UNIVERSIDADE DA FORÇA AÉREA
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIAS AEROESPACIAIS
MESTRADO PROFISSIONAL EM CIÊNCIAS AEROESPACIAIS

PATRÍCIA SALES DE OLIVEIRA

A Segurança da Informação e a Engenharia Social na FAB à Luz dos casos RSA, Sony Pictures e Ubiquiti Networks

Rio de Janeiro
2019

UNIVERSIDADE DA FORÇA AÉREA

PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIAS AEROESPACIAIS
MESTRADO PROFISSIONAL EM CIÊNCIAS AEROESPACIAIS

PATRÍCIA SALES DE OLIVEIRA

A Segurança da Informação e a Engenharia Social na FAB à Luz dos casos RSA, Sony Pictures e Ubiquiti Networks

Dissertação apresentada ao Programa de Pós-Graduação em Ciências Aeroespaciais da Universidade da Força Aérea, como requisito parcial para obtenção do título de Mestre em Ciências Aeroespaciais.

Orientador: Prof. Dr. Newton Hirata
Coorientador: Prof. Dr. Pedro Arthur Linhares Lima

Rio de Janeiro
2019

Ficha catalográfica elaborada pela Biblioteca da UNIFA

O48

Oliveira, Patricia Sales.

A Segurança da Informação e Engenharia Social na FAB à Luz dos casos RSA, Sony Pictures e Ubiquiti Networks / Patrícia Sales Oliveira. – Rio de Janeiro: Universidade da Força Aérea, 2019.

121 f.: il., enc.

Orientador: Newton Hirata.

Coorientador: Pedro Arthur Linhares Lima.

Dissertação (mestrado) – Universidade da Força Aérea, Rio de Janeiro, 2019.

Referências: f. 88-98

1. Emprego do Poder Aeroespacial. 2. Engenharia Social. 3. Redes Sociais. 4. Ciberespaço I. Título. II. Oliveira, Patricia Sales. III. Universidade da Força Aérea

CDU: 335.356(811)

PATRÍCIA SALES DE OLIVEIRA

A Segurança da Informação e a Engenharia Social na FAB à Luz dos casos RSA, Sony Pictures e Ubiquiti Networks

Dissertação apresentada ao Programa de Pós-Graduação da Universidade da Força Aérea, como requisito parcial para obtenção do título de Mestre em Ciências Aeroespaciais.

Aprovado por:

_____

Presidente, Professor Doutor Newton Hirata (AFA/UNIFA)

Professor Doutor Pedro Arthur Linhares Lima (Coorientador) (UNIFA)

Professor Doutor Claudio Rodrigues Corrêa (EGN))

Professor Doutor Gills Vilar Lopes (UNIFA)

Professora Mestre Constança Maria Maia Arruda (CCA-RJ/COMAER)

Rio de Janeiro
Dezembro de 2019

DEDICATÓRIA

Ao longo de nossas vidas somos abençoados com os presentes que Deus nos proporciona experimentar. A presença, junto a nós, de pessoas que nos amam e que amamos. Tudo inicia, em sua essência, no ventre materno e no conforto sereno dos pais. Eles são a base para que aprendamos a valorizar aquilo que há de mais importante em nossas vidas, o alicerce do nosso caminho e a estrutura emocional de cada conquista, a família e a amizade. Dedico este trabalho a três mulheres maravilhosas que tive o privilégio de conviver, a minha Mãe, incondicionalmente apoiadora de tudo que fiz, a minha amiga irmã Simone Já como e a minha prima Simone Coutinho que nos deixaram para prosseguir sua missão em outro plano.

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter me dado as forças necessárias para a conclusão deste trabalho e não permitir que eu desistisse dos meus ideais.

À Força Aérea Brasileira, a minha continência, meu reconhecimento, meu eterno respeito e admiração por ter me permitido realizar este trabalho.

Ao meu orientador, Prof. Dr. Newton Hirata, pela orientação, pela incomensurável paciência e inabalável crença na possibilidade de concretização deste trabalho apesar de todas as dificuldades encontradas pela autora.

Ao Professor Doutor Brigadeiro Intendente Pedro Arthur Linhares Lima, Professor Doutor Goldoni e a Professora Constança Maria Maia Arruda, que compuseram a banca de qualificação, cujas observações pertinentes e precisas tornaram meu caminho mais certeiro nos desafios desta pesquisa.

In memoriam ao meu pai, avó e sogro, sempre presentes em meus pensamentos.

Ao meu marido Narciso e aos meus filhos Bruno e Patrick, embora nem sempre compreendendo, terem aceitado as ausências na busca do ato solitário de escrever.

Aos meus queridos: Pai Hélcio, Coronel Engenheiro Ricardo Andrade Faulhaber e ao irmão de armas Glaucio da Rocha Silveira pelo incentivo e pela mão amiga na hora certa, sempre me apoiando e dando forças e nunca deixando que eu desistisse, mesmo nos momentos mais difíceis.

*"*O Mérito Supremo consiste em quebrar a resistência do inimigo sem lutar."

Sun Tzu

"...o poder é definido como a habilidade de um determinado elemento fazer com que outro realize algo que não faria de outra forma..."

Armistead

"Quem tem a informação, tem o poder."

Provérbio Português

RESUMO

Apesar de todo o avanço tecnológico, o ataque de engenharia social por meio de informações disponibilizadas nas redes sociais ainda é bastante explorado. Na tentativa de compreender melhor a temática, o presente trabalho tem como objetivo contribuir com a identificação de regras e procedimentos com vistas à segurança da informação, particularmente no que diz respeito à engenharia social. Em termos metodológicos, trata-se de uma pesquisa qualitativa, exploratória, descritiva e explicativa com base em estudos de caso. Para alcançar o objetivo, foram definidos os seguintes objetivos específicos: apresentação de uma revisão bibliográfica sobre engenharia social, considerando um contexto de redes sociais, ciberespaço e guerra híbrida; elaboração de um breve panorama da defesa cibernética sob a ótica do Estado brasileiro; identificação das ações de engenharia social, por meio de três casos analisados (RCA, Sony Pictures e Ubiquiti Networks). A partir dessa trajetória, buscou-se fornecer subsídios para a elaboração de uma política de utilização das redes sociais na Força Aérea Brasileira que salvaguarde a segurança da informação, a segurança das operações, e que evite a adoção de condutas pessoais inapropriadas. O trabalho inclui também breves considerações acerca de uma proposta de conscientização em todos os níveis do COMAER.

Palavras-chave: Emprego do Poder Aeroespacial. Engenharia Social. Redes Sociais. Ciberespaço.

ABSTRACT

Despite all the technological advances, the attack of social engineering through information available on social networks is still quite explored. In an attempt to better understand the theme, this present work aims to contribute to the identification of rules and procedures with a view to the security of the information, particularly in regards of social engineering. In methodological terms, it is a qualitative, exploratory, descriptive and explanatory research based on case studies. To achieve the objective, the following specific objectives were defined: presentation of a literature review on social engineering, considering a context of social networks, cyberspace and hybrid war; elaboration of a brief overview of cyber defense from the perspective of the Brazilian State; identification of social engineering actions, through three analyzed cases (RCA, Sony Pictures and Ubiquiti Networks). From this trajectory, we sought to provide subsidies for the elaboration of a policy for the use of social networks in the Brazilian Air Force that safeguards security of the information, the security of operations, in order to avoid the adoption of inappropriate personal conduct. The work also includes brief considerations regarding an awareness proposal at all levels of COMAER.

Keywords: *Aerospace Power Employment. Social Engineering. Social networks. Hybrid War. Cybernetics.*

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ABIN – Agência Brasileira de Inteligência

ABNT – Associação Brasileira de Normas Técnicas

APF – Administração Pública Federal

CCA-BR – Centro de Computação da Aeronáutica de Brasília

CCA-RJ – Centro de Computação da Aeronáutica do Rio de Janeiro

CCA-SJ – Centro de Computação da Aeronáutica de São José dos Campos

COMAER – Comando da Aeronáutica

CTIR – Centro de Tratamento de Incidentes em Redes de Computadores da Força Aérea Brasileira

C² – Comando e Controle

CDCiber – Centro de Defesa Cibernética do Exército

CDN – Conselho de Defesa Nacional

ComDCiber – Comando de Defesa Cibernética

CREDEN – Câmara de Relações Exteriores e Defesa Nacional

DCA – Diretriz do Comando da Aeronáutica

DTI – Diretoria de Tecnologia da Informação da Aeronáutica

DCTA – Departamento de Ciência e Tecnologia Aeroespacial

DCT – Departamento de Ciência e Tecnologia

DCTIM – Diretoria de Comunicações e Tecnologia da Informação da Marinha

ENaDCiber – Escola Nacional de Defesa Cibernética

END – Estratégia Nacional de Defesa

ETIR – Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais

FAB – Força Aérea Brasileira

IBGE – Instituto Brasileiro de Geografia e Estatística

PND – Política Nacional de Defesa

Sefti – Secretaria de Fiscalização de Tecnologia da Informação

STI – Sistema de Tecnologia da Informação do Comando da Aeronáutica

TCU – Tribunal de Contas da União

TI – Tecnologia da Informação

TIC – Tecnologia da Informação e Comunicação

TO – Teatro de Operações

SUMÁRIO

1 INTRODUÇÃO

> Você se lembra da vida antes do fax, do *e-mail* e da busca *online*? Você se lembra de marcar uma consulta no seu médico para ter uma opinião sobre determinada doença sem dar uma olhada no *Google* antes? É como um filme que você assistiu anos atrás, cujo enredo lhe é vagamente familiar, mas sem nenhuma relevância na sua vida cotidiana. É assim que você vai pensar da *web* atual versus a *web* social que está se expandindo diariamente. O epicentro da *social web* é o *Facebook*. Você já sabe que o *site* tem mais de 500 milhões de usuários. Mas você sabia que as pessoas gastam 700 bilhões de minutos na gigantesca rede social por mês, ou que o Facebook acaba de ultrapassar o Google como o site número um da Internet? O planeta é todo Google e Facebook atualmente e nós apenas surfamos em suas ondas (VALLS, 2010, p. 1).

Em um passado recente, seria impossível imaginar todo o avanço tecnológico à disposição hoje, em especial, a utilização da Internet em larga escala. Sem ela, é uma tarefa difícil conseguir trabalhar, estudar e até mesmo viver no século XXI.

De acordo com a Pesquisa Nacional por Amostra de Domicílios (INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA, 2018), foi constatado que a Internet era utilizada em 74,9% dos 70 milhões 382 mil domicílios particulares permanentes do País. Nas cinco grandes regiões brasileiras, o acesso à Rede tem essa distribuição: Sudeste, 76,5%, Centro-Oeste, 76,6%, Sul, 73,2%, Norte, 60,1%; e Nordeste, 58,4%.

A utilização dos s*martphones* contribuiu para um aumento da quantidade de domicílios acessando a Internet, particularmente a região Nordeste, que apontou, como principal motivo da não utilização, o custo de acesso (INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA, 2018). O número de pessoas conectadas à Internet no Brasil chegou a 126 milhões, destes, quase 95% são usuários assíduos de aplicações web, bem como utilizam de forma regular, a troca e compartilhamento de mensagens, áudios, fotos e vídeos em plataformas sociais (INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA, 2018).

Em termos mundiais, os sites *HootSuite* e *We Are Social* apontaram para 4,2 bilhões de usuários de Internet em todo o mundo em outubro de 2018: uma elevação de 7% em relação ao ano anterior (WE ARE SOCIAL, 2018). A pesquisa indica também que cerca de 3,4 bilhões de pessoas no mundo usaram, especificamente, as mídias sociais em setembro de 2018, um aumento de 10% em relação ao mesmo mês do ano anterior.

O relatório da Norton Cyber Security mostra que no Brasil, em 2017, advieram 62 milhões de ocorrências de ataques cibernéticos. A estimava de perda financeira é de quase R$ 83 bilhões, cotação do dólar em julho de 2018, ficando atrás apenas da China, com quase R$ 246 bilhões de prejuízos com ataques cibernéticos (JOHNSON, 2014).

No Brasil, em 2000, o número de usuários da Internet girava em torno de 8,5 milhões e o governo brasileiro alertava que tal número era bastante limitado e precisaria crescer significativamente. Naquele ano, estimava-se que apenas 1% dos usuários da Internet no Brasil compraria em lojas virtuais, com média de gasto de apenas 18 dólares mensais (INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA, 2018).

No final de 2008, passou-se a contar com cerca de 60 milhões de usuários no Brasil segundo a Pesquisa Nacional por Amostra de Domicílios (PNAD) e, aproximadamente, 83 milhões de pessoas com 10 anos ou mais acessaram a Internet nos três meses anteriores à realização da PNAD em 2012, apontando para um crescimento rápido de uso da Internet no Brasil. Com relação à evolução da economia digital no País, os internautas contribuíram com o comércio eletrônico, com faturamento da ordem de 8,2 bilhões de reais em 2008 com crescimento de cerca de 22,5 bilhões de reais em 2012, confirmando as prospecções de avanços preponderantes desta economia digital (INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA, 2018).

Em 2014, o Brasil foi considerado o quarto maior mercado mundial no setor de TIC (Tecnologia da Informação e Comunicação), movimentando em torno de US$ 170 bilhões, e somente o comércio eletrônico faturou 35,8 bilhões de reais, e no mundo o movimento foi de cerca de 1,5 trilhão de dólares, demonstrando quão aquecida e intensa vem sendo a economia digital e com tendência ascendente. Conforme notícia divulgada em 7 de agosto de 2019, o Brasil é o quarto maior mercado de TIC do mundo movimentando US$ 169 bilhões, sendo responsável por 5% dos negócios no referido setor, em âmbito mundial e podendo crescer com o acordo com a União Europeia. Para 2020, estima-se um mercado global de TI na ordem de US$ 3 trilhões, e um mercado nacional da ordem de US$ 200 bilhões (ALMEIDA; CAGNIN, 2019).

De acordo com Cassanti (2014), a informação é um dos ativos mais preciosos da humanidade; aquele que a detém também deterá o poder. Deste modo, sua

busca levará, em muitos casos, à perda do escrúpulo e da ética. Ainda de acordo com o autor, embora a Internet tenha o poder de unir os povos independentemente da religião, cultura, modo de viver ou, até mesmo, a distância, ela deixa todos vulneráveis. Isso ocorre por conta de fraudes eletrônicas, sequestros de dados e ataques de engenharia social.

A expressão engenharia social, especificamente no contexto da segurança da informação, está relacionada à prática de iludir, trapacear e induzir alguém a cometer um erro involuntário. A partir de um conjunto de estratégias, o responsável pela engenharia social desenvolve um plano para acessar dados e informações, sem o uso da força, que contêm valor e algum nível de sigilo. As pessoas, vítimas do plano criminoso, são enganadas e traídas pela boa fé, inocência e falta de experiência para lidar com criminosos e pessoas mal-intencionadas com algum preparo para, sutilmente, atingir seu objetivo. Portanto, pequenas ações e descuidos, aparentemente inofensivos, podem gerar danos reais e potenciais significativos.

Nesse sentido, diversas organizações têm apresentado crescente preocupação quanto ao vazamento de informações e ao meio pelo qual elas são disponibilizadas pelos seus funcionários, muitas vezes em comentários em suas redes sociais. De acordo com Straumsheim (2010), “inconscientemente, os colaboradores contribuem para que os *hackers* consigam informações sobre si, por meio de redes sociais, e daquilo que é considerado a sua vida pessoal” (tradução nossa).

Por meio das redes sociais é criado um elo entre o hacker e a vítima, que, por estar, muitas vezes, desprotegida, acaba fornecendo informações pessoais, fotografias, nomes, localizações, contatos, estado profissional, experiências, formação, grupos de interesse, eventos e aplicativos de envio de mensagens. De posse desses dados, basta o hacker criar a condição certa para o ataque.

Em junho de 2013, a imprensa internacional tomou conhecimento de como é frágil o sistema relacionado à privacidade das informações pessoais em diferentes mídias. As informações foram disponibilizadas por meio do site WikiLeaks, pelo Analista de Sistemas Edward Snowden, ex-funcionário da Agência Central de Inteligência (CIA) e ex-contratado da Agência de Segurança Nacional (NSA), dos Estados Unidos da América (EUA). Snowden revelou documentos secretos que mostraram como o governo americano monitorava seus cidadãos. Segundo essas

fontes, a NSA desenvolveu um sistema chamado Turbine, criado para gerenciar milhões de computadores infectados por códigos espiões. Ele gerenciava os diversos programas instalados pela NSA em computadores que seriam remotamente controlados (SILVA, 2015).

De acordo com os documentos expostos, tais programas permitiam o acesso ao sistema infectado, podendo realizar o acionamento de microfones e webcams para capturar conversas e imagens, além de habilitar rotinas que registram senhas usadas na web e o histórico de navegação. Ainda em 2013, no mês de dezembro, Snowden divulgou que o Brasil também foi objeto de espionagem americana. Ele disponibilizou ligações telefônicas e trocas de e-mails entre empresas e políticos brasileiros.

Pode-se dizer que o “Caso Snowden” foi um marco na história da Internet em geral e, em particular, da percepção das pessoas em relação à privacidade de suas relações e os limites de acesso a dados e assuntos privados. O tema afeta do cidadão comum, em suas relações pessoais e profissionais, até os mais poderosos chefes de Estado e suas decisões nas relações internacionais e em assuntos domésticos. Afeta também grandes grupos empresariais e seus negócios bilionários, bem como, pessoas públicas e líderes das mais variadas áreas.

Há pelo menos dois conflitos de interesse nesse debate. De um lado, o monitoramento das pessoas pode estar ligado a uma questão de segurança nacional, particularmente após o divisor de águas nas relações internacionais que foram os atentados de 11 de Setembro. Em nome do bem maior e da segurança coletiva, há quem considere aceitável a possiblidade de as pessoas serem de alguma forma monitoradas e investigadas se houver necessidade. E, de outro lado, está uma perspectiva ética e moral acerca da privacidade, da liberdade e do direito que os cidadãos têm de resguardar seus assuntos e interesses particulares e também por conta de relações comerciais envolvendo empresas e países (GARNIER; PADILHA, 2019).

Para o presente trabalho, a perspectiva não é o monitoramento das pessoas para o bem da segurança coletiva e tampouco a pauta da garantia da liberdade individual dos cidadãos. O foco está na proteção do Estado e suas instituições, particularmente organizações militares, frente a possíveis incidentes e ataques de engenharia social.

As Forças Armadas em geral, sobretudo de um país da dimensão econômica, política, estratégica, geográfica e geopolítica como o Brasil, têm a necessidade de um olhar mais atento e criterioso quanto ao uso das redes sociais. É uma preocupação que cabe não apenas nas dependências físicas de suas instalações, mas também no comportamento das pessoas fora delas. As Forças Armadas, por definição, resguardam infraestruturas críticas, recursos materiais e humanos, dados e informações que, no seu conjunto, respondem pela garantia da integridade e soberania do país. E as redes sociais, por casos já verificados na literatura, podem representar uma ameaça a essa missão.

Com a Internet e a utilização das redes sociais, a divulgação de informações, que antes era realizada em um ritmo razoavelmente lento, passou a acontecer de um modo mais dinâmico e a um número maior de pessoas. A rede social foi concebida para ser um local informal, que tem como propósito o compartilhamento de informações (TOMAÉL, 2007).

De acordo com Marques (2017), a segurança de perímetro e os "*endpoints*" ajudam a barrar algumas ameaças, mas não serão capazes de lidar com todos os ataques de engenharia social nas redes sociais. As organizações precisam lidar com esses criminosos, por meio de monitoramento e identificação de vulnerabilidades e possíveis armadilhas. As redes sociais com propagandas, anúncios, perfis e e-mails falsos, endereços eletrônicos adulterados e tantas outras estratégias, podem desencadear uma série de problemas para as organizações, especialmente as militares.

Segundo Malafaia (2017), a segurança se faz presente nas arquiteturas e modelos da informação, neles se inserindo em todos os níveis. Entretanto, observa-se um número crescente de ocorrências de incidentes relativos à segurança da informação. Fraudes digitais, furtos de senhas, cavalos de Tróia[1], vírus e outras formas de ameaças têm se multiplicado.

De acordo com Stassun e Assmann (2012), é observado que, com o advento das redes sociais, as vulnerabilidades de caráter humano são potencializadas pelo fenômeno conhecido como "hipermobilidade estética dos internautas". Tem como característica precípua a necessidade de o sujeito se sentir importante por meio do (re)conhecimento e aparência com que se revela nas redes sociais, por meio de

1. Códigos de programas aparentemente inofensivos, mas que guardam instruções danosas ao usuário, ao software ou ao equipamento

suas informações e intimidade expostas de forma intencional e como se fosse um espetáculo. Dessa forma, o ambiente online é identificado como um dos nichos de atuação dos engenheiros sociais, devido à grande acessibilidade, exposição, instantaneidade e a falhas de gestão da segurança da informação.

As Forças Armadas, em particular, caracterizam-se por tornar as suas organizações sensíveis em termos de segurança nomeadamente no que diz respeito à Segurança da Informação. O papel que seus funcionários, militares ou civis, podem ter na revelação de matérias sensíveis ou confidenciais, ainda que o façam, majoritariamente de forma inconsciente ou por não terem conhecimento adequado sobre a exposição desnecessária em redes sociais, constitui a principal ameaça (LIMA, H., 2015).

A motivação para esse estudo é a percepção da relevância do tema Segurança da Informação nas organizações militares, face às expectativas para o cumprimento da missão.

A questão de pesquisa pode assim caracterizar-se como: de que modo uma organização militar pode se preparar para minimizar os riscos de invasão aos sistemas informatizados por meio de um ataque de engenharia social?

Especificamente, a motivação para este trabalho desembocou no conceito de engenharia social, uma estratégia razoavelmente simples e barata, mas com possibilidade de gerar danos sérios. Como questões auxiliares, a engenharia social é de fato uma ameaça para as Forças Armadas mais especificamente à Força Aérea Brasileira? Quais são os riscos envolvidos e de que forma é possível enfrentá-la?

A pesquisa ora apresentada se constitui em um processo de aprendizado, mas também, espera-se, que sirva como uma contribuição ao debate e, eventualmente, às políticas e ações a serem colocadas em prática para fortalecer os sistemas de segurança da informação da Força Aérea Brasileira, das Forças Armadas e de outras instituições públicas e privadas.

Na tentativa de melhor compreender a temática, o presente trabalho tem como objetivo geral contribuir com a identificação de regras e procedimentos com vistas à segurança da informação, particularmente no que diz respeito à engenharia social.

Para alcançar o objetivo geral enunciado, foram definidos os seguintes objetivos específicos (OE):

OE 1: Apresentar uma revisão bibliográfica sobre engenharia social, considerando os contextos de redes sociais, ciberespaço e guerra híbrida;

OE 2: Fornecer um breve panorama da Defesa Cibernética Brasileira;

OE 3: Analisar três casos específicos de engenharia social; e

OE 4: Fornecer subsídios para a elaboração de uma política de utilização das redes sociais que salvaguarde a segurança da informação e das operações no Comando da Aeronáutica, em especial nas Escolas de formação e de pós-formação.

Em termos metodológicos, quanto a seus objetivos o presente estudo classifica-se como uma pesquisa qualitativa, exploratória, descritiva e explicativa. Qualitativa porque foram compreendidos os fenômenos a partir da coleta de dados narrativos, estudando as particularidades e experiências individuais. Utilizam-se observações e comentários para se chegar à conclusão. Exploratória porque, a partir do levantamento bibliográfico, tem-se como escopo proporcionar uma maior familiaridade com o problema, de forma a explicitá-lo (GIL, 2008). De acordo com Lakatos e Marconi (1991, p. 73), “a pesquisa bibliográfica não é mera repetição do que já foi dito ou escrito sobre certo assunto, mas propicia o exame de um tema sob novo enfoque ou abordagem, chegando a conclusões inovadoras”.

A pesquisa é descritiva, de acordo com Mattar (1999, p. 85), por possuir objetivos bem definidos e procedimentos formais para a solução de problemas ou avaliação de alternativas de cursos de ação. Na acepção de Silva e Menezes (2005, p. 21), este tipo de pesquisa “visa descrever as características de determinada população ou fenômeno ou o estabelecimento de relações entre variáveis”. É explicativa porque visa identificar os fatores que determinam ou contribuem para a ocorrência de fenômenos (GIL, 2008).

Quanto aos procedimentos técnicos, a pesquisa utiliza os estudos de caso. De acordo com Yin (2010), tal estudo constitui uma investigação empírica que examina um fenômeno contemporâneo em seu contexto real, especialmente quando seus limites não estão claramente definidos. Deste modo, o estudo foi utilizado porque os objetivos desta pesquisa se concentram na análise de experiências empíricas e na associação destas experiências a formulações teóricas consistentemente embasadas, ou seja, a partir da teoria aplicada, apresentam-se propostas e condições para a ocorrência ou não de determinadas situações.

O presente estudo é uma pesquisa qualitativa fundamentalmente concentrada em pesquisa bibliográfica, tendo como fonte primária: legislações, documentos e relatórios governamentais. Foram consultadas também reportagens e análises da grande mídia, em particular, considerando os três casos escolhidos. Em um primeiro momento, discutiu-se a ideia de analisar possíveis ataques de engenharia social nas Forças Armadas brasileiras, mas, por questões estratégicas, optou-se por selecionar ataques de engenharia social ocorridos fora do País e amplamente divulgados.

Busca-se atender o objetivo geral e os objetivos específicos em cinco seções. Na primeira, a Introdução, é apresentado um panorama do tema estudado, localizando o contexto em que ele se insere, indicando abordagens, evidenciando brevemente conceitos e justificando a relevância da pesquisa. Estão presentes também os objetivos, os aspectos metodológicos utilizados e a estrutura da Dissertação.

A seção 2 trata do referencial teórico abordando os conceitos de engenharia social e técnicas usadas nesse tipo de ataque às organizações. Antes de abordar a engenharia social, optou-se por seguir uma breve trajetória começando com a guerra híbrida, passando pelo tema da cibernética como expressão de poder e chegando às redes sociais, em que o chamado “mundo real” se mistura com o “virtual”. Na sequência, busca-se o entendimento da engenharia social, suas principais definições e pressupostos, objetivos, funcionamento e consequências.

De posse desse arcabouço, o passo seguinte foi apresentar na seção 3 um quadro geral da Defesa Cibernética no Brasil. Percebe-se que há um esforço considerável de instituições civis e militares para melhorar a qualidade e a segurança da informação. Verifica-se a existência de um arcabouço legal complexo e um conjunto de iniciativas que tendem a tornar o sistema mais robusto. Todavia, sabe-se que um marco regulatório, embora seja importante, demanda boas práticas das instituições e seus servidores, uma vez que as ameaças evoluem e se transformam muito rapidamente. Um olhar mais atento para os apêndices permitirá ter uma ideia mais pormenorizada das ações e estratégias que o governo brasileiro tem lançado mão nas últimas décadas.

Para a seção 4 são apresentados três casos de ataques que podem ser caracterizados como exemplos de engenharia social. Eles deixam clara a necessidade de se monitorar constantemente todos os canais possíveis para invasão ou incidente. Como todo evento dessa natureza, fica o efeito pedagógico

para que as organizações envolvidas tomem esses exemplos como aprendizado e parâmetro de ação.

A seção 5 traz uma breve análise dos casos apresentados e correlações pontuais com a estrutura atual de Defesa Cibernética na FAB. São elencadas as principais lições aprendidas com a pesquisa como um todo – do levantamento bibliográfico aos casos analisados – que podem contribuir para mitigar os ataques de engenharia social e possíveis desdobramentos.

Finalmente, as considerações finais encerram a pesquisa.

2 ENGENHARIA SOCIAL NO SÉCULO XXI: A AMEAÇA VEM DO CIBERESPAÇO

A informática faz parte da vida de bilhões de indivíduos nas atividades profissionais, acadêmicas, domésticas, de lazer, incluindo compras, transporte, serviços públicos e de saúde, praticamente em todas as atividades humanas. Pessoas, organizações e sociedades estão cada vez mais vinculadas e dependentes dessa área. A modernização modificou a estrutura e a lógica da informação e dos meios de comunicação. Vive-se hoje de forma conectada, cercados de informação por todos os lados.

A resposta sobre as novas tecnologias, particularmente a Tecnologia da Informação e Comunicações (TICs), serem boas ou ruins não está nelas em si, mas, sim, no uso que se faz delas. É possível pensar nos crimes de roubos eletrônicos envolvendo contas bancárias e violações muito mais severas, mas também é possível pensar na medicina exercida à distância tanto para diagnósticos como para tratamentos.

Nesta seção, pretende-se chamar a atenção para os temas da guerra híbrida, a cibernética, as redes sociais e a engenharia social, que têm em comum o avanço da tecnologia e a mudança de comportamento das sociedades atuais. Partindo de uma visão macro para uma perspectiva micro, busca-se compreender como as pessoas no seu dia a dia, particularmente em organizações militares, podem gerar impasses, conflitos e danos de grandes proporções envolvendo países e seus aliados. O que está por trás disso é a postura e decisão do indivíduo, considerando a política da organização, frente ao simples acesso a uma rede de comunicação, algo relativamente trivial hoje em dia.

2.1 A Guerra Híbrida

De acordo com Nozaki (2019), a guerra híbrida é o emprego do poder a partir de um conjunto de intervenções de toda ordem preparada sobre um Estado nacional, para exercer um fim fundamentalmente político. Os agressores tendem a explorar, simultaneamente, todos os modos de guerra, empregando armas

convencionais avançadas, táticas irregulares, tecnologias agressivas, terrorismo e criminalidade, visando desestabilizar a ordem vigente em um Estado nacional.

Já Eissa (2009) defende que o conceito de guerra híbrida procura fundir a letalidade do conflito estatal com o fervor selvagem e fanático da guerra irregular. Esse modelo híbrido implica novas formas de organização e estratégias de ação. As organizações podem ter uma estrutura política hierárquica, acompanhada de células centralizadas ou redes táticas (HOFFMAN, 2007, p. 28). Hoffman, endossando uma ideia de Cohen, diz que as doutrinas militares convencionais do século 20, dirigidas contra as Nações Unidas e exércitos de massa da Era Industrial estão efetivamente mortas (HOFFMAN, 2007, p. 43).

No que diz respeito à mídia, os protagonistas da guerra híbrida podem recorrer ao uso de sistemas de comando criptografados, mísseis terra-ar portáteis, bem como emboscadas, ataques cibernéticos, dispositivos explosivos improvisados e/ou assassinatos. Além disso, em sua aplicação incluem capacidades convencionais, formações e táticas irregulares, atos terroristas, coerção, violência indiscriminada e desordem criminal (HOFFMAN, 2007).

Nozaki (2019) considera que a guerra híbrida é a criação do caos no território inimigo. Pois, de acordo com a teoria do caos, fatores insignificantes, distantes, podem, eventualmente, produzir resultados catastróficos imprevisíveis e absolutamente desconhecidos no futuro. Tais eventos conduzem o adversário a se defrontar com desdobramentos imprevisíveis e a perdas dos monopólios de gestão intrínsecos a um Estado nacional.

Assim, as guerras híbridas seriam, de acordo com Hoffman (2007, p. 16), as irregulares, que, nesta nova era, serão cada vez mais comuns, com maior rapidez e letalidade do que no passado, devido em parte à disseminação de tecnologia militar avançada. Esse tipo de guerra pode ser realizado por ambos os estados e por atores não estatais que podem usar as duas táticas convencional e não convencional, com uso intensivo da tecnologia (HOFFMAN, 2006).

O campo de batalha desse tipo de guerra serão as cidades do mundo em desenvolvimento. As novas zonas de combate incluem as densas florestas urbanas e as costas congestionadas, com concentração da maioria da população e a economia mundial. Essas áreas fornecem abrigos seguros para terroristas ou guerrilheiros urbanos, onde a densidade populacional, as redes de transporte, a infraestrutura e os serviços públicos e as estruturas oferecem múltiplas rotas de fuga

e a capacidade de se esconder durante o planejamento e a prática de operações (futuras) (HOFFMAN, 2007, p. 15).

