (BRANQUINHO et al, 2014). Todavia, a proteção por *software* não é completamente garantida, pois, caso o *malware* tenha sido criado especificamente para atacar determinada organização, ele pode não ser detectado pelos antivírus e demais *softwares* de segurança (WATSON; MASON; ACKROYD, 2014). A infecção de computadores por *malware* pode ser mitigada ao ser incluir na política de segurança a vedação de uso, por parte dos funcionários, de computadores e dispositivos pessoais conectados ao ambiente corporativo (SLAHDINE, 2019).

Conteh e Schmick (2016) apontam a importância de se segmentar o ambiente cibernético, principalmente com o uso de zonas desmilitarizadas (DMZ[24]), que são segmentos de rede separado da rede interna da organização, utilizados para alocar serviços de tecnologia da informação que possuem conexão direta com a Internet. Como exemplo, cita-se o *site* da organização que, por ser consultado externamente, aconselha-se ser alocado na DMZ. Seguindo esse raciocínio, não convém deixar um banco de dados nessa DMZ, pois os dados corporativos ficariam mais expostos a ataques originados da

[24] DMZ: acrônimo de *Demilitarized Zone*

Internet. Em tais circunstâncias, um atacante que obtivesse *logins* e senhas via engenharia social não conseguiria acesso aos sistemas críticos da organização, uma vez que tais sistemas não estariam expostos na Internet. Eduardo Izycki corrobora o conceito de segregação de redes em ambientes industriais, porém ressalta que é algo de difícil manutenção. No caso do uso de *firewalls*, Branquinho et al (2014) citam modelos específicos para sistemas SCADA, que podem ser implementados de modo a isolar e proteger a rede de produção, permitindo acesso somente aos usuários, aplicações e protocolos específicos e autorizados. Além da segmentação, é recomendável que o tráfego de rede seja criptografado, inclusive o tráfego da rede sem fio (BRANQUINHO et al, 2014).

Segundo Ricardo Gonzaga, o maior risco no uso de dispositivos móveis está nos controles dos equipamentos pelas empresas. Para o entrevistado, muitas empresas permitem que os funcionários utilizem dispositivos pessoais conectados à rede corporativa, o que acarreta uma complexa gestão da segurança. A fim de facilitar a gestão dos dispositivos, e não causar dificuldades para os funcionários, o setor de TI tende a diminuir os níveis de segurança, o que provoca diversas brechas de segurança no ambiente. Além disso, Ricardo Gonzaga afirma que o alto custo alto no mercado brasileiro dos equipamentos dedicados a segurança de redes sem fio (Wi-Fi) faz com que as empresas privilegiem a conectividade, em detrimento à segurança dos dispositivos. Nessa mesma linha, Eduardo Izycki, cita que atualmente o uso de dispositivos móveis e redes *Wi-Fi* é praticamente indispensável na comunicação não apenas entre pessoas, mas também entre dispositivos. Em parte, isso ocorre pelo custo de se estabelecer conexões físicas entre pontos distintos de ambiente industriais em infraestruturas críticas. Para Eduardo Izycki, os riscos inerentes aos protocolos e equipamentos com vulnerabilidades não corrigidas, bem como a ausência de boas práticas na configuração de redes, tornam as redes sem fio um ponto suscetível para ataques cibernéticos. Além do *Wi-Fi*, uma conexão 4G pode ser um risco para a organização. Um computador de consultor externo de empresa prestadora de serviços pode estar com acesso à Internet via conexão 4G, facilitando a entrada de *malware*s, que podem se instalar no ambiente de produção de uma usina nuclear e infectar sistemas de controle industrial (BAYON; BRUNT; LIVINGSTONE, 2015).

O uso de filtro *web* é recomendado por Conteh e Schmick (2016), cuja função é analisar todos os *sites* acessados na organização, bloqueando os que não se enquadram em regras previamente definidas, ou que sejam classificados como maliciosos por possuírem falsos formulários ou *links* inseguros. Esse filtro é capaz, ainda, de registrar todos os acessos de navegação, o que pode ser utilizado em caso de investigação de incidentes de segurança (CISA, 2017). Com isso, protege-se os funcionários de roubo de informação na Internet, o que pode mitigar, por exemplo, ataques q*uid pro quo, reverse social engineering* e *pretexting*.

A utilização de filtros de correio eletrônico tem por finalidade reter as mensagens identificadas como SPAM (CISA, 2017). Denominados de *antispam*, esses *softwares* são capazes de analisar os *emails* que entram na organização, e de realizar a comparação com uma lista de mensagens previamente classificadas com SPAM. Qualquer *email* que seja identificado como suspeito pode ser posto em quarentena ou apagado antes de chegar ao destinatário. Essa estratégia é corroborada por Jakobson (2005), que afirma que o *antispam* deve ser adicionado como uma estratégia de defesa para diminuir o risco de sucesso de ataques cibernéticos, assim como é aconselhável a verificação por antivírus de todas as mensagens de *email* (CISA, 2017). Mas não apenas mecanismos tecnológicos podem ser empregados. Jakobson (2005) cita que a proteção contra *phishing* depende da consciência dos usuários. Assim, torna-se relevante que a gestão da segurança cibernética considere situações em que as atitudes dos funcionários não correspondam as esperadas pela organização. Uma vez que o *phishing* é amplamente utilizado pelos os atacantes, conforme visto no segundo capítulo, o uso de mecanismos *antispam* se torna essencial na mitigação de engenharia social.

Embora não existam *softwares* capazes de impedir ataques de engenharia social, algumas soluções tecnológicas colaboram para melhorar a visibilidade, ao observar o comportamento do que ocorre no ambiente cibernético (NAUMOVSKI, TANESKI, 2019). Com essa abordagem, é possível identificar quando alguma ação realizada por um funcionário diverge do comportamento padrão. No momento em que o *software* identifica esse comportamento anômalo, um alerta é enviado à equipe de segurança

cibernética, que pode analisar se o incidente relatado compromete a integridade do ambiente. Esse método de análise de comportamento pode auxiliar na prevenção de vazamento de informações, pois é capaz de identificar se um determinado funcionário tentou acessar documentos aos quais não tem permissão, ou se uma informação sensível foi acessada fora do horário do expediente. Esses sistemas, denominados *Security Information and Event Management (*SIEM*)*[25], podem realizar a correlação entre registros de vários sistemas digitais, e apresentar as informações relevantes para a equipe de segurança. Segundo Ferrante (2017), o uso de análise de dados com o *Big Data*[26] auxilia na otimização do SIEM, na medida que é capaz de identificar e filtrar automaticamente as ameaças e vulnerabilidades relevantes dentre os inúmeros eventos ocorridos em um ambiente cibernético. Para Eduardo Izycki, o monitoramento ativo das redes para identificação de anomalias se mostra uma medida necessária. Porém, o entrevistado ressalta que o custo é elevado por razão da necessidade de mão de obra especializada.

Para Krombholz et al (2015), à medida que a fronteira organizacional se torna cada vez mais difusa em função do ambiente digital, mais difícil a decisão sobre quais informações podem ser publicadas ou repassadas para as empresas prestadoras de serviço. Por isso, além de se observar quais informações devem ser compartilhadas com terceiros, é aconselhável proteger o caminho por onde percorre a informação. De acordo com Conteh e Schmick (2016), os acessos remotos que porventura a organização possua com empresas prestadoras de serviço e fornecedores devem ser efetuados por meio de uma rede virtual privada (VPN[27]). Nessa rede, qualquer indivíduo que realize a interceptação dos dados ao longo do caminho não conseguirá interpretá-los por razão da criptografia (BAYON; BRUNT; LIVINGSTONE, 2015). Um engenheiro social que consiga capturar os dados, portanto, não conseguirá extrair informações úteis para um ataque de q*uid pro quo, reverse social engineering, pretexting* e *spear phishing.*

[25] SIEM: acrônimo de *Security Information and Event Management*. Trata-se de uma solução de software que realiza a consolidação de registros de sistemas de segurança, de modo a facilitar o armazenamento e interpretação de eventos de segurança da informação.
[26] *Big Data*: "conjuntos de dados extremamente amplos e que, por este motivo, necessitam de ferramentas especialmente preparadas para lidar com grandes volumes, de forma que toda e qualquer informação nesses meios possa ser encontrada, analisada e aproveitada em tempo hábil. (BRASIL, 2019).
[27] VPN: acrônimo de *Virtual Private Network.*

Samadi e McFarland (2014) argumentam que qualquer atividade suspeita deve ser investigada pelas equipes de segurança cibernética, e é recomendável que os funcionários sejam orientados a escalar aos superiores quaisquer dúvidas sobre a execução de procedimentos que possam gerar riscos de vazamento de informações, o que pode interromper um ataque de engenharia social nos estágios iniciais. Em geral, as organizações possuem um setor de segurança da informação ou uma central de serviços, que podem auxiliar os funcionários nesses casos.

Um método eficiente de mitigar ataques cibernéticos consiste em implementar sistemas de monitoração de ambiente e de tráfego (KASPERSKY, 2019b). O uso desses sistemas, contudo, não deve ser adotado apenas no perímetro da rede, mas também nos sistemas de controle, a fim de detectar comportamentos anômalos (BAYON; BRUNT; LIVINGSTONE, 2015). Esse método também é validado por Erbschloe (2019) que, além de indicar o monitoramento dos sistemas de controle, aponta a necessidade de se monitorar quaisquer alterações nos privilégios dos funcionários. Comportamento suspeitos ou fora do padrão podem indicar um funcionário vítima de ataque de engenharia social, cujas credenciais estejam sendo usadas indevidamente para acesso aos sistemas corporativos. Por esse motivo, é importante que os funcionários tenham acesso apenas aos recursos e informações necessárias à execução de seu trabalho, especialmente no caso administradores de sistemas críticos (ERBSCHLOE, 2019). Além de se reduzir o número funcionários com permissão de administradores, convém garantir que o acesso não possa ser feito pela Internet, a fim de evitar que atacantes consigam acesso aos sistemas por fora da organização (CISA, 2017).

Krombholz et al (2015) citam que o uso de aplicativos móveis dentro das organizações é um canal cada vez mais utilizado para ataques de engenharia social. Para os autores, as políticas estabelecidas pelas empresas geralmente incluem o uso de *smartphones* e *tablets* pessoais. No entanto, muitos usuários de *smartphones* usam aplicativos vulneráveis, que podem ser utilizados para realizar ataques de engenharia social. Bayon, Brunt e Livinstone (2015) citam que é prática comum em alguns países levar computadores pessoais para instalações nucleares. Nesse aspecto, carregar a bateria de telefones pessoais nas portas USB dos computadores das usinas nucleares compromete o

isolamento dos ambientes críticos e facilita a propagação de *malware*s (BAYON; BRUNT; LIVINGSTONE, 2015).

A utilização crescente de redes sociais se torna uma fonte rica de dados para os engenheiros sociais. O compartilhamento e divulgação de informações pessoais facilitam o roubo de informações, que podem ser utilizadas em ataques de engenharia social (ABRAHAM; CHENGALUR, 2010). Quando a área de atuação profissional requer lidar com informações sensíveis, esse fato se torna mais grave. Nesse aspecto, o uso da rede social *Linkedin* pode ser um risco, uma vez que tem foco na divulgação de perfis profissionais. Pollack e Ranganathan (2018) argumentam que por meio do *Linkedin* os atacantes podem adquirir informação sobre funcionários. A prospecção pode indicar, por exemplo, a função exercida pelos indivíduos dentro da organização e os vínculos profissionais. O uso de outras redes sociais, tais como *Facebook* e *Instagram* podem ser utilizadas para se obter informações pessoais, como nomes de parentes. Enquanto essas informações por si só não são capazes de provocar danos, elas podem ser utilizadas pelos engenheiros sociais para realizar *pretexting*, a ser utilizado em ataques posteriores. Segundo Mitnick (2003), é uma boa prática que os números de telefone de funcionários, contratados e consultores não sejam divulgados para o ambiente externo à empresa. Para Thomas (2016), *emails* infectados, mídias social e programas de *chats* podem ser usados para rastrear funcionários e obter informações sensíveis, como *login* e senha de equipamentos e sistemas.

