MARINHA DO BRASIL
DIRETORIA DE ENSINO DA MARINHA
CENTRO DE INSTRUÇÃO ALMIRANTE WANDENKOLK

CURSO DE APERFEIÇOAMENTO AVANÇADO EM
SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

SEGURANÇA DA INFORMAÇÃO NAS REDES SOCIAIS

1T(QC-CA) DIOGO CARVALHO DE SOUZA

Rio de Janeiro
2020

1T(QC-CA) DIOGO CARVALHO DE SOUZA

SEGURANÇA DA INFORMAÇÃO NAS REDES SOCIAIS

Monografia apresentada ao Centro de Instrução Almirante Wandenkolk como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações.

Orientadores:
Prof° Dr Carlos Vinício Rodríguez Ron
1T(T) Diogo Gonçalves Soares

CIAW
Rio de Janeiro
2020

DE SOUZA, Diogo Carvalho.
Segurança da Informação nas Redes Sociais / Diogo Carvalho de Souza. — Rio de Janeiro, 2020.
67f.: il.

Orientadores: Primeiro-Tenente(T) Diogo Gonçalves Soares; Prof. Dr. Carlos Vinício Rodríguez Ron.

Monografia (Curso de Aperfeiçoamento Avançado de Segurança da Informação e Comunicações) — Centro de Instrução Almirante Wandenkolk, Rio de Janeiro, 2020.

1. Segurança da Informação. 2. Redes Sociais. 3. Engenharia Social. I. Centro de Instrução Almirante Wandenkolk. II. Título.

1T(QC-CA) DIOGO CARVALHO DE SOUZA

SEGURANÇA DA INFORMAÇÃO NAS REDES SOCIAIS

Monografia apresentada ao Centro de Instrução Almirante Wandenkolk como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações.

Aprovada em: 27/03/ 2020

Banca Examinadora:

Gian Karlo Huback Macedo de Almeida, Capitão de Mar e Guerra (RM1-EN), CIAW

Prof° Dr Carlos Vinício Rodríguez Ron, PUC-RIO

Diogo Gonçalves Soares, Primeiro-Tenente(T), CTIM

CIAW
Rio de Janeiro
2020

Dedico esse trabalho àqueles que estiveram presentes na minha vida ao longo deste curso, dando-me força e motivação para seguir adiante. De forma especial aos meus familiares e amigos.

AGRADECIMENTOS

Primeiramente a Deus, por me abençoar e permitir que finalizasse com êxito este curso.

A Marinha do Brasil, instituição que me acolheu e que me permitiu realizar um sonho de servi-la como seu oficial, por mais esta oportunidade que me foi concedida, de cursar o aperfeiçoamento avançado em Segurança da Informação e das Comunicações, área que era desde o começo a que mais me interessou.

Ao comandante Huback, coordenador do Curso de Segurança da Informação e Comunicações, por ser nosso norte e um porto seguro, dando-nos todo o suporte e tranquilidade necessária, para que nos preocupássemos somente com a parte acadêmica durante nossa estadia neste centro de instrução, conseguindo angariar o respeito e grande admiração de todo o quarto pelo qual foi responsável neste período.

Ao meu orientador acadêmico, professor Carlos Vinício Rodríguez Ron, por toda a ajuda e dedicação ao longo deste curso, não só pela orientação deste trabalho, como em todas as demais disciplinas ministradas por ele.

Ao meu orientador técnico, o tenente Diogo Gonçalves Soares, por toda a sua incansável dedicação e providencial ajuda na composição deste trabalho, que superou todas as minhas expectativas de forma positiva, acompanhando de perto e orientando da melhor forma possível em todas as etapas, se tornando um grande amigo sempre pronto a auxiliar e assistir no que era necessário.

Ao professor Helios Malebranche, por ter ministrado com destreza a disciplina de Metodologia da Pesquisa, que tanto auxiliou para o desenvolvimento deste trabalho, sobretudo na parte inicial.

Sustentar o fogo que a vitória é nossa
Almirante Barroso

RESUMO

Este trabalho busca gerar uma mentalidade de segurança em todo pessoal da Marinha do Brasil, no que concerne a exposição de dados nas redes sociais. Através da revisão bibliográfica são introduzidos os conceitos iniciais de segurança da informação, essenciais para o bom entendimento do trabalho em lide. É exposto um pequeno histórico dos principais sites de redes sociais da atualidade e mostrado também o processo de disrupção dos mesmos. Um apanhado geral sobre a legislação pertinente ao tema de proteção de dados no âmbito digital no Brasil e no mundo, dando-se um enfoque maior na legislação nacional, passando pelo Marco Civil da Internet, até a Lei Geral de Proteção de Dados. Casos de violação de privacidade e uso de dados obtidos nas redes sociais, para variados fins, como por exemplo, empresas de assessoria política e de publicidade, como também uma análise dos tipos de dados e informações pessoais que ficam armazenados em um perfil de usuário nas redes sociais. O conceito de engenharia social é introduzido, relacionando-se a ele, o entendimento da Marinha do Brasil sobre o tema, e como o uso da engenharia social por agentes adversos poderia ser eficiente e maléfico contra os interesses institucionais, utilizando-se de dados abertos sensíveis fornecidos pelos próprios membros da instituição. Foi realizado um experimento prático de engenharia social, para se demonstrar as vulnerabilidades e testar o quão difícil é obter os dados abertos na rede (OSINT) sobre os militares pertencentes a instituição, e consequentemente a própria, utilizando-se de uma metodologia de buscas por *hashtags* que fazem alusão a Marinha. O estudo de como diversas ferramentas que utilizam algoritmos e técnicas próprias, conseguem estruturar dados extraídos das postagens de um determinado usuário nas redes sociais, para fazer predições a respeito deste, como pode-se citar, a determinação de características de sua personalidade. Por fim é apresentado um guia prático de boas práticas nas redes sociais, que busca nortear o uso mais consciente nestas pelo pessoal da Marinha do Brasil, minimizando os principais riscos associados.

Palavras-chave: [Segurança da Informação. Redes Sociais. Engenharia Social]

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE SIGLAS

CCSM	Centro de Comunicação Social da Marinha
CERT.BR	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
DOS	*Denial of Service*
DDoS	*Distributed Denial of Service*
OM	Organização Militar
RECIM	Rede de Comunicações Integradas da Marinha
SIC	Segurança da Informação e Comunicações
SID	Segurança da Informação Digital
SMS	Short Mensage Service
MB	Marinha do Brasil
OSINT	*Open Source Intelligence*
UNIFIL	*United Nations Interim Force in Lebanon*
UBA	*User behavior analytics*
UEBA	*User and Entity Behavior Analytics*
SUBA	*Security User Behavior Analytics*

SUMÁRIO

1 INTRODUÇÃO

Como informações compartilhadas nas redes sociais podem ser fontes de vulnerabilidades, passíveis de serem utilizadas por terceiros para os mais variados fins, sobretudo utilizando técnicas de engenharia social (definida no capítulo 4). Será dado enfoque a necessidade em se criar uma mentalidade de segurança dentro da instituição, que proteja tanto esta como também ao seu pessoal, que é considerado o maior patrimônio da Marinha. Somando-se a isso, haverá uma introdução aos conceitos de segurança da informação, e ao estudo sobre a legislação no Brasil e no mundo sobre proteção de dados na internet, e das principais redes sociais na atualidade, expondo seus principais pontos críticos e possíveis vulnerabilidades.

Será mostrado também de forma simplificada alguns métodos e técnicas de tratamento de dados, para se fazer uma análise de como alguns algoritmos apropriados, conseguem através de postagens dos usuários nas redes sociais, fazer por exemplo uma predição do perfil psicológico do autor com grande precisão.

1.1 Apresentação do Problema

Com a popularização das redes sociais, e a exposição cada vez maior dos indivíduos em geral a esta nova forma de interação, faz-se necessário tomar medidas preventivas, orientadas pelas boas práticas de segurança da informação, que resguardem e protejam os dados pessoais compartilhados na rede, de modo especial dados sensíveis que possam de alguma maneira prejudicar a imagem e os interesses da instituição. Visto que é cada vez mais comum, agentes adversos que trabalham com engenharia social, usarem diversas técnicas para coletarem informações estratégicas, com ou sem uso de recursos tecnológicos, e utilizarem esses dados para os mais variados fins. As redes sociais adquiriram uma importância grande não só para os usuários comuns, mas também para diversas empresas e instituições, que se utilizam destas para divulgarem suas atividades e terem uma relação mais próxima com a sociedade. Portanto não é viável simplesmente se abster do uso destas, mas sim se chegar ao meio termo, entre estar presente nas redes, porém evitando uma exposição excessiva e um uso inconsequente das redes sociais. Portanto na Marinha do Brasil, reconhece-se a importância do uso das mídias e redes sociais, mas alerta-se para a observância dos aspectos de boas práticas no seu uso. (MARINHA DO BRASIL, 2015, P.2)

1.2 Justificativa e Relevância

Não são raros os casos no cotidiano, em que informações compartilhadas nas redes sociais acabaram por gerar situações embaraçosas e verdadeiros problemas, não só para as pessoas que as compartilharam e seus familiares em geral, mas também as instituições, as quais estes indivíduos pertencem. Muitas das vezes as próprias empresas tiveram que se retratar publicamente, e tentar descolar sua imagem à de membros que tiveram condutas impróprias ou que manifestaram alguma opinião que não é condizente com os valores da instituição, ou simplesmente por não serem bem aceitos pela sociedade em geral.

No caso da Marinha do Brasil, uma instituição secular e de caráter permanente, em que sua história se confunde com a própria história da nação, é fundamental que seus membros tenham consciência da grandeza institucional e que toda informação que possa ser compartilhada por estes na rede, podem direta ou indiretamente, afetarem não só a vida pessoal e profissional destes, mas toda a instituição e sua imagem junto a sociedade brasileira. Assim faz-se mister uma análise e orientação no sentido de proteger a instituição e seus integrantes.

Por se tratar de um assunto razoavelmente novo na sociedade, muitas vezes as pessoas e instituições, ainda não têm a total dimensão da grande importância deste tema. Portanto é de grande relevância fazer uma análise mais detalhada dos riscos que a Marinha se expõe na medida em que seus membros fazem um mau uso das redes sociais, estimulando assim a mentalidade de segurança e as boas práticas no uso das redes sociais. A Marinha do Brasil disponibiliza uma publicação que trata do uso Institucional e não Institucional de mídias e redes sociais extra-MB, a DCTIMARINST Nº30-08A. (Marinha do Brasil, 2015)

1.3 Objetivos

O presente trabalho tem os seguintes objetivos:

1.3.1 Objetivo Geral

Gerar uma mentalidade de segurança institucional no que se refere ao uso e a exposição de dados nas redes sociais, estimulando- se assim um conjunto de boas práticas que servirá de alicerce para preservar a instituição e seus membros.

1.3.2 Objetivos Específicos

a) Mostrar de forma geral as diversas análises que podem ser feitas com os dados coletados através das redes sociais através de técnicas de engenharia social (Ex: Levantamento de perfil psicológico da pessoa que compartilhou determinada informação através de metodologia apropriada)
b) Fazer de forma simplificada uma análise técnica de alguns algoritmos e softwares utilizados no tratamento dos dados coletados. (como estes funcionam)
c) Estudo de técnicas de engenharia social.
d) Mostrar como dados abertos compartilhados por membros da instituição podem ser danosos para esta, se caírem em mãos de pessoas mal-intencionadas, através de uma simples coleta na rede destas informações.
e) Mostrar um caso simples de engenharia social usado nas redes e quantas informações podem ser obtidas somente buscando entre dados abertos.
f) Propor mecanismos de proteção, por via da regulamentação e da mentalidade de segurança gerada nos membros da instituição, assim como de uso de ferramentas que permitam identificar vulnerabilidades nas equipes de trabalho em especial os relacionados com missões críticas reservadas.

2 REVISÃO BIBLIOGRÁFICA

Neste tópico serão abordados diversos conceitos e princípios de segurança da informação, através de citações e estudos de variados autores sobre o tema que são fundamentais para o entendimento deste trabalho e, finalmente, uma análise mais detalhada sobre a conduta esperada de indivíduos em sites de redes sociais.

2.1 O valor da Informação

Primeiramente, faz-se necessário para um melhor entendimento sobre o que seria informação, diferenciar entre três palavras que trazem conceitos importantes, que algumas vezes são usadas como sinônimos, mas que possuem significados peculiares que permitem distingui-las: dado, informação e conhecimento. Conforme pode-se visualizar no quadro 1 a seguir:

Quadro 1- Diferença entre dado, informação e conhecimento.