Com relação ao fator tempo, esses adversários, Estados e atores não estatais, tentarão estender o conflito indefinidamente, evitando o confronto imprevisível e decisivo e buscando a vantagem de formas inesperadas e modeladas (HOFFMAN, 2007).

Segundo Eissa (2009) várias guerras tiveram componentes regulares e irregulares, mas geralmente agiram de maneira diferente e em diferentes locais. Nas guerras híbridas, esses tipos de forças serão mesclados no mesmo campo de batalha (HOFFMAN, 2007). Os atores híbridos buscarão a vitória combinando táticas irregulares e os meios mais letais disponíveis para atacar e alcançar seus objetivos políticos. Do mesmo jeito, a atividade criminosa será usada para sustentar a força híbrida ou para facilitar o distúrbio e a perturbação da nação atacada.

Hoffman (2009) explica que serão usados estes métodos por causa de sua eficácia comprovada. O autor também afirma que não haverá diferença entre oponente convencional e oponente assimétrico, mas sim que os futuros adversários se fundirão e embaçarão a distinção entre as duas formas de guerra (HOFFMAN, 2009, p. 5). Aliado a isto, autor também aponta que a mudança mais significativa no caráter do conflito moderno é a exploração dos meios para alcançar as massas e mobilizá-las em apoio à causa.

Segundo a visão de Hoffman (2007), as Forças Armadas deverão aprender a operar com sucesso neste espaço do campo de batalha em expansão, para manobrar contra a mente dos oponentes e a população em geral. Contudo, não se trata apenas do domínio da informação, mas também da mente ou cultura humana. Esse espaço no campo de batalha é relevante porque a percepção importa mais do que os resultados, porque as comunicações alteram os padrões de mobilização popular, incluindo os meios de participação e os fins pelos quais as guerras são travadas.

Em suma, Frank Hoffman acredita que os novos adversários podem explorar as táticas de inteligência e habilidade, apresentando grande alcance e letalidade. Eles podem usar as redes metropolitanas urbanas para se movimentar e se sustentar em conflitos prolongados (HOFFMAN, 2007).

2.2 A cibernética como expressão de poder

Weber (1991, p. 33) apresenta seu conceito de poder como “[...] toda probabilidade de impor a vontade numa relação social, mesmo contra resistências, seja qual for o fundamento dessa probabilidade”. Da mesma forma, Bobbio, Matteucci e Pasquino (1998) trabalham o poder social como uma relação entre pessoas e não coisas. Estas podem ser objeto de análise, como bens materiais e recursos naturais que estão sendo objeto de disputa e dominação entre pessoas e seus respectivos grupos. Bobbio, Matteucci e Pasquino (1998) citam o exemplo do petróleo como um recurso que pode estar no centro da relação de poder entre as pessoas. Enquanto objeto de valor e de disputa, ele que faz com o poder seja exercido.

Para Bobbio, Matteucci e Pasquino (1998), o poder está para a política assim como a moeda está para a economia, é parte indissociável do sistema, o que o torna um elemento legítimo. Para Bianchi (2014), os sistemas de dominação nos quais o poder se afirma necessitam ser legítimos para serem duráveis. Não há dominação estável sem legitimação e, portanto, sem o reconhecimento daqueles que são dominados.

Perissinotto (2003 *apud* HAYWARD, 2003) acredita que o poder funciona como um instrumento que estabelece os limites de atuação dos atores. Por meio de um conjunto de regras social e politicamente elaboradas e aceitas, a sociedade como um todo, considerando um Estado de Direito, está subordinada a um poder limitador. Tem-se aqui a figura do Estado e suas instituições a quem cabem, em última análise, o poder de regular os interesses e as relações dos diversos atores sociais.

Segundo Merendi (2005), muitas são as formas de exercício do poder. O Poder Estatal é aquele derivado do ente denominado Estado, sua concepção, legitimação e atuação. Esse ente, para muitos considerado abstrato, possui faculdade sobre a vida das pessoas, regulamenta relações, cria normas e leis que organizam a sociedade, impõe sanções e tenta construir a paz e a ordem, por meio de poderes jurídicos e políticos. Assim, ele se edifica, estabiliza e sustenta, exercendo seu poder e o legitimando. Esse poder do Estado é legitimado pelo

direito, que é a regra emanada da sociedade e fundamentada na lei moral e na lei social.

Quando as ações de *A* têm por objetivo influenciar o comportamento de *B*, tem-se um agente exercendo seu poder sobre outro. Por um lado, há uma perspectiva de consentimento dessa influência, de ser algo aceito e voluntário. Todavia, ainda que se trate de um poder coercitivo, é possível uma aceitação de *B*, por conta de eventuais ameaças e sanções impostas por *A* (BOBBIO; MATTEUCCI; PASQUINO, 1998). Aceitar a coerção acaba sendo um cálculo de uma escolha racional da alternativa de menor dano. Implica, nesse sentido, aceitar o exercício do poder por outra pessoa.

Alargando um pouco o conceito de poder, Bobbio, Matteucci e Pasquino (1998) falam da *manipulação* a partir de mecanismos e estratégias utilizados para se atingir determinados objetivos. Isso acontece quando *A* camufla suas ações e intenções e faz com que *B* assuma posições e tome decisões desejadas por *A,* ou seja, *A* somente consegue obter o que deseja por meio de manipulação e, de alguma forma, por ocultar a verdade e suas reais intenções em relação a *B*. A engenharia social, objeto de estudo da presente pesquisa, tem uma relação direta com essa manifestação de poder expressa pela *manipulação*.

O referencial teórico ora apresentado não reside no estudo dedicado do poder enquanto conceito central da Ciência Política. Também não está nas possibilidades de verificação e análise do ponto de vista da soberania ou da manifestação do poder nacional de um país. Não há uma preocupação, portanto, em se dissecar as nuances do poder político, econômico, militar, científico-tecnológico, psicossocial ou cultural. Trabalha-se, fundamentalmente, com a tentativa de construir um marco conceitual que permita compreender o fenômeno da engenharia social como fruto do exercício do poder de *A* sobre *B*. E, como pano de fundo, admite-se o contexto das redes sociais no ciberespaço enquanto ameaça em potencial à defesa e segurança de um país, dadas às vulnerabilidades verificadas adiante. Nesse sentido, no limite, têm-se como principal ativo em pauta, os dados, informações e conhecimentos presentes nos principais repositórios eletrônicos disponíveis e que podem ser estratégicos aos países, suas organizações e instituições.

A questão cibernética e a engenharia social estão muito mais próximas do poder científico-tecnológico e psicossocial, entretanto as outras formas de poder, em maior ou menor grau, são influenciadas por esses dois temas. Podem servir como

instrumentos que diretamente exercem poder de persuasão na arena política, econômica e também militar. Dados sigilosos relacionados a campanhas eleitorais e eleições, estratégias e segredos industriais de empresas públicas ou privadas, tecnologias e projetos militares podem ser alvos de adversários e inimigos reais ou potenciais. E, como mecanismo de acesso a esses dados e informações, tem-se engenharia social.

Resgatando o conceito de “centro de gravidade” de Clausewitz, a cada dia aumenta a dependência das organizações, em relação à estrutura de TI, seus produtos e serviços, próprios ou de terceiros. Invadir e corromper os sistemas informatizados pode implicar a paralisação de toda a organização e em casos extremos, de uma sociedade. Historicamente, a informação representa um elemento de poder. Para cada momento histórico, existem tecnologias que atuam em todo o processo, da sua geração ao uso, passando pela disseminação. Na atualidade, tal limite tem sido influenciado pelo desenvolvimento do ambiente cibernético e todo arsenal tecnológico que o ser humano é capaz de criar. Em outros termos, a informação ganha um novo *status* e potencializa sua representação de poder (ARMISTEAD, 2004).

Ainda de acordo com Armistead (2004), o avanço da computação, das telecomunicações e da tecnologia de mídia modificaram a visão desse poder, tornando a informação, com seu componente cibernético, o seu elemento mais importante. Ainda que nem toda informação seja convertida em conhecimento, há estudos que mostram a quantidade de conhecimentos novos criada nas últimas décadas por conta da revolução das tecnologias de informação e comunicações. Isto é, tem aumentado significativamente a capacidade humana de gerar conhecimento, a despeito de uma quantidade grande de dados ou informações *a priori*, sem valor. Dessa forma,

> Lições aprendidas após a Operação Tempestade no Deserto apontam ao fato de que a nação que puder controlar o fluxo de informações irá vencer o conflito. Quer essa informação esteja na forma de inteligência militar, propaganda, comprimento de ondas eletrônicas ou fluxo de dados computadorizados, a habilidade para manipular informação será a conquista primária dos conflitos futuros (ARMISTEAD, 2004, p. 14).

Nye Junior (2012) trata das diversas manifestações do poder nas relações internacionais. Segundo ele, “o ciberespaço” pode ser entendido como um regime

único de propriedades físicas e virtuais. Para esse autor, no espaço cibernético, as relações não ocorrem somente no mundo virtual, elas têm raízes também físico, sendo assim regidas pelas leis de cada Estado.

Gardini (2014) define o poder cibernético como “a capacidade para obter resultados preferidos mediante o uso dos recursos de informação eletronicamente conectados do domínio cibernético.” Entretanto, Starr (2009) apresenta outra conceituação de poder cibernético. Para ele, “poder cibernético é a capacidade de usar o ciberespaço para criar vantagens e influenciar eventos em outros ambientes operacionais e por meio dos instrumentos de poder.”

Nye Junior (2012) aponta a atuação dos atores no espaço cibernético, em três categorias: governos, organizações com redes altamente estruturadas e indivíduos com redes fracamente estruturadas. No Quadro 1 Nye Junior (2012) descreve os recursos de poder relativo dos atores no domínio cibernético, bem como suas respectivas vulnerabilidades. Trata-se de uma representação sintética que traduz, do macro ao micro, algumas possibilidades de preparação e intervenção bem como os riscos atrelados ao domínio cibernético. Seja do Estado ao indivíduo ou vice-versa, o quadro permite ter uma ideia dos alcances e limites de cada ator nesse processo, possibilitando identificar responsabilidades, além de oportunidades e ameaças.

Quadro 1. Recursos de poder relativo dos atores no domínio cibernético.

RESPONSÁVEL	RECURSOS DE PODER	VULNERABILIDADES
GOVERNOS	1. Desenvolvimento e apoio de infraestrutura, educação e propriedade intelectual. 2. Coerção legal e física de indivíduos e intermediários localizados dentro das fronteiras. 3. Tamanho do mercado e controle de acesso por exemplo, União Europeia, China, Estados Unidos. 4. Recursos para ataque e defesa cibernéticos: burocracia, orçamentos, agências de inteligência. 5. Provisão de bens públicos, como as regulações necessárias para o comércio. 6. Reputação para a legitimidade, benignidade e competência que produzem poder brando.	Alta dependência de sistemas complexos facilmente danificáveis, instabilidade política, possível perda de reputação.
Organizações com redes altamente estruturadas	1. Grandes orçamentos e recursos humanos, economias de escala. 2. Flexibilidade transnacional. 3. Controle de desenvolvimento de código e produto, geração de aplicativos. 4. Marcas e reputação.	Perseguição legal, roubo de propriedade intelectual, danos a sistemas, possível perda de reputação (denúncias).
Indivíduos com redes fracamente estruturadas	1. Baixo custo de investimento para a entrada. 2. Anonimato virtual e facilidade de saída. 3. Vulnerabilidade assimétrica em comparação aos governos e às grandes organizações.	Coerção legal e ilegal por parte dos governos e organizações, caso sejam apanhados.

Fonte: Nye Junior (2012) apud Gardini (2014, p. 13-14).

Um olhar mais detalhado para o Quadro 1 pode apontar para a existência de algumas variações como Estados mais fortes e mais fracos, bem como grupos não estatais. Allen e Chan (2017), em um estudo sobre inteligência artificial e segurança nacional, analisam quatro casos de tecnologias militares transformadoras, quais sejam: nuclear, aeroespacial, cibernética e biotecnológica. Abordando o assunto da cibernética, os pesquisadores chamam a atenção para o uso dessa tecnologia por Estados mais fortes que criam uma infraestrutura robusta, incluindo espionagem e armas, e fortalecem suas operações por meio de redes digitais.

Sob uma outra perspectiva, como existem ações e tecnologias relativamente baratas e de fácil acesso, Estados menores podem utilizar ferramentas cibernéticas para monitorar e perseguir dissidentes políticos, seja dentro, seja fora do país (ALLEN; CHAN, 2017). O cenário se torna mais desafiador, quando grupos não estatais – ou mesmo lobos solitários –, utilizam o ciberespaço para cometer toda a sorte de delitos, incluindo ataques terroristas com vítimas civis em alvos inesperados.

As ações podem incluir uma gama de condutas a serem perseguidas, como o planejamento com células criminosas espalhadas pelo mundo, simpatizantes da

causa sendo recrutados, equipes sendo treinadas nas mais variadas habilidades, grupos arrecadando e doando recursos financeiros, dentre outras atividades. E, no lado oposto, serviços de Inteligência dos governos procuram rastrear indício de possível ameaça à ordem estabelecida em que o ambiente do ciberespaço é alvo ou meio para um ataque. Outro grupo que se enquadra nessa vertente são as empresas privadas que estrategicamente identificaram que a proteção a esse tipo de ameaça é um serviço caro e bastante valorizado (CASSANTI, 2014).

Em síntese, por um lado o ciberespaço em si é o próprio teatro de operações, ou seja, é o espaço em que dados e informações são coletados e ações criminosas são colocadas em prática, podendo ter apoio e suporte de fora desse ambiente. Por outro lado, é também uma estratégia, um meio de acesso, praticamente um modal que leva grupos criminosos a atingir seus objetivos. Todo o planejamento e determinadas ações são realizadas no ambiente do ciberespaço, mas os ataques acontecem no mundo físico.

A agência norte americana *Defense Advanced Research Projects Agency* (DARPA) tem trabalhado para incluir a inteligência artificial e o chamado aprendizado de máquina (*machine learning*) no contexto da Defesa Cibernética. Em contrapartida, a Ameaça Persistente Avançada (APT), considerada o tipo de ataque cibernético mais desafiador, pode utilizar também a inteligência artificial e o aprendizado de máquina para tornar seus sistemas de ataque mais robustos e ágeis. A ideia da APT consiste na busca ativa de pontos fracos na segurança do alvo, até que um erro ou uma falha seja detectada para que o ataque se concretize (ALLEN; CHAN, 2017). Como em inúmeras situações ao longo da história, trata-se de uma luta contra o tempo em que dois lados antagônicos estão em uma corrida disputando recursos, ideias, inovações e tecnologias para chegar primeiro a um objetivo e superar o movimento adverso de alguma forma.

Kim (2004) chama a atenção para o fato de que a expressão *cyberspace* apareceu na literatura *cyberpunk* em 1982 na obra de Bruce Sterling. Lembra também que no mesmo ano, outro autor, Willian Gibson apresentou tanto o termo *cyberspace* como *matrix*, este representando uma rede global de simulação. A evolução da tecnologia quase 40 anos depois parece trazer, para a realidade, o que era parte do imaginário de ficção de um universo virtual.

2.3 As redes sociais, do mundo real para o virtual

Para Castells (2006), vive-se uma verdadeira revolução de uma sociedade em rede somente possível pelas redes de comunicação digital. Ele acredita que estas sejam a coluna vertebral dessa nova sociedade. Segundo ele, é inócuo o debate entre defensores e críticos de como a tecnologia está moldando a sociedade por meio de novos hábitos, costumes, formas de agir, comunicar-se e se relacionar-se. Mais do que se colocar a favor ou contra essa realidade, é preciso admitir e compreender que a sociedade está sob uma nova configuração. É representada por redes com estruturas abertas que vão se tornando cada vez mais complexas.

O autor define sociedade em rede como:

> Uma estrutura social baseada em redes operadas por tecnologias de comunicação e informação fundamentadas na microelectrónica e em redes digitais de computadores que geram, processam e distribuem informação a partir de conhecimento acumulado nos nós dessas redes [...] As redes de comunicação digital são a coluna vertebral da sociedade em rede (CASTELLS, 2006, p. 20).

Castells (2006) exemplifica essa nova realidade citando a economia em rede que tem permitido aumentos de produtividade expressivos nas últimas décadas, particularmente nos países mais desenvolvidos. As tecnologias da informação e da comunicação têm um papel relevante, o que acaba por gerar uma dinâmica de acréscimo da riqueza, níveis de consumo e padrões de conforto. Tem-se, portanto, uma sociedade cada vez mais conectada em que os pontos, ou nós, tendem a crescer tornando a rede cada vez mais densa. Da mesma forma, Castells trabalha a ideia do Estado em rede considerando a possibilidade de articulação entre os diferentes níveis decisórios de um país, suas respectivas instituições e agências e mesmo as nações que compartilham valores próximos.

Para Waizbort (2001 *apud* ALVES, 2007), ao refletir a relação indivíduo e sociedade entende o social, o todo, enquanto um conjunto de relações. "Tais relações são sempre relações em processo, isto é: elas se fazem e desfazem, se constroem, se destroem, se reconstroem" (WAIZBORT, 2001 *apud* ALVES, 2007, p. 136).

Deste modo, essa autora então conclui que: “dessa forma, a sociedade pode ser percebida como uma rede de indivíduos em constante relação, sugerindo a ideia da interdependência.”

Elias (1994, p. 13) afirma que:

> numa palavra, cada pessoa que passa por outra, como estranhos aparentemente desvinculados na rua, está ligada a outras por laços invisíveis, sejam estes laços de trabalho e propriedade, sejam de instintos e afetos. Os tipos mais díspares de funções tornaram-na dependente de outrem e tornaram outros dependentes dela. Ela vive, e viveu desde pequena, numa rede de dependências que não lhe é possível modificar ou romper pelo simples giro de um anel mágico, mas somente até onde a própria estrutura dessas dependências o permita; vive num tecido de relações móveis que a essa altura já se precipitaram nela como seu caráter pessoal. [...] Entretanto, este arcabouço básico de funções interdependentes, cuja estrutura e padrão conferem a uma sociedade seu caráter específico, não é criação de indivíduos particulares, pois cada indivíduo, mesmo o mais poderoso, mesmo o chefe tribal, o monarca absolutista ou o ditador, faz parte dele, é representante de uma função que só é formada e mantida em relação a outras funções, as quais só podem ser entendidas em termos da estrutura específica e das tensões específicas desse contexto total.

Nas ciências sociais, o conceito de rede social surgiu na primeira metade do século XX. Para Portugal (2007, p. 3), o conceito de rede social surgiu na Sociologia e na Antropologia Social. Nos anos 1930 e 1940, o termo era usado, sobretudo, em sentido metafórico: não eram identificadas características morfológicas, úteis para a descrição de situações específicas, nem estabelecem relações entre as redes e o comportamento dos indivíduos que as constituem.

Não é recente a necessidade humana de socialização e interação por meio da aglomeração em grupos. No entanto, com o desenvolvimento da Internet, as redes sociais nascem com o objetivo de atender de forma otimizada essa necessidade, gerando oportunidades para novas formas de interação e relacionamento entre os indivíduos no ambiente virtual.

> Redes sociais podem ser definidas como um conjunto de dois elementos: atores sociais e suas conexões. As redes sociais permitem aos indivíduos: construir um perfil público ou semi-público dentro de um sistema limitado; articular-se com uma lista de outros usuários com os quais se compartilhará uma conexão; ver e percorrer a sua lista de ligações e aquelas feitas por outras pessoas dentro do sistema (SILVA, 2013).

Portes (2000, p. 13), por sua vez, afirma que as redes sociais

> [...] são conjuntos de associações recorrentes entre grupos de pessoas ligadas por laços profissionais, familiares, culturais ou afetivos. E que são importantes na vida econômica, na medida em que são meios de aquisição de recursos escassos, como o capital e a informação, e porque impõem simultaneamente constrangimentos eficientes à prossecução ilimitada dos interesses pessoais.

Entender e analisar a fundo o conceito de redes e, especificamente de redes sociais, é fundamental para compreender sua evolução para o conceito atualmente disseminado, aquele de uso de redes sociais na Internet.

Conforme afirma Portugal (2007, p. 7),

> a análise das redes fornece uma explicação do comportamento social baseada em modelos de interação entre os atores sociais em vez de estudar os efeitos independentes de atributos individuais ou relações duais. A análise estrutural das redes baseia-se na premissa de que estas têm uma realidade própria, no mesmo sentido em que os indivíduos e as relações a têm, pelo que a sua influência não pode ser reduzida ao simples efeito de constrangimentos normativos, atributos pessoais ou efeitos cumulativos de múltiplas interações.

Segundo Drucker (1993),

> partimos do princípio de que o poder é o conhecimento gerado pela abundância de informação, estando o mesmo nas mãos dos indivíduos que compõem as organizações e não mais em uma pequena parcela de gerentes ou representantes.

Felinto e Santaella (2012) apontam que a tendência futura é um aumento da interação do ser humano com os dispositivos eletrônicos, e, consequentemente, sua conectividade ao mundo virtual será cada vez maior.

Ressalta-se que “a popularidade do conceito de rede e o reconhecimento das suas capacidades descritivas e explicativas ultrapassam, hoje, os limites das ciências sociais e estendem-se, cada vez mais, a outros domínios científicos.” (PORTUGAL, 2007, p. 1-2).

Conforme Portes (2000, p. 16),

> as redes podem ligar indivíduos no interior de organizações e de comunidades e entre elas. As redes não são as únicas estruturas sociais onde as transações se encontram incrustadas, emergem muitas vezes como características de agregados de maior dimensão. Contudo, as redes constituem geralmente os contextos mais imediatos que influenciam os objetivos dos indivíduos, bem como os meios e os constrangimentos que se lhes apresentam. Dependendo das características das suas redes e das posições sociais no interior delas, os indivíduos podem ser capazes de mobilizar uma quantidade significativa de recursos, de evitar um controlo apertado do seu comportamento egoísta ou, pelo contrário, podem encontrar-se estreitamente condicionados pelas expectativas impostas pelo grupo.

No que se refere à privacidade das informações, ela foi definida por Moor (1990) como uma das questões éticas mais importantes da era da informação, sendo um dos problemas éticos mais paradigmáticos da atualidade, pois envolve a manipulação dos dados armazenados no meio informático. De acordo com o autor, a capacidade de armazenamento de tais informações, bem como a de manipular, armazenar indefinidamente, classificar e localizar informações de maneira ágil faz com que a sociedade se preocupe com a privacidade que pode ser devassada e as informações prejudiciais que são expostas indiscriminadamente.

Deste modo, pode-se concluir que as redes sociais não são seguras por disponibilizarem informações, muitas vezes, de caráter reservado, representando desse jeito uma ameaça às organizações. Em 2012, a rede social LinkedIn foi invadida por criminosos virtuais que podem ter roubado cerca de 6,5 milhões de senhas da rede, que conta com mais de 150 milhões de usuários. As senhas teriam sido postadas em um site russo de crackers (LINKEDIN, 2012).

A empresa especializada em antivírus Kaspersky coordenou uma pesquisa para dimensionar o quão grande é essa ameaça. Foi diagnosticado que 22% dos golpes de *phishing* têm como alvo o Facebook, sendo que mais de 35% estão relacionados a sites falsos que se fazem passar pelas principais redes sociais. A pesquisa revelou ainda que foram também registrados mais de 600 milhões de tentativas de acesso por parte dos usuários a sites de *phishing*. E são produzidos diariamente mais de 20 mil cliques em links que levam a páginas falsas do Facebook (STERN, 2014).

As tentativas de ataques dão conta do alcance e sucesso que estas redes sociais obtiveram. Empresas e organizações procuram, cada vez mais, estar inseridas nesse nicho uma vez que vislumbraram a possibilidade de atingir um maior número de pessoas em espaço de tempo curto.

A partir de um trabalho eficiente de marketing, foi possível a criação de novos mercados e, com o trabalho de relações-públicas, foi possível a construção ou reforço de uma imagem positiva, aumentando a sua notoriedade e credibilidade (PROOF, 2019).

De acordo com Salamon (2010), a utilização das redes sociais trouxe um conjunto de vantagens, mas expôs simultaneamente os seus usuários a riscos indesejados, como a perseguição emocional, o roubo de identidade ou até a exploração de informação pessoal para a criação de oportunidades de ataque físico.

Tal como os usuários, as organizações começaram a se expor aos mesmos riscos já que, sendo tênue a fronteira que separa os conteúdos puramente pessoais dos conteúdos relacionados com a atividade profissional, os usuários acabaram por envolvê-las de forma indireta, dificultando-lhes ou impedindo-lhes o controle dos potenciais efeitos desse envolvimento.

De acordo com Qin e Burgoon (2007), o engenheiro social explora os sentimentos e as emoções da vítima. Apesar de existirem ferramentas e linhas de orientação que têm por objetivo a redução de risco, a detecção dos ataques de engenharia social é difícil devido ao foco no perfil psicológico do usuário que vai sofrer o ataque.

Graças às redes sociais, o engenheiro social tem acesso a todos os tipos de informações da vítima escolhida para o ataque. Não há limite quanto às informações, quanto mais consegue, mais ele procura conhecer melhor sua vítima. Alguns usuários, os mais cautelosos, buscam blindar o seu perfil, mas a grande maioria deixa à mostra suas fotos, atualizações, *check ins* e outras informações que viabilizam um ataque de engenharia social. O engenheiro social não se acanhará caso o perfil esteja fechado, ele tentará se inserir ao ambiente de interesse, ao buscar dados de pessoas próximas à vítima em potencial, até alcançar o que procura (SALAMON, 2010).

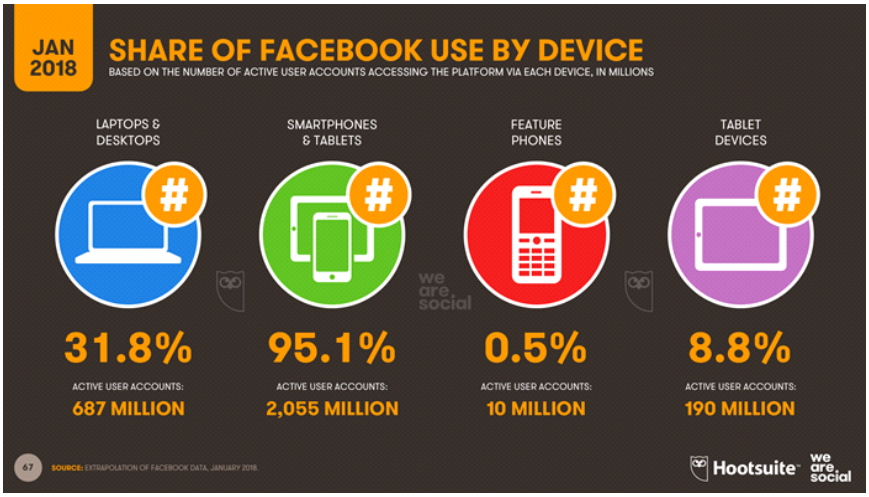
O relatório "*Digital in"* 2018, divulgado pelos serviços *online Hootsuite* e *We are Social,* apontou que são mais de 4 bilhões de pessoas conectadas à rede, enquanto as estimativas mais recentes projetam para uma população global de 7,6 bilhões de pessoas. O ano de 2018 começou com 4,021 bilhões de usuários utilizando a internet (53% de todas as pessoas do planeta), um aumento de 7% em relação ao ano anterior. As redes sociais são utilizadas por cerca de 3,2 bilhões de pessoas (42% de todo o mundo).

Cerca de 1 milhão de pessoas começaram a usar as redes sociais em 2017, aponta o relatório, o que significa um novo usuário a cada 11 segundos. Em termos de proporção, o número de usuários das mídias sociais aumentou 13% ao longo do período, com a Ásia Central e o Sul da Ásia liderando o crescimento.

Tratando-se de países de forma específica, os que mais apresentaram crescimento no número de usuários de redes sociais foram Arábia Saudita (32%), Índia (31%), Indonésia (23%), Gana (22%) e África do Sul e Vietnã (20%).

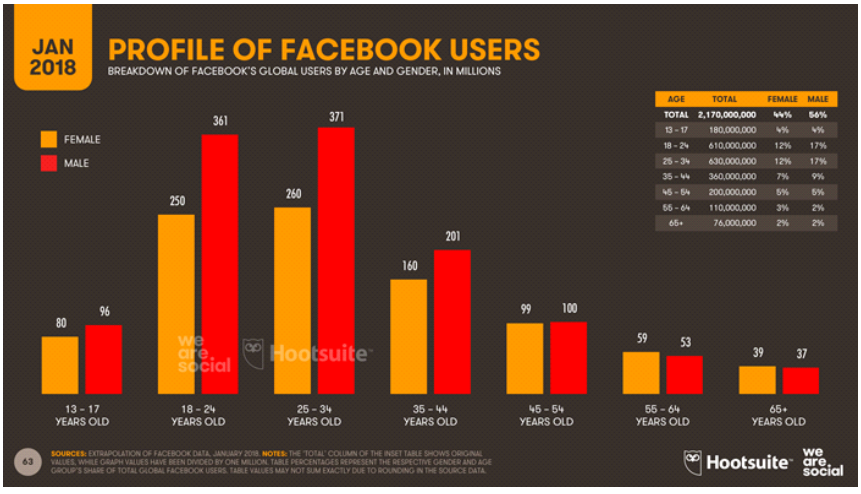
Voltando a ter o *Facebook* como um extrato representativo daquilo que é o uso das redes sociais, verifica-se como os *smarphones* e tabletes representam a principal fonte de acesso às redes sociais (Figura 1). Já o perfil mais comum de usuário de rede social no mundo é masculino com idade entre 25 e 34 anos — 17% dos usuários se encaixam nessa descrição, conforme pode ser observado na figura 2, em que também se destaca o grupo de 18 a 24 anos.

Figura 1. Perfil dos usuários do Facebook por plataforma (JAN 2018)



Fonte: We are Social (2018)

Figura 2. Perfil dos usuários do Facebook por idade (JAN 2018)



Fonte: We are Social (2018).

2.4 Engenharia Social, dos conceitos à aplicação

A engenharia social é uma expressão que vem sendo utilizada desde o início do século XX como a utilização de métodos inteligentes para resolução de problemas sociais. É consenso que a engenharia social envolve métodos que pretendem controlar o comportamento humano como um meio para a concretização de um objetivo, e este objetivo só é atingido depois da aplicação de um conjunto de várias técnicas (SILVA, F., 2013). Muitos são os significados e interpretações dadas à expressão “engenharia social”.

Segundo Peixoto (2006),

> Engenharia Social é a ciência que estuda como o conhecimento do comportamento humano pode ser utilizado para induzir uma pessoa a atuar segundo seu desejo. Não se trata de hipnose ou controle da mente, as técnicas de Engenharia Social são amplamente utilizadas por detetives (para obter informação) e magistrados (para comprovar se um declarante fala a verdade). Também é utilizada para lograr todo tipo de fraudes, inclusive invasão de sistemas eletrônicos.

A expressão ficou mais conhecida em 1990, a partir de um hacker chamado Kevin Mitnick. Designa práticas utilizadas a fim de se obter informações sigilosas ou importantes de empresas, pessoas e sistemas de informação, explorando, muitas vezes, da confiança para enganá-las. Pode-se também definir engenharia social como a arte de manipular a fim de contornar dispositivos de segurança ou construir métodos e estratégias para ludibriar pessoas, utilizando informações cedidas por elas de maneira a ganhar a confiança delas para obter informações.

As vítimas, muitas vezes, se tornam alvos pela inaptidão de manterem-se atualizadas nas questões pertinentes à tecnologia da informação, e também pelo fato de não terem consciência do valor da informação que possuem e, portanto, não se preocuparem em protegê-la.