Além de informações pessoais, é possível prospectar na Internet informações importantes sobre os sistemas supervisórios das organizações. Mecanismos de pesquisa especializados em encontrar sistemas supervisórios conectados à Internet, como o *site Shodan*[28], permitem que sejam exibidos ambientes SCADA/ICS em todo o mundo, incluindo suas localizações (BAYON; BRUNT; LIVINGSTONE, 2015). De posse dessas informações, um engenheiro social pode direcionar ataques para os funcionários que operam sistemas críticos vulneráveis.

[28] O *Shodan* oferece um serviço especializado para encontrar dispositivos conectados à Internet, incluindo sistemas industriais SCADA/ICS.

3.1.2 Educação e treinamento em segurança cibernética

Ataques direcionados aos indivíduos são mais difíceis de serem detectados do que ataques a computadores e sistemas (SALAHDINE, 2019). Por esse motivo, a engenharia social é fator importante a ser considerado na gestão da segurança cibernética da CNAAA. O fato de os funcionários, em geral, não terem conhecimento sobre as vulnerabilidades associadas à engenharia social dificulta ações de mitigação de ataques (MITNICK, 2003). Nesse aspecto, Aldawood e Skinner (2019) argumentam que existem limitações no processo de implementação de controles contra ataques de engenharia social. Para os autores, além do uso da tecnologia, é necessário que os funcionários compreendam seu papel na proteção do ambiente. Nessa linha, Eduardo Izycki esclarece que, como o alvo das ações de engenharia social é o componente humano, as medidas de proteção a serem aplicadas precisam ter foco nas pessoas. Por esse motivo, a instrução dos funcionários sobre questões basilares de segurança torna-se essencial, como saber identificar se uma informação é confidencial, ou como deve ser realizado o tratamento dos dados corporativos. Programas de conscientização sobre o uso de senhas e compartilhamento de informações fora do ambiente corporativo podem fortalecer a cultura da segurança cibernética.

Samadi e McFarland (2014) apontam que o conhecimento sobre segurança cibernética pode ser obtido por programas de conscientização, onde são observados todos os meios pelos quais os funcionários interagem com o meio externo, como telefones, *emails* e equipamentos. O treinamento pode conter tópicos sobre os princípios de segurança cibernética e a importância de não compartilhar senhas com outros funcionários (ABRAHAM; CHEGALUR, 2010), além de fornecer uma lista de verificação sobre como reconhecer um possível ataque de engenharia social (ALLEN, 2019). Mitnick (2019) sugere que os treinamentos abordem os métodos de ataque utilizados pelos engenheiros sociais, os modos de reconhecer um ataque, os procedimentos de tratamento em caso de suspeita de ataque e o fluxo de comunicação em caso de incidente. Em entrevista, Ricardo Gonzaga argumenta que o treinamento ajuda na integração dos funcionários com os sistemas de segurança implementados pelas empresas, o que diminui consideravelmente o risco de incidentes

cibernéticos. O entrevistado cita ainda que o treinamento apresenta aos funcionários as razões pelas quais os controles e sistemas são adotados. Nesse aspecto, Eduardo Izycki esclarece que uma campanha de conscientização pode adotar a simulação de ações de engenharia social por meio de *spear phishing*, de modo a demonstrar aos funcionários como ataques ocorrem no cotidiano das organizações.

Visto que a educação minimiza as possibilidades de ataques de engenharia social (NAUMOVSKY, 2019), é aconselhável que o treinamento seja feito em toda a organização, sendo oportuno que os funcionários recém contratados também sejam contemplados com a capacitação (CONTEH, SCHMICK, 2016). Todavia, a conscientização e o preparo das pessoas tendem a diminuir com o tempo, sendo fundamental que os programas de treinamento sejam efetuados periodicamente (CONTEH; SCHMICK, 2016).

Embora o processo de treinamento seja indicado para o fortalecimento da segurança cibernética, alguns desafios surgem em sua implementação (ALDAWOOD, SKINNER, 2019). Para Aldawood e Skinner (2019), o primeiro desafio é o de convencer os funcionários sobre a importância do treinamento para a segurança da organização. Em geral, os funcionários consideram que a equipe de segurança cibernética da empresa é o único responsável por tratar todas as ameaças à segurança corporativa. Em se tratando estritamente do aspecto tecnológico, de fato o setor de segurança cibernética é o principal responsável pela proteção do ambiente. Contudo, ao se considerar ataques de engenharia social, os funcionários são valiosos para a proteção da organização. A pouca percepção sobre a relevância do seu papel para a segurança provoca falta de interesse no assunto, o que pode acarretar no aumento das vulnerabilidades, uma vez que os funcionários não estarão preparados para reconhecer ataques de engenharia social. Além disso, o problema é agravado pelo pouco orçamento geralmente dedicado aos projetos específicos de segurança cibernética orientados aos funcionários (ALDAWOOD, SKINNER, 2019). Nesse aspecto, é essencial que a alta direção da organização, além de patrocinadora da ideia, participe dos programas ao lado dos funcionários. Essa atitude é capaz de não apenas de demonstrar comprometimento com a segurança, mas de incentivar a participação de todos os colaboradores. Igual comprometimento deve ser demonstrado na atitude

diante dos funcionários vítimas de ataques de engenharia social. A repreensão das vítimas desses ataques pode tornar os demais funcionários receosos em assumir que foram alvo de outros incidentes decorrentes da engenharia social (SAMADI e MCFARLAND, 2014). Portanto, como argumentam Samadi e McFarland (2014), é recomendável que a organização proporcione confiança e liberdade suficientes para que os funcionários questionem quaisquer pedidos considerados fora do padrão de segurança da empresa, mesmo se requisitados por instâncias superiores. O fato de o funcionário receber uma demanda, não o excluí da responsabilidade de refletir criticamente se o procedimento solicitado compromete a segurança. Essa cultura auxilia na prevenção de ataques, e assegura que as vítimas da engenharia social não escondam os ataques de engenharia social sofridos (SALAHDINE, 2019).

3.1.3 Auditoria em segurança cibernética

Procedimentos periódicos de auditoria são importantes para a gestão da segurança do ambiente cibernético (KASPERSKY, 2019). Alguns controles de auditoria contemplam a análise de *logs*[29] e a verificação de autorizações dos funcionários nos sistemas corporativos. No que tange as permissões, quanto maiores os privilégios atribuídos a um funcionário, maior risco suas ações representam. Quanto mais serviços e informações os funcionários tiverem acesso, maior o risco de danos causados por ataques de engenheiros sociais. Portanto, a auditoria deve verificar periodicamente os privilégios de acesso dos funcionários (WATSON; MASON; ACKROYD, 2014). Mitnick (2003), argumenta que é indicado manter o registro do fluxo das informações no ambiente corporativo, assim como verificar periodicamente quais funcionários possuem permissão para acessar informações sensíveis. Nas instalações nucleares, em geral, esse procedimento é constantemente realizado com o monitoramento das atividades dos funcionários que trabalham com equipamentos críticos, na busca por comportamentos suspeitos (NEI, 2020).

Segundo Mann (2017), é aconselhável utilizar métodos que incluam identificação de riscos, detecção de vulnerabilidades, obtenção de novas

[29] Log: registro de eventos relevantes em um dispositivo ou sistema computacional (BRASIL, 2019)

informações sobre vulnerabilidades e elaboração de contramedidas direcionadas à avaliação de risco. Também cabe à auditoria verificar se a documentação sobre o ambiente cibernético está atualizada, e se existe um plano de resposta de incidentes (CISA, 2017). No que concerne a gestão de riscos, Branquinho et al (2014) recomendam a norma NBR/ISO 31000:2009, que apresenta as diretrizes para a gestão de risco, e a NBR/ISO 31010:2012, que contém técnicas para o processo de avaliação de riscos. A aplicação de controles, a partir das normas citadas, pode, segundo Branquinho et al (2014), reduzir o impacto, bloquear uma ameaça ou eliminar uma vulnerabilidade. Assim, é relevante que a gestão de riscos considere a engenharia social como ameaça ao ambiente da organização, e que sejam utilizados controles para mitigar esse modo de ataque.

Além dos procedimentos citados, faz parte do escopo da auditoria verificar se os contratos com os prestadores de serviço estão adequados no que tange a segurança da informação (BAYON; BRUNT; LIVINGSTONE, 2015), assim como a conformidade dos procedimentos da organização com as normas e padrões de segurança adotadas no mercado. Conforme citado no capítulo 1, as organizações do setor nuclear geralmente se baseiam nas normas ISO/IEC 27001 e 27002 (PIGGIN, 2012), nos documentos da IAEA, nos relatórios da NEI e da NRC, nos guias SP 800-82 e SP 800-8 do NIST e na ISA-99 (BRANQUINHO et al, 2014).

3.1.4 Políticas de segurança cibernética

Uma política de segurança cibernética precisa conter abordagens de ordem técnica e não técnica (CONTEH; SCHMICK, 2016). Para os autores, as organizações devem verificar se as políticas de segurança estão sendo seguidas. Em consonância, Allen (2019) afirma que a cultura de segurança inicia com a conscientização das pessoas e com o incentivo da ampla comunicação entre as equipes de segurança, gestores e funcionários. Nessa linha, Branquinho et al (2014, p. 34) argumentam que documentos normativos “organizam processo e ambientes, distribuem responsabilidades e delegam poderes”. Segundo Branquinho et al (2014), as políticas internas da organização precisam deixar claro o papel de cada funcionário e suas

responsabilidades, assim como as sanções cabíveis em cada situação. A política de segurança deve contemplar, também, diretrizes de uso de senhas no ambiente corporativo (CISA, 2017), de modo que os funcionários tenham senhas exclusivas, pessoais e intransferíveis, e que sejam periodicamente alteradas (ERBSCHLOE, 2019), principalmente as relacionadas aos sistemas SCADA (BRANQUINHO et al, 2014).

Do mesmo modo, é válido que a política explicite que os funcionários tenham acesso somente aos sistemas necessários para seus trabalhos, e que não instalem nenhum *software* não autorizado pela organização. Para Branquinho et al (2014), deve haver uma norma de segurança especifica para sistemas SCADA, que considere as diferenças entre as redes de tecnologia da informação tradicionais e as redes de ambientes de operação, conforme abordado no capítulo 1. O autor esclarece que as particularidades sobre o ambiente SCADA podem ser encontradas na norma ANSI/ISA-99. Além das diretrizes citadas, a política pode conter orientações sobre o controle de portas USB (BRANQUINHO et al, 2014). Nessa lógica, a política deve abordar a necessidade de se identificar os ativos cibernéticos críticos em cada instalação nuclear (BAYON; BRUNT; LIVINGSTONE, 2015). No que tange dispositivos móveis, é importante que o documento oriente os funcionários a proteger seus *smartphones* com senha, criptografar os dados, e utilizar aplicativos que evitem o roubo de informações (ERBSCHLOE, 2019). Por fim, cabe informar que não devem ser expostas em redes sociais informações corporativas que possam comprometer a segurança do ambiente nuclear.

Em síntese, a política de segurança cibernética é o documento formal que norteia as ações na organização. A partir dela derivam outras normas de segurança cibernética aplicadas ao ambiente de uma instalação nuclear. A política auxilia na estruturação da segurança corporativa, definindo os caminhos que a organização pode tomar para mitigar ataques de engenharia social contra seus funcionários. Contudo, é importante observar um fato comum nas organizações: uma série de políticas e normas de segurança corporativa são criadas, mas na prática não são transmitidas aos funcionários (WATSON; MASON; ACKROYD, 2014).