Dados	Informação	Conhecimento
Simples observação sobre o estado do mundo.	Dados dotados de relevância e propósito.	Informação valiosa da mente humana. Inclui reflexão, síntese e contexto.
Facilmente estruturado	Requer unidade de análise	De difícil estruturação.
Facilmente obtido por máquinas	Exige consenso em relação ao significado	De difícil captura em máquinas.
Frequentemente quantificado	Exige necessariamente a mediação humana.	Frequentemente tácito
Facilmente transferido		De difícil transferência.

Fonte: Davenport, Prusak- 1998- p.18. Adaptação própria

Do quadro pode-se perceber que o dado é um elemento mais bruto, que por si só, não diz muita coisa a quem o possui. Já a informação, é um dado tratado, interpretado de alguma forma pela mediação humana, passando a ter significado. Finalmente, o conhecimento é uma informação que contém valor para uma determinada aplicação ou proposito.

De acordo com Svaiter (2015), A informação tem um valor intangível, mas isto não significa de forma nenhuma que esta não tenha valor. Isso se reflete nos bilhões que são gastos anualmente, pelas agências de inteligência, conglomerados financeiros, empresas multinacionais, e de provedores de redes sociais, para melhorar a obtenção de informação, através de diversas técnicas, como por exemplo, a mineração de dados ou as mais variadas técnicas de Engenharia Social.

Visto que a informação é tão importante, e dá uma vantagem competitiva imensurável a quem a possui, técnicas para se obter informações sobre um determinado assunto ou ramo de atuação, é a melhor forma de se fazer predições e tentar desvendar como as coisas ocorreram de forma antecipada, assim como entender os fenômenos que ocorrem no presente.

Sabe-se que a informação é um ativo de grande valor, quase que de forma intuitiva, e que ela é fundamental para a tomada de decisões com uma menor probabilidade de erros, sobretudo informações de melhor qualidade, seja na vida pessoal, profissional ou institucional. (LOFRANO, 2017).

Hoje com o advento da internet e o aumento da conectividade em todo planeta, pode-se dizer que o acesso a informações é quase infinito, e esta está armazenada nos inúmeros servidores espalhados pelos datacenters ao redor do globo terrestre. Dentre todos os recursos disponíveis, pode-se dizer que a informação é um que pode ter o maior valor agregado.

Segundo (Toffler, 1980), a informação é tão importante, talvez até mais, do que a terra, o trabalho, o capital e a matéria-prima. Em outras palavras, a informação está se tornando a mercadoria mais importante da economia contemporânea.

A informação, independentemente de seu formato, é um ativo importante da organização. Por isso, os ambientes e os equipamentos utilizados para seu processamento, seu armazenamento e sua transmissão devem ser protegidos. (Fontes, 2006)

A informação sempre foi um bem muito importante para qualquer organização. Há alguns anos, os dados mais importantes da empresa podiam ser guardados “a sete chaves” no interior de algum armário ou gaveta. Modernamente, a quase totalidade das informações, principalmente as de valor estratégico, está digitalizada e armazenada em Estações de Trabalho (computadores pessoais) ou em Servidores (um sistema de computação centralizada que fornece serviços a uma rede de computadores) acessíveis, todos eles, por intermédio da Rede Mundial de Computadores. (Fontes, 2008)

2.2 Segurança da Informação

A segurança da informação é uma área de conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alteração indevida ou sua disponibilidade (SÊMOLA, 2003).

A informação é um recurso crítico não apenas para a realização de tarefas e concretização de negócios, mas também para a tomada de decisões. Pelo fato de estarem armazenadas em meios eletrônicos e até mesmo conectadas a redes externas, as informações poderiam ser divulgadas a concorrentes, corrompidas, apagadas ou mesmo não estar disponíveis quando necessário para as atividades do negócio (FERREIRA, 2003).

> "A Segurança da Informação e Comunicações (SIC) prevê ações que objetivam viabilizar e assegurar a disponibilidade, integridade e confidencialidade de dados e informações de forma a minimizar os incidentes de segurança da informação. Adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não-repúdio e confiabilidade, podem também estar envolvidas.
>
> A SIC é a proteção resultante de todas as medidas postas em execução visando negar, impedir ou minimizar a possibilidade de obtenção do conhecimento de dados que trafeguem ou sejam armazenados digitalmente nos sistemas de redes locais, compreendendo, segundo definição estabelecida pelo Governo Federal, ações voltadas às Seguranças física, lógica, de tráfego e criptológica das Informações Digitais. Portanto, a SIC corresponde não só ao conjunto de procedimentos, como também aos recursos (programas e equipamentos específicos de segurança) e às normas aplicáveis que irão garantir os seus requisitos básicos". (MARINHA DO BRASIL, 2019, P.-3-4.3-5-).

Segundo De Souza (2018), existem quatro pilares básicos que definem a Segurança da informação: Confidencialidade, Autenticidade, Integridade e Disponibilidade.

a) Confidencialidade: Refere-se as informações que só podem ser acessadas dentro das organizações por pessoas autorizadas e precisam ser protegidas de acesso externo.

b) Autenticidade: Tem como objetivo verificar se as informações são verídicas.

c) Integridade: Evidencia a capacidade de se confirmar se a informação está correta e não foi corrompida.

d) Disponibilidade: Ressalta que a informação deve estar sempre disponível para todos aqueles que dela necessitam a todo tempo e em todo lugar.

Estes pilares são também considerados os requisitos básicos de SIC na Marinha do Brasil conforme consta nas Normas de Tecnologia da Informação da Marinha (DGMM-0540, 2019):

> "Requisitos Básicos de SIC
>
> a) Disponibilidade - capacidade da informação digital estar disponível para alguém autorizado a acessá-la no momento próprio.
>
> b) Integridade - capacidade da informação digital somente ser modificada por alguém autorizado;
>
> c) Confidencialidade - capacidade da informação digital somente ser acessada por alguém autorizado;
>
> d) Autenticidade – capacidade da origem da informação digital ser aquela identificada". (MARINHA DO BRASIL, 2019, P.-9-1-).

2.3 Ameaças à Segurança da Informação

Visto que a informação possui grande valor tanto para os indivíduos como para as organizações, faz-se mister conhecer as principais ameaças que podem comprometer este ativo. A segurança da informação pode ser comprometida por diversas ameaças, que podem de alguma maneira comprometer os pilares básicos (requisitos) já estudados. A seguir veremos alguns ataques comuns e quais os requisitos comprometidos por estes.

a) Ataques de DoS

Segundo Alecrim (2012), os ataques DoS (*Denial of Service*), que podem ser interpretados como "Ataques de Negação de Serviços", consistem em tentativas de fazer com que computadores - servidores Web, por exemplo - tenham dificuldade ou mesmo sejam impedidos de executar suas tarefas. Para isso, em vez de "invadir" o computador ou mesmo infectá-lo com malwares, o autor do ataque faz com que a máquina receba tantas requisições que não tem condições de processá-las e, consequentemente, o serviço fica indisponível.

Em outras palavras, o computador fica tão sobrecarregado que "*nega serviço"*. Este ataque compromete o requisito **Disponibilidade.**

b) Spoofing

Assim como os criminosos e estelionatários do mundo real, os ladrões virtuais podem falsificar informações para roubar dados importantes ou, por exemplo, obter acesso a contas bancárias. Essa prática é chamada de *spoofing*, um termo que engloba a falsificação de endereços IP (enviar mensagens para um computador usando um endereço IP que simula uma fonte confiável), de e-mails (falsificar o cabeçalho de um e-mail para disfarçar sua origem) e de DNS (modificar o servidor de DNS para redirecionar um nome de domínio específico para outro endereço IP (AVAST, 2019).

Neste caso, o requisito comprometido é o da **Autenticidade.**

c) MITM (*Man in The Middle)*

Um ataque *Man-in-the-middle* é um nome genérico para qualquer ataque virtual em que alguém fica entre o usuário legítimo, autorizado a realizar alguma operação, e o serviço/recurso que o mesmo acessa, tendo assim, um agente malicioso, acesso indevido a informação ali trafegada. Esse acesso indevido pode ser: entre o usuário e sua transação bancária online, ou em uma interceptação de um diálogo privado de um usuário com um familiar, ou entre seus e-mails de trabalho e os destinatários/remetentes, e assim sucessivamente em inúmeras interceptações de conteúdo possíveis.

Basicamente, ataques MITM permitem que os criminosos virtuais interceptem, enviem e recebam dados que chegam e saem do dispositivo da vítima sem serem detectados até que a transação esteja completa. (TORRES, 2018)

Este ataque pode comprometer o requisito **Confidencialidade** como também a **Integridade** dos dados acessados.

d) Ransomware

É um software malicioso que infecta o computador do usuário, criptografando os arquivos pessoais deste, e depois exibe mensagens exigindo o pagamento de uma determinada taxa de “resgate” dos arquivos perdidos, fornecendo então a chave que vai descriptografar esses arquivos. Essa classe de malware é um esquema de lucro criminoso, que pode ser instalado por meio de links enganosos em uma mensagem de e-mail, mensagens instantâneas ou sites. Ele

consegue bloquear a tela do computador ou criptografar com senha arquivos importantes predeterminados. (Kaspersky, 2020)

Este ataque compromete o requisito **Disponibilidade,** pois impede que o usuário legítimo e habilitado a acessar a informação, tenha acesso a esta.

e) Botnet

Em sua forma literal, botnet é a junção das palavras *robo*t (robô) e *network* (rede). Ameaças deste tipo têm a finalidade de criar uma rede autônoma para disseminar spam ou até mesmo vírus. Uma das formas mais comuns de um computador virar parte de uma botnet é através da instalação de um malware. Geralmente, este tipo de praga é enviado por e-mail, disfarçada de anexo. Outra forma comum é clicar em links ou banners de sites desconhecidos que façam download automático de um arquivo *.exe*, por exemplo. A principal característica de um dispositivo que integra uma botnet é apresentar lentidão repentina. É como se o computador ou smartphone fornecesse poder de processamento para o criminoso virtual. O dispositivo que faz parte de uma botnet ajuda, mesmo que involuntariamente, a propagar crimes virtuais. Além de espalhar spam e vírus, as botnets são usadas para ataques DDoS (*Distributed Denial of Service*). Diversas empresas já foram afetadas por ataques oriundos de botnets. O maior deles aconteceu no início de 2014, quando os servidores da CloudFlare, empresa de distribuição de conteúdo online, receberam um tráfego superior a 400 gigabits por segundo, ocasionada por botnets de todas as partes do mundo. (NOVAES, 2014)

Este tipo de ataque compromete o requisito **Disponibilidade.**

f) Backdoors

O Backdoor tem como finalidade o controle de um único computador. Este tipo de ataque é um dos mais prejudiciais aos usuários, já que, de certa forma, todos os arquivos poderão ser acessados pelo criminoso virtual de forma remota, possibilitando o controle de todos os recursos do computador. A forma mais comum para ter o computador infectado é a instalação de arquivos maliciosos do tipo cavalo de troia. Esses arquivos têm como finalidade deixar o caminho livre para que o cracker consiga voltar e ter controle sobre a máquina, sem passar por verificações de segurança. (NOVAES, 2014).

Este tipo de ataque compromete o requisito **Confidencialidade.**

g) Engenharia Social

Uma outra forma de ataque que pode comprometer a segurança da informação, é o de engenharia social, que diferentemente dos outros ataques baseados em vulnerabilidades técnicas, este tipo de ataque é baseado no fator humano, o que torna seu controle muito mais complexo, como é exposto por Mitnik a seguir:

> Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável. Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança.
>
> Esses indivíduos ainda estarão completamente vulneráveis, devido ao fator humano que torna os dados sensíveis passíveis de serem coletados através de técnicas de Engenharia Social.
>
> À medida que os especialistas contribuem para o desenvolvimento contínuo de melhores tecnologias de segurança, tornando ainda mais difícil a exploração de vulnerabilidades técnicas, os atacantes se voltarão cada vez mais para a exploração do elemento humano. Quebrar a "firewall humana" quase sempre é fácil, não exige nenhum investimento além do custo de uma ligação telefônica e envolve um risco mínimo. (MITINIC, 1963).

Por essa razão é essencial criar uma mentalidade de segurança em todos os membros da instituição. Visto que a informação pode ser comprometida tanto por vulnerabilidades técnicas como, principalmente, pelo fator humano, é necessário tomar medidas de prevenção cabíveis contra estes dois fatores, como corrobora para este conceito Prestes:

> A proteção de dados confidenciais nas empresas é baseada no componente técnico e no fator humano. De acordo com as últimas tendências de desenvolvimento da segurança da informação, o foco passa a ser o indivíduo. Isto é evidenciado por tecnologias como UEBA (User and Entity Behavior Analytics), UBA (User behavior analytics), SUBA (Security User Behavior Analytics) e outras ferramentas de análise de comportamento de usuários, que visam detectar ameaças presentes. (PRESTES,2018).