Segundo a Cartilha de segurança do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT Br), engenharia social é a

> técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações. No contexto desta Cartilha, é considerada uma prática de má-fé, usada por golpistas para tentar explorar a ganância, a vaidade e a boa-fé ou abusar da ingenuidade e da confiança de outras pessoas, a fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes. O popularmente conhecido "conto do vigário" utiliza engenharia social (COMITÊ GESTOR DA INTERNET NO BRASIL, 2012).

Para o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT, 2017), por meio do Grupo de Resposta a Incidentes para a Internet Brasileira, a engenharia social consiste basicamente no uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

De acordo com Alves (2007), o termo “engenharia” foi atribuído a essa prática porque é construída sobre informações e táticas de acesso a informações sigilosas de forma indevida. Já o “social” foi dado porque utiliza pessoas que vivem e trabalham em grupos organizados. Essas práticas simplesmente ganharam esse novo termo, pois são bem antigas e também utilizadas por detetives a fim de obterem informações e também por magistrados com o objetivo de comprovar se um declarante fala a verdade.

No processo de engenharia social existe um cálculo, mas ele não é matemático ou baseado na física, mas, sim, focado na vulnerabilidade das pessoas quanto ao seu modo de agir e à tomada de decisão. Pode ser usado tanto como uma forma de se desafiar e testar o sistema, como para de fato, buscar alguma vantagem ou benefício. O mecanismo em si pode até não ser objeto de julgamento por instrumentos legais, mas certamente há um julgamento ético e moral, e suas consequências e desdobramentos da engenharia social podem sim, ser objeto de sanções legais.

Segundo Johnson (2005) os ataques de engenharia social são muito frequentes porque funcionam bem. Tentar quebrar um algoritmo de criptografia é muito mais difícil do que conseguir alguma informação de um funcionário de uma organização, em relação à sua forma de acesso ao sistema.

De acordo com Mitnick e Simon (2003), “um ataque de Engenharia Social é uma ação elaborada, arquitetada, que explora o humanismo e a boa vontade das pessoas”. Para esses autores, “a Engenharia Social coloca o fraudador em uma posição privilegiada dentro do fluxo da informação, de forma a permitir que ele

alcance seus objetivos". Para Rosa, Silva, B. e Silva, P. (2012), "os ataques podem ser realizados através dos meios de comunicação, como telefonemas, envio de mensagens via correio eletrônico, salas de bate-papo e até mesmo, pessoalmente".

Para Granger (2001), os objetivos básicos da engenharia social são os mesmos dos crackers em geral: obter acesso não autorizado a sistemas ou informações para cometer fraudes, invasões de rede, espionagem industrial, roubo de identidade ou simplesmente para atrapalhar o sistema ou a rede. Os alvos típicos incluem empresas de telefonia e serviços de atendimento, grandes empresas e instituições financeiras, agências militares e governamentais.

Convém destacar que encontrar exemplos exitosos e reais de ataques de engenharia social é difícil, pois as organizações-alvo não querem admitir que foram vitimadas, expor a sociedade que foi uma violação de segurança fundamental não é apenas algo embaraçoso, pode prejudicar a reputação da organização e/ou o ataque não foi bem documentado para que ninguém tenha realmente certeza se houve um ataque de engenharia social ou não (MANN, 2011).

De acordo com Reason (1990 apud BULLÉ *et al*., 2017) os ataques de engenharia social podem ser explicados usando a analogia do modelo de queijo suíço ou de efeito cumulativo. As camadas são os vários componentes de uma organização. Em um mundo ideal, essas camadas estão intactas; no entanto, no mundo real, eles se assemelham a fatias de queijo com buracos. Uma única camada que tenha um buraco não representa nenhum problema. No entanto, se houver furos em várias camadas e estes se alinharem, um erro pode ocorrer, isto é, o sistema se torna penetrável e, portanto, um componente da organização pode se tornar vítima de um ataque de engenharia social.

Toda a preparação para se conhecer as vulnerabilidades do alvo a ser atacado levam de semanas a meses. É comum em todos os ataques a procura por lista telefônica ou organograma da empresa a ser atacada bem como a realização de pesquisas nas redes sociais, como LinkedIn e Facebook, em que os seus funcionários possam ter conta, reunindo informações detalhadas que serão usadas para promover o ataque.

Voltando ao caso de Kevin Mitnick, sua trajetória teve início de forma até despretensiosa fraudando o sistema de bilhetes de ônibus. Na sequência, mirou as redes telefônicas até que encontrou brechas no terreno da informática. Mitnick descobriu as possibilidades diversas para a prática de crimes para invadir a rede

virtual, não apenas de grandes empresas, mas também de unidades do governo americano. Mitnick foi condenado a cinco anos de prisão fechada e mais três de prisão condicional.

Após cumprir a sentença, foi convidado pelo *Federal Bureau Investigation (*FBI) a colaborar com o governo americano, transmitindo seus conhecimentos para proteger instituições, sistemas e pessoas de criminosos que, assim como ele no passado, utilizam as falhas dos sistemas para cometer crimes. Atualmente, ele trabalha como consultor de segurança de sistemas e tem alertado e ensinado sobre as vulnerabilidades dos sistemas e as oportunidades que criminosos têm para colocar em prática seus conhecimentos na área da informática.

As organizações passaram a contratar este ex-criminoso virtual como um aliado para a busca de falhas no sistema, localizando e corrigindo inconsistências. Muitos desse time de especialistas passaram ser colaboradores atuando como agentes de segurança e combatendo tentativas de ataques às brechas nos sistemas. Assim como a sofisticação dos crimes, as competências desses *hackers* éticos também são aperfeiçoadas, sobretudo considerando novos temas e tecnologias como engenharia social, redes sociais e aplicativos de telefonia móvel.

Mitnick e Simon (2003) narram as diversas experiências vivenciadas por eles ou contadas por seus companheiros de engenharia social, mostrando de forma detalhada como são desenvolvidos os ataques, desde o planejamento até os passos de execução. Para Mitnik (2005), o engenheiro social é uma pessoa que manipula a confiança de outra para ter acesso às informações consideradas privadas.

De acordo com Caldwell (2011) os *hackers* estão rapidamente se tornando uma parte essencial do arsenal de segurança de rede de uma organização. Usuários maliciosos ou criminosos virtuais que invadem sistemas, ou mesmo aqueles que conseguem informações importantes sem o uso da força bruta, por meio da persuasão de pessoas e se beneficiando de informações ou dados, são chamados de engenheiros sociais, que têm como atributos essenciais a paciência, o pensamento lateral e a capacidade de acompanhar as rápidas mudanças nas ameaças da rede (CALDWELL, 2011).

Para Rafael (2013 *apud* MAULAIS, 2016, p. 33-34), as principais técnicas utilizadas por engenheiros sociais para obtenção de acesso não autorizado a sistemas, redes ou informações estratégicas para as organizações podem ser identificadas de acordo com o Quadro 2.

Quadro 2. Técnicas e Características de Engenharia Social.

TÉCNICAS	CARACTERÍSTICAS
Análise do lixo	Provavelmente poucas organizações têm o cuidado de verificar o que está sendo descartado da empresa e de que forma é realizado este descarte.
Internet e redes sociais	As informações podem ser coletadas através da Internet e Redes Sociais sobre o alvo.
Contato telefônico	as informações coletadas nas duas técnicas acima, o Engenheiro Social pode utilizar uma abordagem via telefone para obter acesso não autorizado, seja se passando por um funcionário da empresa, fornecedor e terceiros.
Abordagem pessoal	Por meio de uma visita a empresa alvo, o engenheiro social faz-se passar por um fornecedor, terceirizado, amigo do diretor, prestador de serviço, entre outros, no qual através do poder de persuasão e falta de treinamento dos funcionários, consegue sem muita dificuldade convencer um segurança, secretária, recepcionista a liberar acesso ao datacenter onde possivelmente conseguirá as informações que procura.
Spoofing	A técnica consiste no ato de enganar um site, um serviço, um servidor ou uma pessoa afirmando que a fonte de uma informação é legítima, quando não é.
Spoofing de ID	É realizada uma requisição a um site ou servidor se passando por um IP legítimo, de forma que a vítima não consiga identificar o atacante.
Spoofing de e-mail	Consiste em e-mails falsos, se passando por outra pessoa ou uma empresa real. Geralmente ligado a golpes de *phishing.*
Spoofing de DNS	Manipulação de conexões de rede (altera o DNS de roteadores em larga escala) e desvia acessos a um site legítimo para uma cópia falsa, de modo a roubar dados. Sites de bancos são os alvos mais comuns.
Spoofing de chamadas e/ou SMS	O atacante faz chamadas ou envia mensagens SMS se passando por um número legítimo, tentando enganar outros usuários
Caller ID Spoofing	É um método mais elaborado, no qual o hacker tenta acessar serviços de telefonia ou de aplicativos através de um número de celular clonado, com o intuito de invadir contas de e-mail, mensageiros e redes sociais do usuário copiado (Gogoni, 2019).
Phishing	É a técnica mais utilizada para conseguir um acesso na rede alvo. O *Phishing* pode ser traduzido como “pescaria” e “e-mail falso”, que são e-mails manipulados e enviados as organizações e pessoas com o intuito de aguçar algum sentimento que faça com que o usuário aceite o *e-mail* e realize as operações solicitadas.
Falhas Humanas	As vulnerabilidades como, confiança, medo, curiosidade, instinto de querer ajudar, culpa, ingenuidade, entre outros são exploradas pelos Engenheiros Sociais.

Fonte: Rafael (2013 *apud* MAULAIS, 2016, p. 33-34).

Segundo Allan (2005), o ciclo de desenvolvimento de um ataque de engenharia social é constituído por quatro fases: obtenção de informação, desenvolvimento da relação, exploração e execução. Considerando a primeira fase, o engenheiro social pode utilizar várias fontes para obter da informação relativa a seu alvo. Poderá este processo passar por análise do lixo, espionagem, pesquisas

na Internet, redes sociais entre outros. A informação obtida nesta fase servirá de base para a fase seguinte**.**

Depois de definido o objetivo do ataque, do alvo a atacar e do pretexto a utilizar, o engenheiro social procura desenvolver um relacionamento com a vítima de forma a criar uma relação de confiança. A duração desse envolvimento é variável.

O atacante manipula a vítima para obtenção da informação que pretende ou informação que permita executar o seu plano. Esta fase poderá ser a final ou a preparação para a final. O resultado da fase anterior é usado para a concretização das metas ou para reforçar o ataque. O objetivo final poderá ser atingido com apenas um ciclo ou poderá dar início a outro.

Figura 3. Ciclo de Desenvolvimento de um ataque de engenharia social.

Fonte: Martins (2014).

Percebe-se, portanto, que os ataques de engenharia social representam processos relativamente simples e os alvos, consideravelmente vulneráveis. Uma ação que até parece infantil, mas que pode ser utilizada é o "*shoulder surf*", ou seja, surfar por cima dos ombros das pessoas em busca de algum dado valioso. O controle do fluxo de informações no ambiente cibernético é fundamental pois com as brechas e vulnerabilidades existentes nos sistemas podem facilitar uma taque de engenharia social (PEIXOTO, 2014). E quando organizações vitais como as Forças Armadas e suas unidades estratégicas, centros de inteligência e o alto escalão de governos não estão devidamente preparados, os riscos podem ser grandes.

3 BREVE PANORAMA DA DEFESA CIBERNÉTICA NO BRASIL

3.1 Contextualização

Para contextualizar a relevância do tema Defesa Cibernética para o Brasil, evidencia-se um breve trecho do Relatório do XIII - Encontro Nacional de Estudos Estratégicos (ENEE), realizado em Brasília em 2013, que tratou do tema “O setor cibernético brasileiro”:

> A segurança e a defesa cibernética são vetores estratégicos para o Estado, na medida em que afetam positiva ou negativamente aspectos políticos, econômicos e sociais do cotidiano da sociedade da informação. O próprio conceito de realidade foi expandido pelo ambiente virtual.
> Segurança diz respeito à sensação de garantia necessária e indispensável a uma sociedade e a cada um de seus integrantes, contra ameaças de qualquer natureza. Ao Estado compete garantir a segurança de todos, pois a todos deve e pode exigir o cumprimento dos deveres e funções necessários à manutenção dessa condição.
> A segurança cibernética engloba a defesa cibernética, diz respeito a uma atividade abrangente que congrega uma série de aspectos, que vão da proteção física e lógica da informação, em qualquer meio onde ela esteja abrigada, à proteção dos sistemas e redes de informação. Abrange, ainda, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações computacionais destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento – ou seja, um conjunto de ativos de informação denominado de Infraestrutura Crítica da Informação (BRASIL, 2019, p. 150).

Para garantir o rigor na conceituação, é imprescindível recordar alguns conceitos já consagrados em literatura oficial, quais sejam: Defesa, Segurança da Informação e Comunicações, Cibernética, Defesa Cibernética e Segurança Cibernética, termos que são largamente empregados no decorrer deste texto.

De acordo com o Glossário das Forças armadas defesa significa: ato ou conjunto de atos realizados para obter, resguardar ou recompor a condição reconhecida como de segurança, ou ainda, reação contra qualquer ataque ou agressão real ou iminente (BRASIL, 2015). Segurança da Informação e Comunicações (SIC) representa ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

O termo cibernética se refere ao uso de redes de computadores e de comunicações e sua interação dentro de sistemas utilizados por instituições públicas e privadas, de cunho estratégico, a exemplo do MD/FA. No campo da Defesa Nacional, inclui os recursos informatizados que compõem o Sistema Militar de Comando e Controle (SISMC) bem como os sistemas de armas e de vigilância (BARROS; GOMES; FREITAS, 2011).

Já a Defesa Cibernética é o conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com as finalidades de proteger os nossos sistemas de informação, obter dados para a produção de conhecimento de inteligência e causar prejuízos aos sistemas de informação do oponente. No contexto do preparo e emprego operacional, tais ações caracterizam a Guerra Cibernética (BARROS; GOMES; FREITAS, 2011).

E a Segurança Cibernética se refere à proteção e garantia de utilização de ativos de informação estratégicos, principalmente os ligados às infraestruturas críticas da informação (redes de comunicações e de computadores e seus sistemas informatizados) que controlam as infraestruturas críticas nacionais. Também abrange a interação com órgãos públicos e privados envolvidos no funcionamento das infraestruturas críticas nacionais, especialmente os órgãos da Administração Pública Federal (APF) (BARROS; GOMES; FREITAS, 2011).

O Decreto n° 9.637, de 26 de dezembro de 2018, que institui a “Política Nacional de Segurança da Informação”, dispõe sobre a governança da segurança da informação abrangendo a segurança cibernética; a defesa cibernética; segurança física e proteção de dados organizacionais; e ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

Observe-se que, tendo em vista que o Decreto mencionado trata da implementação de uma Estratégia Nacional de Segurança da Informação (E-Ciber), o Gabinete de Segurança Institucional da Presidência da República (GSI/PR), em janeiro de 2019, elegeu a E-Ciber como o módulo inicial da estratégia nacional para a salvaguarda da informação. O contexto mundial, face à evolução experimentada pela tecnologia de informação e comunicações (TIC), a partir da segunda metade do século passado, com o advento da Internet, permitiu benefícios inúmeros, conferidos pela circulação da informação em tempo real e em escala global. No entanto, paradoxalmente, surge um novo tipo de ameaça, a cibernética, que desconhece fronteiras e possui potencial para causar grandes prejuízos. Assim, o espaço

cibernético constitui-se em um novo e promissor cenário para a prática de toda a sorte de atos ilícitos, incluindo o crime, o terrorismo e o contencioso bélico entre nações.

Assim sendo, conforme consta da “Estratégia de segurança da informação e comunicações e de segurança cibernética da Administração Pública Federal 2015-2018”, do GSI/PR, a Segurança da Informação e Comunicações (SIC) e a Segurança Cibernética vêm se caracterizando cada vez mais como função estratégica de Estado, sendo essenciais à manutenção e à preservação tanto das infraestruturas críticas de um país, tais como energia, transporte, telecomunicações, águas, finanças, a própria Informação, entre outras, quanto dos direitos individuais, em especial privacidade e soberania.

No Brasil, os assuntos relacionados à Segurança da Informação e Comunicações, Segurança Cibernética e Segurança das Infraestruturas Críticas são tratados no âmbito do Conselho de Defesa Nacional (CDN) e da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), do Conselho de Governo, por meio do GSI/PR, que exerce as funções de Secretaria-Executiva do citado Conselho e de Presidência daquela Câmara.

Em relação aos Órgãos referenciados, na subseção 3.2, a seguir, serão tratados os órgãos e atores de Segurança e defesa Cibernética no Brasil, destacando-se as competências de cada um deles.

3.2 Legislação brasileira sobre o setor cibernético

Avaliando a produção legal no âmbito da segurança cibernética, é possível distinguir dois momentos: 2000-2005 e 2005-até a atualidade. O primeiro marco legal, no ano 2000, o lançamento de “Sociedade da Informação no Brasil: livro verde”, demonstrando as percepções do Ministério da Ciência e Tecnologia do Brasil sobre o tema mais geral da Sociedade da Informação. A abordagem do assunto Segurança da Informação, pela primeira vez na legislação federal no ano de 2000, com o Decreto Nº 3505/2000, o qual instituía a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Foi estabelecido, assim, um Comitê Gestor da Segurança da Informação, subordinado à Secretaria-Executiva do CDN, pelo qual já se evidenciava ser um tema sensível à segurança do Estado.

A seguir, conforme afirma Mandarino Júnior (2010), ocorre uma superposição de órgãos e funções para tratar da temática de Segurança da Informação, dada a disseminação das novas tecnologias da informação e comunicações na Administração Pública Federal (APF). Colocada a necessidade de evitar a difusão de esforços, foi atribuída a coordenação das atividades de segurança da informação na APF a um órgão governamental, e, por meio da Lei 10.683, de 29 de maio de 2003, esta competência foi atribuída ao GSI/PR, prevendo também a estruturação de um órgão para exercer especificamente a atividade relacionada à segurança de informação, fato ocorrido com a edição do Decreto Presidencial Nº 5.772/ 2006, o qual criou o Departamento de Segurança da Informação e Comunicações (DSIC).

O período iniciado em 2005 é aquele em que a temática da Segurança Cibernética adentra as preocupações da Defesa do Estado brasileiro. O marco inicial para as percepções brasileiras sobre a Ameaça Cibernética é a Política de Defesa Nacional (BRASIL, 2005), documento de alto nível dentro da política de Defesa do Brasil.

Outro momento chave na produção legal brasileira referente à Segurança Cibernética é a Estratégia Nacional de Defesa (END) (publicada inicialmente em 2008 e atualizada em 2012), documento também de alto nível e inédito por tentar inserir a discussão sobre a Defesa Nacional na sociedade brasileira, além de expor quais as perspectivas do Estado sobre sua inserção no sistema internacional e como o Brasil pensa o papel de suas Forças Armadas nesse contexto.

Assim sendo, a END definiu os três setores considerados de importância estratégica para a Defesa Nacional, quais sejam: o nuclear, o espacial e o cibernético. Então, a Segurança e a Defesa Cibernética surgem naturalmente como imperativos de proteção das infraestruturas críticas da informação por sua vez às infraestruturas críticas nacionais do Estado brasileiro.

Cada um dos setores estratégicos está associado a uma Força responsável por seu desenvolvimento prioritário, ficando o Nuclear a cargo da Marinha do Brasil (MB), o Aeroespacial, com a Força Aérea Brasileira (FAB) e o Cibernético, com o Exército Brasileiro.

Visando organizar-se institucionalmente para responder à nova missão atribuída pela END, o Exército Brasileiro instituiu o “Setor Cibernético” em 29 de junho de 2009, logo após, em 4 de agosto de 2010, o Centro de Defesa Cibernética do Exército foi criado.

Além destes, vários outros documentos merecem destaque, entre eles o Livro Verde de Segurança Cibernética no Brasil (2010), o qual ressalta:

> A Segurança Cibernética, desafio do século XXI, vem se destacando como função estratégica de Estado, e essencial à manutenção das infraestruturas críticas de um país, tais como Energia, Defesa, Transporte, Telecomunicações, Finanças, da própria Informação, dentre outras (BRASIL, 2010)

Assim, deste ponto em diante, aborda-se a legislação relativa ao Setor Cibernético na APF e no âmbito da Defesa. Além disso, são identificados eventos que marcam a história do País nessa temática, com eventuais avaliações de especialistas no assunto.

3.2.1 Legislações brasileiras

As principais legislações no âmbito da Administração Pública Federal no que tange à SIC e Segurança Cibernética, no período compreendido entre 2000 até junho de 2015, por ser extensa, encontra-se no Apêndice A. Cabe ressaltar, que o Brasil conta hoje com uma lei que regulamenta o uso, a proteção e a transferência de dados pessoais no território brasileiro; trata-se da Lei nº 13.709/2018, que dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

A Lei 12.737/2012 surgiu a partir do projeto de Lei nº 2.793/2011, que foi aprovado após o caso da atriz Carolina Dieckmann, que teve seus dados acessados no seu computador pessoal por crackers, após a atriz ter clicado em um e-mail infectado, assim os criminosos tiveram acesso às suas fotos íntimas. Em um primeiro momento foi cogitada a versão da invasão ter sido realizada na loja em que ela teria consertado o computador meses antes. Logo depois, ficou comprovado que, de fato, foram crackers do interior de Minas Gerais e de São Paulo que praticaram o delito. Ela foi chantageada pelos criminosos, que exigiram o pagamento de 10 mil reais para que as fotos não fossem divulgadas nas mídias sociais (MENDES, 2012 *apud* SILVEIRA; SOUSA, 2017).

Assim que as fotos foram publicadas, Carolina Dieckmann registrou o boletim de ocorrência, e, então, foram iniciadas as investigações sobre o caso, três dias

após a publicação das imagens a fim de evitar mais exposições. Como no Brasil, nesta época, não se tinha uma lei específica para crimes de informática, os envolvidos foram indiciados por furto, extorsão qualificada e difamação, todos do Código Penal Brasileiro. Cabe ressaltar que outras pessoas já tinham sido vítimas do mesmo golpe, inclusive com registros nos boletins de ocorrência, porém, o caso só se destacou na imprensa por se tratar de uma figura pública (SILVEIRA; SOUSA, 2017).

A Lei Carolina Dieckmann introduziu três tipos penais específicos envolvendo crimes cibernéticos no Código Penal: invasão de dispositivo informático alheio (artigo 154-A); interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública (artigo 266, §§ 1º e 2º); e falsificação de cartão de crédito ou débito (artigo 298) (LIMA, C., 2014).

O comércio eletrônico é mais do que uma tendência; tornou-se uma realidade e de crescimento incontrolável. Contudo, não se tinha até 2013 um dispositivo legal que regulasse esse mercado. Então, o Decreto nº 7.962/2013 regulamentou o Código de Defesa do Consumidor, para dispor sobre a contratação no comércio eletrônico. Este Decreto trouxe diversos esclarecimentos sobre atendimento ao consumidor em relação às compras realizadas pela Internet, direito de arrependimento em comércio eletrônico, abordando até mesmo o tema das compras coletivas (LIMA, C., 2014).

De acordo com o Marco Civil da Internet (MCI), o acesso à Internet é essencial ao exercício da cidadania, e ao usuário está assegurado o direito da inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação, ou seja, as transmissões de informações pessoais realizadas pela rede devem ser armazenadas no mais rigoroso sigilo, assegurando assim que qualquer violação à privacidade dos usuários deve ser ressarcida pela empresa que divulgou ou que não envidou esforços para coibir tal ação.

Nessa esteira, com a criação da Lei de Proteção de Dados (LGPD) em junho de 2018, mas que somente entrará em vigor em 2020, as empresas deverão envidar esforços no sentido de proteger os dados dos seus usuários. A LGPD foi sancionada para unificar diferentes regulamentações sobre uso e troca de informações em ambientes digitais. O principal objetivo é garantir que os cidadãos tenham maior controle quanto ao uso de dados compartilhados em diversos sites e serviços. A

partir de 2020, as empresas deverão prestar contas sobre o que fazem com os dados coletados, informando de maneira clara aos usuários, caso haja alterações nesse sentido. Caso a LGPD já estivesse em vigor, a empresa deveria notificar todos os usuários afetados pelo incidente, um impacto de imagem junto a clientes (OLINDA *et al*., 2018).

3.2.2 Legislações no âmbito da Defesa do Estado Brasileiro

Conforme já citado, o período iniciado em 2005 é aquele em que se iniciam as preocupações da Defesa do Estado brasileiro em relação à temática da Segurança Cibernética. Teve início o ciclo de publicações ligadas ao Setor Cibernético no âmbito da Defesa, conforme pode ser visualizado no Quadro 3.

Quadro 3. Legislações no âmbito da Defesa Cibernética.

ANO	LEGISLAÇÃO	OBJETIVO
2005	Política de Defesa Nacional aprovada pelo Decreto n° 5.484, de 30 de junho de 2005	Aperfeiçoar os dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos e, se for o caso, permitam seu pronto restabelecimento
2008	Estratégia Nacional de Defesa aprovada pelo Decreto nº 6.703, de 18 de dezembro de 2008	Estabelece o setor cibernético entre os 3 setores estratégicos do País, considerados essenciais para a defesa nacional. Realça que para o setor cibernético será constituída organização encarregada de desenvolver a capacitação cibernética nos campos industrial e militar.
2010	Diretriz Ministerial nº 14/2009	Atribuir ao Exército Brasileiro a institucionalização do Núcleo do Centro de Defesa Cibernética do Exército (Nu CDCiber).
	Portarias 666 e 667, do Comandante do Exército	Criação do Centro de Defesa Cibernética do Exército e ativação do Núcleo do Centro de Defesa Cibernética do Exército.
2012	Livro Branco de Defesa Nacional criado pela Lei Complementar nº 136, de 25 de agosto de 2010, e lançado em 2012	Estabelece as atividades de defesa do Brasil. É o 3º nível da Política Nacional de Defesa (ou nível operacional). Abrangente, visa esclarecer a sociedade brasileira e a comunidade internacional sobre as políticas e ações que norteiam os procedimentos de segurança e proteção à nossa soberania.
	Política Cibernética de Defesa" é estabelecida por meio da Portaria Normativa nº 3.389/MD, de 21 de dezembro de 2012	Orientar, no âmbito do Ministério da Defesa (MD), as atividades de Defesa Cibernética, no nível estratégico, e de Guerra Cibernética, nos níveis operacional e tático, com vistas à consecução dos seus objetivos.
2013	Decreto Legislativo nº 3703, de 12 de julho de 2013, atualiza a "Estratégia Nacional de Defesa" e aprova o "Livro Branco de Defesa Nacional"	Entre as premissas sobre o setor cibernético, cita que a proteção do espaço cibernético abrange um grande número de áreas, como: capacitação, inteligência, pesquisa científica, doutrina, preparo e emprego operacional; e gestão de pessoal.
2014	Portaria Normativa MD 2.777, de 27 de outubro de 2014	Implantar a diretriz de medidas com vistas à potencialização da Defesa Cibernética Nacional e cria o Comando de Defesa Cibernética (ComDCiber) e a Escola Nacional de Defesa Cibernética (EnaDCiber) na Estrutura Regimental do Comando do Exército Apoiar à pesquisa e ao desenvolvimento de produtos de defesa cibernética, bem como a criação do Observatório de Defesa Cibernética.
	Doutrina Militar de Defesa Cibernética (MD31-M-07, 1ª Edição/2014)", aprovada por meio da Portaria Normativa nº 3.010/MD, de 18 de novembro de 2014	Conceituar o Sistema Militar de Defesa Cibernética (SMDC) como: é um conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal essenciais para realizar as atividades de defesa no Espaço Cibernético, assegurando, de forma conjunta, o seu uso efetivo pelas FA, bem como impedir ou dificultar a sua utilização contra interesses da Defesa Nacional.

Fonte: Brasil (2015).

Observou-se a institucionalização progressiva da segurança cibernética no Brasil. Grande parte desse processo concentrou-se na atuação de diferentes setores dentro da Administração Pública Federal (APF), tendo como epicentro as áreas de defesa e segurança nacional. A Política de Defesa Nacional, de 2005, foi o primeiro

documento oficial a reconhecer a importância do espaço cibernético, marcando a inserção da segurança cibernética na agenda nacional.

No período de 2010 a 2016, com o ciclo de megaeventos que seriam sediados pelo país foram criadas políticas e estratégias para as questões relacionadas a ameaças à segurança e defesa nacionais, como ciberterrorismo e infraestruturas críticas.

3.3 Governança do setor cibernético na Administração Pública Federal – APF

3.3.1 Órgãos e atores de segurança e defesa cibernética do Brasil na APF

De acordo com Mandarino (2010, p. 107), as atuações dos principais atores e órgãos do governo, no Setor Cibernético, dividem-se em duas vertentes: a da Segurança Cibernética, que contempla ações preventivas ou repressivas; e a da Defesa Cibernética, que são caracterizadas por ações operacionais, de caráter defensivo e ofensivo. Neste sentido, Carneiro (2012) apresenta um quadro-resumo da atuação desses atores, conforme segue:

Quadro 4. Formas de atuação de atores e órgãos do governo no Setor Cibernético.

Vertente	Ações / Atitudes	Medidas
Segurança Cibernética	Preventivas	• Criação e aplicação de metodologias de gestão de risco • Desenvolvimento de planos de contingência e continuidade de infraestruturas críticas • Resposta à incidentes de rede • Correções contra artefatos maliciosos • Disseminação de melhores práticas para proteção de redes e segurança das informações • Especificação e desenvolvimento de algoritmos criptográficos e equipamentos de segurança cibernética
	Repressivas	• Identificação e combate à conduta criminosa caracterizada como crime cibernético • Contraterrorismo cibernético e sabotagem
Defesa Cibernética	Ações operacionais ofensivas e defensivas	• Contraterrorismo cibernético e sabotagem • Apoio às operações militares conduzidas em situação de emprego militar

Fonte: Carneiro (2012, p. 54).

Pode ser visto no Apêndice B uma listagem com os órgãos e atores que, de alguma forma, se relacionam com as vertentes de segurança e defesa cibernética no Brasil.

3.3.2 Outros órgãos envolvidos na defesa cibernética no Brasil

Segundo Lobato (2018), com o crescente aumento do número de ataques cibernéticos e com a fragilidade do país em combatê-los, surgiu uma preocupação cada vez maior sobre o assunto, neste contexto, culminou com o desenvolvimento de uma política de segurança cibernética. Convém ressaltar, que a atual arquitetura da governança da segurança cibernética no país propiciou que fossem criados novos arranjos e iniciativas dedicados a questões de natureza técnica, estratégica e operacional específicas dessa área (LOBATO, 2018). De forma pontual, na sequência são apresentadas algumas ações no Ministério da Justiça e Política Federal.

Segundo Mandarino (2010, p. 117), o Ministério da Justiça tem por missão garantir e promover a cidadania, a justiça e a segurança pública, por meio de ação conjunta entre Estado e sociedade. Na sua área de competência, destacam-se as ações de Polícia Judiciária, prevenção e repressão à lavagem de dinheiro e cooperação jurídica internacional.

A atuação do Ministério da Justiça cresce de importância na medida em que a motivação dos crimes cibernéticos envolve frequentemente obtenção de recursos financeiros de forma ilegal, além de ameaçar o sistema financeiro, como uma infraestrutura crítica. No Ministério da Justiça, a Polícia Federal exerce um papel relevante.

A Polícia Federal é um órgão de caráter permanente, organizado e mantido pela União. Dentre as suas atribuições, merecem destaque, por se relacionarem com o campo cibernético, as seguintes ações: (I) apurar infrações penais contra a ordem política e social ou em detrimento de bens, serviços e interesses da União ou de suas entidades autárquicas e empresas públicas, assim como outras infrações cuja prática tenha repercussão interestadual ou internacional e exija repressão uniforme, segundo se dispuser em lei; e (II) exercer, com exclusividade, as funções de Polícia Judiciária da União.