3.1.5 Proteção física do ambiente cibernético

Um atacante, ao planejar uma ação, considera vários fatores, como a complexidade dos sistemas de segurança da organização, o custo do ataque e o tempo necessário para o êxito (ALI, 2015). Embora a proteção física, em um primeiro momento, aparente não ter correlação com o ambiente cibernético, é no meio físico que ocorrem ações como *baiting* e *tailgating*, utilizadas em ataques de engenharia social. No que tange a segurança física, portanto, recomenda-se utilizar sistemas de controle de acesso em todos os locais onde existam equipamento digitais, assim como adotar a separação física entre as áreas críticas de controle e as áreas administrativas (CONTEH; SCHMICK, 2016). Mesmo com essa separação, Thomas (2016) cita o caso em que os funcionários podem precisar transferir informações e acessar diferentes áreas da organização, o que pode ser um problema caso não haja um controle de acesso adequado. Nesse aspecto, convém adicionar circuitos internos de TV. Além disso, um modo adicional de fortalecer a segurança é incentivar as equipes que trabalham na segurança física do ambiente nuclear a interagirem com as equipes de segurança cibernética, de modo que diferentes pontos de vista possam ser observados (BAYON; BRUNT; LIVINGSTONE, 2015). Ademais, o treinamento e as campanhas de conscientização devem orientar os funcionários a não permitir a entrada de pessoas não identificadas ou não acompanhadas por funcionários da organização. Os funcionários também devem ser orientados a solicitar aos prestadores de serviço que deixem eventuais encomendas na recepção, não permitindo a entrada desses profissionais no ambiente da empresa. Do mesmo modo, qualquer dispositivo de armazenamento encontrado, como *pendrive*, deve ser entregue diretamente para a equipe de segurança cibernética da organização.

3.2 Análise empírica das medidas de segurança cibernética adotadas na CNAAA

Uma vez que esta pesquisa tem por objetivo analisar como as medidas de segurança cibernética adotadas pela CNAAA podem mitigar ataques de engenharia social, é importante observar como o tema da cibernética é tratado

na empresa. A Eletronuclear tem uma área específica para a gestão da segurança cibernética, o Departamento de Governança de Tecnologia da Informação e Comunicação, subordinado à Superintendência de Tecnologia da Informação e Comunicação. Além disso, há um Comitê de Segurança da Informação, composto por representantes das diretorias e das áreas de negócio (ELETRONUCLEAR, 2019c). Por meio da Lei de Acesso à Informação (LAI), a Eletronuclear foi questionada sobre quais documentos normativos são usados para a gestão da segurança cibernética. Em resposta, a empresa informou que, além a Política de Segurança da Informação da Eletrobras, são utilizadas normas da ISO e do NIST, instituições citadas no capítulo 1 deste trabalho. Nesse aspecto, a Eletronuclear esclarece que o Plano de Segurança da Informação é o instrumento fundamental para mensuração e monitoramento da segurança cibernética na empresa (ELETRONUCLEAR, 2019c). A respeito do gerenciamento da segurança cibernética, a empresa declara:

> Esse gerenciamento está fundamentado na Política de Segurança da Informação das empresas Eletrobras (PSIEE); nas normas e padrões de boas práticas adotadas pela indústria, tais como a família de normas ABNT NBR ISO/IEC 27000, ANSI, NIST, NERC-CIP, entre outras; nas recomendações de segurança cibernética em instalações nucleares, advindas de colegiados da Agência Internacional de Energia Atômica (AIEA); nas orientações do Sipron (Sistema de Proteção ao Programa Nuclear); e nos aprendizados conferidos pelo Exercício Anual Guardião Cibernético, promovido pelo Comando de Defesa Cibernética, sob coordenação do Exército Brasileiro. (ELETRONUCLEAR, 2019c, p.37).

No que concerne a Política de Segurança da Informação da Eletronuclear (PSIEE), consta no *site* da empresa que a atualização mais recente do documento foi publicada em 2018, sendo aplicado a todas as subsidiárias do grupo Eletrobras (ELETROBRAS, 2018a). São contemplados pela PSIEE todos os colaboradores da organização que utilizam as informações e recursos corporativos, como os funcionários, prestadores de serviço, diretores e estagiários. Segundo o documento, as diretrizes abrangem as áreas de tecnologia da informação, tecnologia da automação e segurança da informação. Alguns pontos elencados pela Política indicam que os funcionários somente devem acessar informações previamente autorizadas pelo gestor das respectivas informações, assim com mencionam que a

credencial de acesso é considerada de uso individual e intransferível. Nesse ponto, Olivio Napolitano[30] informa os funcionários possuem um crachá individual que permite acesso apenas as áreas as quais eles têm permissão. Além disso, o uso de recursos computacionais é registrado e monitorado, e todo incidente de segurança deve ser reportado internamente. A Política aponta também que todos os relacionamentos formais de compartilhamento de informação com prestadores de serviço devem ser precedidos de termo de confidencialidade, com cláusulas sobre segurança da informação (ELETROBRAS, 2018a). Via e-SIC, a Eletronuclear afirmou que são incluídas cláusulas específicas sobre segurança da informação nos contratos com empresas prestadoras de serviço. Sobre essa questão, a empresa publicou em 2020 o Guia de Conduta para Fornecedores, onde informa aos fornecedores da Eletrobras e de suas subsidiárias o padrão a ser adotado para o suprimento de materiais e a prestação de serviços (ELETROBRAS, 2020a). Além disso, a Eletronuclear cita que os fornecedores são constantemente monitorados durante todo o período de relacionamento com a empresa, por meio da gestão e fiscalização do contrato (ELETRONUCLEAR, 2019c).

Os incidentes de segurança cibernética na Eletronuclear são registrados pela Central de Serviços do Centro de Serviços Compartilhado, e tratados pelo Grupo de Respostas a Incidentes de Segurança da Informação (ELETRONUCLEAR, 2019c). Com base no artigo nº 22 da LAI, a Eletronuclear considerou que não poderia responder o questionamento sobre o número de incidentes decorrentes de ataques cibernéticos ocorridos no período de 2015 a 2019 nas instalações da CNAAA[31]. Contudo, no Relatório Anual 2019, consta que:

> Ao longo de 2019 não registramos incidentes de segurança da informação relacionados à violação de privacidade de empregados, ou fomos comunicados acerca de violações do gênero por qualquer órgão regulador/controlador ou corregedor e, tampouco, averiguamos vazamento, furtos ou perdas de dados de empregados, tendo como origem os sistemas computacionais da empresa. (ELETRONUCLEAR, 2019c, p.38).

[30] Entrevista realizada em novembro de 2019.
[31] A resposta da Eletronuclear encontra-se no Anexo I.

Dentre os documentos publicados no *site* da empresa na Internet está o Plano de Negócios e Gestão 2018-2022, que relaciona as estratégias da companhia para a melhoria de desempenho empresarial (ELETROBRAS, 2017). O documento apresenta o programa denominado Tecnologia da Informação, cuja descrição se refere à atualização das ferramentas de tecnologia da informação da Eletronuclear. O objetivo e metas elencadas no Plano, cuja execução abrange até 2022, trata de "atualizar o parque tecnológico da Eletronuclear, garantindo a segurança e integridade das informações armazenadas na rede corporativa" (ELETROBRAS, 2017, p. 55). Complementa-se a isso o fato de a empresa classificar a segurança da rede corporativa como de risco alto (ELETROBRAS, 2017, pag.77).

Em 2018, a Eletrobras publicou a Política de Gestão de Pessoas, onde apresenta os princípios e diretrizes de gestão de pessoas da empresa (ELETROBRAS, 2018b). No que tange os programas de capacitação, a empresa cita a necessidade de as empresas do grupo estabelecerem um plano de formação continuada dos funcionários. Nessa linha, em 2019 foi aprovado o Programa de Educação e Conscientização em Segurança da Informação da Eletronuclear, com o intuito de promover ciclos de palestras sobre o tema (ELETRONUCLEAR, 2019c). Sobre a sala de controle da CNAAA, a empresa afirma que os profissionais que trabalham nesse ambiente realizam treinamento teórico e prático, passando por todas as situações que ocorrem no funcionamento das usinas, inclusive em emergências (ELETRONUCLEAR, 2011). Por meio do e-SIC, a empresa informou que programas de treinamento e campanhas de conscientização dos funcionários são realizados anualmente. De acordo com Olivio Napolitano, em entrevista concedida para esta pesquisa, os funcionários realizam treinamentos anuais obrigatórios de segurança. Alan Lima[32] cita que os diretores e o presidente também passam por treinamento. De fato, a empresa afirma em seu *site* na Internet que tem por princípio o treinamento e qualificação dos empregados e prestadores de serviço, de modo a "assegurar os conhecimentos relativos aos diversos aspectos da segurança integrada necessários à execução adequada de seus trabalhos" (ELETRONUCLEAR, 2019b). Nesse ponto, Alan Lima menciona que os

[32] Entrevista realizada em outubro de 2019.

funcionários que atuam na sala de controle das usinas recebem treinamento durante anos até se tornarem operadores sêniores, e poderem assumir as responsabilidades do trabalho. O entrevistado afirma, ainda, que todos os funcionários que trabalham nas usinas têm uma forte cultura de segurança, e seguem rigorosamente as especificações técnicas da usina. Alan Lima declara que os funcionários são incentivados a relatar qualquer erro cometido. Segundo ele, o modo de comunicação dentro da sala de controle obedece a um padrão de verificação, a fim de evitar ruído no entendimento, diminuindo a possibilidade de erros e de ações que não estejam estritamente planejadas.

Em termos práticos, Olivio Napolitano aponta para o treinamento dos operadores efetuado em simulador nas instalações da CNAAA. O entrevistado cita que esse simulador é capaz de realizar com exatidão os eventos que ocorrem nas usinas, assim como os incidentes postulados nas análises de segurança, de modo a se obter respostas rápidas para ações necessárias nas salas de controle. Esse treinamento é acompanhado de provas de conhecimentos técnicos, onde se deve demonstrar a capacidade de atuar em incidentes de segurança. Assim, na hipótese de ocorrência de algum problema, inclusive derivado de ataques de engenharia social, os operadores estarão mais bem informados, e poderão ter maior capacidade de perceber e atuar de acordo com o que foi aprendido na simulação. Em casos de incidentes graves, onde os equipamentos ultrapassem os parâmetros pré-definidos de funcionamento, mecanismos de desligamento automático das usinas entram em atuação. Conforme argumenta Alan Lima, por determinação da CNEN, as usinas não podem ser religadas até que se descubra a causa do desligamento. Ressalta-se que, segundo Olívio Napolitano, qualquer incidente que ocorra nas usinas deve ser reportado para a sala de controle.

No que tange treinamentos externos da Eletronuclear, com empresas e órgãos governamentais, cita-se o Guardião Cibernético. Esse exercício consiste no treinamento de ações de proteção cibernética, a fim de realizar simulação e práticas de gestão de incidentes, onde participam as Forças Armadas, órgãos parceiros e representantes de infraestruturas críticas (BRASIL, 2020). A simulação virtual utilizada durante o exercício Guardião Cibernético de 2019 contou a participação da IAEA como observadora internacional. O escopo do exercício incluiu simulações de vazamento de

informações sensíveis e de comprometimento de sistemas SCADA (SILVA, 2019).

A respeito do uso de dispositivos móveis, como smartphones, Olivio Napolitano relata que cada país adota uma conduta específica, sendo alguns mais rígidos do que outros. Como exemplo, o entrevistado cita que na França é possível entrar com celulares dentro das usinas nucleares. Por outro lado, na Inglaterra deve-se deixar o aparelho na portaria das usinas, enquanto nos EUA somente os funcionários podem entrar com o dispositivo. O entrevistado informa que o uso do celular na CNAAA não é autorizado em áreas com equipamentos susceptíveis a interferência eletromagnética ou por radiofrequência. Argumentando se tratar de informação sob sigilo, de acordo com o artigo nº 22 da Lei de Acesso à Informação, a Eletronuclear não respondeu à pergunta, realizada via e-SIC[33], se os funcionários e colaboradores podem utilizar dispositivos digitais pessoais, como celulares e notebooks nos ambientes administrativos e de operação. Contudo, de acordo com a *Nuclear Energy Institute*, as instalações nucleares adotam protocolos de controles restritivos para o uso de *pendrives*, notebooks e demais mídias portáteis. Além disso, os dispositivos são regularmente verificados em busca de *malware*s (NEI, 2020). Sobre o uso de celulares por visitantes, a Eletronuclear informou não poder responder ao questionamento. Todavia, no *site* do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo consta que os alunos da instituição, ao visitar as instalações da CNAAA, não puderam entrar com celulares no ambiente das usinas, tampouco tirar fotos do interior da instalação (IFSP, 2019). Sobre essa questão, Olívio Napolitano esclarece que os visitantes na CNAAA assinam termo de responsabilidade, que menciona o impedimento de se tirar fotografias do interior das usinas. Isso revela procedimentos importantes de segurança da Eletronuclear, dificultando a obtenção de informações sensíveis do local, que poderiam ser utilizadas em ataques de engenharia social.