O esforço para as atividades de SIC deve ser de todos e não somente do pessoal diretamente envolvido com o setor de informática da OM (Organização Militar). O fator mais

importante para a SIC é a existência de uma mentalidade de segurança incutida em todo o pessoal. Pouco adiantará o estabelecimento de rigorosas medidas de segurança se o pessoal responsável pela sua aplicação não tiver delas perfeita consciência. As OM devem, portanto, envidar esforços para desenvolver e manter um alto nível de conscientização do pessoal quanto à SIC. Isto pode ser feito, por exemplo, por meio de notas de ampla divulgação a todo pessoal da Organização Militar e de palestras, adestramentos, exercícios internos e outras atividades cabíveis, englobando publicações, normas e procedimentos afetos ao assunto. Além disso, dentro do Programa de Adestramento de cada OM, devem ser formalmente estabelecidos e continuamente cumpridos adestramentos que abordem todos os aspectos de SIC. (MARINHA DO BRASIL, 2019, P.-9-19-).

3 REDES SOCIAIS

Neste capítulo mostrar-se-á como as redes sociais se tornaram mais presentes no cotidiano das pessoas, assim como sua influência e as razões para o incremento de seu uso, como, por exemplo, a universalização cada vez maior do acesso à Internet. Expor-se-á também as principais redes sociais em uso no Brasil e no mundo, assim como o número de usuários ativos em cada uma.

Será feito também um pequeno histórico das principais redes sociais em uso na atualidade, desde sua fundação até chegarem a ser empresas gigantes de projeção mundial como nos dias de hoje.

As redes sociais são o meio onde as pessoas se reúnem por afinidades e com objetivos em comum, sem barreiras geográficas e fazendo conexão com dezenas, centenas e milhares de pessoas conhecidas ou não (NOGUEIRA, 2010).

> Segundo Gabardo (2015), redes sociais são redes formadas por indivíduos, ou algo que possa ser individualizado, com determinado grau de relacionamento. Ao definir-se redes sociais é comum associarmos diretamente a redes de relacionamento atuais como, Facebook, Twitter, Youtube, etc., porém, como afirma Recuero (2017), é preciso claramente diferenciar redes sociais e sites de rede social. Um, corrobora a definição de Gabardo (2015),o outro define-se como uma plataforma que viabiliza a construção de interações sociais, sendo uma forma de apropriação que as pessoas fazem dele que é capaz de revelar estruturas sociais construídas por esses indivíduos a partir de uma ferramenta online. Contudo, o site de rede social, não é uma tradução das conexões existentes no espaço offiline, pelo contrário, eles amplificam conexões sociais, permitindo que estas apareçam em larga escala (SOARES, 2018).

Pelas diferentes definições, conseguimos distinguir o conceito de “redes sociais” e o de “sites de redes sociais”, apesar de, popularmente, utilizarmos os dois conceitos como se fossem sinônimos.

3.1 Disrupção de redes sociais

As formas de comunicação mudaram, e assim também o modo das pessoas se relacionarem. Atualmente, não é mais necessário se deslocar para se fazer uma reunião de negócios, para se comprar algum produto desejado, ou até mesmo para se iniciar um novo relacionamento amoroso. (CORTEIS, 2020).

Pode-se perceber que existe algum tipo de rede social para satisfazer a praticamente qualquer atividade atualmente. O que faz destas, parte da vida cotidiana dos indivíduos de forma geral, modificando seus hábitos e as formas de interagir com outros e com o mundo.

Reencontrar velhos amigos da época de infância, em que em algum momento da vida se perdeu o contato, poder se juntar a grupos que tenham afinidades em comum, e poder compartilhar momentos importantes, em tempo real, com pessoas que estimamos, são alguns poucos exemplos, dos inúmeros benefícios de se manter um perfil, e uma conta ativa nas redes sociais de maior popularidade.

A utilização cada vez maior das Redes Sociais no Brasil, pode ser explicado também pelo aumento da conectividade, e a universalização do acesso à internet para a população, conforme demostra pesquisa realizada pelo CETIC (Centro de Estudo sobre as Tecnologias da Informação e Comunicação) e Coordenação do Ponto BR (NIC.br), que implementa as decisões e projetos do Comitê Gestor da Internet do Brasil (CGI.br), que realizou uma pesquisa, através de visitas em 16 mil residências em 350 cidades do país entre setembro de 2013 e fevereiro de 2014. Detectou-se que atualmente, a internet é uma ferramenta fundamental para a vida de muitas pessoas no mundo, mas nem todos têm a oportunidade de utilizá-la, já que a web não está disponível para boa parte da população mundial.

Ainda de acordo com os resultados da pesquisa, no Brasil, apesar de todos os problemas enfrentados pela população, a internet vem ganhando espaço e já é utilizada por mais de 50% dos brasileiros acima de dez anos, ou seja, 85 milhões de pessoas. Um fato curioso é que os principais motivos para os brasileiros acessarem a internet nos smartphones são para acessar as redes sociais (30%). (SILVA, 2015)

É possível inferir a existência de uma correlação entre o advento de novas tecnologias e as mudanças comportamentais da sociedade, capaz de induzir a uma espiral – quem sabe infindável – de desenvolvimento social e científico, em que um influência e/ou condiciona o outro. (SILVA, 2011)

Com a importância inegável das Redes Sociais, nas relações interpessoais, modificando as formas de interação e hábitos sociais. As instituições em geral estão se adaptando ao seu uso, não só estando presente com perfis oficiais nas redes, como também orientando o uso destas por seus membros pautado nas boas práticas.

Importância das Mídias e Redes Sociais no Contexto Atual da MB

No mundo atual, onde a conectividade e a interatividade estão cada vez mais presentes no dia a dia, a importância de uma comunicação efetiva e instantânea com a sociedade cresce constantemente. Interagir e engajar com nossas audiências interna e externa

> tornou-se essencial. O uso eficiente de midias e redes sociais para este fim contribui para a MB:
> a) Compreender e responder a questões e preocupações do público em geral;
> b) Divulgar oficialmente as atividades de suas OM;
> c) Aumentar a velocidade na prestação de serviços de interesse da população;
> d) Levar prontamente informações oficiais ao público interno e externo;
> e) Estabelecer uma relação de confiança com o público em geral, por meio da transparência e compartilhamento de informações; e
> f) Divulgar sua história, tradições e costumes. Portanto deve-se utilizar as mídias e redes sociais de forma cautelosa, segura e consciente, a fim de assegurar o correto emprego deste meio de comunicação. (MARINHA DO BRASIL, 2015, P.2).

O ideal é que se chegue a uma situação de equilíbrio entre estar presente nas Redes Sociais, onde pode-se usufruir de todos os benefícios oferecidos, mas tomando-se algumas precauções norteadas em boas práticas de orientação e proteção de dados sigilosos.

3.2 Sites de redes sociais

Diante da pluralidade de sites de redes sociais contendo funcionalidades e recursos específicos as suas plataformas, apresentam-se, a seguir, os principais aplicativos sociais em relevância a quantidade de usuários de acordo o relatório "*Digital in 2018"* (WE ARE SOCIAL, 2018)".

Por conta dessa grande diversidade, foi realizada uma pesquisa, a fim de se conhecer melhor os inúmeros sites disponíveis, assim como o número de usuários ativos em cada uma delas.

Por exemplo na tabela 1, onde são mostradas as redes sociais mais usadas no mundo com o respectivo número de usuários ativos em cada uma delas na atualidade.

Tabela 1 - As redes sociais mais usadas no mundo.

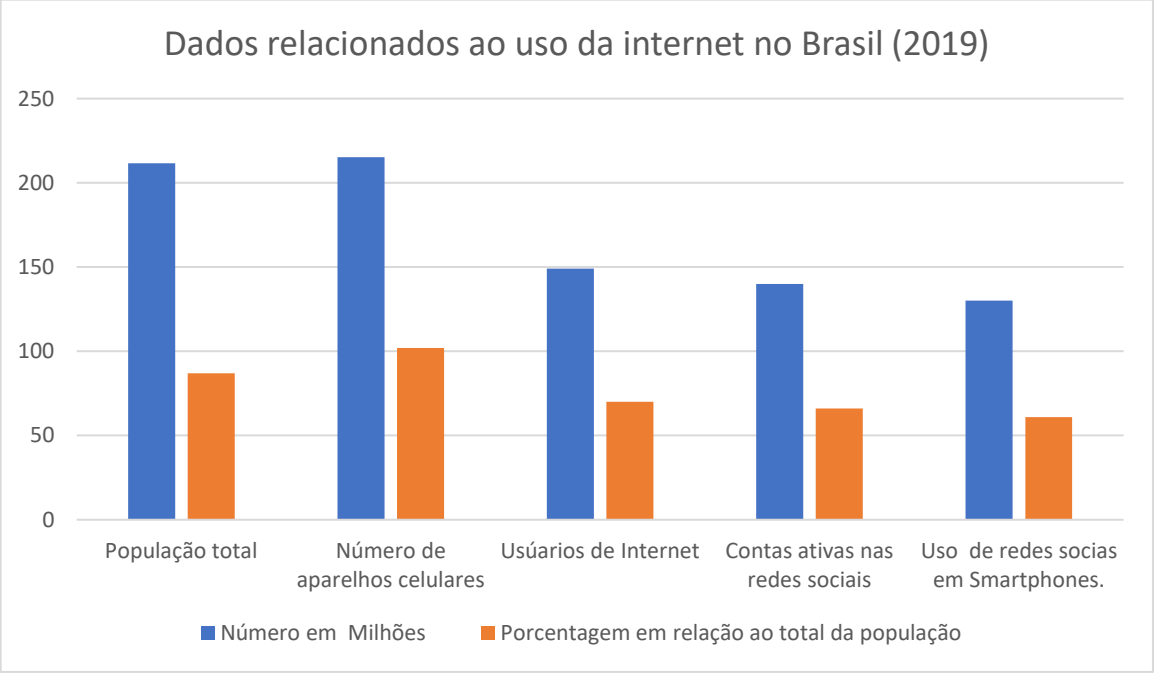
Rede Social	**Usuários ativos * em milhões**
Facebook	2,271
Youtube	1,900
WhatsApp	1,500
Facebook Messenger	1,300
WBXIN/Wechat	1,803
Instagram	1,000
QQ	803
QZone	531
DOUYIN/TicToc	500
Sina Weibo	446
Reddit	330
Twitter	326

Rede Social	Usuários ativos * em milhões
Douban	320
LinkedIn	303
Baidu Tieba	300
Skype	300
Snapchat	287
Viber	260
Pinterest	250
Line	194

Fonte: Site resultados digitais

Para melhor aprofundar o entendimento sobre o uso das redes sociais, visto que há uma relação diretamente proporcional entre o incremento do número de usuários de internet no país e o aumento do uso destas, analisando-se especificamente o Brasil, foi realizado um estudo, conforme demonstrado na figura 1, que correlaciona algumas informações como o número total da população, número de aparelhos celulares em uso, o número de usuários de internet, e finalmente dados sobre o número total de contas ativas nas redes sociais, bem como número de usuários das mesmas utilizando smartphones.

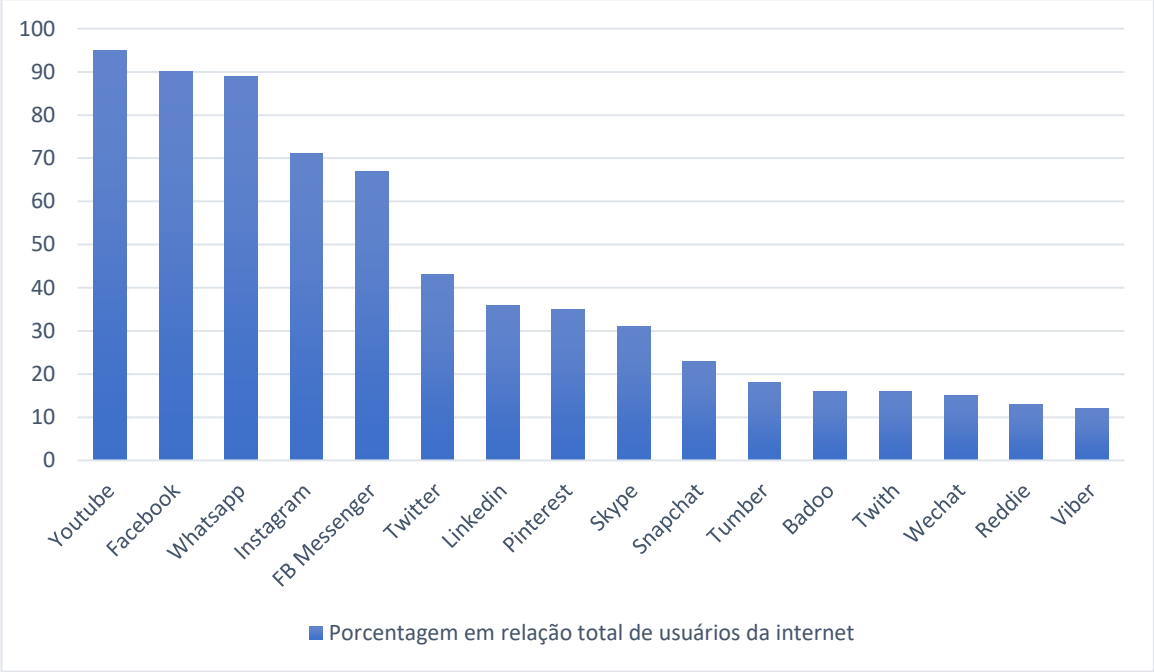
Figura 1 - Estatísticas sobre dados relacionados ao uso das redes sociais no Brasil em 2019



Fonte: Site We are social adaptação própria

Ainda tendo por base esse mesmo estudo, foi demonstrado o número de usuários em cada rede social no Brasil, e demonstrado o percentual em relação ao número total de usuários de internet no país.