Em 4 de junho de 2012, a Polícia Federal inaugurou o Centro de Monitoramento do Serviço de Repressão a Crimes Cibernéticos em Brasília. Este centro se destina a ser um instrumento de prevenção e investigação a ataques cibernéticos contra sistemas de informação e infraestruturas críticas do Governo Federal.

3.3.3 Modelo de Governança Sistêmica de SIC e de Segurança Cibernética da APF

Os órgãos e atores da APF envolvidos no Setor Cibernético de acordo com a Estratégia de SIC e de Segurança Cibernética da APF 2015-2018:

> o modelo de governança sistêmica de SIC e de Segurança Cibernética da APF, de nível político estratégico, apoiará o estabelecimento de competências e respectivas responsabilidades entre os órgãos e entidades da APF, de forma a: somar e otimizar esforços; pactuar ações em prol dos avanços das áreas e efetividade nos resultados; buscar a excelência da gestão e da maturidade; estabelecer mecanismos e critérios de acompanhamento e avaliação contínuos; e promover a articulação multissetorial e a inovação (BRASIL, 2015).

Os integrantes deste modelo de governança sistêmica de SIC e de Segurança Cibernética da APF são:

a) Órgão Central (GSI/PR): que exercerá a coordenação executiva e a integração das ações na definição das respectivas diretrizes político estratégicas daquelas áreas no âmbito da APF;

b) Órgãos Gestores Setoriais Nível A: representados pelos Ministérios e equivalentes, no âmbito da APF;

c) Órgãos Gestores Setoriais Nível B;

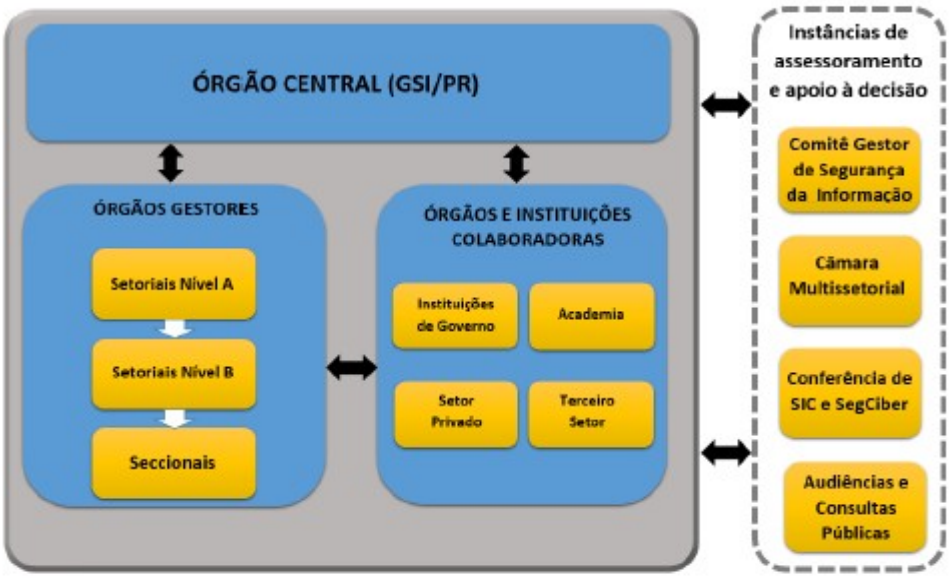
d) Órgãos Gestores Seccionais;

e) Órgãos e Instituições Colaboradoras; e

f) Instâncias de assessoramento e apoio à decisão do Sistema de SIC e SegCiber da APF.

Na figura 4 pode ser observado como os integrantes deste modelo de governança sistêmica de SIC e de Segurança Cibernética da APF interagem.

Figura 4. Modelo de Governança Sistêmica de SIC e de Segurança Cibernética da APF.



Fonte: Brasil (2015).

3.4 Governança do setor cibernético no âmbito da Defesa

3.4.1 Órgãos e atores de segurança e defesa cibernética do Brasil no âmbito da Defesa

A Estratégia Nacional de Defesa (END) afirma que:

> A análise das hipóteses de emprego das Forças Armadas – para resguardar o espaço aéreo, o território e as águas jurisdicionais brasileiras – permite dar foco mais preciso às diretrizes estratégicas. Nenhuma análise de hipóteses de emprego pode, porém, desconsiderar as ameaças do futuro. Por isso mesmo, as diretrizes estratégicas e as capacitações operacionais precisam transcender o horizonte imediato que a experiência e o entendimento de hoje permitem descortinar (BRASIL, 2008).

Visando dar provimento ao estabelecido na END para os três setores estratégicos, o Ministério da Defesa emitiu, em 9 de novembro de 2009, a Diretriz Ministerial nº 014, definindo responsabilidades sobre a coordenação e a liderança na

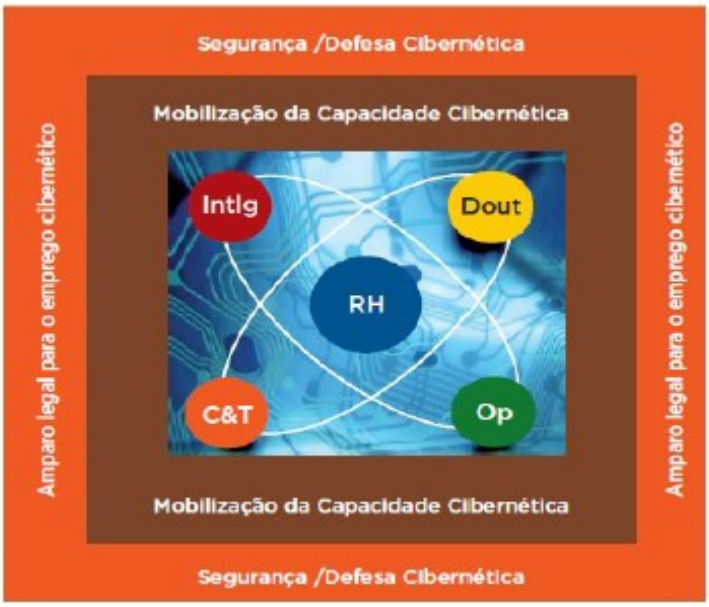
condução das ações referentes aos setores nuclear, cibernético e espacial, respectivamente, à Marinha, ao Exército e à Aeronáutica.

As prioridades em relação ao Setor Cibernético, de acordo com a END, são:

> No setor cibernético, as capacitações se destinarão ao mais amplo espectro de usos industriais, educativos e militares. Incluirão, como parte prioritária, as tecnologias de comunicação entre todos os contingentes das Forças Armadas, de modo a assegurar sua capacidade para atuar em rede. As prioridades são as seguintes:
> (a) Fortalecer o Centro de Defesa Cibernética com capacidade de evoluir para o Comando de Defesa Cibernética das Forças Armadas;
> (b) Aprimorar a Segurança da Informação e Comunicações (SIC), particularmente, no tocante à certificação digital no contexto da Infraestrutura de Chaves-Públicas da Defesa (ICP-Defesa), integrando as ICP das três Forças;
> (c) Fomentar a pesquisa científica voltada para o Setor Cibernético, envolvendo a comunidade acadêmica nacional e internacional. Nesse contexto, os Ministérios da Defesa, da Fazenda, da Ciência, Tecnologia e Inovação, da Educação, do Planejamento, Orçamento e Gestão, a Secretaria de Assuntos Estratégicos da Presidência da República e o Gabinete de Segurança Institucional da Presidência da República deverão elaborar estudo com vistas à criação da Escola Nacional de Defesa Cibernética;
> (d) Desenvolver sistemas computacionais de defesa baseados em computação de alto desempenho para emprego no setor cibernético e com possibilidade de uso dual;
> (e) Desenvolver tecnologias que permitam o planejamento e a execução da Defesa Cibernética no âmbito do Ministério da Defesa e que contribuam com a segurança cibernética nacional, tais como sistema modular de defesa cibernética e sistema de segurança em ambientes computacionais;
> (f) Desenvolver a capacitação, o preparo e o emprego dos poderes cibernéticos operacional e estratégico, em prol das operações conjuntas e da proteção das infraestruturas estratégicas;
> (g) Incrementar medidas de apoio tecnológico por meio de laboratórios específicos voltados para as ações cibernéticas; e
> (h) Estruturar a produção de conhecimento oriundo da fonte cibernética (BRASIL, 2008).

Conforme ressaltam Barros, Gomes e Freias (2011), a Figura 5 sintetiza uma visão inicial e geral de como se pretende organizar os diversos projetos fundamentais que possuem áreas e requisitos indispensáveis à consolidação do Setor Cibernético na Defesa, enfatizando sua integração e o trabalho conjunto.

Figura 5. Visualização do Setor Cibernético na Defesa.



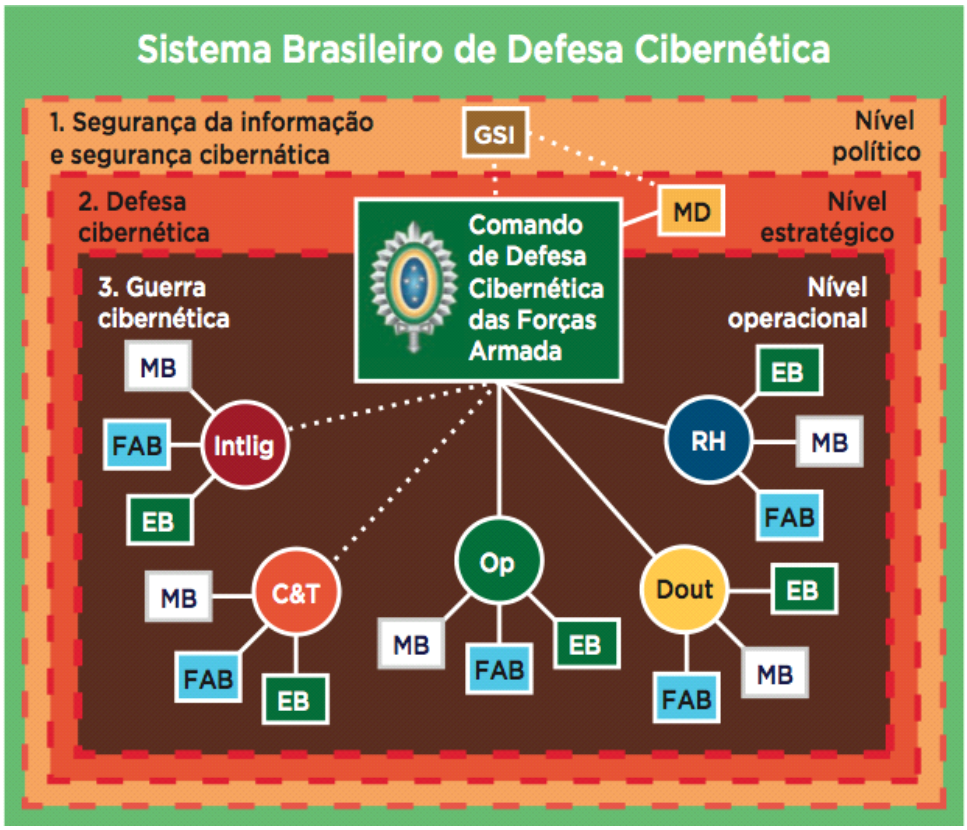
Fonte: Barros, Gomes e Freitas (2011, p. 23).

Ao analisar a Figura 5, verifica-se que a capacitação de recursos humanos constitui a atividade central na consolidação do Setor Cibernético, uma vez que proporciona capacidades cibernéticas, no dizer da própria END, indispensáveis para mobiliar os quatro vetores que o integram: inteligência; doutrina; ciência, tecnologia e inovação; e operações.

A mobilização da capacidade cibernética em nível nacional, atrelada ao amparo legal para a atuação do setor, proporciona os necessários recursos materiais e humanos, com respaldo para a realização das ações no espaço cibernético que caracterizam a Defesa Cibernética (LOBATO, 2018). A Segurança Cibernética faz parte dessa visualização porque o MD dela participa, como órgão da APF.

O Gabinete de Segurança Institucional, a fim de atender os objetivos da END referentes à Defesa Cibernética, visualiza a implantação do Sistema Brasileiro de Defesa Cibernética (SBDC), conforme ilustrado na figura 6.

Figura 6. Sistema Brasileiro de Defesa Cibernética**.**

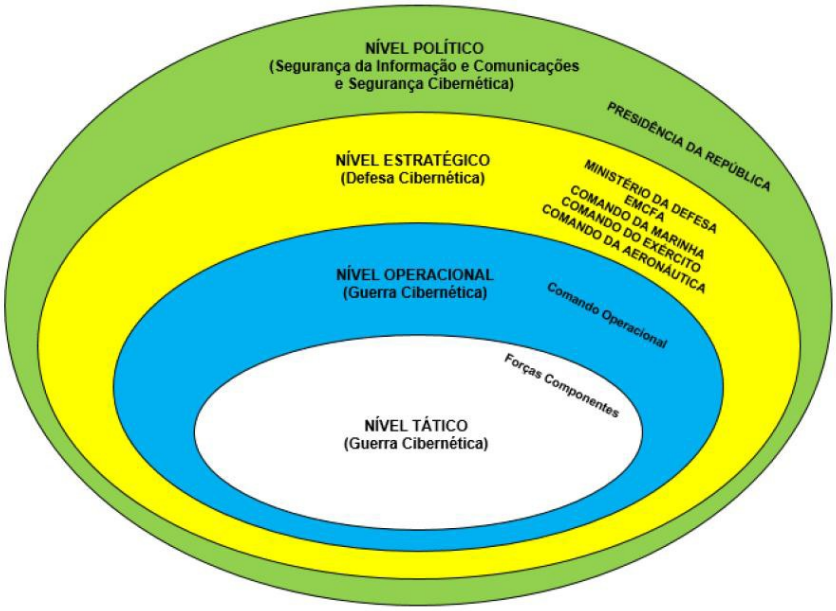


Fonte: Carvalho (2015).

De acordo com a Doutrina Militar de Defesa Cibernética - MD31- M-07 (1ª Edição/2014), a partir do estabelecimento do Setor Cibernético, decorrente da END, dois campos distintos passaram a ser reconhecido no campo cibernético brasileiro: a Segurança Cibernética, a cargo da Presidência da República (PR), e a Defesa Cibernética, a cargo do Ministério da Defesa, por meio das Forças Armadas.

No contexto do Ministério da Defesa, as ações no Espaço Cibernético deverão ter as seguintes denominações, de acordo com o nível de decisão, de acordo com a Figura 7.

Figura 7. Níveis de decisão referentes ao Espaço Cibernético Brasileiro.



Fonte: Carvalho (2015).

No nível político a Segurança da Informação e Comunicações e Segurança Cibernética é coordenada pela Presidência da República e abrange a APF direta e indireta, bem como as infraestruturas críticas da informação nacionais. Já o nível estratégico de Defesa Cibernética ficou a cargo do Ministério da Defesa, Estado-Maior Conjunto das Forças Armadas e Comandos das Forças Armadas, interagindo com a Presidência da República e a APF. E finalizando, os níveis operacional e tático, a chamada Guerra Cibernética, é restrita ao âmbito interno das Forças Armadas.

3.4.2 Modelo de governança do setor cibernético no âmbito da Defesa

A Diretriz Ministerial nº 0014, de 2009 do Ministério da Defesa, de 9 de novembro de 2009, definiu providências para o cumprimento da Estratégia Nacional de Defesa nos setores estratégicos da defesa, estabelecendo as responsabilidades para cada Força Armada. A Defesa Cibernética, por ser um dos componentes da Defesa Nacional, é missão das Forças Armadas (BRASIL, 2014).

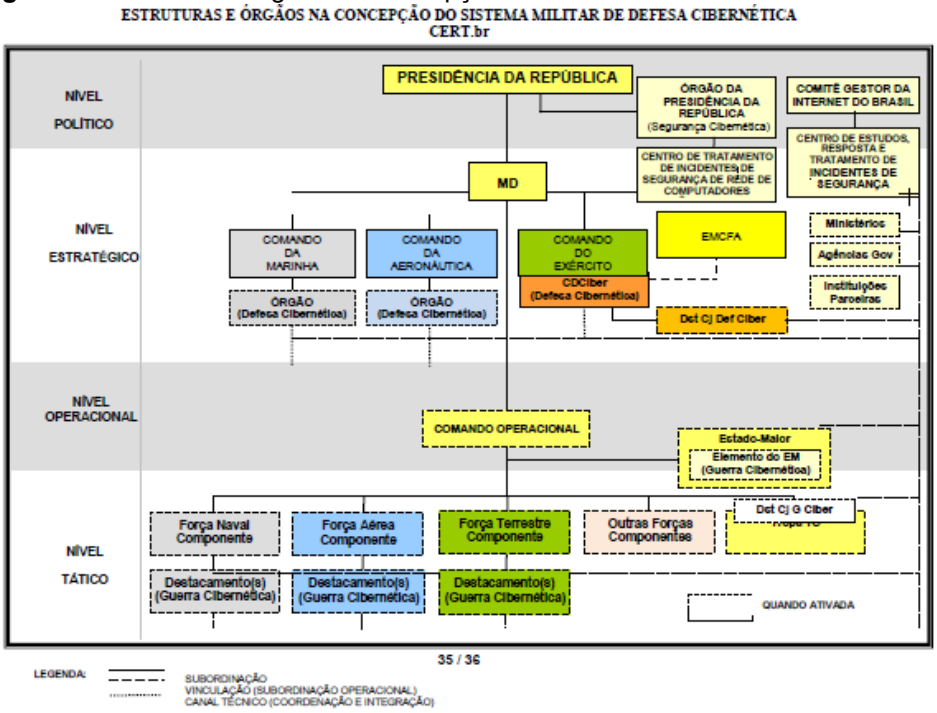
A eficácia das ações de Defesa Cibernética depende, fundamentalmente, da atuação colaborativa da sociedade brasileira, incluindo, não apenas o Ministério da Defesa, mas também a comunidade acadêmica, os setores público e privado e a base industrial de defesa. Nesse contexto, é importante a necessidade de interação permanente entre o Ministério de Defesa e os demais atores externos envolvidos com o Setor Cibernético, nos níveis nacional e internacional, conforme estabelece a Estratégia Nacional de Defesa.

O Sistema Militar de Defesa Cibernética (SMDC) é um conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal essenciais para realizar as atividades de defesa no Espaço Cibernético, assegurando, de forma conjunta, o seu uso efetivo pelas Forças Armadas, bem como impedindo ou dificultando sua utilização contra interesses da Defesa Nacional. E cabe também ao SMDC assegurar a proteção cibernética do Sistema Militar de Comando e Controle (SISMC2), assegurando a capacidade de atuar em rede com segurança, bem como coordenar e integrar a proteção das infraestruturas críticas da Informação de interesse da Defesa Nacional (BRASIL, 2014).

Na figura 8 se tem os níveis de decisão no contexto do Sistema Militar de Defesa Cibernética:

- **Nível político** - abrange as ações de SIC e Segurança Cibernética, cujos principais atores são a Presidência da República e o Comitê Gestor da Internet no Brasil;
- **Nível estratégico** - abrange as ações de Defesa Cibernética, a cargo do EMCFA, por intermédio do Centro de Defesa Cibernética, bem como dos Comandos das FA, por intermédio de seus respectivos órgãos de Defesa Cibernética, além de Centros de Tratamento de Incidentes de Redes (CTIR), da APF, de outras instituições parceiras e do Destacamento Conjunto de Defesa Cibernética, quando constituído;
- **Nível Operacional** - abrange as ações de Guerra Cibernética, a cargo dos Comandos Operacionais e de seus Estados-Maiores, quando ativados; e
- **Nível Tático** - abrange as ações de Guerra Cibernética, a cargo das Forças Componentes com seus elementos de Guerra Cibernética e o Destacamento Conjunto de Guerra Cibernética, quando ativados.

Figura 8. Estruturas e órgãos na concepção do Sistema Militar de Defesa Cibernética.



Fonte: Brasil (2014).

3.4.2.1 O setor cibernético no Exército Brasileiro

Conforme afirmam Barros, Gomes e Freitas (2011), o Exército Brasileiro, como órgão integrante da APF, tem discutido e implementado ações efetivas para desenvolver sua capacidade de enfrentamento às ameaças cibernéticas. Considera a SIC como um recurso capaz de minimizar despesas e aumentar a produtividade, conferindo disponibilidade, integridade, confidencialidade e autenticidade aos dados que trafegam em suas redes e que são processados e armazenados em seus ativos de informação.

Devido ao elevado número de organizações militares (OM) do Exército e às múltiplas realidades regionais onde estão sediadas, é indispensável que se disponha da necessária capilaridade na implantação das medidas estruturantes que assegurem o estado de segurança cibernética adequado à operação da Rede Privativa Corporativa do Exército (EBNet) e dos sistemas informacionais sobre os quais se sustentam os processos gerenciais, operacionais e administrativos da Força, no nível estratégico.

Nesse sentido, o Centro Integrado de Telemática do Exército (CITEx), localizado em Brasília, e suas OM diretamente subordinadas, os Centros de

Telemática de Área (CTA) e os Centros de Telemática (CT), constituem um sistema naturalmente vocacionado a instalar, operar e gerenciar a estrutura de segurança cibernética do Exército, em face de sua competência orgânica de gestão das redes estratégicas de comunicações, de hospedagem de sistemas de informação e de bases de dados corporativos, bem como em função da presença em todas as Regiões Militares e do apoio em serviços de TIC que presta às OM da Força.

O CITEx opera o Centro de Coordenação para Tratamento de Incidentes de Rede do Exército Brasileiro (CCTIR/EB), coordenando as Seções de Tratamento de Incidentes de Rede (STIR) de todas as suas OM subordinadas e atuando junto às demais Equipes de Tratamento de Incidentes de Rede (ETIR) existentes na Força, sendo responsável por diagnosticar falhas de segurança na rede, identificar tráfego malicioso e responder a ataques ou incidentes de segurança que possam ocorrer no âmbito da EBNet, no domínio “eb.mil.br”, preservando dessa forma a qualidade dos serviços oferecidos aos usuários internos.

Já no nível tático, verifica-se que a convergência tecnológica entre computadores e redes de telecomunicações e a proliferação do uso das TICs que provocaram uma grande mudança na arquitetura dos sistemas de comando e controle, permitindo que as forças militares presentes no campo de batalha atuem em redes, aumentando a consciência situacional do comandante e a velocidade do ciclo de tomada de decisão (BRASIL, 2014).

O Sistema de Comando e Controle da Força Terrestre (SC2FTer) é um ambiente de informação que integra computadores e redes de computadores que atendem aos Postos de Comando de diferentes escalões, empregando, para a transmissão de dados, circuitos físicos, equipamentos-rádio e terminais satelitais. Utiliza também, outras porções do espaço cibernético representadas, principalmente, pela EBnet e pela infraestrutura de TIC dos segmentos comerciais que operam os serviços de telecomunicações civis.

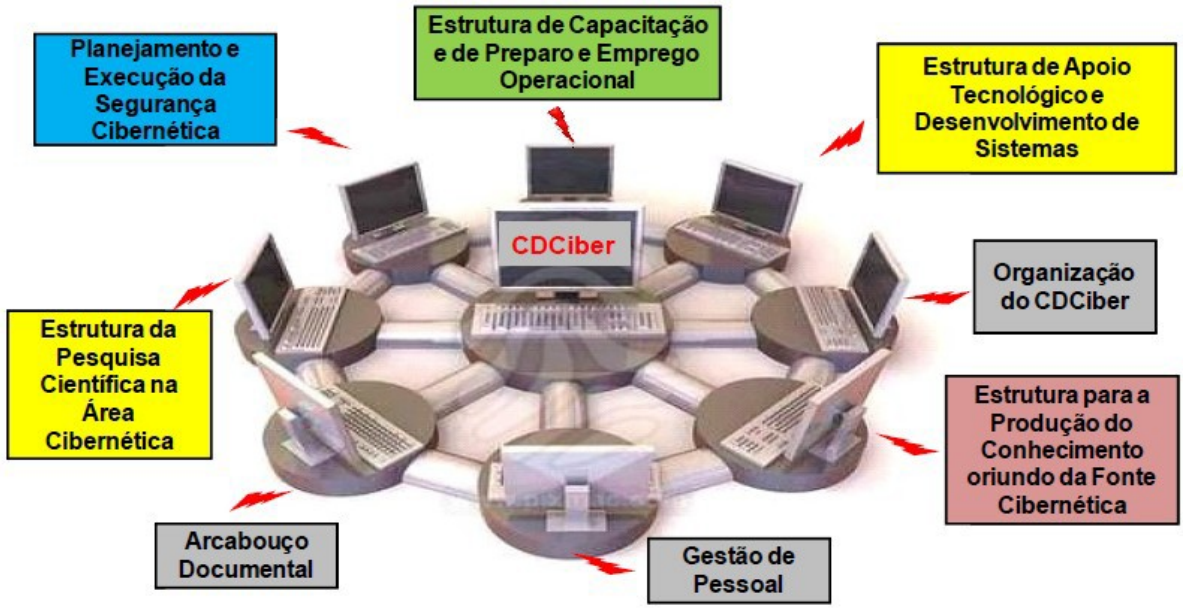
Os recentes conflitos armados, Guerra da Síria, Afeganistão e da Nigéria mostram que o comandante que obtêm, mantêm e explora a superioridade nas dimensões eletromagnética e cibernética do campo de batalha empreende a ação necessária para escolher o momento e o lugar ideais para atuar sobre os sistemas de comando e controle, de armas e de vigilância do oponente. Desta forma, cria condições adequadas para desencadear as demais ações táticas que conduzirão à conquista dos objetivos estabelecidos (BRAUN, 2018).

O Comandante do Exército Brasileiro, antecipando-se às ações que seriam tomadas pelo MD, decorrentes da END, instituiu, por intermédio da Portaria nº 03-RES/2009, o Setor Cibernético no âmbito de Exército Brasileiro, determinando que o Departamento de Ciência e Tecnologia (DCT) apresentasse ao Estado-Maior do Exército (EME), um escopo inicial para seu projeto de implantação (BRASIL, 2015).

Após a conclusão do estudo de viabilidade do escopo inicial do projeto pelo EME, o Comandante do Exército, em Portaria nº 004-RES/2010, aprovou a Diretriz de Implantação do Setor Cibernético no Exército, determinando que fossem conduzidos oito projetos estruturantes, num prazo de quatro anos.

Em agosto desse mesmo ano, foram emitidas novas portarias criando o Centro de Defesa Cibernética do Exército (CDCiber) e ativando o seu Núcleo (Nu CDCiber), inicialmente para dar provimento aos oito projetos previstos naquela Diretriz, sintetizados na Figura 9.

Figura 9. Projetos estruturantes do Setor Cibernético no EB**.**



Fonte: Barros, Gomes e Freias (2011)

3.4.2.2 O setor cibernético na Força Aérea Brasileira

Conforme Veiga (2012), mesmo tendo sido atribuída ao Exército, conforme mencionado, “a responsabilidade pela coordenação e integração desse Setor, cabe à Aeronáutica conceber, planejar e executar as ações necessárias à Def Ciber dos seus ativos.”

Na FAB, o marco regulatório interno é o Aviso Interno Nº 02/GC3/2011 (BRASIL, 2011), que “[...] estabelece orientações relativas à Segurança Cibernética no âmbito do Comando da Aeronáutica”, e determina ao Estado-Maior da Aeronáutica: “[...] propor linhas de ações futuras em prol da governança estratégica do Setor Cibernético, atentando-se para a integração e coordenação de esforços intra e inter organizacionais.”

Afirma ainda esse autor que, em atendimento à orientação de tal Diretriz, o EMAER criou a Comissão Executiva de Def Ciber (COMEX-DC) com a finalidade de estabelecer uma Concepção Operacional da Def Ciber na Aeronáutica (CONOPS), revisar os instrumentos regulatórios, instituir grupos de trabalhos, elaborar programas de conscientização e consolidar a infraestrutura de chaves públicas.

E, ainda, foi atribuída ao Centro de Computação de Aeronáutica de Brasília (CCA-BR) a responsabilidade de gerenciar o Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Força Aérea Brasileira (CTIR.FAB). Tem como missão prioritária facilitar e coordenar as atividades de tratamento e resposta a incidentes em redes computacionais, receber e/ou notificar qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores, a fim de contribuir para a segurança da informação no COMAER.

O Centro de Computação da Aeronáutica do Rio de Janeiro (CCA-RJ) possui em suas dependências uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR). Nele encontram-se profissionais que têm a responsabilidade de receber, analisar e responder às atividades relacionadas a incidentes de segurança em redes de computadores.

A Instrução do Comando da Aeronáutica 7-42/2015 (BRASIL, 2015): Gerenciamento de Incidentes de Segurança em Redes de Computadores no COMAER, está alinhada às instruções do GSI/PR e trata do funcionamento do

CTIR.FAB, também denominado CTIR.AER. Os incidentes da gestão de serviços de TI no COMAER são tratados por meio da Central de serviços do Sistema de Atendimento ao Usuário de Tecnologia da Informação do COMAER. Em complemento, os incidentes de segurança da informação são gerenciados pelo CTIR.FAB, e pelos ETIR que são tratados por meio de tickets do CTIR.FAB.

A partir da identificação das vulnerabilidades existentes nas redes, nos sistemas e nas instalações de TI, é possível prever como "*hackers*" e outras ameaças podem gerar impactos nos recursos e sistemas de TI do COMAER.

Desde 2017 a Força Aérea Brasileira tem atuado em busca de um maior diálogo com outros órgãos do Sistema de Defesa Cibernética. Em outubro do mesmo ano a Universidade da Força Aérea (UNIFA), promoveu o I Seminário de Segurança e Defesa Cibernética que contou com 290 inscritos, entre militares das Forças Armadas, integrantes de entidades de ensino superior, doutores, professores, convidados e interessados nos riscos e nas inovações tecnológicas das estruturas críticas do cenário cibernético. De acordo com um dos palestrantes do evento, o Coronel Aviador Paulo Sergio Porto, pertencente ao efetivo do Comando de Defesa Cibernética: "Para se opor a possíveis ataques cibernéticos é essencial aperfeiçoar os dispositivos de segurança e adotar procedimentos que minimizem a vulnerabilidade dos sistemas que possuam suporte de tecnologia da informação e comunicação" (informação verbal)[2].

Já o consultor em Gestão Estratégica em Riscos Cibernéticos, o Professor Doutor Paulo Pagliusi salientou que "a maioria dos vazamentos e violações de dados, que se tornaram públicos nos últimos anos, demonstram que as organizações comprometidas podem passar semanas ou até meses antes de descobrir o que ocorreu" (informação verbal)[3].

Em julho de 2019, a FAB participou pela segunda vez do Exercício Guardião Cibernético 2.0, um treinamento simulado de proteção a ataques cibernéticos, promovido pelo Comando de Defesa Cibernética (ComDCiber). Tal evento permitiu a interação entre proteção cibernética por meio da atuação colaborativa das três Forças Armadas, órgãos públicos e entidades privadas dos setores elétrico, financeiro, nuclear e de telecomunicações.

---

[2] Palestra ministrada pelo Coronel Aviador Paulo Sergio Porto no I Seminário de Segurança e Defesa Cibernética, no Rio de Janeiro, nos dias 13 e 14 de novembro de 2017.

[3] Idem.

A atividade utilizou o programa Simulador de Operações Cibernéticas (SIMOC), reproduzindo sistemas computacionais. A simulação envolveu gabinetes de crise das áreas de tecnologia da informação, comunicação social, jurídica e alta administração de eventos cibernéticos com impacto nas organizações. As discussões nos gabinetes de crise demandaram ações nos níveis decisório-gerencial (gestão de crise) e técnico (resposta ao incidente), perfazendo um total de 214 participantes e 40 empresas e organizações públicas participando de forma integrada. O evento permitiu a interação no sistema militar de defesa cibernética com as infraestruturas estratégicas do Brasil por meio de um cenário com problemas simulados de nível técnico e de gestão.