De acordo com Olivio Napolitano, existe uma filosofia em diversas usinas nucleares, inclusive no Brasil, de bloquear portas USB nos computadores de monitoramento, controle ou de proteção, a fim de evitar a introdução de vírus

[33] A resposta da Eletronuclear consta no e-SIC, número de protocolo 99908000057202012, conforme Anexo 1 deste trabalho.

ou alteração de algum parâmetro não autorizado. Segundo o entrevistado, as redes de monitoramento das usinas são separadas fisicamente das redes administrativas e da Internet, de acordo com as boas práticas citadas no primeiro capítulo. Esse fato é corroborado pelo Relatório Anual da Eletronuclear, que afirma que “a rede operacional é segregada do ambiente, não tendo conexão com a Internet, o que aumenta o grau de proteção” (ELETRONUCLEAR, 2019c, p.37). Por outro lado, a empresa pondera que “com a transformação digital pela qual as empresas Eletrobras vêm passando, que aumenta e acelera o fluxo de informações corporativas, a cibersegurança deve ser revista e ampliada” (ELETRONUCLEAR, 2019c, p.37).

Bayon, Brunt e Livingstone (2015) argumentam que é relevante que sejam avaliados os riscos relativos à segurança cibernética na indústria nuclear. Nesse aspecto, os riscos corporativos na Eletrobras são orientados por uma política de gestão de riscos única para todas as empresas do grupo. Cada subsidiária, contudo, tem sua própria área de riscos, além de um comitê dedicado ao tema (ELETROBRAS, 2019d). De acordo com o Relatório Anual de Atividades de Auditoria Interna, a Eletrobras estruturou um processo de gestão integrada de riscos, tendo como base metodológica a norma ABNT NBR/ISO 31000:2018 e as diretrizes do *Committee of Sponsoring Organizations of the Treadway Commission* (ELETROBRAS, 2019a). Os resultados gerados são analisados pela Diretoria Executiva e pelo Conselho de Administração, por meio do Comitê de Auditoria e Riscos Estatutário (CAE), composto por três a cinco membros efetivos (ELETROBRAS, 2019c). Na Eletronuclear, o tema é tratado pelo Departamento de Gestão de Riscos e Controles Internos, subordinado à Superintendência de Governança, Gestão de Riscos e Conformidade (ELETRONUCLEAR, 2018a). De acordo com a empresa, os riscos de segurança devem ser identificados, quantificados e priorizados, de modo que sejam aplicadas as proteções adequadas a cada caso (ELETRONUCLEAR, 2018a). Nesse aspecto, foi realizado um contrato de consultoria externa para realizar um projeto de riscos corporativos, que incluiu um tópico dedicado à segurança da informação (ELETRONUCLEAR, 2018a).

De modo a prover transparência da informação, conforme orientação do governo brasileiro, a Eletronuclear publica na Internet uma planilha com os nomes dos funcionários, com os respectivos cargos, função, lotação e data de

admissão (ELETRONUCLEAR, 2016). Contudo, Erbschloe (2019) argumenta que é importante evitar fornecer informações pessoais e da organização. Essas informações podem ser usadas como insumo para ataques de engenharia social. De acordo com Erbschloe (2019), deve-se reduzir a quantidade de dados disponibilizados na Internet, evitando publicar os que não forem necessários, como telefones de funcionários, nomes e cargos. Em resposta, por meio do e-SIC, a Eletronuclear informou que orienta seus funcionários e colaboradores a não divulgar informações corporativas na Internet, como redes sociais e fóruns *online*, que possam prejudicar a gestão da segurança. Essas orientações, segundo a empresa, estão expressas na Política de Segurança da Informação, em manuais de boas práticas e em documentos que apresentam os incidentes mais comuns de segurança da informação. Observou-se que, ao fim de 2019, a Eletrobras publicou a Política de Proteção a Dados Pessoais e Privacidade das Empresas Eletrobras. No documento, a empresa afirma que devem ser promovidas ações de capacitação e conscientização sobre as melhores práticas sobre o tratamento de dados pessoais nas empresas e em suas subsidiárias. Nesse aspecto, é relevante que seja promovida a transparência, com o intuito de maior *accountability* do uso do dinheiro público. Todavia, há necessidade de ter um nível de sigilo proporcional ao nível de criticidade da organização, em especial ao considerar a implementação da Lei Geral de Proteção de Dados (LGPD), que dispõe sobre o tratamento de dados pessoais.

Anualmente é realizado um processo de auditoria interna na CNAAA, cujo resultado é publicado no Relatório Anual de Atividade de Auditoria Interna (ELETROBRAS, 2019). Nesse aspecto, a Eletronuclear esclarece:

> A Auditoria Interna coordena e examina, com inteira liberdade de acesso, as atividades desenvolvidas pelas unidades organizacionais da empresa, com o objetivo de analisar sua gestão, verificando, para tanto, os procedimentos, controles aplicados, sistemas informatizados, registros, arquivos de documentos e dados. (ELETRONUCLEAR, 2019c, p.52).

Em relação às auditorias externas, a empresa afirma que são executadas avaliações independentes por equipes técnicas internacionais, coordenadas pela Agência Internacional de Energia Atômica e pela Associação

Mundial dos Operadores de Energia Nuclear (ELETRONUCLEAR, 2019c). No *site*[34] da IAEA na Internet é possível obter a informação de que em 2018 a Agência realizou uma inspeção de segurança de Angra 1, a pedido da Eletrobras, utilizando como parâmetros de análise as diretrizes de segurança elaboradas pela própria IAEA.

Por fim, a Eletronuclear informa que a proteção física é um dos componentes fundamentais para segurança das usinas da CNAAA (ELETRONUCLEAR, 2011). Para tanto, são utilizados sistemas de circuito de câmeras de vídeo, procedimentos de conduta pessoal nas áreas das usinas, identificação de funcionários e treinamentos específicos (ELETRONUCLEAR, 2011).

3.3 Segurança cibernética na CNAAA e a mitigação de ataques de engenharia social

A partir das informações coletadas na pesquisa, foram elencadas treze medidas de segurança cibernética para mitigação de ataques de engenharia social, que contemplam os pontos relevantes descritos no item 3.1, obtidos por meio da análise da literatura e relatos dos entrevistados. As medidas foram organizadas na primeira coluna do quadro 2. A segunda coluna do quadro apresenta as medidas de segurança cibernética adotadas pela CNAAA, analisadas no item 3.2, a partir de entrevistas, pesquisa na literatura e consulta à Eletronuclear por meio do e-SIC. A terceira coluna apresenta o nível de adequação das medidas adotadas pela CNAAA em relação às medidas de segurança cibernética para mitigação de ataques de engenharia social, apontadas no item 3.1. Foram adotadas quatro classes, de acordo com o nível de adequação: (I) indefinido, nos casos em que não houve informação suficiente para análise; (II) integral, quando houve alinhamento entre as medidas; (III) parcial, quando houve alinhamento de algumas medidas; (IV) insuficiente, quando não houve alinhamento. Ressalta-se, contudo, que a classe “insuficiente” não foi utilizada, pois identificou-se medidas de segurança por parte da CNAAA nos pontos pesquisados, excetuando-se duas medidas

[34] Informação disponibilizada em: https://www.iaea.org/newscenter/pressreleases/iaea-concludes-long-term-operational-safety-review-at-brazils-angra-nuclear-power-plant. Acesso em setembro de 2020.

apresentadas na coluna 1, onde não houve informação suficiente para análise: uso de equipamentos e sistemas de segurança cibernética; gestão de identidades e autenticação de dois fatores.

Quadro 2 - Medidas de segurança cibernética para mitigação de ataques de engenharia social

Medidas de segurança cibernética para mitigação de ataques de engenharia social [35]	Medidas de segurança cibernética adotadas pela CNAAA [36]	Nível de adequação das medidas adotadas pela CNAAA [37]
Uso de equipamentos e sistemas de segurança cibernética (IPS, *firewalls*, antivírus, filtro *web* e *antispam*)	Não especificadas. [38]	Indefinido
Tratamento adequado de acesso a informações e de uso de senhas.	Os funcionários acessam apenas informações ou dados previamente. As credenciais de acesso são individuais e intransferíveis.	Integral
Adoção de procedimentos de segurança com empresas prestadoras de serviço.	Os relacionamentos formais de compartilhamento de informação com prestadores de serviço são precedidos de Termo de Confidencialidade, assim como treinamento de pessoal. Os fornecedores são monitorados por meio da gestão e fiscalização do contrato.	Parcial [39]
Monitoração do ambiente administrativo e operacional.	O uso de recursos computacionais é registrado e monitorado.	Integral

[35] As medidas de segurança cibernética dessa coluna foram elencadas a partir de análise da literatura e das entrevistas com profissionais, conforme item 3.1.
[36] As medidas dessa coluna correspondem as adotadas pela CNAAA, e foram relatadas pelos entrevistados, por documentos e pela consulta via e-SIC, de acordo com o exposto no item 3.2.
[37] Essa coluna apresenta o nível de adequação entre as medidas adotadas pela CNAAA (coluna 2) e as medidas dispostas na coluna 1.
[38] As medidas foram classificadas como não especificadas por não haver informações suficientes para a análise.
[39] A análise não identificou a existência de procedimentos técnicos de segurança, como o uso de VPN ou outros mecanismos de proteção cibernética.

(continuação)

Gestão de identidades e autenticação de dois fatores.	Não especificadas	Indefinido
Desativação de portas USB nos computadores.	As portas USB nos computadores das áreas críticas são bloqueadas.	Integral
Segmentação de redes de ambientes SCADA/ICS e administrativo.	As redes SCADA/ICS são separadas fisicamente das redes administrativas e da Internet.	Integral
Tratamento na divulgação de informações sensíveis para o ambiente externo.	Os funcionários e colaboradores são orientados a não divulgar informações corporativas na Internet, como redes sociais e fóruns online.	Parcial[41]
Programas corporativos de conscientização em segurança da informação.	São realizadas campanhas anuais de conscientização para todos os funcionários e prestadores de serviço, assim como ciclos de palestras sobre segurança da informação.	Integral
Gestão de riscos	Existe um departamento de gestão de riscos e controles internos. Os processos de gestão integrada de riscos são definidos. Os riscos de segurança são identificados, quantificados e priorizados.	Integral
Adoção de política de segurança da informação	Existe uma política de segurança da informação própria da empresa.	Integral
Capacitação dos funcionários e colaboradores	São realizados treinamentos anuais obrigatórios de segurança, plano de formação continuada dos funcionários e participação em eventos externos de capacitação.	Integral

[41] Identificou-se publicação na Internet contendo informações que podem ser usadas como insumo para ataques de engenharia social, como nomes, cargos e funções dentro da empresa.

(conclusão)

Restrição de dispositivos móveis em ambientes críticos.	O uso de dispositivos móveis pelos funcionários não é autorizado nas áreas críticas da empresa; os visitantes não podem utilizar celulares durante a visita.	Integral

Fonte: o autor

O uso de sistemas de segurança como *firewall*, IPS, antivírus, filtro *web* e *antispam* pela CNAAA não foram identificados na pesquisa. Em se tratando de infraestruturas críticas é compreensível que informações técnicas sobre as defesas do ambiente cibernético não sejam ostensivas. Considerando que a Eletronuclear afirma seguir as normas do NIST, e que recebe auditorias periódicas da IAEA e WANO, esse fato sugere que a CNAAA possa adotar sistemas de segurança dessa categoria. Esses sistemas são capazes, por exemplo, de mitigar métodos de *phishing* e *spear phishing,* pois podem bloquear *emails* e *malwares* enviados por engenheiros sociais por meio de filtros *antispam* e antivírus. Nessa mesma linha, a segmentação de redes é uma medida comumente adotada. A CNAAA utiliza a segmentação de rede, o que pode diminuir o risco de que incidentes com *malware*s, decorrentes do uso de *baiting,* se propaguem para as redes SCADA/ICS, o que poderia acarretar prejuízos na operação de equipamentos e sistemas responsáveis por processos operacionais críticos.