Figura 2 - As redes sociais mais usadas no Brasil em 2019



Fonte: Site We are social adaptação própria.

3.2.1 Facebook

De acordo com Kleina (2018), a história do *Facebook* começa oficialmente em 04 de fevereiro de 2004, com o lançamento de um site chamado *Thefacebook*. Os estudantes eram da universidade de *Harvard*. O serviço era simples e só funcionava no campus, e a logo ficava entre colchetes e uma ilustração do ator *Al Pacino* ocupava o topo da página inicial.

Em 2003, o estudante *Mark Zuckerberg* já tinha um site que havia conseguido um maior êxito e então cria uma página chamada *FaceMash*. Ela comparava fotos de estudantes da universidade e deixava escolher a pessoa mais atraente entre as duas. Inicialmente logrou-se algum sucesso, mas o site acabou saindo do ar pouco tempo depois, por usar a base de dados da instituição sem autorização. A universidade emitiu uma advertência e ele se desculpou. Em janeiro de 2004, ele começa a escrever um novo código que se tornaria o Facebook. Em setembro de 2005, o site deixou de ser “Thefacebook” e passou a se chamar Facebook.

No mesmo ano, a rede começa a permitir o compartilhamento de imagens com amigos. Em 2007, foi liberado o compartilhamento de vídeos e, no ano seguinte, a rede social criou um chat. (Fernandes, 2018).

O nome é bem simples: um *face book*, ou livro de rostos, é um diretório que possuia perfis e fotos de alunos ou participantes de algum grupo. Na rede, era possível adicionar amigos e conferir informações do perfil, e desta vez o projeto obteve um ótimo resultado.

A partir disso, quando o Facebook se tornou grande demais, Marck inteligentemente decidiu priorizar o caminho que a sua empresa deveria seguir. Depois de algumas conversas, ele chegou à conclusão que aquilo que o Facebook fazia excepcionalmente bem era manter os perfis pessoais e as redes de conexão de amigos, esse era o seu foco, apenas em cima disso ele deveria se especializar. (Andreasi, 2011).

Em relação as funcionalidades que o Facebook disponibiliza aos seus usuários, destacam-se: Permitir a manutenção do seu perfil pessoal, no qual compartilha sua foto e outras informações pessoais, como: local de trabalho, instituições onde estudou, gosto musical e literário, e-mail, lista de membros da família, e muitas outras informações. É possível enviar e receber convites de amizade, adicionando novos membros a sua rede de amigos, e estes têm acesso privilegiado ao conteúdo que é exposto por você na rede.

Figura 3 - Página de Login do Facebook.

Fonte: Site da plataforma na internet

Existe uma política de privacidade pela qual o usuário deve autorizar o tipo de conteúdo e quais pessoas terão acesso a cada tipo de informação que este compartilha, e se esta ficará visível somente aos seus “amigos”, “amigos de amigos”, ou a qualquer usuário da rede que

acesse o seu perfil. Faz-se mister então que o usuário tenha atenção ao preencher esses formulários, pois pode estar autorizando o uso de seus dados pessoais ou o acesso a dados sensíveis a terceiros, que poderão se utilizar dessas informações para ações maliciosas.

Houve alguns casos ao longo dos anos de vazamento de dados e de violação de privacidade nessa rede social.

Alguns casos notáveis em que informações compartilhadas nas Redes Sociais foram usadas contra as pessoas que compartilharam estas informações, foram casos de assaltos na grande São Paulo conforme noticiado pelo site Globo.com (2011), onde assaltantes especializados na coleta desse tipo de informação privilegiada, as usa para o planejamento do ato criminoso, estudando o perfil, e muitas vezes os tipos de bens que as vítimas possuem.

3.2.2 Twitter

Segundo Smaal (2010), O *Twitter* foi fundado em março de 2006 por *Jack Dorsey*, *Evan Williams* e *Biz Stone* como um projeto paralelo da *Odeo*. A ideia surgiu de *Dorsey* durante uma reunião de discussão de ideias (*brainstorming*) em que ele falava sobre um serviço de troca de status, como um *SMS*.

Figura 4 - Layout do Twitter

Fonte: Google imagens.

Chamado simplesmente de *Status*, a versão precursora do Twitter tinha como conceito exatamente o envio de mensagens curtas através do celular, onde era possível receber um *twich* (vibração, em tradução livre) no seu bolso quando um update era enviado.

Entretanto, a palavra não agradou, pois não demostrava exatamente o que era o serviço. Ao buscar nomes similares no dicionário, *Dorsey* dentre outros encontraram a palavra *twitter*, que em inglês tem dois significados: “uma pequena explosão de informações inconsequentes” e “pios de pássaros”.

A limitação de caracteres se dá exatamente pelo conceito inicial da ferramenta: mensagens SMS. Além disso, enviar mensagens curtas é o principal foco do serviço e principal difusor de sites encurtadores de URL, como o *Bit.ly*, *Migre.me* e outros. Uma das principais ferramentas do *Twitter* não foi lançada logo no começo. Os *Trending Topics* (ou tópicos da moda, em tradução livre) traz os assuntos mais discutidos no mundo do Twitter naquele momento.

A inserção de uma busca em tempo real de assuntos indexados no sistema se deu em abril de 2009, quando ao observar as marcações feitas pelos próprios usuários, a equipe responsável pela plataforma resolveu incorporar o que antes era um aplicativo em mais uma ferramenta própria através da compra da empresa responsável pelo mecanismo. A cada dia surgem novas atualizações e novidades, como as listas de amigos e filtros de *Trending Topics* por países. O serviço não parou de evoluir e conta com usuários fiéis, que trocam diariamente cerca de três milhões de mensagens diariamente.

Atualmente o *Twitter* continua como umas das principais redes sociais do mundo, sendo amplamente usado por diversas personalidades, como: O papa, presidentes de diversas nações, e a família real, por exemplo, têm uma conta nesta rede e mantém um canal aberto com seus seguidores.

Neste trabalho, serão vistas análises que poderão ser feitas através da coleta de postagens de uma pessoa no *Twitter* que permitam deduzir, por exemplo, características de sua personalidade.

Como mostra Arnoux (2017), existem diversos modelos de incorporação de palavras que são usados para determinar características da personalidade de uma pessoa. A incorporação de palavras é uma técnica que representa as palavras como um vetor denso, de baixa dimensão e com valor real. Baseia-se em relações sintáticas e semânticas entre as palavras. Geralmente apreendidas em grandes quantidades de dados de textos não estruturados, essa representação ajuda os algoritmos de aprendizado a obter melhores resultados em tarefas de processamento de linguagem natural, aproximando palavras semelhantes.

3.2.3 Instagram

Segundo Aguiar (2016), O Instagram é uma rede social principalmente visual, onde um usuário pode postar fotos e vídeos de curta duração, aplicar efeitos a eles e interagir com publicações de outras pessoas, através de comentários e “curtidas”.

Além disso, um usuário pode “seguir” o outro para poder acompanhar suas postagens e suas atividades dentro da rede. O número de seguidores inclusive contribui para a visibilidade do perfil.

Nele também encontramos as hashtags, que servem como um mecanismo de busca das publicações, e ajuda na hora de segmentar o seu público, caso possua uma página comercial.

O Instagram surgiu da parceria entre o empresário norte-americano Kevin Systrom e o engenheiro de software brasileiro Mike Krieger, no início dos anos 2010.

O novo projeto foi chamado de Instagram, que é uma junção de instant camera com telegram – um telegrama instantâneo de imagens.

Finalmente, em março de 2012, o Facebook comprou o Instagram por US$ 1 bilhão, com a promessa de manter sua gestão independente. (Patel, 2019).

Além dos filtros inspirados na câmera Polaroid, o Instagram apresenta uma série de recursos que contribuem para a experiência do usuário no aplicativo e que foram implementados ao longo de seus 6 anos de existência.

Figura 5 - Página de Login do Instagram

Fonte: Site da plataforma na internet

Segundo Costa (2019), O Instagram atualmente é uma das principais redes sociais usadas no Brasil, sendo esta, uma grande fonte de informações e dados que podem ser usados para os mais variados fins, como por exemplo, a aplicação de técnicas de engenharia social.

4 LEGISLAÇÃO ESPECÍFICA

Com todas as mudanças que ocorreram na sociedade nos últimos anos, sobretudo na forma que as pessoas se relacionam entre si, especialmente instigado pelo incremento das relações digitais presentes em quase todas as etapas do cotidiano, fez-se necessário que os governos de vários países começassem a se preocupar com a necessidade de rever as suas legislações, para atender a esta nova demanda social, a fim de buscar uma regulamentação efetiva para garantir os direitos e deveres de seus cidadãos nesse "novo mundo" então desvelado.

A leis ao longo da história sempre tiveram uma característica de dinamismo, tendo que se adaptarem, e muitas vezes se criarem leis para se atender as modificações e aos novos anseios sociais, não sendo diferente agora com a chamada "era digital".

Em vários países do mundo começaram a se criar legislações que tentam regulamentar o uso da internet e das relações digitais que se assomam, e no Brasil não foi diferente, como será visto neste capítulo.

a) Marco civil da internet

O marco civil da internet, oficialmente Lei n.º 12.965, de 23 de Abril de 2014, foi a legislação pioneira no Brasil relativa ao tema da proteção de dados e também a tentar regulamentar as relações digitais, oriundas do advento da modificação das relações pessoais trazidas pelo avanço tecnológico e a popularização na sociedade de cada vez mais serviços usando a internet e o mundo digital. Surgindo assim, de uma grande demanda e da necessidade social de se ter uma legislação específica para esse fim. Esta lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. No que diz respeito mais especificamente a questão da privacidade dos usuários, este tema é tratado nos artigos 10 º e 11 º.

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
>
> § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º .
>
> § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial,

> nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.
>
> § 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.
>
> § 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.
>
> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
>
> § 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
>
> § 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.
>
> § 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.
>
> § 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo. (BRASIL, 2014)

O primeiro garante, dentre outras coisas, que um provedor não pode violar o direito à intimidade e a vida privada de seus usuários, sendo assim vedado a divulgação das informações destes ou ainda monitorar os dados trafegados de seus clientes. E o segundo diz que o monitoramento e armazenamento desses dados podem ser feitos, desde que o provedor receba ordem judicial com esta instrução.

No artigo 7 º em seus incisos se garantem ainda o não fornecimento a terceiros dos dados pessoais dos usuários, inclusive registros de conexão, o de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado nas hipóteses previstas em lei;

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
>
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
>
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
>
> IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;
>
> V - manutenção da qualidade contratada da conexão à internet;
>
> VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
>
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
>
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
>
> a) justifiquem sua coleta;
>
> b) não sejam vedadas pela legislação; e
>
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
>
> IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
>
> X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;
>
> XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;
>
> XII – acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e
>
> XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet. (BRASIL, 2014)

E que deverão ainda os provedores fornecerem informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção dos dados pessoais do usuário, que somente poderão ser utilizados para finalidades que: Justifiquem sua coleta, não sejam vedados pela legislação; e que estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações na internet.

Mais recentemente houve modificações no marco civil da internet, através da Lei Geral de Proteção de Dados, que foi aprovada em abril de 2018

b) Lei Geral de Proteção de Dados

Seguindo uma tendência de âmbito global, em se criar legislações que protegessem a privacidade e os dados pessoais de seus cidadãos, como por exemplo o *General Data Protection Regulation* (GDPR), que pode ser traduzido de forma literal como: Regulação Geral de Proteção de Dados, que passou a ser obrigatório em 25 de Maio de 2018, para todos os países-membros da União Europeia, ou o California *Consumer Privacy Act* (CCPA), ou em português, Lei de Privacidade do Consumidor da California nos Estados unidos da América, aprovado no dia 28 de Junho de 2018.