4 CASOS DE ATAQUE DE ENGENHARIA SOCIAL

Esta seção apresenta três casos de engenharia social, o Token de Segurança da RSA de 2011, o caso da Sony Pictures de 2014 e o caso da Ubiquiti Networks de 2015. Busca-se compreender antecedentes, *modus operandi*, principais características, atores envolvidos, consequências e desdobramentos. Espera-se que a compreensão dessas experiências seja útil para a FAB, eventualmente, (re)pensar suas estruturas, políticas, estratégias e ações.

4.1 Caso 1 – *Token* de Segurança RSA (2011)

Comenta-se, com frequência, a respeito do aumento da quantidade de usuários que utilizam serviços de Internet banking para realizar suas transações financeiras. Da mesma forma, cresce também o número de pessoas mal-intencionadas e que fazem de tudo para roubar senhas e acessar essas contas. Deste modo, as instituições bancárias precisaram criar novos mecanismos de segurança que auxiliem a proteção do usuário, como é o caso do *token* (FONSECA, 2009).

Os *tokens* são dispositivos físicos similares a um chaveiro. Eles geram uma senha temporária que garante maior segurança ao usuário, particularmente em transações bancárias realizadas pela Internet. Dado o curto espaço de tempo de vida útil da senha, episódios de roubo de senhas praticamente desaparecem.

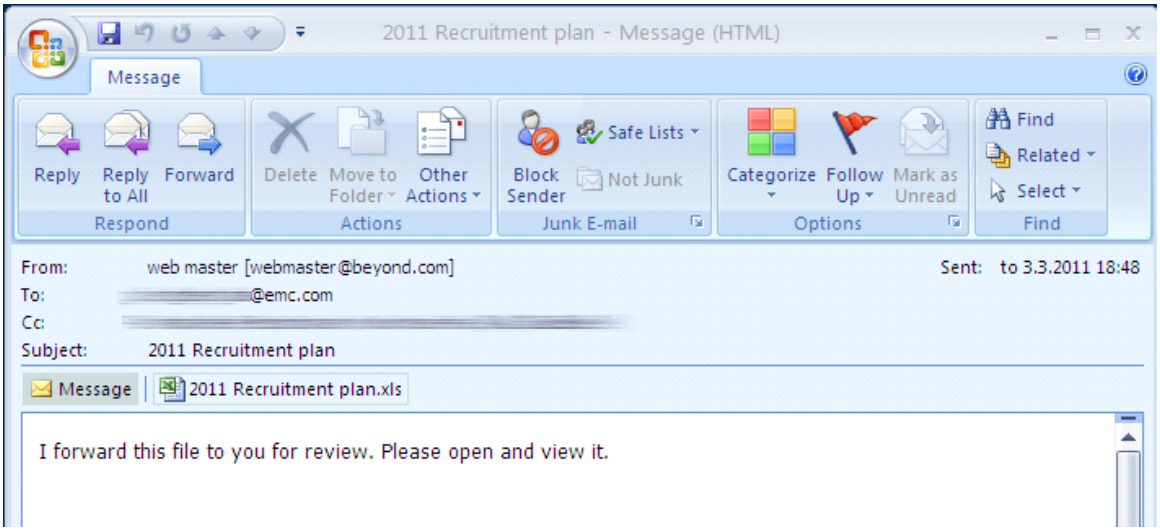
Em abril de 2011, a empresa responsável pela criação de *tokens* de segurança, a RSA, foi alvo de ataque de engenharia social por meio da técnica de *spear phishing* (LIMA, Y., 2011). De acordo com informações publicadas no site da empresa F-Secure Labs, um Estado-nação tentou invadir a Lockheed-Martin e Northrop-Grumman para roubar segredos militares do Governo dos Estados Unidos. Contudo, não logrou êxito na invasão pois as empresas usavam os *tokens* RSA SecurID para autenticação de rede.

Em retaliação, os *hackers* invadiram a empresa RSA, por meio de um ataque por email. Eles plantaram um *backdoor* e obtiveram as informações que eram necessárias, finalizando o ataque. Após esse evento, a RSA foi forçada a substituir os *tokens* do SecurID para seus clientes em todo o mundo. Convém destacar que

este sistema de segurança é utilizado por diversas instituições bancárias no Brasil (MIKKO, 2011).

Inicialmente, os *hackers* encaminharam um e-mail, conforme pode ser observado na figura 10, para um funcionário da EMC – proprietária da empresa RSA –, com cópia para mais três funcionários da mesma empresa. Cabe ressaltar que os funcionários escolhidos não eram considerados alvos de alto escalão, como um alto executivo ou administrador de TI com privilégios de redes especiais, por exemplo.

Figura 10. E-mail com planilha infectada.

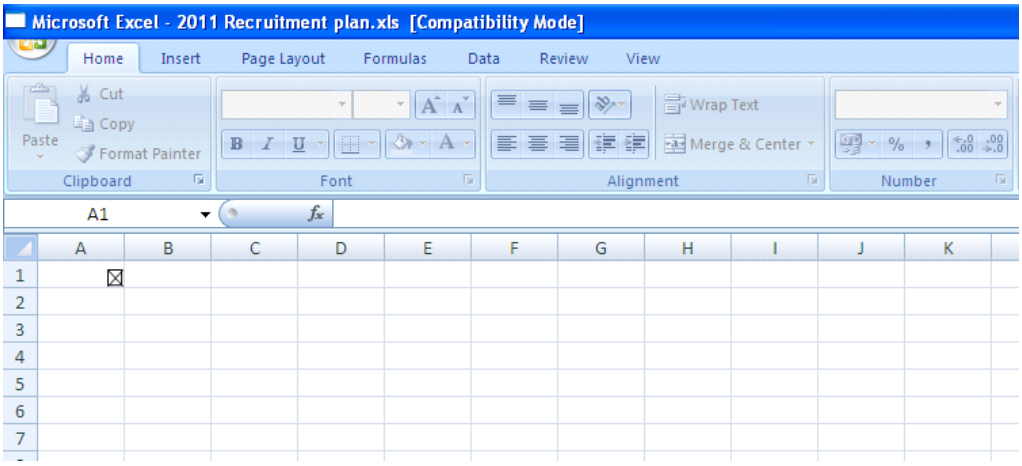


Fonte: Mikko (2011).

No e-mail nomeado “Plano de Recrutamento 2011”, estava anexada uma planilha eletrônica, figura 11, confeccionada em EXCEL, que continha um elemento em ADOBE FLASH. No momento em que um dos funcionários clicou na planilha foi acionada uma vulnerabilidade do tipo Zero Day. A expressão “zero-day” refere-se à natureza desconhecida da vulnerabilidade, menos para os *hackers*. Este ponto cego de segurança é então explorado antes que o servidor tenha conhecimento e possa corrigi-lo.

Ao abrir a planilha, o destinatário se deparava com um símbolo [X] incorporado que utiliza a vulnerabilidade CVE-2011-0609, conforme pode ser observado na figura 11.

Figura 11. Planilha infectada com CVE-2011-0699.



Fonte: Mikko (2011).

A CVE-2011-0609 é uma vulnerabilidade não especificada do Adobe Flash Player na versão 10.2.154.13 e versões anteriores no Windows, Mac OS X, Linux e Solaris. Tal vulnerabilidade permite que atacantes remotos executem código arbitrariamente ou causem uma negação de serviço, como falha no aplicativo, por exemplo, por meio de conteúdo Flash criado.

Deste modo, a CVE-2011-0609 executou o código e soltou o *backdoor* chamado *Poison Ivy*, também conhecido como *Poison,* que é muito popular da Ferramenta de Administração Remota (RAT) disponível na Deep Web. Em circulação há anos, esses tipos de arquivos são facilmente encontrados em ataques direcionados. O *Poison* faz parte de um kit que pode ser adquirido em fóruns da Deep Web.

Tal arquivo pode ser personalizado para atender às necessidades de seus compradores e é capaz de copiar no Fluxo de Dados Alternativo, evitando a detecção pelo sistema de antimalware. Logo após o código de exploração ser ativado, fecha a planilha eletrônica e a infecção termina. Depois disso, o *Poison Ivy* se conecta novamente ao domínio mincesur.com, comumente utilizado em outros ataques de espionagem.

Assim, logo que a conexão é estabelecida, o invasor tem acesso remoto completo à estação de trabalho infectada e às unidades de rede a que o usuário tinha acesso. Desse modo, os invasores foram capazes de alavancar esse vetor até obterem acesso aos dados críticos do SecurID que estavam procurando.

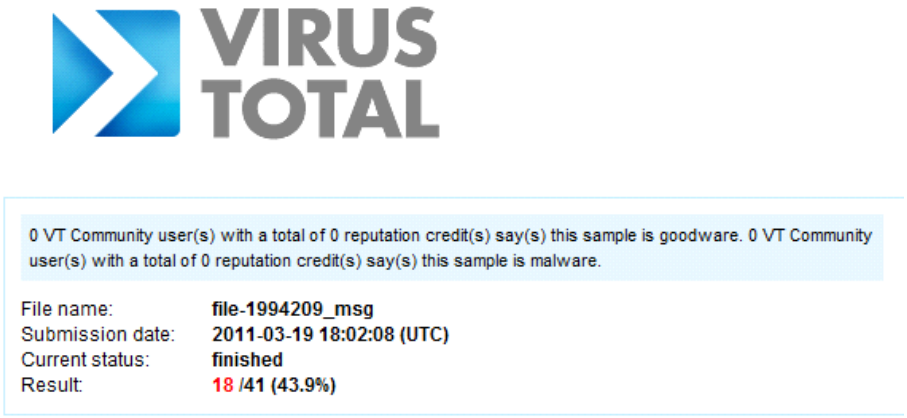
Após vir à tona o ataque da RSA, era de interesse comum saber como se deu o evento, contudo não houve cooperação da empresa RSA e, aliada a essa situação, os peritos contratados não foram capazes de descobrir como se deu a dinâmica do ataque. Mas o principal problema era que, até aquele momento, não se tinha o arquivo. Tal situação perdurou por cinco meses. Os pesquisadores de antivírus não sabiam onde achar o arquivo, e as listas de discussão sobre o assunto na Internet ficaram movimentadas em um debate a respeito de onde encontrá-lo.

Incomodado com esta situação, o consultor sênior de segurança cibernética Timo Hirvonen escreveu uma ferramenta de análise de dados que era capaz de identificar as amostras para objetos Flash. Sabia-se que o arquivo XLS em questão usava um para assumir o controle do sistema. A nova ferramenta localizou várias amostras relevantes. No entanto, uma delas não era um arquivo de Excel; era um arquivo de mensagens do Outlook (MSG).

No momento que Timo Hirvonen abriu o arquivo, percebeu que havia algo importante. O consultor de segurança tinha conseguido o e-mail original encaminhado à EMC no dia 3 de março de 2011, completo, com a planilha eletrônica.

A empresa F-Secure Labs já possuía então o arquivo, sem saber. Acredita-se que, provavelmente, um dos quatro funcionários enviou o e-mail e o anexo para o Virustotal, um serviço de digitalização on-line, e os mesmos foram compartilhados com as partes relevantes do setor de *antimalware* e segurança (Figura 12).

Figura 12. Scanner do e-mail infectado no Vírus Total.



Fonte: Mikko (2011).

A empresa já tinha o arquivo, mas não o conhecia, por não ter a ferramenta adequada naquele momento, o que se tornou possível a partir da criação de Timo Hirvonen. Cabe ressaltar que o ataque por e-mail não parece ser algo tão difícil, porém, a exploração por meio do Zero Day na planilha EXCEL foi algo inusitado na época. Estima-se que a RSA, tenha gasto cerca de US$ 66 milhões de dólares por causa desta violação de dados.

4.2 Caso 2 - *Sony Pictures* (2014)

O ataque cibernético à *Sony Pictures* ocorrido em 2014 gerou grande repercussão nas mídias. Após investigações, o Federal Bureau of Investigation (FBI) divulgou que milhares de acordos comerciais, documentos financeiros e informações de funcionários foram roubados. A incursão foi realizada a partir de um e-mail falso que foi encaminhado a alguns funcionários, supostamente o e-mail era da empresa *Apple*, um típico ataque de *spear phishing* (DONOHUE, 2014).

De acordo com o FBI, tal evento seria proveniente do Governo da Coreia do Norte em retaliação ao filme “A entrevista”, uma comédia, cujo enredo envolvia o assassinato do ditador norte-coreano Kim Jong-un (ROMANI, 2015). O FBI culpou a Coreia do Norte pela invasão à *Sony Pictures*. Documentos corroboraram esta denúncia, tendo em vista que a National Security Agency (NSA) tem monitorado há anos a Coreia do Norte (CONDLIFFE, 2015).

De acordo com uma reportagem do *The New York Times*, os Estados Unidos estavam preocupados com o aumento das capacidades da Coreia do Norte na área cibernética, por terem descoberto que ela mesma possuía, na ocasião, cerca de seis mil pessoas trabalhando em ataques cibernéticos. O exército de *hackers* era comandado pelo principal serviço de inteligência do país norte-coreano, *Reconnaissance General Bureau* e pelo *Bureau 121*, sua unidade secreta de *hackers*, possuindo ainda um posto avançado na China (SANGER; FAKLER, 2015).

Ainda de acordo com os autores, a NSA inseriu um programa espião que tinha a finalidade de monitoramento das atividades cibernéticas naquele país. Isso fez com que o Presidente Obama viesse a público e acusasse o governo de Kim Jong-un de ordenar o ataque à *Sony Pictures*. A pergunta na época foi: como os Estados Unidos chegaram tão rápido a esta conclusão?

Por meio de entrevistas e documentos, foi levado a público que o governo norte americano, por meio da NSA, vem invadindo as redes norte-coreanas há anos. Ainda assim, não foi possível prevenir a tempo o ataque à *Sony Pictures*, mesmo com as pistas que foram deixadas (DONOHUE, 2014).

No entanto, havia diversos sinais de que o ataque estava próximo de acontecer. Em 2013, um ano antes, os *hackers* norte-coreanos atacaram bancos e empresas de mídia na Coreia do Sul derrubando com o ato 50.000 computadores e servidores (ROMANI, 2015).

Em junho de 2014, a Coreia do Norte manifestou desagravo com o filme *A Entrevista* e o governo americano fez um alerta à Sony Pictures. Em setembro de 2014, funcionários da empresa começaram a receber e-mails com links maliciosos, mas não foi motivo de intervenção. Além disso, aliado aos e-mails, o estúdio não tinha uma firme política de segurança da informação. Ao contrário, possuía uma pasta no servidor denominada "*Password*" com senhas registradas (CONDLIFFE, 2015).

Em entrevista realizada com Stuart McClure, fundador e CEO da *Cylance* e ex-CTO da *McAfee*, ele relatou que, após analisar os arquivos e o *malware* que os *hackers* deixaram na Internet, concluiu que começou por meio de encaminhamentos de e-mails utilizando a técnica de *spear phishing* direcionados a funcionários que tinham acesso à rede da Sony Pictures (KEISER, 2015).

De acordo com Keiser (2015), os e-mails que pareciam ser da *Apple* exigiam que os destinatários verificassem suas credenciais de ID, conta usada pelos proprietários de *iPhone*, *iPad* e *Mac* para se conectar ao *iCloud* e adquirir conteúdo no *iTunes*, por causa de uma atividade não autorizada. Se qualquer link fosse clicado, a vítima era conduzida ao site falso que continha uma solicitação não oficial para verificação da conta.

Tal suposição foi alicerçada pelo fato de terem sido encontrados diversos e-mails de *phishing* de ID da Apple no conteúdo das caixas de entrada dos funcionários da Sony que foram publicados posteriormente na Web pelos *hackers*. Contudo, para se chegar aos nomes ideais para ataque de *spear phishing* os *hackers* realizaram uma pesquisa em uma rede social de carreiras, o LinkedIn. Fato comprovado, já que existia uma conexão entre as listagens da referida rede social e as senhas obtidas.

Os *hackers* trabalharam com o pressuposto de que as senhas do ID da *Apple* eram também utilizadas internamente. Convém destacar que os *hackers* conseguiram convencer alguns destinatários a divulgarem suas credenciais da Sony diretamente, pedindo-lhes para inserir os nomes de usuário e senhas da conta nas telas falsas de verificação do *Apple ID*.

Um nome achado no *LinkedIn* foi o do administrador de redes que tinha acesso privilegiado à distribuição de softwares para os computadores pessoais dos funcionários. Portanto, os hackers tiveram acesso à distribuição de software em toda a empresa. O administrador de redes era responsável pelo gerenciamento do *System Center Configuration Manager (SCCM)* da empresa (DONOHUE, 2014).

Ainda de acordo com Donohue (2014), foi facilitada a distribuição do *malware* chamado *Destover* para toda a Sony Pictures, pois com as credenciais roubadas da SCCM, o *malware Destover* foi encaminhado aos funcionários como uma atualização necessária ou até mesmo, como um novo software de utilização interna e, por ser originário do SCCM.

O *malware Destover* utilizado no ataque à *Sony Pictures* já tinha sido utilizado em dois outros grandes ataques direcionados à Coreia do Sul. Algumas amostras do *Destover* reportam para um servidor de comando e controle (C&C) que também foi usado por uma versão do *Trojan.Volgmer* criada para atacar alvos sul-coreanos. O *Trojan.Volgmer* pode ser usado para coletar informações do sistema e baixar outros arquivos para execução. A versão do *Volgmer* que compartilha um *C&C* com o *Destover* foi configurada especificamente para atacar alvos sul-coreanos e foi executado apenas em computadores coreanos (JOHNSON, 2014). O prejuízo com esse caso foi estimado em US$ 200 milhões, sendo que US$ 44 milhões somente em decorrência do filme “A Entrevista”. (CONDLIFFE, 2015).

4.3 Caso 3 – *Ubiquiti Networks* (2015)

A *Ubiquiti Networks* é uma empresa americana de tecnologia que começou suas atividades em 2005 no ramo de fabricação de tecnologia de redes de dados sem fio para provedores corporativos e de banda larga. Em 2015, teve a conta de e-mail de um de seus funcionários invadida.

Foram realizadas solicitações fraudulentas de uma empresa externa para o departamento financeiro. A fraude resultou em uma transferência de fundos que somaram US$ 46,7 milhões. As transferências foram realizadas diretamente por funcionários da Ubiquiti que foram enganados ao pensar que estavam recebendo pedidos legítimos do executivo, graças a endereços de e-mail falsos e domínios parecidos (PROOF, 2019).

A fraude que atingiu a Ubiquiti é sofisticada e cada vez mais comum para empresas que trabalham com fornecedores estrangeiros e empresas que realizam regularmente pagamentos por transferência eletrônica (HACKETT, 2015). Ainda segundo Hackett (2015), a empresa Ubiquiti Networks divulgou o ataque em um relatório financeiro trimestral à Comissão de Valores Mobiliários dos EUA (SEC). Entre outras informações, a Ubiquiti disse que a fraude foi descoberta em 5 de junho de 2015 e que o incidente envolveu a representação de funcionários e solicitações fraudulentas de uma entidade externa visando o departamento financeiro da empresa.

> Essa fraude resultou em transferências de fundos que totalizam US$ 46,7 milhões mantidos por uma subsidiária da empresa constituída em Hong Kong para outras contas no exterior mantidas por terceiros", escreveu Ubiquiti. “Assim que a Companhia tomou conhecimento dessa atividade fraudulenta, iniciou o contato com o banco de sua subsidiária de Hong Kong e iniciou imediatamente processos judiciais em várias jurisdições estrangeiras. Como resultado desses esforços, a Companhia recuperou US$ 8,1 milhões dos valores transferidos (Trecho retirado do Relatório que foi encaminhado à Comissão de Valores Mobiliários dos EUA) (HACKETT, 2015).

De acordo com a definição da empresa de segurança Kaspersky, a técnica de Whaling – mecanismo usado nesse caso – consiste na prática de o hacker assumir uma posição de alguém importante dentro da empresa a ser atacada. Este método é usado por criminosos cibernéticos para o roubo de dinheiro, informações confidenciais ou obtenção de acesso às redes internas para fins criminais. É também comumente chamada de “fraude do CEO”. É uma técnica semelhante ao phishing, por usar métodos como a falsificação de e-mail e sites para induzir um alvo a realizar ações específicas, como revelar dados confidenciais ou transferência de dinheiro (STERN, 2014).

Convém destacar que os golpes de phishing são direcionados a indivíduos não específicos e o spear phishing a indivíduos específicos. Já o whaling tem como

alvo pessoas em posição de destaque na empresa, que supostamente têm o poder de encaminhar comunicações que, via de regra, não são questionadas. Pode-se fazer aqui um registro quanto aos valores, normas, padrões e princípios do país. Nas sociedades asiáticas, por exemplo, há uma característica cultural de não se colocar em dúvida as ordens superiores, ainda que pairem incertezas ou suspeitas sobre encaminhamentos e decisões a tomar (PROOF, 2019).

O ser humano está preparado para respeitar a autoridade, ou em muitos casos, preparado a respeitar as pessoas que agem como se tivessem autoridade para fazer o que estão fazendo. Com isto, é possível explorar vários graus de conhecimento dos processos internos de uma empresa para convencer as pessoas de que você tem o direito de estar em lugares ou ver coisas que não deveria, ou que uma comunicação vinda de você é realmente de alguém que elas respeitam (FRULINGER, 2019).

De acordo com Frulinger (2019), técnica semelhante era utilizada pelos repórteres investigativos que trabalhavam em jornais britânicos no final dos anos 2000. Frequentemente, encontravam maneiras de obter acesso às contas de correio de voz das vítimas, fingindo ser outros funcionários da companhia telefônica por meio de um blefe e assim obtinham as informações desejadas.

Os funcionários que exerciam funções no setor financeiro da Ubiquiti Networks realizaram as transações financeiras de milhões de dólares do dinheiro da empresa para os cibercriminosos que se passavam por executivos, provavelmente usando uma URL semelhante em seu endereço de e-mail.

Sobre esses golpes, o FBI recomenda que as empresas adotem a autenticação em duas etapas, quando disponível, e estabeleçam outros canais de comunicação, como ligações telefônicas, para verificar transações significativas. As empresas também são aconselhadas a ter restrições ao publicar informações sobre as atividades dos funcionários em seus sites ou nas mídias sociais, pois os agressores que praticam esses esquemas geralmente tentam descobrir informações sobre quando os executivos da organização visada não estão no escritório (STERN, 2014).

5 ANÁLISE DOS CASOS E MITIGAÇÃO DA ENGENHARIA SOCIAL

5.1 Semelhanças e diferenças entre os casos estudados

Apesar de os três casos serem em um primeiro momento similares, cada um deles tem a sua peculiaridade. Os três foram iniciados pelo encaminhamento de *e-mails*, contudo as características dos alvos eram distintas.

No primeiro caso, da RSA, ocorrido em 2011, a empresa foi atacada pela técnica *phishing* na qual funcionários receberam e-mail que continha em seu anexo uma planilha infectada, com uma vulnerabilidade na época não muito difundida, a ZERO DAY, que libera *malwares* que forneceriam o caminho até o objetivo dos *hackers*, ou seja, à carteira de clientes da RSA. Além disso, os criminosos contaram com a inocência e a curiosidade de quatro funcionários selecionados que receberam o *e-mail*.

O ataque é considerado avançado, contudo, as etapas intermediárias executadas pelo hacker não o são, tendo em vista o modo pelo qual foi realizado. O *hacker* conseguiu a partir de um e-mail invadir um fornecedor de segurança somente para ter acesso aos sistemas dos seus clientes.

Já no caso da Sony Pictures, foi utilizada a técnica *spear phishing*, ou seja, ele tinha em mente o que queria acessar, para isto, foi utilizado e-mail e o um *site* de cadastro falsos. Assim foram conduzindo toda a situação durante meses antes da data em que veio a público o ataque. Como no primeiro caso, a motivação do ataque foi a retaliação aos Estados Unidos da América e causar prejuízo econômico e denegrir a imagem da empresa, pelo fato de o governo norte americano, por meio da NSA, estar espionando a Coreia do Norte.

Do mesmo modo, foram expostos diversos segredos e disponibilizados na Internet cerca de 1 terabyte (Tbyte) por meio de sites de compartilhamento de arquivos. Além disso, os servidores da Sony ficaram *off-line* por vários dias seguidos, pagamentos foram suspensos e até mesmo produções cinematográficas interrompidas momentaneamente.

Figura 13. Escândalos da Sony Pictures**.**

Fonte: Romani (2014)

Cabe destacar que a Sony Pictures não tinha uma Política de Segurança da Informação forte. Especialistas apontam que a Sony faz uma espécie de "economia burra", pois julgava ser mais vantajoso cobrir os custos de correção de eventuais ataques do que investir em uma política de segurança eficaz que impedisse alguma invasão.

Diversos eventos corroboram para esta linha de pensamento, por exemplo: em abril de 2011, o grupo Anonymous invadiu a PlayStation (PSN), deixando os jogadores do PSN fora do ar por 23 dias. Ela é constantemente atacada, e não é raro que fique fora do ar. Os dados de 77 milhões de contas foram roubados, o que resultou em um prejuízo de pelo menos US$ 171 milhões à companhia, e nos seis

meses seguintes, a empresa sofreu outros 21 ataques graves em várias de suas divisões.

O terceiro caso é bem similar aos dois primeiros, já que também foi realizado através de *e-mail*, mas a similaridade fica neste ponto, pois a motivação e alvos eram bem diferentes. Enquanto os dois primeiros casos foram motivados pela vingança e a vontade de causar caos e expor as duas empresas ao mundo, a motivação no terceiro era o roubo simplesmente. E o alvo foi uma pessoa que tinha autoridade suficiente para dar uma ordem para ser realizada, uma transação bancária sem questionamentos de terceiros, ou seja, o CEO da empresa.

Para finalizar, o fio que une esses três casos é a conhecida engenharia social. Quando um engenheiro social precisa conhecer melhor seu alvo, ele realiza buscas nas redes sociais de informações úteis de funcionários da empresa, cargos, amizades, perfil pessoal, entre outros. E muitas informações podem ser coletadas por meio das redes sociais, acessadas no mesmo *smartphone* que o usuário utiliza para suas tarefas corporativas.

5.2 Medidas adotadas para coibir a engenharia social na fab

Com o intuito de incrementar a conscientização a respeito do uso de recursos computacionais, a FAB adotou uma Diretriz que estabelece sua Política de Segurança da Informação (DCA 14-7) que norteia a adoção, ao longo de toda a cadeia hierárquica, de atitude favorável quanto à Segurança da Informação.

A FAB tem adotado medidas para adaptar-se à TI que se desenvolve a passos largos. O efetivo emprego da TI na atividade-fim do COMAER foi acentuado, isto é, principalmente nas operações militares propriamente ditas. A necessidade de utilizar recursos de TI é evidente. Sem auxílio de meios informatizados, é praticamente impossível analisar todas as informações de interesse militar disponíveis, as quais variam de conteúdo em tempo muito reduzido. A TI, portanto, é uma ferramenta indispensável da administração, da logística, da inteligência e das operações militares para o gerenciamento dos processos e atividades e para a tomada de decisão (BRASIL, 2006).

Em consonância com as políticas específicas do Governo Federal e com a Política da Aeronáutica, as atividades de TI devem promover aumento na efetividade

do emprego da FAB e das ações administrativas do COMAER. Convém destacar que os sistemas que utilizam TI devem restringir o acesso às informações somente às pessoas autorizadas e disponibilizá-las no local e na oportunidade adequadas, devendo garantir que seu conteúdo não seja indevidamente alterado e que a origem e o destino sejam os declarados; e que o conhecimento do conteúdo de uma informação e seus efeitos não possam ser negados (BRASIL, 2006).

Já a Política de Segurança da Informação do Comando da Aeronáutica (DCA 14-8) cita que as facilidades no acesso a ferramentas de ataque estão disponíveis na Internet. Isso aumenta significativamente a exposição dos ativos informacionais a novas ameaças e fez-se necessário um cuidado contra ações ofensivas aos sistemas do COMAER. Essas ações sempre visarão comprometer pessoas, processos, infraestruturas de comunicação e, consequentemente, os requisitos de confidencialidade, integridade e disponibilidade da informação e do conhecimento.

Nesse contexto, deverão ser consideradas as ações defensivas e proativas com o intuito de proteger o patrimônio da organização e os investimentos feitos em equipamentos, processos e capital humano de forma a assegurar o cumprimento da missão institucional do COMAER (BRASIL, 2006).

Apesar de uma Política de Segurança da Informação expressar as intenções da alta administração com o assunto, pode não constituir um esforço suficiente na conscientização do usuário. E nem mesmo a implantação de tal política de segurança pode ser suficiente para se garantir a confidencialidade, integridade e disponibilidade das informações, nem a aquisição de tecnologias de segurança ou o desenvolvimento isolado de programas também não o são.

O ideal é o entrelaçamento das tecnologias de segurança de informação e o controle dos processos organizacionais por meio da disponibilização de informações sobre o assunto ao usuário que poderão ser obtidas por meio do desenvolvimento de Programas de Conscientização em Segurança da Informação. Estes são de fundamental importância para que a segurança da informação seja aplicada de forma efetiva, pois os impactos das falhas causadas por profissionais, presentes no ambiente interno das organizações, é maior do que todas as outras fontes de recursos combinadas tais como vírus, *hackers*, falhas de *hardware,* entre outras (BRASIL, 2006).

Ainda de acordo com a DCA 14-8 (2006), os usuários do STI do COMAER em função de comando ou equivalente, devem estar comprometidos com o tema em

foco e adotar medidas necessárias para que seus subordinados conheçam e cumpram as regras contidas nos documentos normativos gerenciais e técnicos de Segurança da Informação, nos seus níveis de atribuições.

Além disso, deverão ter em mente três palavras-chave: gestão da segurança, conscientização e treinamento, que devem acompanhar a trajetória de todas as organizações militares, independentemente da sua missão. O efetivo precisa estar ciente do modo adequado da importância da informação que utilizam; ou seja, se o militar não souber a relevância do dado que maneja, não saberá protegê-lo adequadamente (BRASIL, 2006).

O STI deve possuir programas educativos destinados à conscientização e à capacitação do capital humano, no contexto da Segurança da Informação, quanto ao adequado uso dos sistemas de informação e dos recursos computacionais associados aos ativos disponíveis e em uso no STI. Deve também estimular a participação do capital humano em cursos e estágios realizados em organizações militares e civis, no Brasil e no exterior, cujos temas estejam afetos à Segurança da Informação (BRASIL, 2014).

5.3 Propostas de prevenção de ataques de engenharia social

Aposkitis (2009) entende que a atual situação social no mundo é um produto de técnicas de engenharia social que operam no fundo das questões políticas, assistência social, economia, informação, cultura, indústria, entretenimento e marketing. Face à literatura existente e às pesquisas realizadas, é possível afirmar que a melhor forma de combater ou evitar a engenharia social é por meio de treinamento de usuários, pois, em última análise, são eles os grandes alvos do engenheiro social.

A propaganda interna é um instrumento que pode contribuir para se obter ou até mesmo resgatar o comprometimento dos usuários contra a engenharia social. A implantação deste programa de conscientização e treinamento terá como intento principal influenciar os usuários a mudarem seus hábitos. Quando cônscios que fazem parte da segurança da informação da sua organização e que estão suscetíveis ao ataque de engenharia social, não se tornarão um alvo fácil para esse tipo de ameaça (GUELMAN, 2006).