Apontadas pelos entrevistados como importantes medidas, a autenticação de dois fatores e a gestão de identidade evitam que, em caso de vazamento de senha, a credencial de um funcionário possa ser utilizada, uma vez que seria necessário que o atacante possuísse um fator de autenticação adicional. Todavia, não foi possível, durante a pesquisa, obter informações que pudessem indicar o uso dessas medidas pela CNAAA. Por outro lado, observou-se que a Central Nuclear adota o princípio de desativação de portas USB em setores críticos do ambiente, o que previne que dispositivos como celulares e *pendrives* possam infectar computadores corporativos com *malware*. Essa medida diminui o risco que ações de *baiting* seja bem

sucedidas, pois caso um funcionário encontre um *pendrive,* e tente usá-lo dentro do ambiente corporativo, o dispositivo não irá funcionar.

O tratamento adequado do acesso às informações corporativas é essencial para diminuir o risco de ações de engenharia social aplicadas aos recursos humanos. A Eletronuclear restringe o acesso dos funcionários apenas às informações ou dados previamente autorizados. Essa medida dificulta a aquisição de informações sensíveis pelos atacantes com o uso de *pretexting, reverse social engineering* e *quid pro quo.* Caso um funcionário da CNAAA seja vítima de um engenheiro social, e tenha sua senha comprometida, a segregação de acesso às informações não permite que todas a informações corporativas sejam capturadas pelo atacante.

A fim de diminuir a possibilidade de ação dos atacantes, é recomendável também o tratamento das informações sensíveis divulgadas para o ambiente externo à empresa. A orientação dos funcionários sobre os riscos da divulgação de informações sensíveis é uma medida capaz de auxiliar na mitigação de ataques de engenharia social. Nesse aspecto, de acordo CNAAA, os funcionários e colaboradores da empresa são orientados a não divulgar informações corporativas na Internet, como redes sociais e fóruns online. Contudo, observa-se que funcionários da Eletronuclear utilizam redes sociais, como o *Linkedin*. Uma verificação do perfil da Eletronuclear nessa rede social revelou que 1529 funcionários possuíam perfil cadastrado[42], incluindo diretor, superintendentes, chefes de departamento, engenheiros e analistas de diversos setores, como de recursos humanos e tecnologia da informação. Em alguns casos, as informações disponibilizadas no *Linkedin* incluem formação acadêmica, cargo, rede de contatos e interesses profissionais. Outro fato relevante se refere a publicação na Internet de uma planilha com os nomes dos funcionários da Eletronuclear[43], com os respectivos cargos, funções, lotação e data de admissão. Se por um lado isso promove a transparência para a sociedade, por outro favorece a prospecção de dados internos, que podem ser usados para ataques de engenharia social, em especial *spear phishing.*

[42] Consulta realizada em 4 de setembro de 2020.
[43] Publicada em 2016, a planilha está disponível em: https://www.eletronuclear.gov.br/Acesso-a-Informacao/Documents/Lista_de_Empregados.pdf. Acesso em 3 de setembro de 2020.

Assim como o tratamento de acesso às informações, a adoção de procedimentos de segurança com empresas prestadoras de serviço é um fator importante para mitigar *pretexting, quid pro quo* e *reverse social engineering*. Ao adotar um termo de confidencialidade com prestadores de serviço, a CNAAA demonstra atenção ao tema. Contudo, durante a pesquisa, não foram identificadas medidas técnicas de segurança cibernética, como VPN, entre as empresas prestadoras de serviço e a CNAAA, ponto fundamental para evitar interceptação de informações que possam ser usadas em ataques de engenharia social.

Uma política de segurança da informação corporativa, aliada a uma gestão de riscos, é responsável por manifestar como a empresa aborda aspectos da segurança em seu ambiente, tanto em nível de planejamento, como de melhorias. Nesse quesito, a CNAAA tem uma política própria de segurança da informação, além de ter instituído um projeto relacionado a riscos corporativos. Por serem de ordem normativa e estruturante, essas medidas são capazes de colaborar na mitigação de ataques de engenharia social.

Para haver visibilidade sobre o que ocorre no ambiente administrativo e de operação é necessário que se empregue ações de monitoramento. Na CNAAA os recursos computacionais são monitorados e possuem os registros armazenados. Esses procedimentos dificultam a ação dos atacantes, uma vez que possibilitam que as equipes de segurança cibernética identifiquem a ocorrência de ataques, assim com viabilizam a auditoria dos registros de eventos.

A necessidade de adoção de programas de conscientização foi amplamente citada pelos entrevistados, e apontada na literatura como essencial para a formação de uma cultura de segurança corporativa. Campanhas de conscientização para os funcionários, colaboradores e prestadores de serviço podem tornar os indivíduos mais aptos a identificar ataques de engenharia social, e a relatar incidentes que eventualmente ocorram no ambiente da CNAAA, como *email* falsos, *pendrives* encontrados no ambiente, ou atacantes simulando atendimento técnico, o que caracteriza respectivamente ações de *phishing, baiting e quid pro quo*. A pesquisa identificou que a CNAAA realiza campanhas anuais de conscientização para

todos os funcionários, o que diminuir os riscos de ataques bem sucedidos de engenharia social.

À semelhança das campanhas de conscientização, a capacitação dos funcionários tem papel fundamental para a segurança do ambiente nuclear. Essa medida possibilita maior aprofundamento sobre o tema junto aos funcionários, de modo que eles possam não apenas identificar uma ação de engenharia cibernética em curso, mas adotar uma atitude proativa para mitigar ataques no local de trabalho. A capacitação é especialmente importante para os funcionários que atuam em atividades críticas, como os operadores das salas de controle e funcionários com elevado nível de acesso. Nesse ponto, a CNAAA realiza treinamentos anuais obrigatórios de segurança, e promove formação continuada dos funcionários. Destaca-se a participação da empresa no treinamento Guardião Cibernético, onde a Eletronuclear pode simular ataques cibernéticos e praticar métodos de defesa com participação de outras empresas e órgão governamentais.

Um ponto relevante a ser observado refere-se ao uso de dispositivos móveis, que pode facilitar o contato entre engenheiros sociais e funcionários da organização. Nesse aspecto, embora a CNAAA não tenha respondido, via e-SIC, o questionamento sobre o uso de dispositivos móveis pelos funcionários e visitantes, Olivio Napolitano cita que o uso desses equipamentos não é permitido nas áreas críticas da instalação. A adoção dessa medida pode auxiliar na mitigação de *vishing*, *smishing* e *pretexting*.

3.4 O uso de tecnologia, processos e capacitação de pessoas para a mitigação de ataques de engenharia social

O capítulo final desse trabalho analisou como as medidas de segurança cibernética adotadas na CNAAA podem mitigar ataques de engenharia social. A partir das entrevistas e da literatura, verificou-se que a segregação entre o ambiente SCADA e o ambiente administrativo, assim como a adoção de *firewalls* e IPS, dificultam a ação de atacantes. Para minimizar a ação de *phishing*, pode-se adotar ferramentas *antispam* e o monitoramento de anomalias no ambiente. A criptografia na rede e a aplicação de autenticação de dois fatores no ambiente operacional podem ajudar no reforço da segurança

cibernética. O uso de dispositivos móveis no ambiente de trabalho foi apontado como fator que aumenta o risco de ação de *malware*s capazes de infectar ambientes críticos. De modo semelhante, o uso de portas USB favorece a exploração de vulnerabilidades pelos engenheiros sociais. Para se mitigar ataques de engenharia social por meio de *baiting*, a utilização de programas periódicos de conscientização dos funcionários pode auxiliar, assim como a orientação para que quaisquer dispositivos encontrados sejam entregues ao setor de segurança da empresa.

Não menos relevante foi a identificação da necessidade de monitorar as ações que empresas prestadoras de serviço realizam no ambiente da organização. Nesse caso, convém que todas as conexões com os prestadores de serviço utilizem VPN. Soma-se a isso a importância da análise contínua do ambiente, por meio de um SIEM, que indique eventual comprometimento das redes, seja por razão de uma invasão em curso, seja por ação de um *malware* nos computadores. Em simultâneo, o uso de *Big Data* associado ao *SIEM* pode otimizar a filtragem e a classificação da grande quantidade de eventos gerados no ambiente cibernético. As ações técnicas podem ser acompanhadas de um programa periódico de treinamento dos funcionários em segurança cibernética e na identificação de ataques de engenharia social. A mesma relevância pode ser dada à política de segurança da informação. É importante que a política seja clara, abrangente, e divulgada não apenas para os funcionários, mas para colaboradores e empresas prestadoras de serviço. Um trabalho amplo de auditoria pode identificar vulnerabilidades no ambiente que, se não tratadas, podem aumentar os riscos de ataques de engenharia social e, consequentemente, facilitar ataques cibernéticos.

Embora a Eletronuclear não tenha fornecido todos os esclarecimentos solicitados, foi possível obter e analisar um volume de informações suficientes para a estudo pretendido neste trabalho. A empresa não forneceu, por meio do e-SIC, informações sobre o uso de *firewall*, IPS e de outros recursos técnicos de segurança, o que revela senso de responsabilidade, na medida que expor essas informações pode facilitar ataques externos. A empresa adota o bloqueio de portas USB, que é uma importante medida para evitar a disseminação de *malware* por meio de dispositivos de armazenamento, como *pendrives*. Faz parte dos procedimentos internos a negação de uso de dispositivos móveis,

como celulares, dentro das instalações da CNAAA. Em relação à adoção de procedimentos de segurança com empresas prestadoras de serviço, houve um alinhamento parcial, pois não foi possível identificar requisitos técnicos de segurança, apenas questões de ordem administrativa. Constatou-se ênfase na capacitação e conscientização dos funcionários, o que permite que eles se tornem mais atentos às tentativas de ataque e mais interessados em colaborar para a segurança da instalação. Ao se verificar a política de segurança da Eletronuclear, observa-se que ela aborda pontos importantes para a segurança cibernética, como processos definidos para compartilhamento de informações, credenciais de acesso e uso de recursos computacionais. Inclui-se nos procedimentos da empresa a gestão de riscos e a auditoria, assim como aspectos relacionados a monitoração do ambiente. A Eletronuclear orienta seus funcionários sobre a divulgação de informações para o ambiente externo, contudo, identificou-se algumas informações disponíveis na Internet, que podem ser utilizadas por engenheiros sociais.

Em síntese, a partir da análise realizada nesta pesquisa, verificou-se que das treze medidas de segurança cibernética para mitigação de ataques de engenharia social elencadas no quadro 2, a CNAAA obteve um nível de adequação integral em nove medidas. Embora haja oportunidades de melhoria, observa-se que a Central Nuclear Almirante Álvaro Alberto adota medidas de segurança cibernética adequadas para mitigar de ataques de engenharia social direcionados aos seus funcionários.

CONSIDERAÇÕES FINAIS

Este trabalho propôs um questionamento: de que modo as medidas de segurança cibernética adotadas pela Central Nuclear Almirante Álvaro Alberto podem mitigar ataques de engenharia social direcionados aos seus funcionários? Tal questionamento, sobre como as medidas de segurança cibernéticas adotas pela CNAAA podem mitigar ataques de engenharia social, partiu da premissa de que os funcionários dessa instalação nuclear podem ser alvos de ataques de engenharia social. De fato, durante a pesquisa observou-se que a engenharia social não apenas representa risco à segurança das organizações, como por diversas vezes foi efetivamente empregada, em conjunto com ataques cibernéticos, para causar prejuízos em instalações nucleares no mundo. O objetivo principal dessa pesquisa foi de analisar como as medidas adotadas pela Central Nuclear Almirante Álvaro Alberto podiam mitigar ataques de engenharia social direcionadas aos seus funcionários. Além disso, sustentava-se a hipótese de que as medidas de segurança cibernética adotadas pela CNAAA eram adequadas para a mitigação de ataques de engenharia social.