O Brasil se juntou aos países que contam com uma legislação específica para este fim, sancionando a Lei Geral de Proteção de Dados, Lei n º 13.709, de 14 de agosto de 2018. Essa lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, que tratamos de forma especial neste, e tem como objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Quando esta lei entrar em vigor, o que deverá ocorrer de forma integral somente dezoito meses após a data que foi sancionada, será garantida a todos a ampla informação sobre como empresas públicas e privadas tratam os dados de seus usuários ou clientes, o modo e a finalidade da coleta destes, sua forma de armazenamento, por quanto tempo guardam e com quem compartilham. Quanto as empresas, estas deverão garantir a transparência e o direito ao acesso a estas informações.

Podemos citar a própria lei para definir o tratamento que deve ser dado aos dados pessoais sensíveis do usuário, que são elencados no artigo 11 desta lei.

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
>
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
>
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
>
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
>
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
>
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
>
> e) proteção da vida ou da incolumidade física do titular ou de terceiros;
>
> f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou
>
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. (BRASIL, 2018)

5 CASOS DE VIOLAÇÃO DE PRIVACIDADE E USO DE DADOS OBTIDOS NAS REDES SOCIAIS

As redes sociais se tornaram uma fonte quase inesgotável de informações sobre a vida das pessoas, pela quantidade de dados expostos nelas por cada usuário, e pela abrangência destas, fato que pode causar sérios problemas para os donos legítimos das informações, pois estas podem ser alvo de agentes adversos, que estarão habilitados a fazer uso destes dados para seu próprio benefício, ignorando muitas vezes a privacidade e o quão sensível esses elementos podem ser.

Neste capítulo a seguir são expostos alguns casos de vazamentos e violação de dados de usuários, através do Facebook e será demonstrado a quantidade e a qualidade de informações que é mantida armazenada nesta rede, para cada perfil de usuário e como é possível a este ter acesso aos seus dados pessoais armazenados.

5.1 Dados obtidos pela *CAMBRIDGE ANALYTICA*

De acordo com a BBC News Brasil (2018) , são cada vez maiores as denúncias pelo uso de dados indevidos de usuários pelo Facebook, como no caso da empresa de análise de dados Cambridge Analytica, uma empresa de consultoria política que trabalhou na campanha do presidente americano Donald Trump, e teve acesso inapropriado aos dados de mais de 50 milhões de usuários dessa rede social.

Essas notícias geram problemas sistêmicos com o modelo de negócios da empresa, e criam cada vez mais desafios para os Estados nacionais, quanto a regulação mais profunda das redes sociais, a fim de proteger e zelar pelos direitos de privacidade de seus cidadãos.

O presidente e fundador da empresa Mark Zuckerberg, disse acreditar que a consultoria Cambridge Analytica tenha obtido indevidamente os dados de 87 milhões de usuários, dentre os quais 443.117 são brasileiros, e a maior parte dos usuários está nos Estados Unidos. O número total admitido pela empresa é maior do que as estimativas iniciais de 50 milhões. A informação está em um texto assinado por seu diretor de tecnologia Mike Schroepfer, em uma seção no site da própria empresa sobre as medidas que a mesma vem tomando para restringir o acesso de aplicativos e outras companhias aos dados de mais de seus 2,2 bilhões de membros no mundo.

O método usado pela empresa Cambridge Analytica, que é baseada no Reino Unido, para obter os dados desses usuários, foi um teste de personalidade, que não só obtinham

informações destes, como também as de seus amigos na plataforma, sem obter nenhum tipo de permissão para isso. A empresa é acusada de ter usado as informações coletadas para influenciar no pleito.

5.2 Dados obtidos através de aplicativos

Segundo Vásquez (2018), muitos aplicativos usados pelo Facebook, que a primeiro momento parecem ser simples brincadeiras, com as quais não deveríamos nos preocupar muito, e que prometem revelar coisas do tipo: “A que pessoa famosa você se parece?”, “Quem você foi numa vida passada?”, ou “Como você seria se fosse do sexo oposto?” ou ainda “ Quem é seu melhor amigo?”. O que muitas vezes não é percebido pelo usuário é que: para se ter acesso e o resultado dos referidos testes, faz-se necessário a aceitação dos termos e condições destes aplicativos, dando acesso as suas informações pessoais como: listas de contato, endereço de e-mail, fotos, lista de amigos e também de terceiros atrelados a seu perfil na plataforma da rede social, ou seja, praticamente todas as informações existentes no Facebook.

Figura 6 - Layout de um teste de aplicativo do Facebook.

Fonte: Google Imagens.

Vale-se ressaltar que nos contratos de condições dos aplicativos, muitas vezes é dito de forma explícita, que estas informações poderão ser vendidas a terceiros ou empresas, sem especificarem os fins, o que demonstra, de forma geral, a falta de mentalidade de segurança e zelo por seus dados compartilhados na rede, por parte dos usuários. Ao concordar com tal, suas preferências poderão ser vendidas para empresas de publicidade, ou suas fotos, de seus amigos e familiares, serem usadas em campanhas publicitárias .E ainda pior que isso, muitas vezes

esses aplicativos podem criar uma porta aberta, para que alguém intercepte seu computador ou celular e instalem algum tipo de vírus.

5.2.1 Dados pessoais armazenados no Facebook

Muitos desses dados utilizados de forma indevida, ficam armazenados na própria plataforma do Facebook, podendo serem utilizados tanto por busca direta em seu perfil pessoal, por um agente adverso que tenha interesse nessas informações, como por aplicativos vistos no tópico anterior, que utilizando-se da autorização dada pelo usuário no termo de condições, e obtém livre acesso a estes dados armazenados, podendo inclusive fornecê-los a terceiros.

O que não é conhecido pela maioria das pessoas, é que é possível saber o quanto de informações que essa Rede Social mantém armazenada de uma determinada pessoa, sendo inclusive possível baixar uma cópia destes dados para análise, algumas das informações que ficam disponíveis na plataforma, podem ser vistas a seguir no quadro 3:

Quadro 2 - Informações pessoais armazenadas no Facebook.

1) Publicações	8) Mensagens
2) Fotos e Vídeos	9) Grupos
3) Comentários	10) Eventos
4) Curtidas e reações	11) Informações do perfil
5) Amigos	12) Páginas
6) Histórias	13) Atividades de compras
7) Pessoas seguidas e seguidores	14) Localizações

Fonte: Site do Facebook com adaptação própria

Para isso basta entrar no menu em configurações, em seguida no ícone com o logotipo da marca “suas informações no Facebook”, e depois finalmente clicar em baixar suas informações. Conforme pode ser ilustrado na figura a seguir:

Figura 7 - Ilustração da página de download de dados pessoais

Fonte: Site do Facebook

Depois de se fazer o download, se obtém um arquivo comprimido na ordem de grandeza de algumas dezenas de Megabytes, onde se obtém vários tipos de informação, divididas em diversas pastas

Cada pasta possui um determinado tipo de informação pessoal, por exemplo na pasta "*about you*" é possível obter todos os endereços de e-mail dos contatos da pessoa em questão, assim como seus respectivos números de telefone. Muitas informações podem ser obtidas como: Histórico de pesquisas, itens salvos, informações do perfil, acesso a fotos e vídeos, histórico de pagamentos digitais realizados, reações, grupos e contato de amigos, dentre muitas outras.

Outro exemplo que pode ser usado para exemplificar a grande quantidade de dados sensíveis armazenados, é a pasta "location" que armazena as coordenadas geográficas exatas (latitude, longitude) enviadas pelo dispositivo que fez o *login* na plataforma, inclusive sendo possível também indicar o tipo/modelo desse dispositivo, como também os endereços IP utilizados na conexão.

Sendo assim, pode-se concluir que o Facebook é uma grande fonte de dados pessoais que ficam armazenados na plataforma, sendo assim, uma ótima opção para se obter informações sobre um indivíduo pelo qual se tenha algum interesse em particular em se analisar.

6 ENGENHARIA SOCIAL

De acordo com Mitinic (1963), A Engenharia Social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não é. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem o uso da tecnologia. Com consequência, é possível desenvolver ações de convencimento ou manipulação para influenciar pessoas a realizarem atos que normalmente não fariam para um desconhecido. Em contrapartida, a Marinha do Brasil define a Engenharia Social da seguinte forma:

> A Engenharia Social corresponde ao conjunto de técnicas para se obter ou comprometer informações sobre uma organização ou seus sistemas computacionais, utilizando-se como ferramenta de ataque a interação humana ou as habilidades e fragilidades sociais do ser humano. A Engenharia Social deve ser tratada por todos da OM como uma ameaça à SIC, onde toda informação sobre as características da OM e de sua rede local é considerada sigilosa, exigindo o tratamento adequado de segurança. Para minimizar a probabilidade de estranhos à OM obterem sucesso na aplicação de tais técnicas pelos meios de comunicação disponíveis, devem ser seguidas, no mínimo, as seguintes orientações:
> a) não passar informações de nomes, telefones e outras informações pessoais de qualquer servidor civil ou militar da OM;
> b) não confirmar a estranhos a existência de determinada pessoa na OM;
> c) não atender uma chamada telefônica, não se identificar sem que antes o interlocutor, que efetuou a ligação, tenha se identificado;
> d) não passar a estranhos nenhuma informação sobre os sistemas utilizados na rede local, tais como: sistemas operacionais, aplicativos, serviços disponibilizados, endereços de rede, computadores, roteadores, servidores, localizações físicas, topologia da rede, sistemas de segurança, entre outros; e
> e) não passar a estranhos informações a respeito da rotina e dos procedimentos internos da OM. (MARINHA DO BRASIL, 2019, P.-9-21-)

Com a popularização do uso dos sites de redes sociais, praticamente todos os integrantes de Organizações Militares possuem uma conta ativa nestas plataformas. Diante da exposição de informações, um elemento adverso interessado em obter informações sensíveis de determinada OM, ou da instituição como um todo, pode utilizar técnicas de Engenharia Social para a obtenção de tais dados, tanto estudando o perfil do alvo como coletando informações compartilhadas de forma aberta. Com base nas informações reunidas é possível a elaboração de "histórias de cobertura" que possam dar respaldo ao elemento adverso na busca dessas informações, gerando, muitas vezes, a empatia e vontade de ser útil no elemento vítima deste ataque de Engenharia Social, como afirma KLEIN, 2019:

> A engenharia social atua sobre a inclinação natural das pessoas de confiar umas nas outras e de querer ajudar. Nem sempre, a intenção precisa ser de ajuda ou de confiança. Pelo contrário, pode ser por senso de curiosidade, desafio,

> vingança, insatisfação, diversão, descuido, destruição, entre outros. (KLEIN, 2004, P.9)

É importante destacar que o sucesso no ataque de engenharia social ocorre, geralmente, quando os alvos são pessoas ingênuas ou aquelas que simplesmente desconhecem as melhores práticas de segurança. (FERREIRA & ARAÚJO, 2006, P. 92).

Tendo em vista que em sites de redes sociais é muito difícil se ter um processo que certifique a autenticidade de uma pessoa ser quem realmente diz ser, o ideal é evitar diálogos que envolvam qualquer informação sensível, pois não se pode confiar na veracidade das informações proferidas.

O aconselhável é não utilizar as redes sociais para fornecer nenhum tipo de informação que possa comprometer a instituição, seja por postagens deliberadas utilizando conteúdo que possa ser de interesse da instituição que seja mantido em sigilo e desconfiar de abordagens de quaisquer elementos, conhecidos ou não, em tentar obter qualquer tipo de informação sensível neste meio.