Assim, entende-se que as ações a serem desenvolvidas, no âmbito da FAB, no sentido de obter soluções para o problema identificado, poderiam ser:

a) Promover a capacitação de usuários, tanto servidores civis quanto militares do COMAER, por meio de programas de conscientização, a serem desenvolvidos em cursos de formação, pós-formação e de carreira, procurando orientar e treinar a todos quanto ao tema; e

b) Promover palestras, workshops e seminários, visando a conscientização, em alto nível, em relação ao tema engenharia social.

Entende-se que é necessário que sejam realizados programas de conscientização específicos, para que todos no COMAER compreendam exatamente o que é a engenharia social e como é possível mitigar seus riscos, em especial, por meio da mudança do comportamento das pessoas. A engenharia social está relacionada ao comportamento, (des)confiança, lado emocional e psicológico, em detrimento do lado racional das pessoas. Daí a dificuldade de se resguardar a organização e todos seus ativos, sobretudo dados e informações de possíveis ameaças.

Especificamente para o efetivo do CCA-RJ, Organização do COMAER que trata de informações corporativas disponíveis em bancos de dados, trafegando em redes e sendo processadas, entende-se que as ações a serem desenvolvidas, serão mais complexas, pois, além do trabalho inicial de conscientização, outros treinamentos precisam ser realizados, visando evitar prejuízos ao COMAER e até mesmo em face da Lei de proteção de dados, do Marco Civil da Internet, dentre outros, para o cumprimento da legislação em vigor.

Assim, uma segunda etapa desse treinamento teria como objetivo fazer com que todos os servidores civis e militares, tenham consciência de que toda e qualquer informação por eles tratada, ou à qual tenham acesso, por objeto de seu trabalho, são de total sigilo e, principalmente, são de responsabilidade deles. E, desta forma, assegurar-se de que todos estão conscientes de que somente é permitido que tais informações sejam repassadas perante autorização prévia de instâncias superiores, em respeito as regras estabelecidas e, ainda, as pessoas e/ou instituições autorizadas a receber tais informações.

Entende-se, ainda, ser de fundamental importância que tais treinamentos e conscientizações sejam feitos regularmente, pois, caso contrário, o assunto acaba por cair no esquecimento. Hoje em dia, com uma série de dispositivos eletrônicos, particularmente os smartphones, a exposição é muito maior e, portanto, os riscos são potencializados. O trabalho deve ser gradual, permanente, e, assim, permitir obter sucesso.

Paralelamente a estas ações, outras iniciativas devem ser postas em prática:

1. Estabelecer claramente cargos e funções, apresentá-los a todo o efetivo e explicar de forma explícita, quais são os integrantes do setor responsável pela segurança da organização, tanto do ponto de vista físico quanto lógico;
2. Orientar os usuários de sistemas corporativos a trocarem suas senhas regularmente e, principalmente, utilizar senhas fortes, que não estejam relacionadas com dados pessoais ou com dados da organização;
3. Orientar os usuários a não fornecer senhas por telefone nem quaisquer outras informações importantes da organização. Mesmo autorizada, a informação deve ser encaminhada via e-mail corporativo;
4. Bloquear *sites* de relacionamento, entretenimento, de compras, dentre outros. Esta é uma maneira prática e eficaz para prevenir diretamente os ataques da engenharia social;
5. Criar regras rígidas para circulação (física) interna, haja vista que a engenharia social pode ser executada pessoalmente e/ou pelos próprios componentes da organização. Assim, controles aperfeiçoados na utilização dos crachás, tanto para o efetivo, quanto para as pessoas que eventualmente estão circulando, tais como alunos em curso, participantes de reuniões, prestadores de serviços e representantes de empresas e demais visitantes;
6. Realizar adequadamente o gerenciamento do lixo, pois documentos importantes podem ser descartados sem o devido cuidado. Assim, é essencial que as organizações disponham de triturador de papéis e que o efetivo seja permanentemente orientado para assegurar que nenhum documento importante foi para a lixeira; e
7. Implantar política de restrição do uso de *pen drives*, CDs e outros dispositivos externos, os quais devem ser monitorados, quando autorizados, tendo em vista que

um programa invasor pode estar em um destes dispositivos, e, quando conectados ao computador, irá contaminá-lo imediatamente.

Observa-se, assim, que a engenharia social, mesmo que pareça de pouco valor ofensivo, pode causar danos irreversíveis às organizações. A forma mais eficaz de combatê-la é a prevenção, capacitando usuários de sistemas e serviços de TI, em especial o efetivo de organizações que atuam na área de TI, como é o caso do CCA-RJ. Isso pode ser feito por meio de cursos, palestras, oficinas, simulados e controles, sempre deixando claro que as pequenas ações são essenciais para mitigar os riscos que envolvem os ataques de engenharia social.

Evitar completamente ataques de engenharia social é praticamente impossível. Portanto, caso as pessoas não estejam preparadas com conhecimento sobre a engenharia social e não mudem seus comportamentos em relação às ações para mitigar sua ocorrência, de nada adianta adquirir *software* e *hardware* avançados. Costuma-se dizer que uma corrente é tão forte quanto seu elo mais fraco. Em se tratando de engenharia social, as pessoas representam a maior vulnerabilidade para as organizações, daí a necessidade de seu constante treinamento.

Depois que se compreende a variedade de ameaças que existem, três etapas são necessárias para se projetar uma defesa contra ameaças de Engenharia Social voltada aos colaboradores da organização:

1. Desenvolver uma estrutura de gerenciamento da segurança. É preciso definir um conjunto de objetivos da segurança contra a engenharia social e um grupo de colaboradores responsáveis pelo cumprimento desses objetivos;
2. Avaliar o gerenciamento do risco. Ameaças semelhantes não apresentam o mesmo nível de risco a organizações distintas. É preciso analisar cada uma das ameaças da engenharia social e avaliar o perigo que esta representa para a sua organização; e
3. Implementar defesas contra engenharia social em sua diretiva de segurança. Desenvolver um conjunto de procedimentos que estipulem como os funcionários devem lidar com situações que possam ser ataques de engenharia social. Esta etapa parte do pressuposto da existência de uma diretiva de segurança, independentemente da ameaça apresentada. Caso a OM não a tenha será

necessário o desenvolvimento de uma. Os elementos identificados pela avaliação do risco serão um início, mas será preciso avaliar outras ameaças potenciais.

O desafio é fazer com que o usuário de TI se conscientize da importância das informações que ele manipula. Por desconhecimento da maneira correta de lidar e proteger as informações organizacionais, pode-se comprometer, inclusive, os resultados apresentados por tecnologias desenvolvidas para resguardar as informações de forma controlada e segura.

Como alternativa, recomenda-se a realização de programas educativos destinados à conscientização e à capacitação do usuário de TI na área da engenharia social. Os profissionais de TI precisam ser motivados a mudar seus hábitos e a participar de programas de treinamentos. Com essa consciência já adquirida, os usuários podem fazer a sua parte para proteger o ativo mais importante das organizações hoje em dia: a informação.

Cabe ressaltar que os programas de treinamento e conscientização devem ser realizados periodicamente, pois, com o passar do tempo, o preparo das pessoas diminui. Além disso, o surgimento constante de novas ameaças e técnicas usadas pelos engenheiros sociais faz com que seja necessário reforçar e atualizar os princípios da segurança da informação nas mentes dos usuários. A aplicação de técnicas de marketing interno faz-se relevante para se obter o comprometimento dos usuários para com o programa, o que contribui consequentemente para sua efetividade.

CONSIDERAÇÕES FINAIS

Dentre os autores apresentados ao longo do texto, destacam-se os clássicos Bobbio, Matteucci e Pasquino (1998) e Castells e Cardoso (2006). Os primeiros, particularmente para representar o contexto em que a informação e o conhecimento podem ser objeto de cobiça e instrumento para exercício de poder e dominação. Os proprietários e responsáveis legais e legítimos desses ativos devem saber protegê-los sob o risco de serem dominados e ficarem reféns de pessoas mal-intencionadas. Quando esses ativos são bens públicos, a responsabilidade aumenta. Bobbio, Matteucci e Pasquino (1998) descrevem inclusive o poder da manipulação para se atingir objetivos desejados.

As redes sociais e os recursos tecnológicos têm facilitado o trabalho daqueles que querem confundir, ludibriar e enganar seus interlocutores, em última instância, para exercer algum tipo de poder. Diante da dependência tecnológica nos processos de comunicação e de relacionamento, é pertinente a elaboração de Castells e Cardoso (2006) acerca da sociedade em rede como uma perspectiva inescapável. Os pontos de conexão dessas redes se intensificam tornando o mundo mais complexo e sujeito a novas oportunidades, mas também a novas ameaças.

Como parte de um processo de amadurecimento intelectual, as inquietações iniciais da pesquisa aumentaram. A investigação permitiu ampliar os horizontes de conhecimento quanto às ameaças à segurança da informação, mas também às possibilidades de enfrentamento do problema. Há um embate diuturno entre forças que devem preservar a ordem e a estabilidade e; forças que se articulam para quebrar as regras e corromper o sistema.

A leitura dos casos à luz da literatura sobre guerra híbrida, cibernética, redes sociais e engenharia social possibilitou uma compreensão melhor da engenharia social enquanto fenômeno que pode ser o estopim para crises de grandes proporções. Estas incluem o cenário de guerras híbridas e, portanto, precisa encontrar respostas à altura. Acredita-se que o presente estudo contribuiu para a melhor compreensão desse processo como um todo, da percepção da ameaça à necessidade de mitigá-la. A experiência profissional da pesquisadora foi enriquecida pelos meios e possibilidades de se incrementar a segurança da informação a partir de regras e procedimentos adequados.

Destaca-se também que o estudo permitiu identificar as iniciativas governamentais e o aparato legal que podem contribuir para lidar com os crimes ligados à segurança da informação. É importante que o tema seja objeto de debate na esfera macro, podendo envolver outros países e suas respectivas políticas e legislações. Todavia, é na esfera micro, ou seja, no interior das organizações que a engenharia social deve ser combatida e os casos estudados endossam a necessidade dessa preocupação. Dentre as limitações da pesquisa, pode-se citar que alguns detalhes que ajudariam a compreender os casos de forma mais minuciosa não estão disponíveis para acesso, ou mesmo publicados.

Na seção anterior, os subitens apresentam direcionadores para estudos futuros. Pode-se elencar aqui outras alternativas, entre elas a interface com diferentes áreas do conhecimento. A engenharia social no âmbito da Defesa e, consequentemente, da Ciência Política e Relações Internacionais pode ter o suporte teórico e conceitual das lentes da gestão organizacional e da psicologia. Essas áreas do conhecimento podem ajudar a compreender o fenômeno de forma mais sistêmica.

Adicionalmente, a partir da experiência adquirida com esta dissertação, enquanto um produto da pesquisa, pode-se construir um banco de casos de engenharia social para divulgação ao público interno da FAB e, se houver interesse, o compartilhamento no âmbito do Ministério da Defesa em um primeiro momento e eventualmente outras unidades do governo. Em um segundo momento, pode-se extrapolar esse banco de casos para outros ataques e incidentes cibernéticos cuja causa não tenha sido de engenharia social, mas que tenham um caráter pedagógico para ajudar a garantir a Segurança da Informação nos patamares mais elevados que se esperam das Forças Armadas no Brasil.

REFERÊNCIAS

ABRAHAM, Sherly; CHENGALUR-SMITH, Indushobha. An overview of social engineering malware: trends, tactics, and implications. **Technology In Society**, [*s. l.*], v. 32, n. 3, p. 183-196, ago. 2010.

AGRELA, Lucas. **O escândalo de vazamento de dados é muito pior do que parecia**. São Paulo, 06 abr. 2018. Disponível em: https://exame.abril.com.br/tecnologia/o-escandalo-de-vazamento-de-dados-do-facebook-e-muito-pior-do-que-parecia/. Acesso em: 25 out. 2019.

ALMEIDA, Julio Sergio Gomes de; CAGNIN, Rafael Fagundes (Org.). **A indústria do futuro no Brasil e no mundo**. [*S. l.: s. n.*], 2019. 622 p. Disponível em: https://iedi.org.br/media/site/artigos/20190311_industria_do_futuro_no_brasil_e_no_mundo.pdf. Acesso em: 14 abr. 2019.

ALVES, Andréa Moraes. **A dama e o cavalheiro**: um estudo antropológico sobre envelhecimento, gênero e sociabilidade. Rio de Janeiro: Editora FGV, 2004.

ALVES, Cássio Bastos. **Segurança da informação vs. Engenharia social**. São Paulo: Clube de autores, 2007.

ALLAN, A., NOAKES-Fry, K., Mogull, R. **Business Update**: how businesses can defend against social engineering attacks**.** 2005. Disponível em: https://pt.scribd.com/document/174320313/SOCIAL-ENGINEERING-A-MEANS-TO-VIOLATE-A-COMPUTER-SYSTEM-By-Malcolm-Allen-updated-June-2006. Acesso em: 20 ago. 2018.

ALLEN, G. and CHAN, T. **Artificial inteligence and national security**. Cambridge: Harvard Kennedy School, 2017. 132 p.

APOSKITIS, L. Social Engineering: the absolute war in full development. **Journal of Hellenic Nexus**, [*s. l.*], dez. 2009. Disponível em: http://thegreek.hubpages.com/hub/Social-Engineering-The-absolute-war. Acesso em: 05 jul. 2018.

ARMISTEAD, L. **Information operations**: warfare and the hard reality of soft power. Washington: Brassey'sinc, 2004. 277 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001:** Tecnologia da informação: técnicas de segurança: sistemas de gestão da segurança da informação: requisitos. Rio de Janeiro: 2013. 30 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27005**: Tecnologia da informação: técnicas de segurança: gestão de riscos de segurança da informação. Rio de Janeiro: 2019. 66 p.

BAPTISTA, Ricardo C. **Antimalware.** [*S. l.*], 25 ago. 2016. Disponível em: https://www.mycybersecurity.com.br/glossario/antimalware/. Acesso em: 15 ago. 2018

BARROS, Otávio Santana Rêgo; GOMES, Ulisses de Mesquita; FREITAS, Whitney Lacerda de (Org.). **Desafios estratégicos para segurança e defesa cibernética**. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011. 216 p

BERGER, Peter; LUCKMANN, Thomas. **A construção social da realidade**. Petrópolis: Vozes, 1998.

BIANCHI, Ivaro. O conceito de Estado em Max Weber. **Lua Nova**, São Paulo, n. 92, p. 79-104, 2014.

BOBBIO, Norberto; MATTEUCCI, Nicola; PASQUINO, Gianfranco. **Dicionário de Política.** Brasília: Editora Universidade de Brasília, 11. ed., 1998.

BRASIL. Comando da Aeronáutica. **Aviso Interno Nº 02/GC3/2011**. Estabelece orientações relativas à Segurança Cibernética no âmbito do Comando da Aeronáutica e determina ao Estado-Maior da Aeronáutica propor linhas de ações futuras em prol da governança estratégica do Setor Cibernético, atentando-se para a integração e coordenação de esforços intra e inter organizacionais. [Brasília, DF], 2011.

BRASIL. Comando da Aeronáutica. Comando Geral de Apoio. Portaria EMAER n° 41/3SC, de 9 de setembro de 2016. Aprova a edição da Instrução que trata do Gerenciamento de Incidentes de Segurança em Redes de Computadores no Comando da Aeronáutica (ICA 7-42). **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 158, f. 7427, 16 set. 2016.

BRASIL. Comando da Aeronáutica. Centro de Inteligência da Aeronáutica. Portaria nº 23/DCI, de 9 de maio de 2019. Aprova a reedição da instrução que dispõe sobre as Medidas de Segurança para Equipamentos Criptotécnicos e de Comunicações no âmbito do SINTAER. (ICA 200-8). **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 80, f. 5767, 14 maio 2019.

BRASIL. Comando da Aeronáutica. Centro de Inteligência da Aeronáutica. Portaria nº 3 /CIAER, de 19 de dezembro de 2008. Aprova a edição do Folheto que dispõe sobre Mentalidade de Segurança (FCA 200-2). **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 13, f. 349, 21 jan. 2009.

BRASIL. Comando da Aeronáutica. Estado Maior da Aeronáutica. Portaria nº 1/CONTI, de 05 de setembro de 2018. Aprova o Plano de Tecnologia da Informação da Aeronáutica (PCA 11-319). **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 159, f. 9693, 11 set. 2018.

BRASIL. Comando da Aeronáutica. Política de Segurança da Informação do Comando da Aeronáutica (DCA 14-8). **Boletim do Comando da Aeronáutica**, Brasília, DF, out. 2006.

BRASIL. Comando da Aeronáutica. Centro de Inteligência da Aeronáutica. Portaria nº 02/CIAER, de 8 de outubro de 2009. Aprova a edição do Folheto que dispõe sobre Prevenção à Engenharia Social (FCA 200-3). **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 2016, f. 7414, 6 nov. 2009.

BRASIL. Comando da Aeronáutica. Centro de Inteligência da Aeronáutica. Portaria nº R-650/GC3, de 31 de maio de 2007. Aprova a edição da Instrução que versa sobre a Concessão de Credencial de Segurança de Pessoa Jurídica (ICA 200-4). **Boletim do Comando da Aeronáutica**, Rio de Janeiro, 29 jun. 2007.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2015]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 20 maio 2015.

BRASIL. **Decreto Nº 3.505, de 13 de junho de 2000**. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Brasília, DF: Presidência da República, 2000.

BRASIL. **Decreto nº 5.484, de 30 de junho de 2005**. Aprova a Política de Defesa Nacional, e dá outras providências. Brasília, DF: Presidência da República, 2005. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5484.htm. Acesso em: 19 set. 2019.

BRASIL é um dos principais alvos de ataques de hackers. VEJA, São Paulo, 10 mar. 2019. Disponível em: https://veja.abril.com.br/tecnologia/brasil-e-um-dos-principais-alvos-de-ataques-de-hackers/. Acesso em: 09 nov. 2019.

BRASIL. Ministério da Defesa. Escola Superior de Guerra. **Fundamentos do poder nacional**. Rio de Janairo: ESG, 2019.

BRASIL. Ministério da Defesa. **Portaria no 9/GAP/MD, de 13 de janeiro de 2016.** Aprova o Glossário das Forças Armadas (MD35-G-01). 5. ed. Brasília, DF: Ministério da Defesa, 2015.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018**: versão 01. Brasília, DF: Presidência da República, 2015.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Guia de Orientações ao Gestor em Segurança da Informação e Comunicações**: versão 01. Brasília, DF: Presidência da República, 2014.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Livro Verde de Segurança Nacional.** Raphael Mandarino Junior e Claudia Canongia (Org.). Brasília, DF: Presidência da República, 2010.

BRASIL. Portaria nº 45, de 08 de setembro de 2009. Institui, no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), o Grupo Técnico de Segurança Cibernética e dá outras providências. **Diário Oficial da União**: Brasília, DF, n. 172, 09 set. 2009.

BRASIL. Tribunal de Contas da União. **Boas Práticas em Segurança da Informação**. 3. ed. Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2008. Disponível em: http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/biblioteca_tcu/biblioteca_digital/Boas_praticas_em_seguranca_da_informacao_3a_edicao.pdf. Acesso em: 22 jun. 2009.

BRAUN, Julia. **Jogo de forças mundial**: as guerras que continuam em 2019. VEJA, São Paulo, 2018. Disponível em: https://veja.abril.com.br/mundo/jogo-de-forcas-mundial-as-guerras-que-continuam-em-2019/. Acesso em: 11 nov. 2019.

BULLÉE, Jan-willem Hendrik; MONTOYA, Lorena; PIETERS, Wolter; JUNGER, Marianne; HARTEL, Pieter. On the anatomy of social engineering attacks-A literature-based dissection of successful attacks. **Journal Of Investigative Psychology And Offender Profiling**, [*s. l.*], v. 15, n. 1, p. 20-45, 14 jul. 2017.

CALDWELL, Tracey. Ethical hackers: putting on the white hat. **Network Security,** [*s. l.*], v. 2011, n. 7, p. 10-13, jul. 2011.

CANONGIA, Claudia; MANDARINO JUNIOR, Raphael. Segurança cibernética: o desafio da nova sociedade da informação. **Parcerias Estratégicas**, Brasília, DF, v. 14, n. 29, p. 21-46, jun./dez. 2009.

CARNEIRO, João Marinonio Enke. **A guerra cibernética:** uma proposta de elementos para a formulação doutrinária no Exército Brasileiro. 2012. Tese (Doutorado em Ciências Militares) – Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2012.

CARR, Jeffrey. **Inside cyber warfare**: mapping the cyber underworld. Sebastopol: O'Reilly Media, 2009.

CARVALHO, Paulo. **Sistema Brasileiro de Defesa Cibernética**. Exército Brasileiro, 2015. Disponível em: http://defesacibernetica.ime.eb.br. Acesso em: 26 dez. 2019.

CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais**. Rio de Janeiro: Brasport, 2014. 136 p.

CASTELLS, Manuel; CARDOSO, Gustavo (Org.). **A sociedade em rede:** do conhecimento à ação política. Livro organizado a partir de Conferência promovida pelo então Presidente da República de Portugal, Jorge Sampaio, em 4 e 5 de Março de 2005, no Centro Cultural de Belém. Lisboa: Imprensa Nacional: Casa da Moeda, 2006. 435 p.

CERT. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de Segurança para Internet**. [*S. l.*], 2017. Disponível em: https://cartilha.cert.br/golpes. Acesso em: 23 nov. 2019.

CIALDINI, Robert. B.. **Influence**: science and practice. Boston: Ally & Bancon, 2001.

COMITÊ GESTOR DA INTERNET NO BRASIL. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança. **Cartilha de Segurança para Internet**. São Paulo, 2012. Disponível em: http://cartilha.cert.br/sobre/old/cartilha_seguranca_1.0.pdf. Acesso em: 24 fev. 2014.

COMO o avanço da tecnologia beneficia a Medicina?. Exame, São Paulo**,** 3 set. 2018. Disponível em: https://exame.com/negocios/dino_old/como-o-avanco-da-tecnologia-beneficia-a-medicina/. Acesso em: 05 nov. 2019.

CONDLIFFE, Jamie. **NSA invadiu redes da Coreia do Norte e não sabia que ataque à Sony Pictures iria acontecer**. São Paulo, 2015. Disponível em: https://gizmodo.uol.com.br/nsa-coreia-norte. Acesso em: 28 nov. 2019.

CONHEADY, Sharon. **Social engineering in IT security**: tools, tactics, and techniques**.** Estados Unidos: McGraw-Hill Education, 2014.

DONOHUE, Brian. **A Coreia do Norte é realmente culpada pelo ataque à Sony?**. São Paulo, 24 dez. 2014. Blog: https://www.kaspersky.com.br. Disponível em: https://www.kaspersky.com.br/blog/coreia-norte-ataque-sony/4582/. Acesso em: 28 nov. 2019.

DRUCKER, P. F.. **Sociedade pós-capitalista**. São Paulo: Pioneira, 1993.

EISSÁ, Sergio G. **Guerra Hibrida:** ¿una nueva forma de pensar la guerra en siglo XXI. [*S. l.*], 2009. Disponível em: https://www.academia.edu/31286309/GUERRA_HIBRIDA_UNA_NUEVA_FORMA_DE_PENSAR_LA_GUERRA_EN_EL_SIGLO_XXI. Acesso em 29 nov. 2019.

ELIAS, N. **A sociedade dos indivíduos**. Rio de Janeiro: Jorge Zahar, 1994. 201 p.

FAUSTINO, Rafael. **Nunca houve tanta violação de dados pessoais, diz promotor que investiga casos.** ÉPOCA NEGÓCIOS, São Paulo, 2018. Disponível em: https://epocanegocios.globo.com/Mercado/noticia/2018/09/nunca-houve-tanta-violacao-de-dados-pessoais-diz-promotor-que-investiga-casos.html. Acesso em: 26 out. 2019.

FELINTO, Erick; SANTAELLA, Lucia. **O explorador de abismos**: Vilém Flusser e o pós-humanismo. São Paulo: Paulus, 2012.

FONSECA, William. **O que é token?**. São Paulo, 11 nov. 2009. Blog: https://www.tecmundo.com.br. Disponível em: https://www.tecmundo.com.br/senha/3077-o-que-e-token-.htm. Acesso em: 20 ago. 2018.

FRUHLINGER, Josh. **Social engineering explained:** how criminals exploit human behavior. Massachusetts, 25 set. 2019. Disponível em: https://www.csoonline.com/article/2124681/what-is-social-engineering.html. Acesso em: 31 out. 2019.

GARDINI, Mayara Gabrielli. Terrorismo no ciberespaço: o poder cibernético como ferramenta de atuação de organizações terroristas. **Fronteira**: Revista de iniciação científica em relações internacionais, Belo Horizonte, v. 13, n. 25 e 26, p. 7-33, 2014.

GARNIER, Cintia; PADILHA, Tamyris. **Ética, privacidade e novas tecnologias**: impacto da lei de proteção de dados na sociedade. Migalhas, 2019. Disponível em: https://www.migalhas.com.br/depeso/311142/etica-privacidade-e-novas-tecnologias-o-impacto-da-lei-de-protecao-de-dados-na-sociedade. Acesso em: 10 out. 2019.

GEIS, John P.; HAMMOND, Grant T.; FOSTER, Harry A.; HAILES, Theodore C.. **Blue Horizons IV:** deterrence in the age of surprise. Alabama: Air University Press, 2014.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social.** 3. ed. São Paulo: Atlas, 2008.

GRANGER S. **Social engineering fundamentals, part I**: hacker tactics. Security Focus, 2001. Disponível em: http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-ihacker-tactics. Acesso em: 18 ago. 2018.

GUELMAN, Luiz. **Conscientização de usuários:** como envolver seu público com a Segurança da Informação. Rio de Janeiro, 2006. Disponível em: https://www.modulo.com.br/comunidade/entrevistas/616-conscientizacao-de-usuarios-como-envolver-seu-publico-com-a-seguranca-da-informacao. Acesso em: 19 set. 2015.

HACKETT, Robert. **Fraudsters duped this company into handing over $40 million**. [*S. l*], 2015. Disponível em: https://fortune.com/2015/08/10/ubiquiti-networks-email-scam-40-million/. Acesso em: 30 nov. 2019.

HADNAGY, Cristopher. **Social engineering**: the art of human hacking. Indianapolis: Wiley Publishing, 2011.

HAYWARD, Clarissa Rite. **O poder sem face**: de volta à velha antinomia “estrutura” e “prática”?. Cambridge: Cambridge University Press, 2000.

HOFFMAN, Frank G.. Complex Irregular Warfare: the next revolution in military affairs. **Orbis**, [*s. l.*], v. 50, n. 3, p. 395-411, jun. 2006.

HOFFMAN, Frank G.. **Conflict in the 21th century**: the rise of hybrid wars. Virginia: Potomac Institute for Police Studies, 2007. 72 p.

HOFFMAN, Frank G. Hybrid threats: reconceptualizing the evolving character of modern conflict. **Strategic Forum**, Washington, DC, n. 240, abr. 2009.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. **Acesso à Internet e à televisão e posse de telefone móvel celular para uso pessoal**: 2016. Rio de Janeiro: IBGE, 2018. Disponível em: https://agenciadenoticias.ibge.gov.br/media/com_mediaibge/arquivos/c62c9d551093e4b8e9d9810a6d3bafff.pdf. Acesso em: 12 ago. 2018.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. **PNAD Contínua TIC 2016**: 94,2% das pessoas que utilizaram a Internet o fizeram para trocar mensagens. Rio de Janeiro, 21 fev. 2018. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/20073-pnad-continua-tic-2016-94-2-das-pessoas-que-utilizaram-a-internet-o-fizeram-para-trocar-mensagens. Acesso em: 23 out. 2019.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. **PNAD Contínua TIC 2017**: Internet chega a três em cada quatro domicílios do país. Rio de Janeiro, 20 dez. 2018. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/23445-pnad-continua-tic-2017-internet-chega-a-tres-em-cada-quatro-domicilios-do-pais. Acesso em 23 out. 2019.

JOHNSON, A. L.. **Destover:** destructive malware has links to attacks on South Korea. [*S. l.*], 2014. Disponível em: https://www.symantec.com/connect/blogs/destover-destructive-malware-has-links-attacks-south-korea. Acesso em: 27 nov. 2019.

JOHNSON, R. J. **The weakest link**. [*S. l.*], 2005. Disponível em: http://prescientconsulting.com/content/view/43/30.2005. Acesso em: 03 nov. 2015.

KEISER, Gregg. **Sony hackers targeted employees with fake Apple ID e-mails.** Estados Unidos, 2015. Disponível em:

https://www.computerworld.com/article/2913805/sony-hackers-targeted-employees-with-fake-apple-id-emails.html. Acesso em: 28 nov. 2019.

KIM, Joon Ho. Cibernética, ciborgues e ciberespaço: notas sobre as origens da cibernética e sua reinvenção cultural. **Horizontes Antropológicos**, Belo Horizonte, v. 10, n. 21, p. 199-219, jun. 2004.

LAKATOS, Eva Maria; MARCONI, Marina A. **Fundamentos de metodologia científica.** 3. ed. São Paulo: Atlas, 1991.

LÉVY, Pierre. Cibercultura. São Paulo: Editora 34, 1999.

LÉVY, Pierre. **O que é virtual?**. São Paulo: Editora 34, 1996.

LIMA, Caio. **Você conhece as principais leis do Direito Digital e Eletrônico?**. [*S. l.*], 2014. Disponível em: https://caiocesarlima.jusbrasil.com.br/artigos/182558205/voce-conhece-as-principais-leis-do-direito-digital-e-eletronico. Acesso em: 01 nov. 2019.

LIMA, Hélio. **Percepção e riscos na utilização de redes sociais (Facebook) por parte dos militares caboverdianos**. 2015. Dissertação (Mestrado em Formação e Comunicação Multimédia) – Faculdade de Filosofia e Ciências Sociais. Universidade Católica Portuguesa, Lisboa, 2015. Disponível em: https://repositorio.ucp.pt/bitstream/10400.14/20791/1/Tese%20Final%20H%C3%A9lio%20Lima.pdf. Acesso em: 13 nov. 2019.

LIMA, Yeltsin. **Combinação de Excel e Flash em ataque contra a RSA**. Tecnoblog, 2011. Disponível em: https://tecnoblog.net/75126/ataque-virus-excel-flash/. Acesso em: 09 nov. 2019.

LINKEDLN confirma invasão de crackers. ÉPOCA NEGOCIOS, São Paulo, 6 jun. 2012. Disponível em: https://epocanegocios.globo.com/Informacao/Acao/noticia/2012/06/linkedin-confirma-invasao-de-crackers.html. Acesso em: 23 out. 2019.

LOBATO, Louise. Uma estratégia para a governança da Segurança Cibernética no Brasil. **Nota Estratégica**, Rio de Janeiro, n. 30, set. 2018. Disponível em: https://igarape.org.br/wp-content/uploads/2018/09/Uma-estrate%CC%81gia-para-a-governanc%CC%A7a-da-seguranc%CC%A7a-ciberne%CC%81tica-no-Brasil.pdf. Acesso em: 11 maio 2019.

MALAFAIA, Renato. Cibersegurança: uma reflexão sobre a educação digital à luz do Direito. **Fonte**, Belo Horizonte, ano 14, n. 18, p. 94-108, dez. 2017. Disponível em: https://www.prodemge.gov.br/images/com_arismartbook/download/22/revista_18.pdf. Acesso em: 18 jul. 2018.

MALHOTRA, Naresh. **Pesquisa de Marketing:** uma orientação aplicada. 4. ed. Porto Alegre: Bookman, 2006.

MANDARINO JUNIOR, Raphael. **Segurança e defesa do espaço cibernético brasileiro.** Recife: Cubzac, 2010.

MANN, Ian. **Engenharia Social**. São Paulo: Longarina, 2011.

MANN, Ian. **Hacking the human**. Hampshire: Gower, 2008.