A fim de verificar a hipótese, e atingir o objetivo da pesquisa, o trabalho foi dividido em três capítulos, que exploraram desde questões de ordem operacional de uma usina nuclear, até tópicos sobre métodos psicológicos usados por engenheiros sociais. No primeiro capítulo, constatou-se que atualmente as usinas nucleares utilizam equipamentos digitais em seus ambientes operacionais e administrativos. Esses dispositivos digitais, contudo, são operados por funcionários, que podem ser vítimas de ataques de engenharia social, uma vez que ela é capaz de explorar vulnerabilidades psicológicas humanas. Como ataques dessa natureza podem ser utilizados em conjunto com ataques cibernéticos, o segundo capítulo apresentou os métodos utilizados pelos engenheiros sociais. A partir da literatura e das entrevistas com especialistas, identificou-se quais medidas de segurança cibernética podiam ser utilizadas para mitigar ataques de engenharia social em instalações nucleares. Por fim, o terceiro capítulo se aprofundou na análise do uso de medidas de segurança cibernética pela CNAAA e na verificação se essas medidas eram adequadas para a mitigação de ataques de engenharia social.

No estudo, verificou-se que os métodos de mitigação de ataques de engenharia social não se limitam aos procedimentos técnicos, mas compreendem também o treinamento dos funcionários, campanhas de conscientização, uso de políticas e auditorias periódicas. Trata-se, portanto, de uma atividade contínua, exercida não apenas pelos responsáveis pela segurança cibernética, mas por cada funcionário que utiliza os recursos tecnológicos no ambiente da CNAAA. Algumas medidas usadas na Central Nuclear tinham caráter estritamente técnico, como a segmentação de redes administrativas e operacional, dificultando a ação de engenheiros sociais que adotassem vetores de propagação de *malware*, tal como o *phishing*. Medidas estruturantes foram identificadas, como a adoção de política de segurança e gestão de risco, capazes de organizar ações técnicas e não-técnicas relativas à segurança cibernética.

No que tange a proteção de informações corporativas, verificou-se a restrição de acesso dos funcionários apenas às informações previamente autorizadas, de modo a mitigar ataques de *pretexting*, *reverse social engineering* e *quid pro quo*. Soma-se a isso as campanhas de conscientização dos funcionários, colaboradores e prestadores de serviço, a fim de torná-los cientes sobre os riscos e métodos de ataques de engenharia social, de modo a de auxiliar na mitigação de ações de *phishing*, *baiting* e *quid pro quo*. De igual importância, a não permissão do uso de dispositivos pessoais, como celulares, no interior das áreas críticas da CNAAA dificulta a prática de *vishing*, *smishing* e *pretexting*. Os procedimentos adotados com empresas prestadoras de serviço, no que concerne a formalização e alinhamento de práticas de segurança cibernética, podem mitigar atos de *pretexting*, *quid pro quo* e *reverse social engineering*. Notou-se que o treinamento e a capacitação dos funcionários da CNAAA é um elemento chave para garantir a segurança do ambiente nuclear. Esse fato converge para o entendimento de que para mitigar ataques de engenharia social convém não se ater apenas à tecnologia, sendo essencial um contínuo processo de treinamento e de campanhas de conscientização.

A análise de como as medidas de segurança cibernéticas utilizadas na CNAAA podem mitigar ataques de engenharia social, realizada no capítulo 3, permitiu atingir o objetivo dessa dissertação. Além disso, verificou-se que a

Central Nuclear Almirante Álvaro Alberto adota medidas alinhadas com os procedimentos que podem mitigar ataques de engenharia social, de acordo com a pesquisa realizada na literatura e com os relatos de profissionais dos setores cibernético e nuclear. Contudo, a partir do estudo, identificou-se que duas medidas estão apenas parcialmente alinhadas, e outras duas medidas não puderam ser analisadas por falta de informações. Desse modo, infere-se que pode haver oportunidades de melhorias no ambiente da CNAAA.

Em retrospecto, observou-se nessa pesquisa que poucos são os estudos científicos no Brasil que relacionam ataques de engenharia social simultaneamente aos setores nuclear e cibernético. A análise empírica sobre a CNAAA desenvolvida nesse estudo, portanto, pode contribuir para preencher a lacuna existente no país, colaborando para a gestão da segurança cibernética das usinas nucleares nacionais, em consonância com os trabalhos iniciados pela CNEN sobre segurança cibernética no setor nuclear. Pode ser válida, ainda, a expansão da pesquisa para além do setor nuclear, contemplando a dimensão humana na segurança cibernética de setores considerados críticos para o Brasil, como as diversas usinas de geração de energia que compõem o parque gerador nacional. Esse fato mostra-se atual e relevante ao constatar que o Operador Nacional do Sistema Elétrico tem conduzido um trabalho para estabelecer controles de segurança cibernética com agentes do setor.

No que concerne o domínio acadêmico, o estudo pode iluminar outros trabalhos científicos semelhantes, além de fomentar a interdisciplinaridade entre grupos de pesquisa nacionais que atuem nas áreas nuclear e cibernética, auxiliando na produção de novos conhecimentos e na formação de profissionais. Por razão do recorte temático, essa dissertação foi orientada à CNAAA. Contudo, futuras pesquisas podem avançar na direção de um estudo comparativo entre as medidas adotadas no Brasil para a segurança cibernética de instalações nucleares com as medidas utilizadas em outros países que possuam instalações nucleares compatíveis com as brasileiras. Tais pesquisas têm o potencial de incentivar uma busca constante pela segurança do indivíduo. Em último grau, é ele quem lida com as complexidades da tecnologia, e que enfrenta diariamente as eventuais adversidades dos ambientes nuclear e cibernético. Ao assegurar sua proteção, promove-se não apenas a segurança das usinas nucleares, mas a segurança da sociedade brasileira.

REFERÊNCIAS BIBLIOGRÁFICAS

ABRAHAM, Sherly; CHENGALUR-SMITH, InduShobha. An overview of social engineering *malware*: Trends, tactics, and implications. **Technology in Society**, v. 32, n. 3, p. 183-196, 2010.

ALLEN, Malcom. Information Security Reading Room. **Social Engineering: a Means to Violate a Computer System**. SANS Institute. 2019.

ALDAWOOD, Hussain; SKINNER, Geoffrey. Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. **Future Internet**, v. 11, n. 3, p. 73, 2019.

ALEXEY, Komarov. **Charging your smartphone's battery over USB can be dangerous**. 2016. Disponível em: https://www.kaspersky.com/blog/usb-battery-charging-unsecurity/12206/. Acesso em : 23 maio de 2020.

ALI, Abdul. Social Engineering: Phishing latest and future techniques. **Retrieved March**, v. 10, p. 2016, 2015.

BAYLON, Caroline; BRUNT, Roger, LIVINGSONE, David. **Cyber security at civil nuclear facilities: understanding the risks.** Chatam House. 2016.

BISSON, David. **5 Social engineering attacks to watch out for**. The state of security. Disponível em: http://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/. Acesso em 11 outubro de 2019.

BRANDENBURG UNIVERSITY. **Cyber Security at Nuclear Facilities: National Approaches**. Brandenburg University of Applied Sciences. 2015.

BRANQUINHO, Marcelo Ayres et al. **Segurança de Automação Industrial e SCADA**. Rio de Janeiro: Elsevier, 2014.

BRASIL. **Estratégia Nacional de Defesa**. Ministério da Defesa. 2020a.

_____. **Política Nacional de Defesa**. Ministério de Defesa. 2020b.

_____. **Decreto nº 10.222**. Aprova a Estratégia Nacional de Segurança Cibernética. Presidência da República. Secretaria-Geral. Subchefia para Assuntos Jurídicos. 2020c.

_____. **Portaria nº 93**, de 26 de setembro de 2019. Aprova o Glossário de Segurança da Informação. GSI-PR. 2019.

_____. **Decreto nº 9.600**. Presidência da República. Consolida as diretrizes sobre a Política Nuclear Brasileira. Casa Civil. 2018.

_____. **Lei nº12.527**, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216

da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. 2011.

_____. **Guia de Referência para a Segurança das Infraestruturas Críticas da Informação**. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. 2010.

CAMPBELL, Alexander; SINGH, Vickram. **Lessons from the cyberattack on India's largest nuclear power plant**. 2019. Disponível em: https://thebulletin.org/2019/11/lessons-from-the-cyberattack-on-indias-largest-nuclear-power-plant. Acesso em: 15 de março de 2020.

CARNEGIE MELLON UNIVERSITY. **Unintentional Insider Threats: Social Engineering**. The CERT Insider Threat Center. 2014.

CARVALHO, R. **Proposta de arquitetura para coleta de ataque cibernéticos às infraestruturas críticas**. Dissertação de Mestrado. Instituto Militar de Engenharia. Rio de Janeiro. 2014.

CERTBR. **Grupo de Resposta a Incidentes de Segurança para a Internet no Brasil Incidentes Reportados**. Disponível em: https://www.cert.br/stats/incidentes/2018-jan-dec/analise.html. Acesso em: 02 de julho de 2019.

CISA. **Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors**. Cybersecurity and Infrastructure Security Agency. 2017. Disponível em: https://www.us-cert.gov/ncas/alerts/TA17-293A. Acesso em: 19 de abril de 2019.

CONTEH, Nabie Y.; SCHMICK, Paul J. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. **International Journal of Advanced Computer Research**, v. 6, n. 23, p. 31, 2016.

COSTA, Luciano. Reuters. **Ataques cibernéticos disparam com pandemia e atingem elétricas no Brasil e no mundo**. Disponivel em: https://br.reuters.com/article/internetNews/idBRKBN2432M4-OBRIN. Acesso em: 2 de junho de 2020.

CYBERBIT. **Dtrack: In-depth analysis of APT on a nuclear power plant**. 2019. Disponível em: https://www.cyberbit.com/blog/endpoint-security/dtrack-apt-*malware*-found-in-nuclear-pow.

CARVALHO, Paulo Sérgio Melo de. A defesa cibernética e as infraestruturas críticas nacionais. **Coleção Meira Mattos-Revista das Ciências Militares**, 2011.

CHO, Chi-Shiang; CHUNG, Wei-Ho; KUO, Sy-Yen. Cyberphysical security and dependability analysis of digital control systems in nuclear power plants. **IEEE Transactions on Systems, Man, and Cybernetics: Systems**, v. 46, n. 3, p. 356-369, 2015.

CHO, Hyo Sung; WOO, Tae Ho. Cyber security in nuclear industry: Analytic study from the terror incident in nuclear power plants (NPPs). **Annals of Nuclear Energy**, v. 99, p. 47–53, 2017.

CIALDINI, Robert B. **Influence: Science and practice**. Boston: Pearson education, 2009.

CNEN. **Quem Somos**. 2019. Disponível em: http://www.cnen.gov.br/quem-somos. Acesso em: 05 de outubro de 2019.

_____. **Reator Multipropósito vai ampliar acesso da população à medicina nuclear**. 2018. Disponível em: http://www.cnen.gov.br/ultimas-noticias/450-lancamento-da-pedra-fundamental-do-rmb. Acesso em: 20 de setembro de 2019.

_____. **Programa Política Nuclear PPA 2016-2019**. Comissão Nacional de Energia Nuclear, 2016.

CONTEH, Nabie Y.; SCHMICK, Paul J. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. **International Journal of Advanced Computer Research**, v. 6, n. 23, p. 31, 2016.

DAS, Sanchari et al. All About Phishing: Exploring User Research through a Systematic Literature Review. **arXiv preprint arXiv:1908.05897**, 2019.

DECKER et al. **Nuclear Cybersecurity: Risks and Remedies**. Fissile Material Working Group. Vienna: 2018.

DEMIRÖZ, Özkan. A Pragmatic and Structured Method to Secure the Systems That Control the Nuclear Environment. In: Guido GLUSCHKE, Mesut Hakkı CAŞIN; Marco MACORI. Cyber Security Policies and Critical Infrastructure Protection. **Potsdam: Institute for Security and Safety (ISS) Press**, 2018. p.341.

DENNING, Dorothy E. Stuxnet: What has changed?. **Future Internet**, v. 4, n. 3, p. 672-687, 2012.

DRAGOS. **Assessment of Reported *Malware* Infection at Nuclear Facility**. 2019. Disponível em: https://dragos.com/blog/industry-news/assessment-of-reported-*malware*-infection-at-nuclear-facility/. Acesso em: 17 de janeiro de 2020.

DRIAS, Zakarya; SERHROUCHNI, Ahmed; VOGEL, Olivier. Analysis of cyber security for industrial control systems. *In*: 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC). **IEEE**, 2015. p. 1-8.