Uma recomendação para evitar-se o compartilhamento de informações não autorizadas e a propagação de possíveis "*fakenews*", é compartilhar informações e conteúdo, que foram postados pelo próprio perfil oficial da Marinha nas diversas redes sociais. Desta forma, o militar consegue expressar o seu orgulho em fazer parte da instituição, divulgando para a sociedade as atividades desenvolvidas pela Marinha do Brasil, tendo a certeza de que aquele conteúdo foi aprovado por quem de direito para ser divulgado, evitando o uso indevido do nome da instituição e de conteúdo pertencente a esta, o que pode acarretar danos à imagem institucional e aos interesses desta. O uso e a administração do perfil oficial da Marinha do Brasil nas diversas redes sociais, é normatizado em publicação própria:

> **Instruções de Uso Institucional de Mídias e Redes Sociais pela MB**
>
> a) O CCSM é a única OM autorizada a administrar perfis institucionais da MB nas mídias sociais, sendo seu Diretor o Administrador de Perfil Institucional da MB.
> b) O CCSM deverá nomear, por Ordem de Serviço, os Agentes Responsáveis pelo registro, controle, revisão, aprovação de conteúdo e monitoramento de todos os perfis institucionais da MB nas mídias sociais;
> c) O CCSM deverá expedir uma Ordem Interna sobre uso seguro das mídias sociais, a fim de estabelecer os procedimentos internos e regular a atuação dos Agentes Responsáveis designados, em consonância com esta instrução e as normas;
> d) A criação de novos perfis institucionais da MB será proposta pelo CCSM e autorizada pelo Comandante da Marinha;

> e) O CCSM poderá criar perfis para tratar sobre temas específicos da MB. Nesses casos, poderá, a seu critério, delegar a gestão de conteúdo e a interação com o público para a OM detentora de competência técnica sobre o tema. O perfil deverá ser configurado de forma a que o CCSM mantenha direitos administrativos plenos sobre o mesmo e a OM delegada deverá designar o(s) Agente(s) Responsável(is).
> f) Por questões de Segurança da Informação Digital (SID), informações publicadas em caráter Institucional não podem conter informações sigilosas, o que poderia colocar em risco o pessoal ou as operações da MB. (MARINHA DO BRASIL, 2015, P.2)

A manutenção de um perfil oficial da Marinha do Brasil nas principais redes sociais, além dos inúmeros benefícios de fornecer informação de qualidade sobre a força, para toda a sociedade, aumentando assim o prestígio da instituição e mostrando a importância de todas as atividades de rotina, para a soberania nacional e também demonstrando as outras funções subsidiárias e de apoio social, não menos importantes, ainda tem a característica de evitar ações de desinformação contra a força e seus membros, que possam ser tomadas, abalando a confiança e o respeito pela instituição.

Na figura a seguir, é mostrado um exemplo do uso do perfil oficial da Marinha, para divulgar suas ações de rotina, e que promovem o conhecimento destas pela sociedade em geral, aumentando-se o respeito e a admiração pela instituição.

Figura 8- Divulgação de ação de rotina da Marinha do Brasil.

Fonte: Site do Facebook

Ao acontecer qualquer incidente com os meios navais ou com o pessoal pertencente a instituição, tem-se a oportunidade de dar esta notícia em primeira mão, criando-se assim uma relação de confiança e presença junto a sociedade e, evitando-se assim distorções e desinformação sobre esses incidentes que podem chegar ao público pela grande mídia causando sérios danos à imagem institucional.

Aconselha-se também a todo membro da instituição que ao se deparar com qualquer desinformação que envolva a boa reputação da força e seus membros, que compartilhe as informações verídicas e o posicionamento oficial da Marinha do Brasil proveniente de suas contas oficiais nas redes sociais.

Todo membro da instituição deve se sentir como um "embaixador" da Marinha do Brasil, zelando pelas informações verídicas e conteúdo oficial, verificando, e combatendo qualquer tipo de desinformação ou qualquer outra ação de efeito danoso nas redes sociais que possam denegrir a imagem da instituição.

6.1 OSINT

Segundo Souza (2019), OSINT (*Open Source Intelligence*) é um modelo de inteligência que visa encontrar, selecionar e adquirir informações de fontes públicas e analisá-las para que junto com outras fontes possam produzir um conhecimento. Na comunidade de inteligência, o termo "aberto" refere-se a fontes disponíveis publicamente. Este modelo é também usado pelos serviços secretos de muitos países.

Analistas de Inteligência Competitiva e jornalistas investigativos se valem dessas fontes de Inteligência justamente porque, além de eficazes, não representam crimes nem tampouco infração de ordem ética.

6.2 Utilizando as Redes Sociais para se obter dados abertos (OSINT) sobre a Instituição e seus membros

As redes sociais mudaram a forma como as pessoas se relacionam no mundo moderno e, por estarem presentes em cada momento do dia a dia, acabam sendo uma fonte inesgotável de informações sobre a vida, o trabalho, os vínculos afetivos, e praticamente, sobre toda a vida de um indivíduo. Logo, uma pessoa inclinada a levantar informações sobre um terceiro ou instituição, a que este pertence, não teria muito trabalho para obter as informações de que necessita, visto que estão em sua maioria publicadas em redes sociais de forma pública.

Nos quadros abaixo seguem informações que podem ser coletadas tanto da área Pessoal como Profissional:

Quadro 3 - Informações pessoais que podem ser coletadas pelas Redes Sociais.

ÁREA PESSOAL
1) É casado?
2) Tem filhos?
3) Onde vive?
4) Onde Estudou?
5) Quais locais frequenta?
6) Viaja com frequência?
7) Onde os filhos estudam?
8) Onde o cônjuge trabalha?
9) Quem são seus melhores amigos?
10) Quais as formas de lazer preferidas?
11) Consome bebidas alcoólicas?
12) Locais onde já morou?
13) É religioso?
14) Tem animais de estimação?
15) Fala outros idiomas?
16) Torce para alguma equipe?
17) Prática algum esporte?
18) Qual o seu posicionamento político?

Fonte: Autoria própria.

Quadro 4 - Informações profissionais que podem ser coletadas pelas Redes Sociais.

ÁREA PROFISSIONAL
1) Em que OM serve?
2) A quanto tempo serve na mesma OM?
3) Em quais OM já serviu?
4) É possível identificar outros membros da OM?
5) É possível identificar a localização da OM e outros meios navais?
6) Revela o acontecimento de missões sigilosas?
7) Revela a derrota e planejamento de comissões?
8) Revela a capacidade de algum meio naval?
9) Revela a situação operativa de algum meio naval?
10) Revela o domínio de uma capacidade profissional sensível?
11) Demonstra aspirações e interesses profissionais na carreira?
12) Revela a frequência de operações de um meio?
13) Revela atividades não apropriadas no meio profissional?
14) Revela que o militar está de serviço em algum meio?

Fonte: Autoria própria.

7 EXPERIMENTO PRÁTICO DE ENGENHARIA SOCIAL

Através de uma conta na rede social Facebook, foi feito um experimento prático de se acessar diversos perfis particulares de militares pertencentes a MB em busca de dados abertos, e verificar a possibilidade de responder a todas essas analisando o conteúdo disponível. Seja na análise da descrição do perfil ou em conteúdo compartilhado ao longo do tempo armazenado na rede.

No experimento foram analisados 50 (cinquenta) perfis de militares, e se utilizou como recurso de busca, *hashtags* relacionadas com a Marinha do Brasil, como por exemplo, as mostradas no quadro 4 a seguir:

Quadro 5 - Hashtags utilizadas para fazer a busca.

#marinha	#marinhadobrasil

Fonte: Autoria própria.

Sendo assim, não é necessário ser amigo do perfil analisado na plataforma para conseguir visualizar as informações disponíveis publicamente. Mas utilizando um perfil que possua vínculos de amizade com militares da Marinha, estes perfis aparecerão primeiro nas buscas, e em seguida os perfis sem nenhum vínculo.

7.1 Informações Pessoais

Basicamente, foi possível responder a todas as perguntas apresentadas no quadro relativo à área pessoal, sem longos esforços. Em alguns perfis, sem utilizar o recurso de ser amigo da pessoa estudada na plataforma em questão, nem todas as informações estavam disponíveis no perfil. Por outro lado, analisando os perfis propostos tendo algum tipo de relação de amizade dentro da rede social estudada, todas as informações estavam disponíveis sem qualquer tipo de restrição. Contudo, alguns perfis ainda não apresentavam a totalidade das informações buscadas, tendo em vista o detentor do perfil não ter disponibilizado esse dado. Alguns exemplos das informações pessoais que podem ser coletadas são mostrados abaixo:

Figura 9- Informações disponíveis no perfil

Fonte: Site do Facebook.

Essas são informações gerais que ficam disponíveis no perfil de um determinado usuário no Facebook, e que permitem fazer uma busca mais detalhada em vários temas pertinentes a vida pessoal de um determinado militar, como por exemplo, as instituições em que estudou, locais onde morou, membros da família e status de relacionamento.

Figura 10- Layout de como as informações pessoais são apresentadas no perfil.

Fonte: Site do Facebook.

Na imagem acima é exposto um exemplo de como essas informações são expostas no perfil pessoal do usuário.

7.2 Informações Profissionais

Foi utilizado o mesmo método de coleta anterior, para tentar responder as perguntas pertinentes a área profissional. Em geral percebe-se uma cautela maior no compartilhamento dos dados profissionais, não sendo possível responder a todas as perguntas propostas no quadro de questões relativas a essa área. Mas algumas condutas tiveram uma incidência maior, como por exemplo, a indicação no campo profissional, da pessoa pertencer a "Marinha do Brasil", acredita-se que até por uma questão de status e orgulho pessoal em se fazer parte da instituição, esta informação é compartilhada de forma aberta nos perfis pela maioria dos militares.

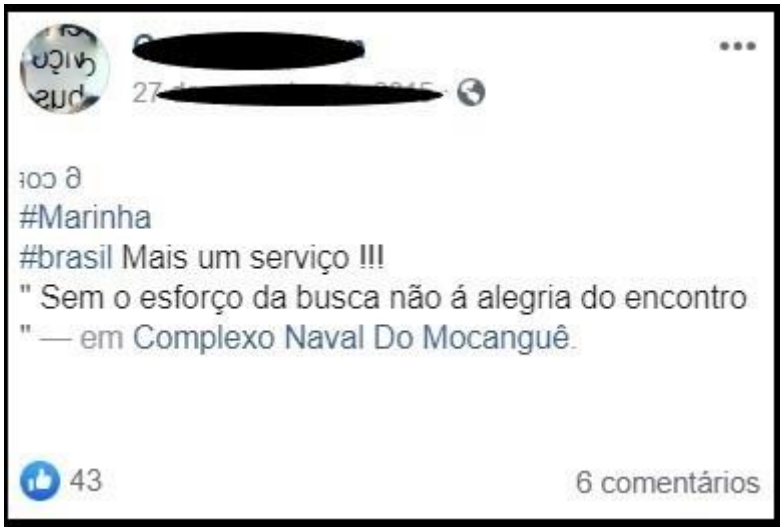
Outra conduta que facilmente identifica os militares como membros da instituição, é o compartilhamento de fotos utilizando uniformes e participando de eventos militares. Também é comum o militar se identificar como membro de uma determinada OM, seja utilizando-se de *hashtags* na marcação de suas fotos com o nome da organização militar, ou quando participa de confraternizações, como por exemplo, as que ocorrem no final de ano, marcando outros membros da OM nas fotos, o que permite identificar a outros integrantes da OM.

Outra prática corriqueira, é o militar se identificar como pertencente a determinadas missões, sobretudo as de maior importância e que supostamente geram uma maior satisfação profissional e orgulho, podemos citar como um dos maiores exemplos: A missão de paz da UNIFIL, que acontece já há algum tempo com a participação do Brasil, que mantém um meio naval permanente na região. Mas outras comissões também são compartilhadas como a "Operação Dragão", "Misselex" e "Aspirantex", dentre outras.

Mas em relação a todas as perguntas apresentadas no quadro, uma que teve grande incidência foi a que o militar revela estar de serviço em uma determinada OM, inclusive fazendo o check-in na plataforma com sua localização.

Alguns exemplos de informações coletadas no experimento são mostrados nas figuras abaixo, com os perfis sendo devidamente descaracterizados, a fim de que seja mantido o sigilo sem a exposição dos militares que participaram do experimento.

Figura 11 - Informação que revela que um militar está entrando de serviço numa determinada OM.



Fonte: Site do Facebook.

Figura 12 - Informação que revela a OM em que serve o militar e seu trajeto pessoal.

Fonte: Site do Facebook.

Figura 13 - Informação que revela a rotina do militar.

Fonte: Site do Facebook.

7.3 Considerações sobre o experimento:

Percebe-se que os militares costumam deixar as suas informações relacionadas a área pessoal, abertas e expostas nas redes sociais. Sendo estas informações de grande valia, nas mãos de um engenheiro social, possibilitando até a criação de uma possível história de cobertura, para tentar alguma interação com a vítima na busca de dados sensíveis. Para um engenheiro social com maiores habilidades, este requisito pode ser cumprido com facilidade. Por exemplo, clonando o perfil de algum amigo real da vítima, e lhe enviando um convite de amizade com a foto de uma pessoa conhecida desta, ou simplesmente, criando um perfil com a foto de uma pessoa atraente do sexo oposto. Tais ações visam o convencimento da vítima em aceitar o pedido de amizade e, por fim, permitir o acesso privilegiado a informações restritas.