MARQUES, Cleber. **Engenharia social**: os perigos das redes sociais para empresas. São Paulo, 2017. Linkedin: https://br.linkedin.com/in/cleberm?trk=author_mini-profile_title. Disponível em: https://www.linkedin.com/pulse/engenharia-social-os-perigos-das-redes-sociais-para-empresas-marques. Acesso em: 25 jul. 2018.

MARTINS, Rodrigo. **Engenharia social**. [*S. l.*], 2014. Blog: https://atitudereflexiva.wordpress.com. Disponível em: https://atitudereflexiva.wordpress.com/2014/08/26/engenharia-social/. Acesso em: 04 dez. 2019.

MATTAR, Fauze Najib. **Pesquisa de Marketing.** 3. ed. São Paulo: Atlas, 1999.

MAULAIS, Claudio Nunes dos Santos. Engenharia Social: técnicas e estratégias de defesa em ambientes vulneráveis. 2016. Dissertação (Mestrado em Sistemas de Informação e Gestão do Conhecimento) – Faculdade de Ciências Empresariais. Universidade Fundação Mineira de Educação e Cultura, Belo Horizonte, 2016. *In*: **Projetos, Dissertações e Teses em Sistemas de Informação e Gestão do Conhecimento**, v. 5, n. 1, 2016. Disponível em: http://www.fumec.br/revistas/sigc/article/view/3733. Acesso em: 24 ago. 2018.

MELLO, Gabriela. **Comércio eletrônico brasileiro deve crescer 12% em 2018**. São Paulo, 09 mar. 2018. Disponível em: https://exame.abril.com.br/economia/comercio-eletronico-brasileiro-deve-crescer-12-em-2018/. Acesso em: 21 ago. 2018.

MERENDI, Tatiana Peghim. O poder do Estado. **Âmbito Jurídico**, São Paulo, ano 8, n. 22, ago. 2005. Disponível em: http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=331. Acesso em 25 ago. 2018.

MICROSOFT. **The Security Risk Management Guide**. *[S. l.*], 2016. Disponível em: https://www.computerweekly.com/tip/How-to-use-the-free-Microsoft-Security-Risk-Management-Guide. Acesso em: 24 ago. 2018.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar**. São Paulo: Pearson Makron Books, 2003.

MITNICK, Kevin D.; SIMON, William L. **The art of intrusion:** the real stories behind the exploits of hackers, intruders, and deceivers. Indianapolis: Wiley Publishing, 2005.

MIKKO. **How we found the file that was used to hack RSA.** [*S. l.*], 26 ago. 2011. Disponível em: https://archive.f-secure.com/weblog/archives/00002226. Acesso em: 27 nov. 2019.

MOOR, James. Ethics of privacy protection. **Library Trends**, Maryland, v. 39, n. 1-2, p. 69-82, 1990.

NOZAKI, William. **Guerras híbridas**: militarização da teoria do caos. São Paulo, 23 ago. 2019. Disponível em: https://fpabramo.org.br/2019/08/23/guerras-hibridas-militarizacao-da-teoria-do-caos/. Acesso em: 15 dez. 2019.

NYE JÚNIOR, Joseph S.. **O futuro do poder**. São Paulo: Benvirá, 2012.

OLINDA, Alessandra; SACCARDO, Carol; SOUZA, Ramon; SANTOS, Thauan. **Caso C&A**: o que muda com a nova Lei Geral de Proteção de Dados?. São Paulo, 3 set. 2018. Blog: https://www.flipside.com.br. Disponível em: https://www.flipside.com.br/blog/2018/9/2/caso-cea-o-que-muda-com-a-lgpd. Acesso em: 26 out. 2019.

O QUE sabemos do escândalo do Facebook e por que você deve se preocupar. UOL, São Paulo, 21 mar. 2018. Disponível em: https://www.uol.com.br/tilt/listas/o-que-sabemos-do-escandalo-do-facebook-e-por-que-voce-deve-se-preocupar.htm. Acesso em: 27 out. 2019.

PEIXOTO, Mário C. P. **Engenharia social e segurança da informação na gestão corporativa**. Rio de Janeiro: Brasport, 2006.

PEIXOTO, Mário C. P. **Engenharia Social versus Security Officer**. [*S. l.*], 2014. Disponível em: https://webinsider.com.br/engenharia-social-versus-security-officer/. Acesso em: 15 ago. 2018.

PIMENTA, Francisco J. P.. **Cadernos Semióticos**: as bases tecnológicas do novo jornalismo realista. 1993. Tese (Doutorado em Comunicação e Semiótica) – Pontifícia Universidade Católica de São Paulo, São Paulo, 1993.

PINDJAK, Peter. **Deterring hybrid warfare a chance for nato and the EU to work together?**. Bruxelas, 18 nov. 2014. Disponível em: https://www.nato.int/docu/review/articles/2014/11/18/deterring-hybrid-warfare-a-chance-for-nato-and-the-eu-to-work-together/index.html. Acesso em: 27 dez. 2019.

PINHEIRO, Patricia. Segurança da Informação na Era Digital. **GV Executivo**, São Paulo, v. 11, n. 2, p. 55-57, jul./dez. 2012. Disponível em: http://bibliotecadigital.fgv.br/ojs/index.php/gvexecutivo/article/view/22460/21229. Acesso em: 02 nov. 2019

PORTES, Alejandro. Capital Social: origens e aplicações na Sociologia contemporânea. **Sociologia, problemas e práticas**, Lisboa, n. 33, p. 133-158, set. 2000.

PORTUGAL, Silvia. Contributos para uma discussão do conceito de rede na teoria sociológica. **Oficina do CES**, Coimbra, n. 271, mar. 2007.

PROOF. **Ataques de Engenharia Social:** tudo que você precisa saber!. Rio de Janeiro, 2019. Disponível em: https://www.proof.com.br/blog/ataques-de-engenharia-social. Acesso em: 09 nov. 2019.

PROOF. **Tudo que você precisa saber sobre spear phishing**. Rio de Janeiro, 2019. Disponível em: https://www.proof.com.br/blog/sobre-spear-phishing. Acesso em: 09 nov. 2019.

QIN, Tiantian; BURGOON, Judee K.. An Investigation of Heuristics of Human Judgment in Detecting Deception and Potential Implications in Countering Social Engineering. **Intelligence and Security Informatics**, New Brunswick, maio 2007.

RAFAEL, Gustavo C.; **Engenharia Social:** as técnicas de ataques mais utilizadas. [*S. l.: s. n.*], 24 out. 2013. Disponível em: http://www.profissionaisti.com.br/2013/10/engenharia-social-as-tecnicas-de-ataques-mais-utilizadas/. Acesso em: 04 nov. 2017.

RICHARDSON, R. J. **Pesquisa social:** métodos e técnicas. 3. ed. São Paulo: Atlas, 1999.

ROMANI, Bruno. **'Hack do século', caso Sony chama atenção para segurança de dados**. Folha de São Paulo, São Paulo, 11 dez. 2014. Disponível em: http://temas.folha.uol.com.br/futuro-digital/seguranca-e-o-mundo-digital/hack-do-seculo-caso-sony-chama-atencao-para-seguranca-de-dados.shtml. Acesso em: 09 nov. 2019.

ROSA, Adriano Carlos; SILVA, Bruno Donizete da; SILVA, Pedro Lemes da. Análise de redes sociais aplicada à engenharia Social. In: SIMPÓSIO INTERNACIONAL DE GESTÃO DE PROJETOS, INOVAÇÃO E SUSTENTABILIDADE, 1., 2012, São Paulo. **Anais eletrônicos** […]. São Paulo: Universidade Nove de Julho, 2012. Disponível em: https://repositorio.uninove.br/xmlui/handle/123456789/163. Acesso em: 02 dez. 2015.

SALAMON, Mauricio. **Evolução e poder das redes socais**. São Paulo, 28 set. 2010. Disponível em: http://www.infoq.com/br/articles/evolucao-poder-redes-sociais. Acesso em: 28 nov. 2019.

SANGER, David E.; FACKLER, Martin. **N.S.A. breached North Korean networks before Sony attack, officials say.** Nova York, 18 jan. 2015. Disponível em**:** https://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html?_r=0. Acesso em: 28 nov. 2019.

SANTOS, Abimael. **Lei Carolina Dieckmann:** Lei nº. 12.737/12, art. 154-a do Código Penal. [*S. l.*], 2013. Disponível em: https://abimaelborges.jusbrasil.com.br/artigos/111823710/lei-carolina-dieckmann-lei-n-12737-12-art-154-a-do-codigo-penal. Acesso em: 04 nov. 2019.

STAIR, M.; REYNOLDS, G. **Princípios de Sistemas de Informação:** uma abordagem de informação gerencial. São Paulo: LTC, 2002.

STARR, Stuart H. Toward a preliminary theory of cyberpower *In:* KRAMER, Franklin; STARR, Stuart; WENTZ, Larry. **Cyberpower and National Security**. Dulles: Potomac Books Inc, 2009. Disponível em: http://ctnsp.dodlive.mil/2009/04/01/cyberpower-and-national-security. Acesso em: 15 ago. 2018.

STASSUN, Cristian C. S.; ASSMANN, Selvino J. Hipermobilidade estética e dispositivos de controle de circulação: o desejo de ser notado e encontrado na internet**. Cadernos de Pesquisa Interdisciplinar em Ciências Humanas**, Florianópolis, v. 13, n. 102, p. 153-177, ago. 2012. Disponível em: https://periodicos.ufsc.br/index.php/cadernosdepesquisa/article/view/24238. Acesso em: 15 ago. 2018.

STASSUN, Cristian C. S., **Sociedade do Espetáculo:** Facebook Gadget como dispositivo de governo das informações, das circulações e do desejo. Florianópolis, 26 out. 2016. Disponível em: https://consultapsicologo.com.br/2016/10/26/sociedade-do-espelhaculo-facebook-gadget-como-dispositivo-de-governo-das-informacoes-das-circulacoes-e-do-desejo/. Acesso em: 15 ago. 2018.

STERN, Aaron. **Cuidado com as redes sociais:** Facebook é o maior portal de phishing. São Paulo, 23 jun. 2014. Blog: https://www.kaspersky.com.br. Disponível

em: https://www.kaspersky.com.br/blog/cuidado-com-as-redes-sociais-facebook-e-o-maior-portal-de-phising/3301/. Acesso em: 25 jul. 2018.

SILVA, Edna L.; MENEZES, Estera Muszkat. **Metodologia da pesquisa e elaboração de dissertação**. 4. ed. rev. atual. Florianópolis: UFSC, 2005. 138 p. Disponível em: http://tccbiblio.paginas.ufsc.br/files/2010/09/024_Metodologia_de_pesquisa_e_elaboracao_de_teses_e_dissertacoes1.pdf. Acesso em: 05 nov. 2011.

SILVA, Francisco J. A. F. C.. **Classificação taxonômica dos ataques de Engenharia Social**: caracterização da problemática da segurança de informação em Portugal relativamente à Engenharia Social. Tese (Mestrado em Segurança dos Sistemas de Informação) – Faculdade de Engenharia, Universidade Católica Portuguesa, Lisboa, 2013. Disponível em: https://repositorio.ucp.pt/handle/10400.14/15690. Acesso em: 15 jul. 2017

SILVA, Narjara Bárbara Xavier; ARAUJO, Wagner Junqueira de; AZEVEDO, Patrícia Morais de. Engenharia social nas redes sociais online: um estudo de caso sobre a exposição de informações pessoais e a necessidade de estratégias de segurança da informação. **Revista Ibero-americana de Ciência da Informação**, Brasília, DF, v. 6, n. 2, p. 37-55, 31 dez. 1969. Biblioteca Central da UNB. Disponível em: https://periodicos.unb.br/index.php/RICI/article/view/1782/1573. Acesso em: 15 ago. 2018.

SILVA, Vergilio; LUCIANO, Edimara; WIEDENHÖFT, Guilherme. Ameaças Potenciais à privacidade das Organizações causadas pelo comportamento inseguro de usuários: uma análise segundo o fair information principles. *In*: SIMPÓSIO INTERNACIONAL DE GESTÃO DE PROJETOS, INOVAÇÃO E SUSTENTABILIDADE, 2 e 3., 2014, São Paulo. **Anais** […]. São Paulo: Universidade Nove de Julho, 2014

SILVA, Vergilio Ricardo Britto da Silva. **Preocupação com a privacidade na internet:** uma pesquisa exploratória no cenário brasileiro. Tese (Mestrado em Administração e Negócios) – Faculdade de Administração, Contabilidade e Economia, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2015. Disponível em: http://tede2.pucrs.br/tede2/bitstream/tede/6018/2/468737%20-%20Texto%20Completo.pdf. Acesso em: 04 nov. 2019.

SILVEIRA, Neil; SOUSA, Miriam; MELO, Antonia. **Crimes cibernéticos e invasão de privacidade à luz da lei Carolina Dieckmann**. [*S. l.*], out. 2017. Disponível em: https://jus.com.br/artigos/61325/crimes-ciberneticos-e-invasao-de-privacidade-a-luz-da-lei-carolina-dieckmann. Acesso em: 04 nov. 2019.

STANDISH, Reid. **Inside a European center to combat Russia's hybrid warfare**. Washington, 18 jan. 2018. Disponível em: https://foreignpolicy.com/2018/01/18/inside-a-european-center-to-combat-russias-hybrid-warfare. Acesso em: 25 nov. 2019.

STRAUMSHEIM, Jan Henrik S. **Protecting organizations from social engineering threats in.** [*S. l.*], 2010. Blog: http://www.janhenrik.com. Disponível em: http://www.janhenrik.com/blog/2010/08/protecting-organizations-from-social-engineering-threats. Acesso em: 04 nov. 2019.

STERLING, Bruce. **The hacker crackdown:** law and disorder on the electronicfrontier. New York: Bantam Books, 1992.

TARVARES, Joelmir. **Empresa que ajudou Trump roubou dados de 50 milhões de usuários do Facebook.** São Paulo, 17 mar. 2018. Disponível: https://www1.folha.uol.com.br/mundo/2018/03/empresa-que-ajudou-trump-roubou-dados-de-50-milhoes-de-usuarios-do-facebook.shtml. Acesso em: 11 nov. 2018

TOMAÉL, Maria Inês. Redes Sociais, conhecimento e inovação localizada. **Informação & Informação**, Londrina, v. 12, n. esp., 2007. Disponível: https://www.brapci.inf.br/_repositorio/2010/07/pdf_369affa90f_0011339.pdf. Acesso em: 10 jul. 2019

UPTON, David M.; CREESE, Sadie. **O perigo vem de dentro:** roubo de dados. São Paulo, 2019. Disponível em: https://www.perallis.com/news/o-perigo-vem-de-dentro-roubo-de-dados. Acesso em: 09 nov. 2019.

VALLS, C.. A revolução do Facebook Places: o geolocalizador da maior rede do mundo. [*S. l.*], 2010. Blog: https://claudiavalls.wordpress.com. Disponível em: https://claudiavalls.wordpress.com/2010/11/07/a-revolucao-do-facebook-places-o-geolocalizador-da-maior-rede-do-mundo. Acesso em: 07 nov. 2019.

VEIGA, Ricardo Queiroz da. A defesa cibernética (Def Ciber) na visão da Força Aérea Brasileira (FAB). **Coleção Meira Mattos**: Revista das Ciências Militares, Rio de Janeiro, 2012.

VENTRE, Daniel. **Cyberwar and information warfare**. Londres: Iste, 2011.

VERMELHO, Sônia Cristina; VELHO, Ana Paula Machado; BERTONCELLO, Valdecir. Sobre o conceito de redes sociais e seus pesquisadores. **Educação e Pesquisa**, São Paulo, v. 41, n. 4, p. 863-881, 10 abr. 2015.

WARDEN III, John A.. The enemy as a system. **Airpower Journal**, Alabama, v. 9, n. 1, p. 41-55, 1995. Disponível em: http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm. Acesso em: 20 jun. 2014.

WE ARE SOCIAL. **Digital in 2018**: world's internet users pass the 4 billion mark. New York, 2018. Disponível em: https://wearesocial.com/blog/2018/01/global-digital-report-2018. Acesso em: 23 out. 2019.

WEBER, Max. **Ciência e Política:** duas vocações. 3. ed. São Paulo: Martin Claret, 2001.

WIENER, Norbert. **Cibernética e sociedade:** o uso humano de seres humanos. São Paulo: Cultrix, 1984.

WIENER, Norbert. **Cybernetics:** or the control and communication in the animal and the machine. New York: MIT Press, 1948.

YIN, R. K. **Estudo de caso:** planejamento e métodos. Tradução Ana Thorell; revisão Técnica: Cláudio Damacena. 4. ed. Porto Alegre: Bookman, 2010.

ZETTER, Kim. **Researchers uncover RSA Phishing Attack, hiding in plain sight.** New York, 2011. Disponível em: https://www.wired.com/2011/08/how-rsa-got-hacked/. Acesso em: 27 nov. 2019.

APÊNDICES

APÊNDICE A - PRINCIPAIS LEGISLAÇÕES DA ADMINISTRAÇÃO PÚBLICA FEDERAL POR ANO

Em 2000:

▪ Decreto nº 3.505/2000, instituindo a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal (APF). Esse Decreto criou o Comitê Gestor da Segurança da Informação (CGSI).

Em 2001:

▪ MP nº 2.200 de 28/06/2001, instituindo a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), incluindo o GSI/PR como membro do Comitê Gestor da ICP-Brasil.

▪ Decreto nº 3.872 de 18/072001, que dispõe sobre o Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira (CG ICP-Brasil). Revogado pelo Decreto nº 6.605/2008.

▪ Decreto nº 3.996 de 31/102001, que dispõe sobre a prestação de serviços de certificação digital no âmbito da APF.

Em 2002:

▪ Decreto nº 4.553 de 27/12/2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesses da segurança da sociedade e do Estado, no âmbito da APF. Revogado pelo Decreto nº 7.845/2012.

Em 2003:

▪ Lei nº 10.683, de 28/05/2003, em seu art. 6º, estabelece ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR) a competência de

coordenar as atividades de inteligência federal e de segurança da informação do governo, entre outras.

▪ Decreto nº 4.801, de 06/08/2003, cria a Câmara de Relações Exteriores e Defesa Nacional (CREDEN) do Conselho de Governo.

▪ Decreto nº 4.829, de 03/09/2003, que dispõe sobre a criação do Comitê Gestor da Internet no Brasil - CGI.br, sobre o modelo de governança da Internet no Brasil, e estabelece a coordenação do mesmo a ser exercida pelo, então, MCT, contando com governança multissetorial.

Em 2004:

▪ Criação da equipe de tratamento de incidentes em redes computacionais do governo, CTIR Gov, no GSI/PR;

▪ Lei nº 10.973, de 02/12/2004, publicada como instrumento legal de fomento à inovação.

Em 2005:

▪ "I Conferência de Segurança para o Governo (SECGOV-2005)", sob a coordenação do GSI/PR, para tratar de temas atinentes à segurança da informação e comunicações.

▪ 13 de outubro o Brasil assina com Portugal, na Cidade do Porto, Acordo de Troca e Proteção Mútua de Informações Classificadas.

▪ Decreto nº 5.563, de 11/12/2005, regulamenta a Lei de Inovação (Lei nº 10.973/2004).

Em 2006:

▪ Decreto nº 5.772, de 08/05/2006, dispõe sobre a reestruturação do GSI/PR, com inserção de novas atribuições relacionadas à Segurança da Informação no rol de competências da secretaria executiva. Fica, então, criado o Departamento de Segurança da Informação e Comunicações (DSIC), com a missão de planejar e coordenar as atividades de Segurança da Informação e Comunicações (SIC) na APF.

▪ Ação orçamentária 6232 (Capacitação de RH na Área de Segurança da Informação) destinada à formação e ao aprimoramento de recursos humanos com vistas à definição e à implementação de mecanismos capazes de fixar e fortalecer o desenvolvimento e a execução da Segurança da Informação.

▪ Parceria do GSI/PR, como órgão coordenador das atividades de Segurança da Informação no Governo Federal, com vários órgãos, entre eles, MTur, CGU, AGU, SRF, SRP, INSS, EMBRAPA, SERPRO, Radiobrás, ABIN, BCB, BB, CEF, Petrobrás, RNP, com a finalidade de organizarem atividades em conjunto que possibilitassem a disseminação da cultura da Segurança da Informação.

Em 2007:

▪ 17/09 o Brasil assina com a Espanha, em Madri, Acordo de Troca e Proteção Mútua de Informações Classificadas.

Em 2008:

▪ IN GSI nº 01, de 13/06/2008, elaborada de forma colaborativa com os membros do Comitê Gestor de Segurança da Informação (CGSI), disciplinando a Gestão de Segurança da Informação e Comunicações na APF.

▪ Primeiras Normas Complementares (NC) da IN 01 GSI/PR, a NC nº 01 sobre atividade de normatização e NC a nº 02 sobre metodologia de gestão de SIC.

▪ Acórdão 1.603/2008-TCU-Plenário de 13 de agosto, divulga o resultado do levantamento da governança de TI, realizado no processo do TCU nº 008.380/2007-1, e recomenda ao GSI/PR que oriente os órgãos e entidades da APF sobre a importância do gerenciamento da segurança da informação, promovendo, inclusive mediante orientação normativa, ações que objetive estabelecer e/ou aperfeiçoar a gestão da continuidade do negócio, a gestão de mudanças, a gestão de capacidade, a classificação da informação, a gerência de incidentes, a análise de riscos de TI, a área específica para gerenciamento da segurança da informação, a política de segurança da informação e os procedimentos de controle de acesso.

▪ Instrução Normativa nº 04 da Secretaria de Logística e Tecnologia da Informação – SLTI, do Ministério do Planejamento, Orçamento e Gestão – MP, dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática – SISP, do Poder Executivo Federal.

▪ Em 13 de agosto, o Brasil assina com a Rússia, em Moscou, o Acordo de Troca e Proteção Mútua de Informações Classificadas.
▪ Foi publicado o Decreto nº 6.605 de 14 de julho de 2008, dispondo sobre o Comitê Gestor da ICP-Brasil, revogando o Decreto nº 3.872/2001 e fazendo nova redação.

▪ Portaria GSI/PR nº 31, de 06 de outubro de 2008, institui a Rede Nacional de Excelência em Segurança da Informação e Criptografia – RENASIC.

Em 2009:
▪ Foram publicadas mais quatro Normas Complementares à IN 01 GSI/PR:
NC 03/IN01/DSIC/GSI/PR - Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da APF;
NC 04/IN01/DSIC/GSI/PR - Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal;
NC 05/IN01/DSIC/GSI/PR - Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal; e
NC 06/IN01/DSIC/GSI/PR - Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta.

▪ Foi realizado o “III Congresso de Segurança da Informação e Comunicações (SICGov-2009)”, na Universidade Corporativa dos Correios, Brasília – DF, com foco em segurança cibernética.

▪ O DSIC/SE/GSI/PR apoiou o evento da Organização dos Estados Americanos (OEA), realizado nos dias 16 a 20 de novembro de 2009, no Rio de Janeiro, que contou com a presença de 136 participantes estrangeiros, representantes dos países do continente americano, com a finalidade de estabelecer proposta de “Estratégia Nacional de Segurança Cibernética do Hemisfério”, para os países da região.

▪ Decreto nº 7.009, de 12 de novembro de 2009, inclui o tema segurança cibernética nos objetivos da Câmara de Relações Exteriores e Defesa Nacional – CREDEN do

Conselho de Governo, e realça o acompanhamento e estudo de questões e fatos relevantes com potencial de risco à estabilidade institucional, para prover informações ao Presidente da República. A composição foi então atualizada contemplando os seguintes Ministérios: GSI/PR (que a preside); Casa Civil/PR; Justiça; Defesa; Relações Exteriores; Planejamento, Orçamento e Gestão; Meio Ambiente; Ciência e Tecnologia; Fazenda e SAE/PR, sendo convidados a participar das reuniões, em caráter permanente, os Comandantes da Marinha, do Exército, da Aeronáutica e o Chefe do Estado-Maior Conjunto das Forças Armadas (composição atualizada em 2013).

▪ Portaria CREDEN nº 45, de 8 de setembro de 2009, institui o Grupo Técnico de Segurança Cibernética, com o objetivo de propor diretrizes e estratégias para a Segurança Cibernética, no âmbito da Administração Pública Federal. Órgãos integrantes: GSI/PR; MRE; MJ; MD; MD/EB; MD/MB; e MD/COMAER.

Em 2010:

▪ Foi publicado o Guia de Referência para a Segurança das Infraestruturas Críticas da Informação. v.01. Gabinete de Segurança Institucional da Presidência da República. 2010.

▪ Foi publicado o Acórdão 2.308/2010 -TCU-Plenário de 8 de setembro de 2010 divulgando o resultado do levantamento da governança de TI realizado no processo do TCU nº 000.390/2010-0. O referido Acórdão descreve que não houve melhora nos processos de segurança da informação na APF, porém, ressalva que a piora em parte dos indicadores pode não refletir deterioração da situação segurança da informação da APF, mas sim uma possível melhora na compreensão dos conceitos questionados, e por fim, reconhece o trabalho do GSI/PR a respeito da Segurança da Informação com a publicação da IN 01 GSI/PR e respectivas Normas Complementares.

▪ Foram publicadas mais 3 Normas Complementares à IN 01 GSI/PR:

NC 07/IN01/DSIC/GSI/PR - Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;

NC 08/IN01/DSIC/GSI/PR - Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal; e
NC 09/IN01/DSIC/GSI/PR - Estabelece orientações específicas para o uso de recursos criptográficos em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal (APF), direta e indireta.
▪ Em 22 de novembro, o Brasil assina com a Itália, em Roma, o Acordo de Troca e Proteção Mútua de Informações Classificadas.
▪ Em 24 de novembro, o Brasil assina com Israel, em Tel Aviv, o Acordo de Troca e Proteção Mútua de Informações Classificadas.

Em 2011:
▪ Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) traz a primazia da transparência das informações sob a custódia do Estado.

▪ Decreto nº 7.579, de 11 de outubro de 2011, dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação - SISP, do Poder Executivo federal, e estabelece que o Órgão Central do SISP, Ministério de Planejamento, Orçamento e Gestão, elaborará, em conjunto com os Órgãos Setoriais e Seccionais do SISP, a “Estratégia Geral de Tecnologia da Informação – EGTI” para a Administração direta, autárquica e fundacional do Poder Executivo Federal, revisada e publicada anualmente, para servir de subsídio à elaboração dos PDTI pelos órgãos e entidades integrantes do SISP.

▪ Foi publicado o Acórdão 1.145/2011-TCU-Plenário de 4 de maio de 2011, realizado no processo TCU nº 028.772/2010-5, especificando que o GSI/PR, dentre outros, é um Órgão Governante Superior (OGS) com a responsabilidade de normatizar aspectos da Segurança da Informação e Comunicações, em seus respectivos segmentos da APF.

▪ Publicado pela SAE/PR o e-book: Desafios estratégicos para segurança e defesa cibernética / organizadores Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes, Whitney Lacerda de Freitas. – Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011.

▪ Transferência da Rede Nacional de Excelência em Segurança da Informação e Criptografia – RENASIC do GSI/PR para o CDCiber/EB/MD.

Em 2012:

▪ Foi publicado o Acórdão 1.233/2012-TCU-Plenário de 23 de maio de 2012 referenciando o resultado do levantamento da governança de TI realizado no processo do TCU nº 011.772/2010-7. O referido Acórdão recomenda ao GSI/PR que:

Articule-se com as Escolas de Governo, notadamente à ENAP, a fim de ampliar a oferta de ações de capacitação em segurança da informação para os entes sob sua jurisdição;

Oriente os órgãos e entidades sob sua jurisdição que a implantação dos controles gerais de segurança da informação positivados nas normas do GSI/PR não é faculdade, mas obrigação da Alta Administração, e sua não implantação sem justificativa é passível da sanção prevista na Lei; e

Reveja a Norma Complementar 4/IN01/DSIC/GSIPR, uma vez que aborda o tema gestão de riscos considerando apenas ativo de informação e não ativo em sentido amplo, como o faz a NBR ISO/IEC 27.002 no item 7.1.1.

▪ Foram publicadas mais sete Normas Complementares à IN 01 GSI/PR:

NC 10/IN01/DSIC/GSI/PR - Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

NC 11/IN01/DSIC/GSI/PR - Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF;

NC 12/IN01/DSIC/GSI/PR - Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;

NC 13/IN01/DSIC/GSI/PR - Estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF);

NC 14/IN01/DSIC/GSIPR - Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;

NC 15/IN01/DSIC/GSI/PR - Estabelece diretrizes de Segurança da Informação e Comunicações para o uso de redes sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta; e

NC 16/IN01/DSIC/GSIPR - Estabelece as Diretrizes para o Desenvolvimento e Obtenção de Software Seguro nos Órgãos e Entidades da Administração Pública Federal, direta e indireta.

▪ Foi publicado o Acórdão 2.585/2012-TCU-Plenário de 26 de setembro de 2012 divulgando o resultado do levantamento da governança de TI realizado no processo do TCU nº 007.887/2012-4.

▪ O Decreto nº 7.724, de 16 de maio de 2012 regulamenta a LAI no âmbito do Poder Executivo Federal, estabelecendo as diretrizes para a transparência ativa e passiva. No mesmo dia, a Lei de Acesso à Informação entra em vigor.

▪ O Decreto nº 7.845, de 14 de novembro de 2012 é publicado encerrando a regulamentação da LAI, estabelecendo o tratamento para as informações com restrição de acesso e dispondo sobre o Núcleo de Segurança e Credenciamento (NSC) no GSI/PR.

▪ Foram publicadas duas leis contra o crime cibernético:

Lei nº 12.737, de 30 de novembro de 2012, a qual dispõe sobre a tipificação criminal de delitos informáticos.

Lei nº 12.735, de 30 de novembro de 2012, a qual tipifica as condutas realizadas mediante uso de sistema eletrônico, digital ou semelhante, que sejam praticadas contra sistemas informatizados e similares.

Em 2013:

▪ Foram publicadas mais duas Normas Complementares à IN 01 GSI/PR:

NC 17/IN01/DSIC/GSI/PR - Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF).

NC 18/IN01/DSIC/GSI/PR - Estabelece as Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF).

▪ Com a publicação da LAI em 2011 e seus Decretos regulamentadores no âmbito do Poder Executivo Federal, fez-se necessário revisar a NC 09/IN01/DSIC/GSI/PR, principalmente, em relação ao conceito de algoritmo de Estado.

▪ Conforme determinação do Acórdão nº 1.233/2012-TCU-Plenário de 23 de maio de 2012, foi feita a primeira revisão da NC 04/IN01/DSIC/GSI/PR, na qual foi incluído item 2, nas considerações gerais, o seguinte texto:

A Gestão de Riscos de Segurança da Informação e Comunicações, objeto desta Norma Complementar, está limitada ao escopo das ações de Segurança da Informação e Comunicações e tais ações compreendem apenas as medidas de proteção dos ativos de informação, conforme definido nesta Norma.

▪ Portaria SAE/PR nº 124 institui Grupo de Trabalho Interministerial (GTI) com o objetivo de elaborar proposta de Plano Estratégico para promover ou subsidiar o aperfeiçoamento das políticas públicas voltadas à segurança e defesa do espaço cibernético nacional. O art. 3º da citada Portaria nomeia os membros Titulares e Suplentes que representam os seguintes órgãos que integram o GTI: SAE/PR; MD; MRE; MEC; MDIC; MP; MCTI; MC; GSI/PR; CGI.br; ANATEL; SERPRO; DATAPREV; e TELEBRÁS.

▪ IN GSI/PR 02, de 5 de fevereiro de 2013, regulando o Credenciamento de Segurança e o tratamento de informação classificada em grau de sigilo.

▪ IN GSI/PR 03, de 6 de março de 2013, estabelecendo os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado.