ELETROBRAS. **Guia de Conduta para Fornecedores.** 2020a.

_____. **Plano de Trabalho. Comitê de Auditoria e Riscos Estatutário**. 2020b

_____. **Relatório Anual de Atividades de Auditoria Interna.** 2019a.

_____. **Política de Proteção a Dados Pessoais e Privacidade das Empresas Eletrobras.** 2019b.

_____. **Deliberação.** Conselho de Administração 852ª Reunião. 2019c.

_____. **Carta Anual de Políticas Públicas e de Governança Corporativa**. 2019d

_____. **Política de Gestão de Riscos das Empresas Eletrobras**. 2019e.

_____. **Política de Segurança da Informação das Empresas Eletrobras**. 2018a.

_____. **Política de Gestão de Pessoas das Empresas Eletrobras**. 2018b.

_____. **Plano de Negócios e Gestão 2018-2022**. 2017.

ELETRONUCLEAR. **Tecnologia**. 2019a. Disponível em: https://www.eletronuclear.gov.br/Seguranca/Paginas/Tecnologia.aspx. Acessado em: 03 de dezembro de 2019. Acesso em: 9 de maio de 2019.

_____.**Política de Segurança Nuclear**. 2019b. Disponível em: https://www.eletronuclear.gov.br/Seguranca/Paginas/Politica-de-Seguranca-Nuclear.aspx).

_____. **Relatório Anual 2019**. 2019c.

_____. **Relatório da Administração e de Responsabilidade Social**. 2018a.

_____. **Relatório de Gestão**. 2018b.

_____. **Relatório: atualização do padrão técnico e de segurança do Projeto de Angra 3.** 2017.

_____. **Lista de Acesso de Empregados**. 2016. Disponível em: https://www.eletronuclear.gov.br/Acesso-a-Informacao/Documents/Lista_de_Empregados.pdf.

_____. **Critérios de segurança adotados para as usinas nucleares Angra 1, Angra 2 e Angra 3**. 2011. Disponível em: http://www.eletronuclear.gov.br/Quem-Somos/Governanca/Documents/Relat%C3%B3rios%20e%20Balan%C3%A7os/Relat%C3%B3rios%20de%20Seguran%C3%A7a/12052011RSFA.pdf.

ERBSCHLOE, Michael. **Social Engineering**. CRC Press. 2019.

FERRANTE, Anthony. **Enhancing Security with Big Data Analytics**. 2017. Disponível em: http://www.rmmagazine.com/2017/10/02/enhancing-security-with-big-data-analytics/. Acesso em: 15 de setembro de 2019.

FIRJAN. **Impacto da Conclusão de Angra 3 para a segurança energética e o desenvolvimento do Rio de Janeiro e do Brasil**. 2019. Disponível em:

https://www.eletronuclear.gov.br/Imprensa-e-Midias/Documents/Nota%20Firjan_apoio%20Angra%203.pdf

FGV. **Boletim de Conjuntura do Setor Energético**. FGV Energia, 2019.

FORD, Neil. **Nuclear operators urged to tackle growing threat from cyber attack emails**. 2017. Disponível em: https://analysis.nuclearenergyinsider.com/nuclear-operators-urged-tackle-growing-threat-cyber-attack-emails. Acesso em: 14 de junho de 2019.

GAO, Hongyu et al. Detecting and characterizing social spam campaigns. In: **Proceedings of the 10th ACM SIGCOMM conference on Internet measurement**. ACM, 2010. p. 35-47.

GELBSTEIN, Eduardo. Protecting Critical Information Infrastructures. Instituto de Defesa Nacional. **Revista Nação e Defesa** n°133. Lisboa: 2012.

GIAUROV, Vesselin. **The Cyber-Nuclear Security Threat: Managing the Risks**. Vienna Center for Disarmament and Non-Proliferation. 2017.

GLUSCHKE, Guido. Cyber Security of Nuclear Power Plants. In: Guido GLUSCHKE, Mesut Hakkı CAŞIN; Marco MACORI. Cyber Security Policies and Critical Infrastructure Protection. Potsdam: **Institute for Security and Safety (ISS) Press**, 2018. p.167.

HARTIGAN, Kelsey et al. **A New Approach to the Nuclear Fuel Cycle: Best Practices for Security, Nonproliferation, and Sustainable Nuclear Energy**. Rowman & Littlefield, 2015.

HOANCA, Bogdan; KENRICK, Mock. Effects of Digital Convergence on Social Engineering Attack Channels. *In:* GUPTA, Manish; SHARMAN, Raj (org.). Social and Human Elements of Information Security: Emerging Trends and Countermeasures. IGI Global, 2009 p. 133 -147.

HURST, William; SHONE, Nathan; CHALMERS, Carl. Cyber Security Education and Training for Critical Infrastructure Protection. In: Guido

GLUSCHKE, Mesut Hakkı CAŞIN; Marco MACORI. Cyber Security Policies and Critical Infrastructure Protection. Potsdam: **Institute for Security and Safety (ISS) Press, 2018**. p.167.

IAEA. **Conducting Computer Security Assessments at Nuclear Facilities**. Vienna: 2016.

_____. **Computer security of nuclear facilities**. IAEA guideline. Vienna: 2013.

_____. Information Circular n° 449. **Convention on Nuclear Safety**. Viena: 1994.

IFSP. **Estudantes de Física do IFSP-Caraguatatuba visitaram a Usina Nuclear de Angra. 2019**. Disponível em:

https://www.ifspcaraguatatuba.edu.br/noticias/estudantes-de-fisica-do-ifsp-caraguatatuba-visitaram-a-usina-nuclear-de-angra. Acesso em: 11 novembro 2019. Acesso em: 11 de janeiro de 2020.

ITU. Series x: data networks, open system communications and security. X.1205. **Overview of cybersecurity**. 2008.

IVATURI, Koteswara; JANCZEWSKI, Lech. A taxonomy for social engineering attacks. In: International Conference on Information Resources Management. **Centre for Information Technology, Organizations, and People**, 2011. p. 1-12.

JAKOBSSON, Markus. **Modeling and Preventing Phishing Attacks**. 2005. Disponível em: http://markus-jakobsson.com/papers/jakobsson-psci07.pdf.

KASPERSKY. DTrack: **previously unknown spy-tool by Lazarus hits financial institutions and research centers**. 2019a. Disponível em: https://usa.kaspersky.com/about/press-releases/2019_dtrack-previously-unknown-spy-tool-hits-financial-institutions-and-research-centers Acessado em: 5 de dezembro de 2019.

_____. **O que é smishing e como se proteger?** 2019b. Disponível em: https://www.kaspersky.com.br/resource-center/threats/what-is-smishing-and-how-to-defend-against-it . Acesso em 28 setembro de 2019.

KAY, Russell. **Sidebar: the origins of phishing.** 2014. Disponível em: http://computerworld.com/article/2575094/security0/sidebar-the-origins-of-phishing.html, Acesso em 11 outubro de 2019.

KROMBHOLZ, Katharina et al. Advanced social engineering attacks. **Journal of Information Security and applications**, v. 22, p. 113-122, 2015.

KNAPP, Eric. **Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems**. Elsevier. 2011.

KIM, Do-Yeon. Cyber security issues imposed on nuclear power plants. **Annals of Nuclear Energy**, v. 65, p. 141–143, Mar 2014.

KNOWLES, William. A Survey of Cyber Security Management in Industrial Control Systems. **International Journal of Critical Infrastructure Protection**, v. 9, p. 52–80, 2015.

KROMBHOLZ, Katharina et al. Advanced social engineering attacks. **Journal of Information Security and applications**, v. 22, p. 113-122, 2015.

LEAVITT, Harold. **Applied Organizational Change in Industry: Structural, Technological and Humanistic Approaches**. Carnegie Institute of Technology. Graduate School of Industrial Administration.1962.

LENDVAY, R.L. **Shadows of Stuxnet: Recommendations for US policy on critical infrastructure cyber defense derived from the Stuxnet attack**. Naval Postgraduate School Monterey CA Monterey United States, 2016.

LUIIJF, Eric. Threats in industrial control systems. In: **Cyber-security of SCADA and Other Industrial Control Systems**. Springer, Cham, 2016. p. 69-93.

LUO, Xin et al. Social engineering: The neglected human factor for information security management. **Information Resources Management Journal (IRMJ)**, v. 24, n. 3, p. 1-8, 2011.

MANN, Ian. **Hacking the Human: Social Engineering Techniques and Security Countermeasures**. Gower Publishing Limited. England: 2008.

MASOOD, Rahat. Assessment of Cyber Security Challenges in Nuclear Power Plants Security Incidents, Threats, and Initiatives. **Cybersecurity and Privacy Research Institute the George Washington University**, 2016.

MEDEIROS, Breno Pauli. **Ciberespaço e relações internacionais: rumo a construção de um novo paradigma?**. Dissertação (Mestrado em Ciências Militares) – Instituto Meira Mattos, Escola de Comando e Estado-Maior do Exército. Rio de Janeiro. 2019.

MEDEIROS, Breno Pauli; CARVALHO, Alessandra Cordeiro; GOLDONI, Luiz Rogério Franco. Uma análise sobre o processo de securitização do ciberespaço. **Coleção Meira Mattos: revista das ciências militares**, v. 13, n. 46, p. 45-66, 2019.

MEHAN, Julie. **CyberWar, CyberTerror, CyberCrime and CyberActivism: An i-depth guide to the role of standards in the cybersecurity environment**. IT Governance Publishing, 2014.

MILLER, Bill; ROWE, Dale. A survey SCADA of and critical infrastructure incidents. In: **Proceedings of the 1st Annual conference on Research in information technology**. p. 51-56, 2012.

MITNICK, Kevin D.; SIMON, William L. **A Arte de Enganar: Controlando o Fator Humano na Segurança da Informação**. Pearson Education. São Paulo: 2003.

MUSCANELL, Nicole L.; GUADAGNO, Rosanna E.; MURPHY, Shannon. Weapons of influence misused: A social influence analysis of why people fall prey to internet scams. **Social and Personality Psychology Compass**, v. 8, n. 7, p. 388-396, 2014.

NAUMOVSKI, Toni; TANESKI, Nenad. Social engineering in the context of cyber security. In: **10 th International scientific conference The great power influence on the security of small states**. Univerzitet" Sv Kliment Ohridski" Bitola-Fakultet za bezbednost-Skopje, 2019. p. 282-292.

NEI. **Cybersecurity**. 2020.Disponivel em: https://www.nei.org/fundamentals/safety/cybersecurity. Acesso em: 20 de janeiro de 2020.

NICHOLSON, A. e colab. SCADA security in the light of Cyber-Warfare. **Computers & Security**, v. 31, n. 4, p. 418–436, 2012.

NIST. SP-800-82-Revison2. **Guide to Industrial Control System (ICS) Security**. 2015.

NOHLBERG, Marcus. Why Humans are the Weakest Link. In: GUPTA, Manish; SHARMAN, Raj (org.). Social and Human Elements of Information Security: Emerging Trends and Countermeasures. **IGI Global**, 2009 p.15-26.

NORTON. **Ameaças Emergentes: O que é smishing**. [S.l] [2019?] Disponível em: https://br.norton.com/internetsecurity-emerging-threats-what-is-smishing.html. Acesso em 28 setembro de 2019.

NPCIL. **Nuclear Power Corporation of India Limited.** Press Release. 2019.

NTI. **Building a Framework for Assurance, Accountability and Action**. Nuclear Security Index. 2018.

NUNES, Paulo. **Ciberameaças e quadro legal dos conflitos no ciberespaço: ameaças e riscos transnacionais no novo mundo global**. Fronteira do Caos. Porto: 2016.

NYE, Joseph. Nuclear Lessons for Cyber Security? United States Air Force. **Strategic Studies Quarterly**, vol 5, n°4, p.18-38, 2011.

ONS. **ONS propõe procedimento de rede sobre segurança cibernética**. Disponivel em: http://www.ons.org.br/Paginas/Noticias/20200424-procedimentoderedesegurancacibernetica.aspx. Acesso em 2 de setembro de 2020.