Em relação aos dados atinentes a área profissional, percebeu-se uma maior cautela, quanto ao compartilhamento de informações, mas houve também informações expostas.

Uma das condutas mais comuns, foram os militares revelaram estarem de serviço numa determinada OM. A conduta que a princípio parece ser simples e não gerar nenhum tipo de perigo em um primeiro momento, pode ser crítica e trazer complicações tanto para segurança pessoal do militar e de sua família, como para segurança da Instituição. Por exemplo, ao saber que um militar está de serviço, ao se conhecer um pouco da rotina das OM, logo pode-se concluir que este estará longe de seu lar por um período aproximado de 24 horas, abrindo caminho para um agente subversivo mal intencionado, que esteja pensando em assaltar a casa deste militar, ou então atentar contra algum membro de sua família.

No que diz respeito a segurança da instituição, mais especificamente de uma organização militar qualquer, saber que certo militar está de serviço, pode incentivar alguma ação adversa por um elemento. Por exemplo, se um militar é conhecido por ser displicente em serviço e não cumprir de forma eficaz os procedimentos de segurança orgânica. Assim seria um momento oportuno de uma pessoa que conhece a rotina da OM, tentar uma invasão, roubo de equipamentos, informações sigilosas, ou praticar qualquer outro ato danoso.

8 TÉCNICAS DE ANÁLISES DE DADOS APLICADAS A POSTAGENS DO *TWITTER*

Existem diversas ferramentas desenvolvidas para realizar a mineração de dados em redes sociais, utilizando-se de técnicas distintas, que coletam os dados postados na rede pelos usuários, para de alguma forma, tentar estruturá-los para se gerar algum tipo de informação útil, após um processo de análise.

Essas aplicações que oferecem este tipo de serviço, utilizam-se de algoritmos de inteligência artificial, que permitem relacionar dados similares e agrupá-los por grupos de interesse. Por exemplo, técnicas que se utilizam do texto de autoria dos usuários para prever as características do indivíduo medida pelas dimensões da personalidade do Big-5: Abertura, Consciência, Extroversão, Agradabilidade, Neuroticismo. Com centenas de milhões de usuários participando de mídias sociais e compartilhando conteúdo de autoria própria, as mídias sociais oferecem uma tremenda oportunidade para modelagem de personalidade. (MCCRAE,1992).

A maioria dos métodos de modelos de personalidade, requerem textos muito grandes, o que dificultariam o seu uso em cenários da vida real, onde a maioria dos usuários possuem pequenas quantidades de textos para análise, como nas usuais postagens do Twitter. Mas alguns métodos como o de Incorporação de palavras com processos gaussianos, desenvolvido por Arnoux, são capazes de modelar a personalidade de um usuário, usando textos de tamanho bem menores. (ARNOUX, 2017, P.472).

Uma ferramenta muito utilizada por sua facilidade e interface amigável, sem a necessidade de aprofundar-se em questões técnicas, é o IBM *Watson Personality Insights*. Esta plataforma permite obter dados e informações das mídias sociais, dados corporativos ou outras comunicações digitais.

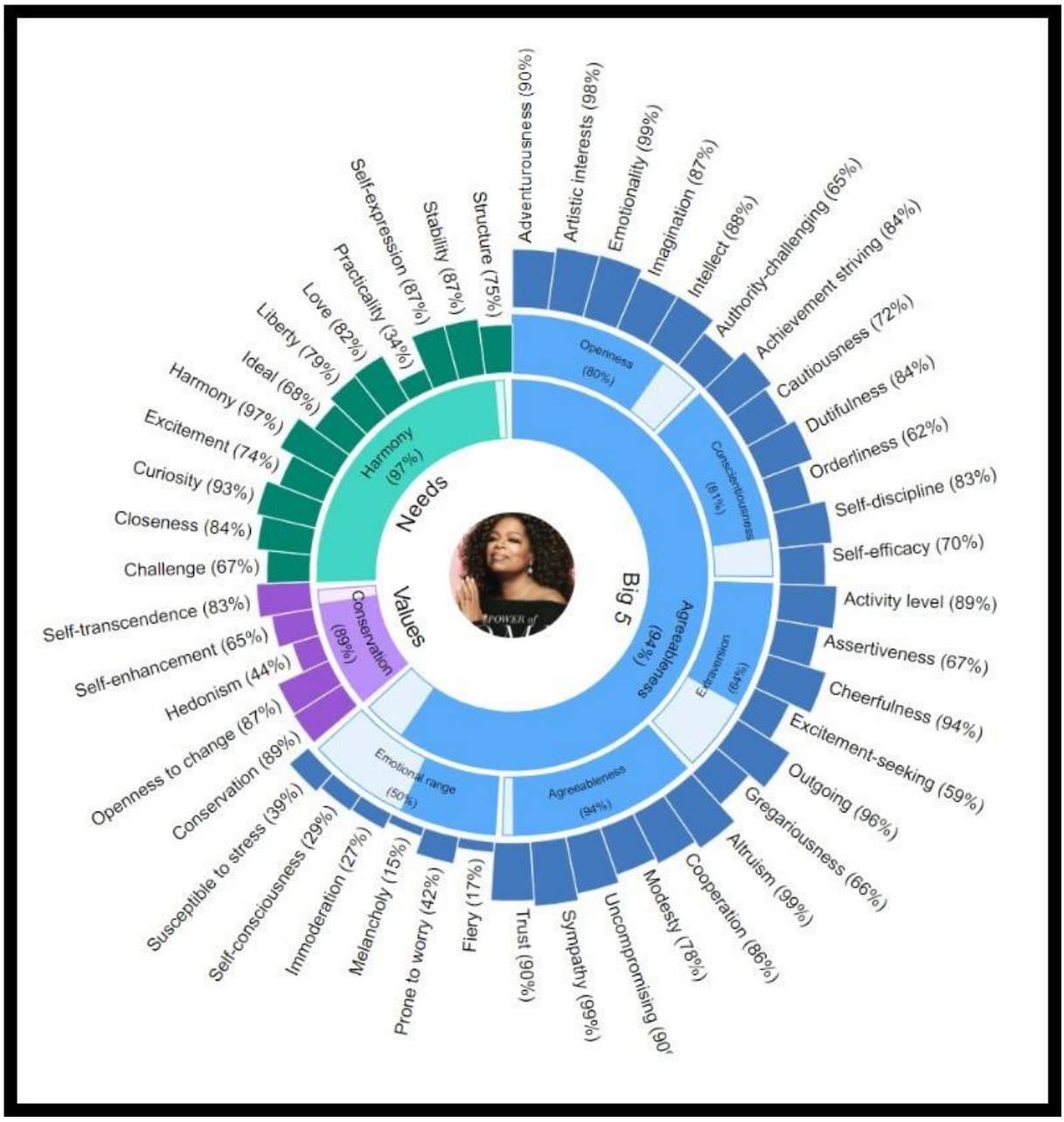
Esse serviço usa uma análise linguística para inferir as características intrínsecas da personalidade dos indivíduos incluindo o *Big Five,* como também as necessidades e valores dos indivíduos estudados, a partir de suas comunicações digitais nas redes, como e-mail, mensagens de texto, tweets e mensagens em fóruns. (IBM CLOUD, 2019)

Além disso de acordo com Pakzad (2019), o Personality Insights pode demonstrar ainda as características de consumo de uma pessoa e o comportamento temporal desta (Se o texto de entrada estiver com informações de data e hora)

Na figura abaixo temos um resultado de um teste utilizando a ferramenta *Personality Insights* da IBM, onde são mostradas as porcentagens de cada área da personalidade que compõe o *Big Five,* assim como as características que formam cada subárea, também com as

respectivas porcentagens para um determinado usuário, como também as necessidades e valores deste.

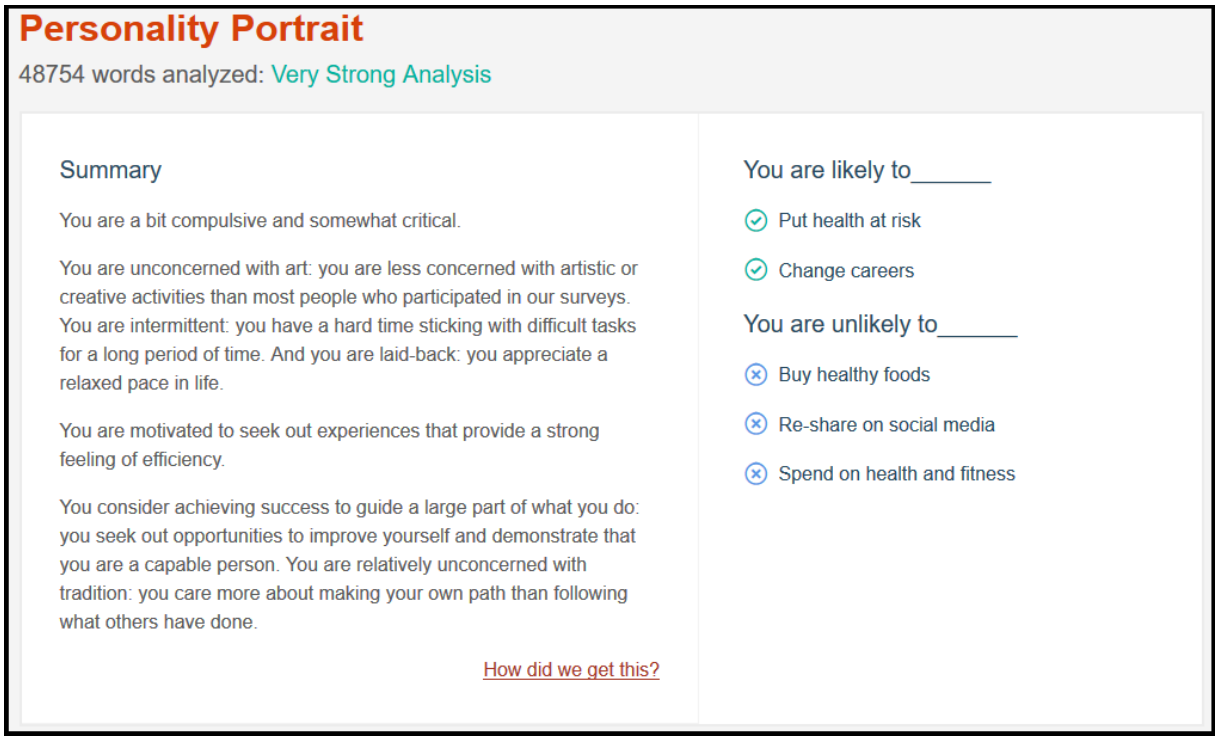
Figura 14 - Resultado de um teste utilizando a ferramenta Personality Insights com postagens de uma conta do Twitter.



Fonte: Site Medium

Ainda é possível com o resultado do mesmo teste, desenvolver um “retrato da personalidade” do usuário, que consiste em um pequeno relatório sobre as supostas características da personalidade que foram descobertas através das amostras de texto analisados pela ferramenta.

Figura 15- "Retrato da personalidade" do usuário analisado.

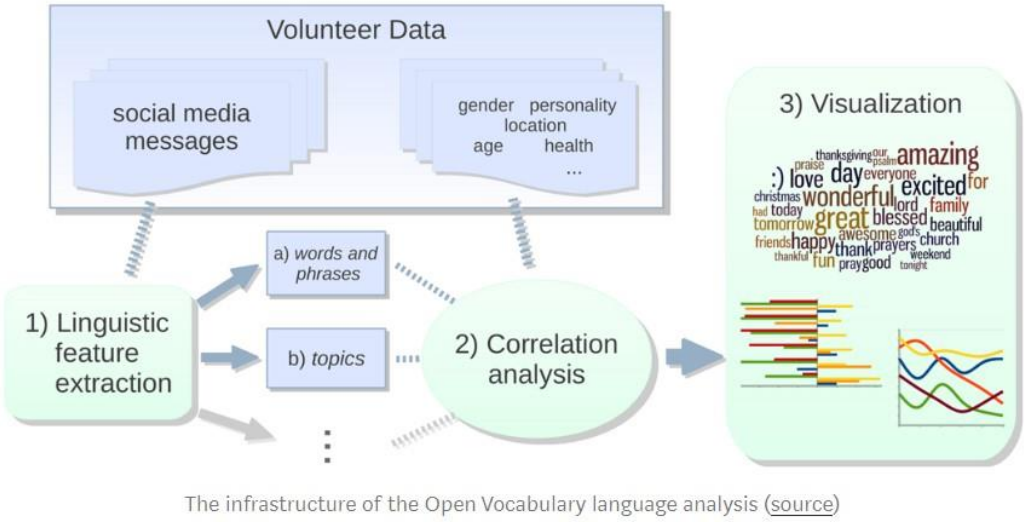


Fonte: Site Medium

Esse método denominado, "Abordagem de vocabulário aberto" foi desenvolvido por pesquisadores da Universidade da Pensilvânia que analisaram o status do Facebook de 75.000 usuários voluntários. Com base nessa análise e nos questionários de personalidade que os acompanham, eles construíram modelos para prever a idade, gênero e personalidade de um indivíduo. (PAKZAD ,2019).