▪ NC 01/IN02/DSIC/GSI/PR, de 27 de junho de 2013, inaugura os trabalhos de Credenciamento sob a égide das novas regras para o tratamento das informações classificadas em grau de sigilo.

▪ Decreto nº 8.096, de 04 de setembro de 2013, atualiza a composição da CREDEN, e a Câmara passa a contar com os seguintes Ministérios: GSI/PR (que a preside); Casa Civil/PR; Justiça; Defesa; Relações Exteriores; Planejamento, Orçamento e Gestão; Meio Ambiente; Ciência e Tecnologia; Fazenda; SAE/PR; Integração Nacional; Minas e Energia; e Transportes, sendo convidados a participar das reuniões, em caráter permanente, os Comandantes da Marinha, do Exército, da Aeronáutica e o Chefe do Estado-Maior Conjunto das Forças Armadas.

▪ Editado pelo IPEA o texto para discussão: Cruz Júnior, Samuel César da. Texto para Discussão 1850. A Segurança e Defesa Cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço Virtual. IPEA. Brasília, julho de 2013.

▪ Decreto nº 8.135, de 04 de novembro de 2013, dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional.

▪ Realizada Audiência Pública no Senado Federal em 06 de dezembro de 2013; TEMA: SEGURANÇA CIBERNÉTICA E SOBERANIA NACIONAL.

Em 2014:

▪ A NC 09/IN01/DSIC/GSI/PR recebeu a segunda revisão, destacando-se o novo conceito de algoritmo registrado:

Algoritmo Registrado: função matemática utilizada na cifração e na decifração de informações não classificadas, para uso exclusivo em interesse do serviço de órgãos ou entidades da APF, direta e indireta, cujo código fonte e método de processo sejam passíveis de controle e auditoria.

▪ A NC 07/IN01/DSIC/GSI/PR recebeu a primeira revisão, sendo incorporado o tema “Biometria” como controle de acesso.

▪ Foram publicadas três normas complementares à IN 01 GSI/PR:

NC 19/IN01/DSIC/GSI/PR estabelece Padrões Mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes da Administração Pública Federal (APF), direta e indireta;

NC 20/IN01/DSIC/GSI/PR estabelece as Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta; e

NC 21/IN01/DSIC/GSI/PR estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta. No mesmo ano, essa NC recebeu a primeira revisão.

▪ Foi publicado o Acórdão 3.051/2014-TCU-Plenário de 5 de novembro de 2014, referente ao processo do TCU nº 023.050/2013-6. Esse Acórdão contextualiza as auditorias realizadas em diversos órgãos e entidades da Administração Pública

federal com o objetivo de avaliar a implementação dos controles de TI informados em resposta ao levantamento do perfil de governança de TI de 2012. Pontos de interesses da segurança da informação:

A segurança da informação segue sendo objeto de preocupação. Há baixa conformidade das organizações para com os normativos e com as boas práticas aplicáveis. Na maioria das organizações fiscalizadas na primeira fase, falhas foram observadas:

a) 80% - falhas na gestão de continuidade de negócio;
b) 70% - falhas no controle de acesso;
c) 75% - falhas na gestão de incidentes; e,
d) 85% - falhas na gestão de riscos de segurança da informação.

Principais causas estão ligadas a falhas típicas de governança, como a falta de designação de um responsável pela segurança da informação, fato observado em 40% das organizações.

Houve tendência de mudança de comportamento dos dirigentes públicos sobre a segurança da informação.

A redução dos percentuais observados não se traduz necessariamente em retrocesso, mas pode ser interpretado como amadurecimento dos gestores de TI no sentido de compreender melhor os conceitos relacionados à segurança da informação.

Ainda não há, por exemplo, um planejamento estratégico do Estado brasileiro que reúna e coordene ações dos diversos atores responsáveis por assuntos ligados a essa área.

Recomendações ao GSI/PR: elabore e acompanhe periodicamente planejamento que abranja a estratégia geral de segurança da informação para o setor sob sua jurisdição; e alerte as organizações sob sua jurisdição que a elaboração periódica de planejamento das ações de segurança da informação é obrigação expressa prevista no item 3.1 da Norma Complementar 02/IN01/DSIC/GSI/PR.

▪ Foi publicado o Acórdão 3.117/2014-TCU-Plenário de 12 de novembro de 2014, referente ao processo do TCU nº 003.732/2014-2. Trata-se de relatório de

levantamento realizado com o objetivo de acompanhar a situação da Governança de Tecnologia da Informação na Administração Pública Federal, realizado a cada dois anos pelo TCU.

Pontos de interesses da segurança da informação:

- A segurança da informação tem sido objeto de preocupação em todos os levantamentos anteriores por causa da baixa conformidade das organizações em relação aos normativos e às boas práticas aplicáveis.
- Como referência para elaboração das questões da auditoria, foram utilizadas principalmente a norma técnica ABNT NBR ISO/IEC 27002:2005 e as normas complementares do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (DSIC/GSI/PR).
- Apesar de ser o principal instrumento direcionador da gestão da segurança da informação, preocupa que apenas 66% (15% parcialmente e 51% integralmente) das organizações participantes declarem dispor de uma política de segurança da informação formalmente instituída, como norma de cumprimento obrigatório.

Apesar de ser o principal instrumento direcionador da gestão da segurança da informação, preocupa que apenas 66% das organizações participantes declarem dispor de uma política de segurança da informação formalmente instituída, como norma de cumprimento obrigatório;

O comitê de segurança da informação formalmente instituído, composto por representes das áreas relevantes da organização e responsável por formular e conduzir diretrizes para a segurança da informação corporativa, é encontrado em 62% das organizações, segundo declarado.

Observa-se que apenas 50% das organizações declararam possuir gestor da segurança da informação formalmente designado, responsável pelas ações corporativas de segurança da informação.

Quanto à política que normatiza o acesso às informações e aos recursos e serviços de TI, somente 52% (declararam dispor desse normativo formalmente instituído, com cumprimento obrigatório).

Quanto à política de cópias de segurança (backup), que são necessárias para garantir a disponibilidade das informações em casos de falhas de sistemas ou pessoas, somente 54% declararam dispor desse normativo formalmente instituído, com cumprimento obrigatório.

▪ Lei nº 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet, estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.
▪ Em 14 de abril o Brasil assina com a Suécia, em Estocolmo, o Acordo de Troca e Proteção Mútua de Informações Classificadas.
▪ Durante todo o ano, na qualidade de Autoridade Nacional de Segurança (ANS), exercida GSI/PR, manteve estreita relação com o Ministério das Relações Exteriores na articulação, tanto de ajustes nos Acordos de Troca e Proteção Mútua de Informações Classificadas assinados com seis países, visando alinhamento à LAI, quanto de novos acordos demandados por outros 14 países.
▪ Portaria Interministerial MP MD MC nº 141, de 02 de maio de 2014, regulamenta o Decreto nº 8.135/2013, dispõe para toda a administração pública federal o dever de realizar as suas comunicações, armazenamentos e recuperações de dados através de redes de telecomunicações e serviços de tecnologia de informação fornecidos por órgãos ou entidades da própria administração pública federal (SERPRO, TELEBRÁS, DATAPREV, entre outros), com exceção de serviço móvel pessoal e serviço telefônico fixo comutado, garantindo-se a segurança da informação e comunicações conforme normativos do GSI/PR. O SERPRO inicia implantação do serviço de mensageria Expresso V3 na APF.
▪ Relatório Final da CPI da Espionagem, elaborado pela Comissão Parlamentar de Inquérito destinada a investigar a denúncia de existência de um sistema de espionagem, estruturado pelo governo dos Estados Unidos, com o objetivo de monitorar e-mails, ligações telefônicas, dados digitais, além de outras formas de captar informações privilegiadas ou protegidas pela Constituição Federal aponta para diversos aspectos essenciais e recomendações à segurança da informação e segurança cibernética, entre eles:

> Elaboração de uma Estratégia Nacional de Segurança Cibernética, realçando que houve unanimidade entre os convidados à CPI, de que mais urgente do que a Estratégia, é que sejam delineadas as principais medidas de segurança

cibernética para o Estado brasileiro, englobando ações coordenadas entre os setores público e privado.

Criação de uma agência para a segurança cibernética no âmbito da Administração Pública Federal, favorecendo visão de conjunto no tema e ações mais eficazes e efetivas. Alternativamente à criação de um novo órgão, poderia ser alterada a estrutura de órgão já existente, modificando suas atribuições, para lhe conferir capacidade de atuar, com independência, em sua totalidade e em estreita coordenação com os demais órgãos atuantes nos mais diversos temas que englobam a segurança cibernética.

▪ Portaria Interministerial n° 1.424, de 31 de dezembro de 2014, dos Ministérios da Defesa e da Ciência, Tecnologia e Inovação. Institui o Programa de Pesquisa, Desenvolvimento e Inovação em Defesa Cibernética.

▪ Regulamentação do Marco Civil da Internet, processo de regulamentação da Lei nº 12.965/2014, em andamento por meio de consultas públicas pelo Comitê Gestor da Internet e pelo Ministério da Justiça.

▪ Projeto de Lei de Dados Pessoais. Em consulta pública disponibilizada pelo Ministério da Justiça

▪ Alteração da Instrução Normativa SLTI nº 04, em 12 de janeiro de 2015, estabelecendo a “Estratégia Geral de Tecnologia da Informação e Comunicações (EGTIC) – 2014/2015”, a qual compreende um instrumento de gestão do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), traçando a direção da Tecnologia da Informação e Comunicações (TIC), e definindo o plano estratégico que visa promover a melhoria contínua da gestão e governança de TIC no governo.

▪ Decreto nº 8.414, de 26 de fevereiro de 2015, institui o Programa “Bem Mais Simples Brasil” com a finalidade de simplificar e agilizar a prestação dos serviços públicos e de melhorar o ambiente de negócios e a eficiência da gestão pública. Objetivos: (i) simplificar e agilizar o acesso do cidadão, das empresas e das entidades sem fins lucrativos aos serviços e informações públicos; (ii) promover a prestação de informações e serviços públicos por meio eletrônico; (iii) reduzir formalidades e exigências na prestação de serviços públicos; (iv) promover a integração dos sistemas de informação pelos órgãos públicos para oferta de serviços públicos; (v) celebrar o “Pacto Bem Mais Simples Brasil” com os demais

Poderes da União e com os Estados, o Distrito Federal e os Municípios; e (vi) modernizar a gestão interna da administração pública.

▪ Portaria Nº 7 - CDN, de 17 de março de 2015: Designa membros para compor o Comitê Gestor de Segurança da Informação (CGSI).

▪ Portaria n° 13 - CDN, de 24 de abril de 2015: Designa membros para compor o Grupo de Trabalho de Especialistas em Comunicação Segura, sob a Coordenação do Departamento de Segurança da Informação e Comunicações - DSIC deste Gabinete. Este Grupo terá por objetivo a elaboração da proposta de um normativo com vistas a promover a disponibilidade, integridade, confidencialidade e autenticidade das informações, nas comunicações de governo, em consonância com as Instruções Normativas 01 e 03 do GSI/PR e Normas Complementares, em especial as de nº 09/IN01/DSIC/GSI/PR e nº 12/IN01/DSIC/GSI/PR.

▪ Portaria Nº 14 - CDN, de 11 de maio de 2015: Homologa a "Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal - 2015/2018, versão 1.0", desdobramento da Instrução Normativa GSI/PR nº 01/2008.

▪ Portaria Nº 20 - CDN, de 25 de junho de 2015: Institui no âmbito do Comitê Gestor de Segurança da Informação - CGSI, 2 (dois) Grupos de Trabalho para estudo, análise e proposição sobre os temas abaixo relacionados:

I - definição de metodologia e mecanismo de autodiagnóstico de Segurança de Informação e Comunicações (SIC) e de Segurança Cibernética (SegCiber) da Administração Pública Federal (APF); e

II - elaboração do Guia de Boas Práticas e Planejamento de SIC e SegCiber para os órgãos e entidades da APF.

APÊNDICE B – LISTA DOS ÓRGÃOS E ATORES QUE, DE ALGUMA FORMA, SE RELACIONAM COM AS VERTENTES DE SEGURANÇA E DEFESA CIBERNÉTICA NO BRASIL.

CONSELHO DE DEFESA NACIONAL (CDN)

O Conselho de Defesa Nacional foi instituído pelo Decreto nº 17.999 de 29 de novembro de 1927 e organizado pelo Decreto nº. 23.873 de 15 de fevereiro de 1934.

A nova Constituição, ratificada em 1988, renomeou o Conselho de Segurança Nacional para Conselho de Defesa Nacional. Atualmente a organização e o funcionamento do Conselho de Defesa Nacional são regulados pela Lei n° 8.183, de 11 de abril de 1991, alterada pela Medida Provisória nº 2216-37, de 2001.

O CDN é um órgão de consulta do Presidente da República nos assuntos relacionados à soberania nacional e à defesa do Estado democrático. Sua composição abrange o Vice-Presidente da República, o Presidente da Câmara dos Deputados, o Presidente do Senado Federal, o Ministro da Justiça, o Ministro de Estado da Defesa, o Ministro das Relações Exteriores, o Ministro do Planejamento e os Comandantes da Marinha, do Exército e da Aeronáutica. Cabe ao Gabinete de Segurança Institucional da Presidência da República executar as atividades permanentes necessárias ao exercício da competência do Conselho de Defesa Nacional.

Suas competências constitucionais são:

I - opinar nas hipóteses de declaração de guerra e de celebração da paz, nos termos da Constituição;

II - opinar sobre a decretação do estado de defesa, do estado de sítio e da intervenção federal;

III - propor os critérios e condições de utilização de áreas indispensáveis à segurança do território nacional e opinar sobre seu efetivo uso, especialmente na faixa de fronteira e nas relacionadas com a preservação e a exploração dos recursos naturais de qualquer tipo;

IV - estudar, propor e acompanhar o desenvolvimento de iniciativas necessárias a garantir a independência nacional e a defesa do Estado democrático.

MANDARINO (2010, p.110) afirma que, dada a sua importância estratégica, o CDN deve manter-se como palco para as decisões estratégicas relativas às ações de segurança e de defesa cibernética.

CÂMARA DE RELAÇÕES EXTERIORES E DEFESA NACIONAL (CREDEN)

A Câmara de Relações Exteriores e Defesa Nacional (CREDEN) do Conselho de Governo foi criada pelo Decreto nº 4.801, de 6 de agosto de 2003 48. É presidida pelo Ministro-Chefe do GSI/PR e tem por finalidade formular políticas, estabelecer diretrizes, bem como aprovar e acompanhar programas e ações a serem implantados em matérias relacionadas à: cooperação internacional em assuntos de segurança e defesa; integração fronteiriça; populações indígenas; direitos humanos; operações de paz; narcotráfico e outros delitos de configuração internacional; imigração; atividade de inteligência; segurança para as infraestruturas críticas; segurança da informação; e segurança cibernética. Cabe, ainda, à CREDEN o permanente acompanhamento e estudo de questões e fatos relevantes, com potencial de risco à estabilidade institucional, para prover informações ao Presidente da República. Como se trata de um órgão de governo, suas atribuições podem ser alteradas e até mesmo a sua existência não está assegurada no próximo governo.

A CREDEN é integrada pelos seguintes Ministros de Estado: Chefe do Gabinete de Segurança Institucional da Presidência da República, que a preside; Chefe da Casa Civil da Presidência da República; Justiça; Defesa; Relações Exteriores; Planejamento, Orçamento e Gestão; Meio Ambiente; e da Ciência e Tecnologia. Os comandantes das Forças Armadas são convidados para participar das reuniões em caráter permanente.

No âmbito do CREDEN, sob a coordenação do GSI/PR, foi criado também o Grupo Técnico de Segurança Cibernética, através da Portaria GSI/PR n° 45, de 8 de setembro de 2009.

O Grupo Técnico é integrado por dois representantes, titular e suplente, de cada um dos seguintes órgãos: Gabinete de Segurança Institucional da Presidência da República, a quem cabe a coordenação dos trabalhos por intermédio do

Departamento de Segurança da Informação e das Comunicações; Ministério da Justiça; Ministério da Defesa; Ministério das Relações Exteriores; Comando da Marinha; Comando do Exército; Comando da Aeronáutica.

CASA CIVIL DA PRESIDÊNCIA DA REPÚBLICA

A Casa Civil o órgão diretamente ligado ao chefe do Poder executivo do país, criado pelo Decreto-Lei n° 920 de 1 de dezembro de 1938.

A Lei nº 10.683, de 28 de maio de 2003, alterada pela Lei nº 10.869, de 13 de maio de 2004, somado ao Decreto nº 5.135, de 7 de julho de 2004 e novamente alterada pela Lei nº 12.462, de 4 de agosto de 2011 definem as competências, a organização e a estrutura regimental da Casa Civil da Presidência da República. Dentre as suas competências que estão diretamente relacionadas com o assunto da segurança cibernética e segurança da informação estão:

I - assistir direta e imediatamente ao Presidente da República no desempenho de suas atribuições, especialmente:

a) na coordenação e na integração das ações do Governo.

A estrutura da Casa Civil conta com três órgãos importantes na elaboração das normas e regulamentos da segurança da informação e comunicações e segurança cibernética: o Instituto Nacional da Tecnologia da Informação (ITI), a Diretoria de Tecnologia da Informação (DIRTI) e a Diretoria de Telecomunicações (DITEL).

O ITI tem a sua Estrutura Regimental definida pelo decreto nº 4.689, de 7 de maio de 2003, sendo uma autarquia federal vinculada à Casa Civil da Presidência da República, com a finalidade de ser a Autoridade Certificadora Raiz - AC Raiz, da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil. A ele compete estimular e articular projetos de pesquisa científica e de desenvolvimento tecnológico voltados à ampliação da cidadania digital, por meio da utilização de certificação e assinatura digitais ou de outras tecnologias que garantam a privacidade, autenticidade e integridade de informações eletrônicas. Nesse sentido, o ITI visa à popularização da certificação e a inclusão digitais, atuando sobre temas como sistemas criptográficos, software e hardware compatíveis com padrões abertos e universais, convergência digital de mídias, entre outras.

A DIRTI é responsável pelo desenvolvimento, manutenção e acompanhamento de todos os sistemas informatizados utilizados na Presidência da República.

A DITEL é responsável pela instalação, manutenção e acompanhamento de todos os sistemas de comunicações empregados na Presidência da República.

GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA – GSI/PR

A Lei nº 10.683, de 28 de maio de 2003, estabelece no seu artigo 6º as competências do GSI/PR, dentre as quais destacam-se:

> [...]
>
> II - prevenir a ocorrência e articular o gerenciamento de crises, em caso de grave e iminente ameaça à estabilidade institucional;
>
> III - realizar o assessoramento pessoal em assuntos militares e de segurança; e
>
> IV - coordenar as atividades de inteligência federal e de segurança da informação;

O Decreto n° 4801, de 6 de agosto de 2003, criou a Câmara de Relações Exteriores e Defesa Nacional e atribuiu a sua presidência ao GSI/PR, tornando o mesmo responsável pela coordenação das medidas de Segurança da Informação e das Comunicações, Segurança Cibernética e Segurança das Infraestruturas Críticas, a serem tomadas pelos diversos órgãos da Administração Pública Federal. Assim, o GSI/PR tem a responsabilidade pelo gerenciamento de crises graves envolvendo a Administração Pública Federal (APF) ou o Estado brasileiro, que tenham potencial de afetar a segurança nacional, coordenando a inteligência e a segurança da informação, compondo o Conselho de Defesa Nacional (CDN) e a CREDEN do Conselho de Governo. O Ministro Chefe do GSI é o Secretário-Executivo do CDN e Presidente da CREDEN.

O GSI/PR coordena com os órgãos da Administração Pública Federal: atividades relativas à Segurança das Infraestruturas Críticas nacionais; Segurança da Informação e das Comunicações, visando, principalmente, à proteção das informações estratégicas nacionais, que transitam por documentos, redes de comunicações e redes computacionais; e Segurança Cibernética, visando à proteção e à própria garantia de utilização das redes e dos sistemas informatizados

estratégicos do País. Essas atribuições fazem do GSI/PR a engrenagem central da coordenação da estratégia de segurança cibernética do Brasil.

Deve ser ressaltado que as atividades de Segurança da Informação e das Comunicações e de Segurança Cibernética permeiam todas as infraestruturas críticas nacionais, razão pela qual, em 2008, foram criados, os Grupos Técnicos de Segurança das Infraestruturas Críticas (GTSIC). Estes encontram-se sob coordenação do GSI/PR, no âmbito do Comitê Gestor de Segurança da Informação.

Da estrutura do GSI/PR destacam-se os órgãos descritos a seguir.

DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (DSIC)

De acordo com MANDARINO (2010, p. 113 e 114), o DSIC tem como atribuição operacionalizar as atividades de segurança da informação e comunicações (SIC) na APF nos seguintes aspectos: regulamentar a SIC para a APF; capacitar todos os servidores públicos federais, bem como os terceirizados a respeito de SIC; realizar acordos internacionais de troca de informações sigilosas; operar o sistema de credenciamento de pessoas e entidades no trato de informações sigilosas; ser o ponto de contato junto à OEA para assuntos de terrorismo cibernético; e manter o centro de tratamento e resposta de incidentes nas redes de computadores da APF – CTIR Gov. As atribuições do DSIC são aquelas contidas no Decreto nº 7.411, de 29 de dezembro de 201053 (conforme seu Anexo I art 6º):

> I - adotar as medidas necessárias e coordenar a implantação e o funcionamento do Sistema de Segurança e Credenciamento - SISEC, de pessoas e empresas, no trato de assuntos, documentos e tecnologia sigilosos;
>
> II - planejar e coordenar a execução das atividades de segurança cibernética e de segurança da informação e comunicações na administração pública federal;
>
> III - definir requisitos metodológicos para implementação da segurança cibernética e da segurança da informação e comunicações pelos órgãos e entidades da administração pública federal;

IV - operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da administração pública federal;

V - estudar legislações correlatas e implementar as propostas sobre matérias relacionadas à segurança cibernética e à segurança da informação e comunicações;

VI - avaliar tratados, acordos ou atos internacionais relacionados à segurança cibernética e à segurança da informação e comunicações, referentes ao inciso I;

VII - coordenar a implementação de laboratório de pesquisa aplicada de desenvolvimento e de inovação metodológica e tecnológica, bem como de produtos, serviços e processos, no âmbito da segurança cibernética e da segurança da informação e comunicações; e

VIII - realizar outras atividades determinadas pelo Ministro de Estado ou pelo Secretário-Executivo.

Da estrutura do DSIC, destaca-se o Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, o CTIR Gov.

CTIR Gov

A área de tratamento de incidentes (CTIR Gov), opera e mantém o Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal – APF, que tem como finalidade o atendimento aos incidentes em redes de computadores da APF.

A iniciativa da criação do CTIR Gov se deu por meio do relatório final do grupo de trabalho instituído no âmbito do Comitê Gestor de Segurança da Informação, por meio da Portaria nº 12 - CH/GSI, de 27 de junho de 2003, para estudar e propor as medidas necessárias para a criação e implantação de um centro de emergência de computação do Governo Federal.

Como conclusão dos trabalhos, o referido grupo destacou a relevância estratégica de criar um centro de tratamento de incidentes em redes da Administração Pública Federal. Enfatizou ainda, a importância da articulação entre

administrações de redes por intermédio de um permanente serviço à disposição de todo o Governo Federal.

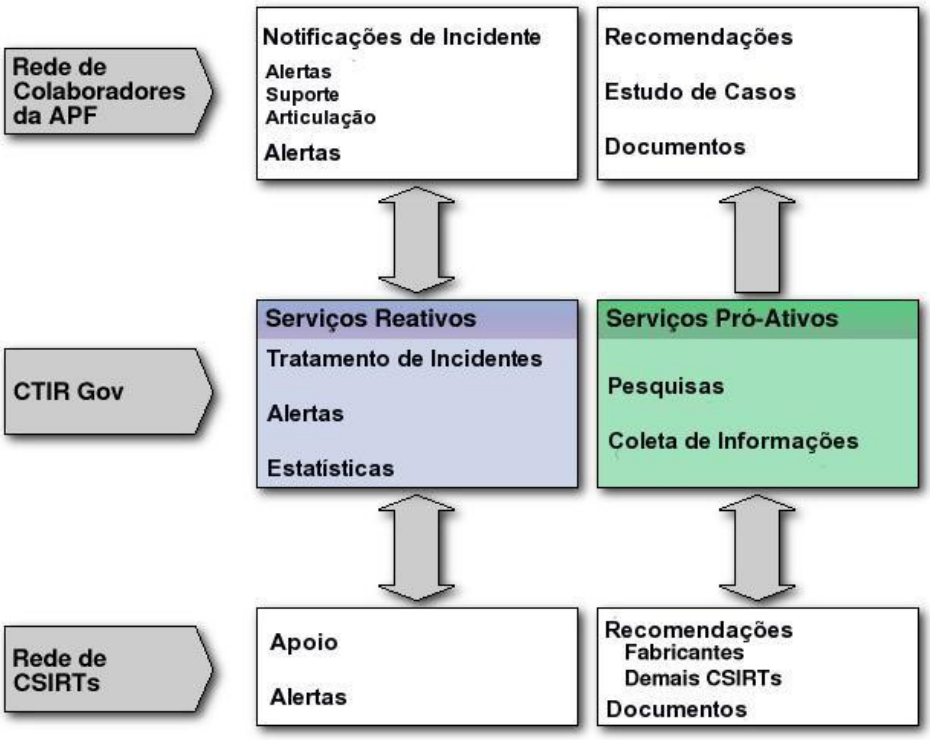
O modelo de referência que pauta o trabalho do CTIR Gov é o de articulação, coordenando os esforços dos órgãos da administração pública federal.

Dentre as missões do CTIR Gov estão o auxílio ao desenvolvimento da cooperação entre os grupos de respostas de incidentes existentes no Brasil e no exterior; o fomento das iniciativas de gerenciamento de incidentes; e a distribuição de informações, alertas e recomendações para os administradores de segurança em redes de computadores da APF.

Os serviços prestados pelo CTIR Gov podem ter caráter reativo ou proativo. Em ambos os casos, o Centro tem condições de determinar tendências e padrões das ameaças no ciberespaço que afetam não só a APF, mas, trabalhando em conjunto com os demais Centros, também as instituições que compõem as infraestruturas críticas de Estado.

O CTIR Gov funciona, portanto, como o ponto central da rede colaborativa de grupos de tratamentos de incidentes de segurança computacionais por todo o país, com destaque para o CERT.br.

Figura 14. Interações do CTIR Gov



Fonte: CTIR Gov (Disponível em http://www.ctir.gov.br/sobre-CTIR-gov.html#interacoes). Acesso em 18 de agosto de 2015.)

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA (ABIN)

A Lei nº 9.883, de 7 de dezembro de 1999 instituiu o Sistema Brasileiro de Inteligência (SISBIN) e criou a Agência Brasileira de Inteligência (ABIN) como o seu órgão central. É atualmente subordinada ao GSI/PR e tem como missões planejar, executar, coordenar, supervisionar e controlar as atividades de inteligência do País; planejar e executar ações, inclusive sigilosas, relativas à obtenção e análise de dados para a produção de conhecimentos destinados a assessorar o Presidente da República; planejar e executar a proteção de conhecimentos sensíveis, relativos aos interesses e à segurança do Estado e da sociedade; avaliar as ameaças, internas e externas, à ordem constitucional; e promover o desenvolvimento de recursos humanos e da doutrina de inteligência, e realizar estudos e pesquisas para o exercício e aprimoramento da atividade de inteligência.

Seu objetivo estratégico é desenvolver atividades de inteligência voltadas para a defesa do Estado Democrático de Direito, da sociedade, da eficácia do poder público e da soberania nacional.

A atribuição de avaliação das ameaças, citada anteriormente, propicia melhores condições para que se construam mecanismos de segurança cibernética de forma mais eficiente, uma vez que se disponha da percepção das ameaças em tempo útil. Na estrutura da ABIN, merece destaque o Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações (CEPESC).

Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações (CEPESC)

De acordo com a ABIN, o CEPESC foi criado em 19 de maio de 1982 para sanar a deficiência em salvaguardar o sigilo das transmissões oficiais, uma vez que havia, naquela época, falta de meios criptográficos próprios e de capacitação nesta área no Brasil. Dentre outras atribuições, destaca-se a promoção da pesquisa científica e tecnológica aplicada a projetos de segurança das comunicações, tais como o projeto e fabricação de soluções de criptografia utilizadas pelas Forças Armadas e Ministério das Relações Exteriores. Sua importância está na capacidade de desenvolver soluções criptológicas próprias, construindo algoritmos cujo nível de segurança seria adequado a proteger informações de Estado e equipamentos de

proteção e de transmissão de informações. Além de fornecer equipamentos e sistemas de segurança, criptográfica a diversos órgãos governamentais, o CEPESC tem participação técnica no Comitê Gestor de Segurança da Informação (CGSI) e na elaboração das especificações do sistema de infraestrutura de chave pública para o País.

A área do sistema de credenciamento, após a promulgação da LAI, foi reformulada e estabeleceu-se o Núcleo de Segurança e Credenciamento (NSC) como órgão central de credenciamento de segurança no âmbito do Poder Executivo federal, com o objetivo de promover e regular o tratamento da informação classificada em qualquer grau de sigilo. O NSC busca assegurar a manutenção da cadeia de confiança entre os entes, públicos e privados, que tratam informação classificada em qualquer grau de sigilo do Governo Federal, inclusive com organismos internacionais.

REFERÊNCIAS

Norma Complementar nº 01/IN01/DSIC/GSIPR, **Atividade de Normatização**. Disponível em:<http://dsic.planalto.gov.br/documentos/nc_1_normatizacao.pdf> Acesso em 20/08/13.

Norma Complementar nº 02/IN01/DSIC/GSIPR, **Metodologia de Gestão de Segurança da Informação e Comunicações**. Disponível em:<http:// dsic.planalto.gov.br/documentos/nc_2_metodologia.pdf> Acesso em 25/08/17.

Norma Complementar nº 03/IN01/DSIC/GSIPR, **Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal**. Disponível em <dsic.planalto.gov.br/documentos/nc_3_psic.pdf> Acesso em 20/08/17.

Norma Complementar nº 04/IN01/DSIC/GSIPR, **Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações** - GRSIC nos órgãos e entidades da Administração Pública Federal. Disponível em<dsic.planalto.gov.br/documentos/nc_04_grsic.pdf> Acesso em 20/08/13 e seu anexo, Disponível em <dsic.planalto.gov.br/documentos/anexo_nc_04_grsic.pdf> Acesso em 20/08/17.

Norma Complementar nº 05/IN01/DSIC/GSIPR, **Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais** - ETIR nos órgãos e entidades da Administração Pública Federal. Disponível em: <dsic.planalto.gov.br/documentos/nc_05_etir.pdf> Acesso em 10/02/12, e seu anexo Disponível em <dsic.planalto.gov.br/documentos/anexo_nc_05_etir.pdf> Acesso em 20/08/17.

Norma Complementar nº 06/IN01/DSIC/GSIPR, **Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta** – APF. Disponível em <dsic.planalto.gov.br/documentos/nc_6_gcn.pdf> Acesso em 20/08/17.

Norma Complementar nº 07/IN01/DSIC/GSIPR, **Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF**. Disponível em <dsic.planalto.gov.br/documentos/nc_7_controle_acesso.pdf> Acesso em 25/08/17.

Norma Complementar nº 08/IN01/DSIC/GSIPR, **Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal.** Disponível em: <dsic.planalto.gov.br/documentos/nc_8_gestao_etir.pdf> Acesso em 10/02/18.

Norma Complementar nº 09/IN01/DSIC/GSIPR, **Estabelece orientações específicas para o uso de recursos criptográficos como ferramenta de controle**

de acesso em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal, direta e indireta. Disponível em <dsic.planalto.gov.br/documentos/nc_9_criptografia.pdf> Acesso em 25/08/17.