____. **Impactos da Suspensão da Operação das UTNs**. 2017.

ORGILL, Gregory L. et al. The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. In: **Proceedings of the 5th conference on Information technology education**. p. 177-181, 2004.

ONYEJI, Ijeoma; BAZILIAN, Morgan; BRONK, Chris. Cyber Security and Critical Energy Infrastructure. **The Electricity Journal**, v. 27, n. 2, p. 52–60, 2014.

OWEN-JACKSON, Charles; CASEY, Suraya. **A proteção para quem trabalha em casa não envolve apenas tecnologia, mas também a cultura corporativa**. 2020. Disponível em: https://www.kaspersky.com.br/blog/secure-futures-magazine/securing-home-workers/14830/. Acesso em 9 de abril de 2020.

PAGANINI, Pierluigi. **The Most Common Social Engineering Attacks**. Disponível em: https://resources.infosecinstitute.com/common-social-engineering-attacks/#gref. Acesso em 17 outubro de 2019.

PEREKALIN, Alex. **Weaponized USB devices as an attack vector**. 2019. Disponível em: https://www.kaspersky.com/blog/weaponized-usb-devices/26495/. Acesso em: 23 de maio de 2020.

PIB. **Cyber Attacks on Indian Nuclear Power Plants**. 2019. Disponível em: https://pib.gov.in/newsite/PrintRelease.aspx?relid=195144. Acesso em 19 de janeiro de 2020.

PIGGIN, R. S. H. Emerging good practice for cyber security of Industrial Control Systems and SCADA. In: **7th IET International Conference on System Safety, incorporating the Cyber Security Conference 2012**. IET, p. 1-6, 2012.

PMI. **A Guide to the Project Management Body of Knowledge** (PMBOK® Guide). Project Management Institute. Pensilvania: 2017.

POLLACK, J; RANGANATHAN, P. Social Engineering and Its Impacts on Critical Infrastructure: A Comprehensive Survey. In: **Proceedings of the International Conference on Security and Management (SAM)**. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2018. p. 122-128.

PROFPOINT. **Human Factor Report**. 2019.

PWC. **Cybersecurity in the nuclear industry: Growing threats and evolving practices**. 2019.

RHEE, Hyeun-Suk; KIM, Cheongtag; RYU, Young U. Self-efficacy in information security: Its influence on end users' information security practice behavior. **Computers & Security**, v. 28, n. 8, p. 816-826, 2009.

SALAHDINE, Fatima; KAABOUCH, Naima. Social engineering attacks: A survey**.** **Future Internet**, v. 11, n. 4, p. 89, 2019.

SAMANI, Raj.; MCFARLAND, Charles. **Hacking the human operating system: The role of social engineering within cybersecurity**. 2015. Disponível em: https://community.mcafee.com/t5/Documents/Hacking-the-Human-Operating-System-Raj-Samani/ta-p/550808?attachment-id=6539. Acesso em: 10 julho de 2019.

SAMUEL, Cherian; SHARMA, Munish. **Kudankulam: One Incident, Many Facets**. 2019. Diponível em: https://idsa.in/system/files/issuebrief/kudankulam-incident-cherian-munish-161219.pdf. Acesso em: 06 fevereiro 2020.

SANTOS JUNIOR, E. R.; Naves, G.A.. Segurança e Defesa Cibernéticas: Melhores Práticas e Lições Aprendidas. Inter-American Defense College - **Cyber Security and Defense Conference**, Washington D.C., EUA, p. 8 - 24.

SHU, Xiaokui et al. Breaking the target: An analysis of target data breach and lessons learned. **arXiv preprint arXiv:1701.04940**, 2017.

SILVA, Walbery Nogueira de Lima. **Atuação colaborativa da Defesa Cibernética na proteção de infraestruturas críticas**. 2019.

SIMONENKO, Maksim. Stuxnet and Nuclear Enrichment ff the Cyber Security Regime. **Security Index: A Russian Journal on International Security,** v. 19, n. 2, p. 85-97, 2013.

SONG, Jae-Gu et al. A Cyber Security Risk Assessment for the Design of I&C Systems in Nuclear Power Plants. **Nuclear Engineering and Technology**, v. 44, n. 8, p. 919–928, 2012.

SONICWALL. **Undermasking the Threats that Target Global Enterprises, Governments & SMBs**. 2019.
SPRINGER, Paul J. (Ed.). Encyclopedia of Cyber Warfare. ABC-CLIO, 2017.

STEINMETZ, K. F.; PIMENTEL, A.; GOE, W.R. Decrypting Social Engineering: An Analysis of Conceptual Ambiguity. **Critical Criminology**, p. 1-20, 2019.

STOUTLAND, Page; DUMBACHER, Erin; MILLER, Margaret Nina. Enhancing Global Cybersecurity Capacity at Nuclear Facilities. **International Conference on Nuclear Security. 2020**.

SUDHAKAR, P. **No cyberattack on Kudankulam Nuclear Power Plant, say officials**. Disponivel em: https://www.thehindu.com/news/national/tamil-nadu/kudankulam-nuclear-power-plant-says-network-is-safe/article29820186.ece. Acesso em: 5 de janeiro de 2020.

TOMAS, Karen. **Social engineering seen as rising cyber threat to nuclear industry**. 2016. Disponível em: https://analysis.nuclearenergyinsider.com/social-engineering-seen-rising-cyber-threat-nuclear-industry. Acesso em: 4 de fevereiro de 2019.

TUGRUL, a. Breril. Cyber security for nuclear installations. In: Guido GLUSCHKE, Mesut Hakkı CAŞIN; Marco MACORI. Cyber Security Policies and Critical Infrastructure Protection. Potsdam: **Institute for Security and Safety (ISS) Press**, 2018. p.139.

ZIEME, Nicole; TURCOTTE, Jaiden. **Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies**. 2016.

VAN DINE, Alexandra; Dine, ASSANTE, Michael; STOUTLAND, Page. **Outpacing Cyber Threats: Priorities for Cybersecurity at Nuclear Facilities**. Nuclear Threat Iniciative. 2016.

VARVARA. **10 Most Common Phishing Attacks**. 2018. Disponível em: https://resources.infosecinstitute.com/10-most-common-phishing-attacks. Acesso em 15 outubro de 2019.

VARUTTAMASENI, Athi; BARI, R.; YOUNGBLOOD, Robert. **Construction of a Cyber Attack Model for Nuclear Power Plants**. Brookhaven National Laboratory, 2017.

VERIZON. **2019 Data Breach Investigation Report.** 2019.

WATSON, Gavin; MASON, Andrew; ACKROYD. Richard. **Social Engineering Penetration Testing: Executing Social Engineering Pen Tests, Assessments and Defense**. Elsevier. 2014.

WORLD ECONOMIC FORUM. **The Global Risk Report 2019**. 2019.

YEBOAH-BOATENG, Ezer Osei; AMANOR, Priscilla Mateko. Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. **Journal of Emerging Trends in Computing and Information Sciences**, v. 5, n. 4, p. 297-307, 2014.

YIN, R. K. **Estudo de caso: planejamento e métodos**. 2 ed. Porto Alegre: Bookman, 2001.

ZETTER, Kim. **Countdown to Zero Day: Stuxnet and the Launch of the World´s First Digital Weapon**. Broadway Books. Nova Iorque: 2014.

ZULKURNAIN, Ahmad Uways et al. Social engineering attack mitigation. **International Journal of Mathematics and Computational Science**, v. 1, n. 4, p. 188-198, 2015.

ANEXO I

Consulta realizada à empresa Eletronuclear, por meio do Sistema Eletrônico do Serviço de Informação do Cidadão (e-SIC). As perguntas e respectivas respostas encontram-se na íntegra, sem alteração de conteúdo ou grafia, apenas de diagramação.

Órgão superior destinatário: ELETROBRAS – Centrais Elétricas Brasileiras S.A
Órgão vinculado destinatário: ELETRONUCLEAR – Eletrobrás Termonuclear S.A
***Site*:** https://esic.cgu.gov.br
Protocolo de consulta: 99908000057202012
Data do envio: 27/01/2020
Data da resposta: 04/02/2020

Pergunta 1 - Além dos documentos normativos internos da Eletrobras, como a Política de Segurança da Informação, quais outros instrumentos normativos, nacionais e internacionais, são utilizados pela Eletronuclear para orientar a segurança cibernética da empresa?
Resposta: Normas da ISO\IEC, NIST, CNEN, não se limitando a estes.

Pergunta 2 - Existem programas internos de treinamento e campanhas de conscientização corporativa para os funcionários e colaboradores da Eletronuclear, em especial para o ambiente da CNAAA, no que tange a segurança cibernética? Caso positivo, qual a periodicidade desses treinamentos?
Resposta: Sim. Anual.

Pergunta 3 - Existem documentos internos que orientam os funcionários e colaboradores a não divulgar informações corporativas na Internet (redes sociais, fórum online etc.) que possam prejudicar a gestão da segurança da Eletronuclear? Caso positivo, quais são esses documentos?
Resposta: Sim. Política de Segurança da Informação; Boas Práticas? Tipos mais comuns de incidentes de Segurança da Informação etc.

Pergunta 4 - Nos contratos da Eletronuclear com as empresas prestadoras de serviço são incluídas cláusulas específicas sobre segurança da informação?
Resposta: Sim.

Pergunta 5 - Quantos incidentes cibernéticos, ocasionados por ataques cibernéticos, ocorreram no ambiente da CNAAA de 2015 a 2019?
Resposta: Sem resposta, conforme Art. 22 da LAI. (ABAIXO)

Pergunta 6 - Existem procedimentos para evitar que pendrives e dispositivos de armazenamento externos possam infectar os computadores da CNAAA, tal como bloqueio de portas USB?
Resposta: Sem resposta, conforme Art. 22 da LAI. (ABAIXO)

Pergunta 7 - É permitido aos visitantes o uso de dispositivos digitais, como smartphones e notebooks, no interior das instalações da CNAAA?
Resposta: Sem resposta, conforme Art. 22 da LAI. (ABAIXO

Pergunta 8 - Os funcionários e colaboradores da CNAAA podem utilizar dispositivos digitais pessoais, como smartphones e notebooks, nos ambientes administrativo e de operação?
Resposta: Sem resposta, conforme Art. 22 da LAI. (ABAIXO)

Pergunta 9 - Das seguintes tecnologias, quais são utilizadas para a proteção do ambiente cibernético da CNAAA: firewall, IDS/IPS, antivírus, SIEM, AntiSpam?
Resposta: Sem resposta, conforme Art. 22 da LAI. (ABAIXO)

CAPÍTULO IV - DAS RESTRIÇÕES DE ACESSO À INFORMAÇÃO
Art. 22. O disposto nesta Lei não exclui as demais hipóteses legais de sigilo e de segredo de justiça nem as hipóteses de segredo industrial decorrentes da exploração direta de atividade econômica pelo Estado ou por pessoa física ou entidade privada que tenha qualquer vínculo com o poder público.

ANEXO II

Este anexo apresenta as perguntas realizadas nas entrevistas por email com os especialistas citados no quadro 1.

1. Qual o grau de importância da engenharia social nos ataques cibernéticos atuais?
2. Quais os possíveis riscos, para ambientes cibernéticos em infraestruturas críticas, de ataques de engenharia social? Quais os impactos para esses ambientes críticos?
3. Quais são os métodos de ataques de engenharia social mais utilizados em ataques cibernéticos que visem os ambientes críticos industriais?
4. Que mecanismos de proteção podem ser aplicados para mitigar ações de engenharia social em ambientes cibernéticos de infraestruturas críticas?
5. Quais instrumentos normativos, nacionais e internacionais, podem ser utilizados para orientar a segurança cibernética de infraestruturas críticas?
6. Quais métodos de proteção podem ser implementados em ambientes cibernéticos para mitigar ataques de engenharia social?
7. Quais os riscos do uso de dispositivos móveis e de Wi-Fi em ambientes de infraestruturas críticas?
8. Qual o grau de importância da capacitação de pessoal e das campanhas de conscientização para a mitigação de incidentes cibernéticos no setor nuclear?
9. Qual o grau de maturidade do setor nuclear nacional no que concerne à segurança cibernética, isto é, o nível de segurança cibernética do setor nuclear no Brasil equivale aos níveis adotados internacionalmente?