Na figura 15 é mostrado um diagrama simplificado de como esse método funciona. Mensagens de usuários voluntários são coletados nas redes sociais, depois são feitas extrações das características linguísticas desses textos, analisando palavras e frases e os assuntos correspondentes, em seguida é feita uma análise de correlação com outros dados e por fim é possível a atribuição de sentimentos e diferentes estados de ânimo com relação aos textos analisados.

Figura 16 - Modelo de análise do método de “Abordagem de vocabulário aberto”



Fonte: Site Medium

A linguagem é a maneira mais comum e confiável das pessoas traduzirem seus pensamentos e emoções internas de uma forma que outras pessoas possam entender. Palavras e linguagem, então, são o próprio material da psicologia e da comunicação. (TAUSCZIK, 2010)

9 GUIA PRÁTICO DAS BOAS PRÁTICAS NAS REDES SOCIAIS.

Após constatar-se, o quão sensível pode ser o compartilhamento de dados nas redes sociais, podendo gerar ao usuário que os expõe de forma aberta, muitos problemas não só para sua vida pessoal e de seus familiares, como também para as instituições a que estes pertencem.

E levando-se também em consideração a importância de se estar presente nas redes sociais nos dias de hoje, não só para os indivíduos, mas também para as instituições, devido aos inúmeros benefícios oferecidos por estas, já listados neste trabalho.

Faz-se então necessário elencar proposições que norteiem boas práticas de uso nas redes sociais, que sejam esse ponto de equilíbrio necessário entre o estar presente nestas e evitar exposição em demasia de dados que podem ser sensíveis.

De forma especial nesse trabalho tem-se a preocupação em resguardar e preservar os interesses da Marinha do Brasil, e de seu pessoal, visto que este é um dos maiores patrimônios da instituição, devendo ser protegido e devidamente orientado em cada aspecto crítico que se faça presente. Á vista disso serão propostas ao longo deste capítulo as recomendações, que serão um guia prático de bom uso das redes sociais.

9.1 Compartimentar o acesso as informações publicadas

Um dos maiores problemas ao se compartilhar conteúdo nas redes sociais, é perder o controle de quem efetivamente terá acesso aquela informação. Sem se tomar nenhuma precaução, muitas vezes informações mais intimas e potencialmente sensíveis, poderão ser vistas por amigos, amigos de amigos, e até mesmo pessoas sem nenhum vínculo com o usuário, logo perdendo-se totalmente o controle sobre este ativo tão importante.

Para tentar mitigar um pouco esse efeito, é aconselhável sempre dividir os amigos em cada rede social em grupos distintos, dando diferentes graus de permissão de visualização de conteúdo para cada grupo. Pois é costumeiro que pessoas que não se tem intimidade e, muitas das vezes, apenas conhece o usuário de vista, busquem relações precoces de amizade, contudo não é sensato abrir toda a privacidade perante tais pessoas que nem sequer conhecemos, ou nos relacionamos muito pouco.

No quadro a seguir, segue um exemplo dos diferentes grupos que podem ser criados para um usuário, para criar um filtro que ajude a proteger e a selecionar quem tem acesso ao conteúdo presente no seu perfil.

Quadro 6 – Sugestão de grupos para compartimentar a informação

a) Melhores Amigos	e) Família
b) Amigos	f) Vizinhos
c) Conhecidos	g) Trabalho

Fonte: Autoria própria.

Essa medida muito simples de criar diferentes grupos como: Trabalho, Família, Amigos, Vizinhos e assim sucessivamente, a fim de se limitar e compartimentar o acesso ao conteúdo de suas redes sociais, é uma prática muito eficaz. Isto poderá evitar que pessoas alheias a instituição tenha acesso a dados sobre esta e a sua atividade profissional.

O mecanismo de precaução também protege de forma efetiva a privacidade do indivíduo, pois evita, por exemplo, que um colega de trabalho, que possa ter lhe enviado um convite de amizade nas redes, tenha acesso a sua intimidade.

9.2 Principais Riscos

Como as redes sociais são um espaço público, onde não se tem o total controle sobre as informações e pessoas que poderão acessá-las, existem alguns riscos ao usá-las e conhecê-los é de importância fundamental para que um usuário tome medidas pertinentes para minimizar os danos que podem ser gerados por esses riscos.

A seguir seguem algumas informações sobre possíveis riscos no uso das redes sociais:

Quadro 7 – Principais Riscos nas redes sociais

Invasão de perfil: seu perfil pode ser invadido por meio de ataques de força bruta, do acesso a páginas falsas ou do uso de computadores infectados.
Uso indevido de informações: aquilo que você divulga pode vir a ser mal interpretado e usado contra você.
Invasão de privacidade: quanto maior a sua rede de contatos, maior é o número de pessoas que possui acesso ao que você divulga, e menores são as garantias de que suas informações não serão repassadas.
Recebimento de mensagens maliciosas: alguém pode lhe enviar uma mensagem contendo boatos ou induzi-lo a clicar em um link que o fará instalar um código malicioso ou acessar uma página Web comprometida.

Acesso a conteúdos impróprios ou ofensivos: como não há um controle imediato sobre o que as pessoas divulgam, pode ocorrer de você se deparar com mensagens ou imagens que contenham pornografia, violência ou que incitem o ódio e o racismo.
Danos à imagem e à reputação: calúnia e difamação podem rapidamente se propagar, jamais serem excluídas e causarem grandes danos às pessoas envolvidas.
Contato com pessoas mal-intencionadas: qualquer um pode criar um perfil falso e, sem que saiba, você pode ter na sua lista de contatos pessoas com as quais jamais se relacionaria no dia a dia.
Furto de identidade: assim como você pode ter um impostor na sua lista de contatos, também pode acontecer de alguém tentar se passar por você e criar um perfil falso.

Fonte: Cartilha de segurança para internet fascículo Redes Sociais de CERT.br adaptação própria

9.3 O que fazer para se prevenir?

Ao se saber dos riscos principais e dos perigos que o usuário se expõe ao estar com uma conta ativa nas redes sociais, é pertinente tomar-se algumas medidas de prevenção, que são cuidados que podem minimizar esses riscos, tornando o uso destas mais seguro. A seguir são apresentadas algumas dessas medidas que podem ser adotadas. A Marinha do Brasil possui uma publicação com instruções sobre o uso das redes sociais. Nesta publicação existe um tópico com instruções específicas de uso não institucional de mídias e redes sociais pelo pessoal da MB, como pode-se ver no extrato abaixo:

> **Instruções de Uso Não Institucional de Mídias e Redes Sociais pelo pessoal da MB**
>
> Reconhece-se a importância do uso das mídias e redes sociais, mas alerta-se para a observância dos aspectos descritos a seguir, a fim de evitar possíveis comprometimentos da SID das OM, da segurança física do pessoal da MB e da RECIM. Um dos principais reflexos das redes sociais é o alcance da veiculação de comentários, fotos e vídeos. Neste ponto é importante ressaltar que o comportamento nas redes sociais deve ser compatível com o esperado, tal como se fossem ambientes sociais, valorizando a atividade militar e as tradições marinheiras. Desta forma, destacam-se as seguintes instruções para o uso não institucional adequado nas redes e mídias sociais:
>
> a) É proibida a divulgação de informações sigilosas, documentos internos, informações pessoais, ou qualquer tipo de informação que possa comprometer a Instituição. Quando em dúvida, o autor da publicação deverá consultar o respectivo Titular da OM, respeitando a cadeia hierárquica;
>
> b) As opiniões pessoais dos militares e servidores civis das OM da MB devem ser feitas de forma responsável,

obedecendo às normas e regulamentos em vigor, mesmo quando manifestando opinião pessoal;

c) Depois de o conteúdo ser publicado na Internet, perde-se seu controle. É possível, porém, a solicitação ao Poder Judiciário para a retirada do conteúdo disponibilizado na internet que afete à honra, à reputação ou a direitos de personalidade, nos termos do art. 19 e, que trata do Marco Civil da Internet;

d) O autor das publicações deverá deixar claro que as mesmas refletem sua opinião particular e não a posição Institucional da MB, tendo cuidado para não expor negativamente a imagem da Força;

e) O autor deverá fornecer seu e-mail pessoal e não o profissional ("OM.mar.mil.br") para contatos com pessoas interessadas em dar continuidade a discussões e assuntos particulares. Comunicações particulares devem ser feitas por e-mails particulares e não pelo endereço eletrônico da MB, o qual deve ser utilizado exclusivamente para assuntos de serviço;

f) Como em qualquer outra forma de comunicação, todas as normas e regulamentos de conduta e comportamento permanecem válidas no ambiente virtual da Internet. Violações poderão ser investigadas e julgadas apropriadamente, podendo resultar em consequências disciplinares.

g) Estar ciente de que a Internet é com frequência utilizada como fonte de informações que podem ser usadas em atividades criminosas. A fim de evitar este tipo de problema, ressalta-se a necessidade de observar as instruções de segurança das normas em vigor e o cuidado em evitar a disseminação de falsas informações sobre a MB;

h) Criar o hábito de rever suas contas periodicamente a fim de verificar mudanças indesejáveis ou uso indevido por pessoas não autorizadas (senha comprometida);

i) Ter cuidado no uso de aplicações de terceiros, comuns em redes sociais. Estas aplicações são famosas por apresentar problemas de segurança e de buscar acesso às informações pessoais de seus usuários;

j) Adicionalmente, o conteúdo das publicações deverá atender aos seguintes aspectos:

- não disseminar boatos; - não ofender as Forças Armadas;

- não ofender a honra de outra pessoa; e

- não desrespeitar qualquer um dos símbolos nacionais;

k) Orientações gerais aos usuários, a fim de aprimorar sua segurança pessoal e de seus familiares:

- considerar a privacidade em redes sociais como se estivesse em local público;

- ser cauteloso ao fornecer a localização geográfica;

- respeitar a privacidade alheia, evitando divulgar, sem autorização, imagens em que outras pessoas apareçam;

- proteger o perfil por meio de emprego de senhas fortes;

- proteger a vida profissional, avaliando se uma informação publicada pode afetar a si próprio ou a terceiros perante um processo de seleção; e

> - proteger a família por meio de conscientização dos familiares dos riscos envolvidos no uso das redes sociais. (MARINHA DO BRASIL, 2015, P.3)

De forma geral, podemos dizer ao analisar as recomendações que não deve haver nenhum tipo de distinção entre o relacionamento mantido nas redes sociais, para as relações mantidas em qualquer outro local público pelos membros da força. Sendo assim, como em qualquer outro local público, recomenda-se manter descrição sobre tudo que é dito e divulgado, sobretudo assuntos sigilosos e sensíveis, como estes não devem ser tratados no neste âmbito, não deverão assim estar presentes neste ambiente que se equipara a tal.

Deve-se manter ainda nestas redes os mesmos aspectos de conduta esperados de um membro da Marinha do Brasil, pois todas as normas e regulamentos de conduta e comportamento continuam válidos neste ambiente, podendo o militar ser punido pela via disciplinar, se qualquer excesso chegar ao conhecimento de alguma autoridade que faça cumprir o que está previsto.

Por exemplo, se um militar for insubordinado ou faltar com o respeito a algum superior hierárquico nas redes sociais, este deverá ser punido da mesma forma que o seria no trato convencional nas OM.

Cabe ainda fazer algumas recomendações para minimizar os riscos ao se fazer uso das redes sociais, como aconselha o CERT.br:

Quadro 8- Cuidados a serem tomados para minimizar riscos nas redes sociais.

• Acesse o site da rede social sempre usando conexão segura (HTTPS)
• **Seja cuidadoso ao usar e ao elaborar as suas senhas** ➢ Use senhas longas, compostas de diferentes tipos de caracteres ➢ Não use dados pessoais, como nome, sobrenome e datas ➢ Evite usar a mesma senha para acessar diferentes sites
• Habilite a notificação de login e a verificação em duas etapas, sempre que estes recursos estiverem disponíveis
• Evite cadastrar perguntas de segurança que possam ser facilmente descobertas.
• Procure cadastrar um e-mail de recuperação que você acesse regularmente.
• Solicite o arquivo com suas informações ou verifique o registro de atividades, caso desconfie que seu perfil tenha sido indevidamente usado.
• Use opções como silenciar, bloquear e denunciar, caso identifique abusos.
• Mantenha todos os programas instalados com as versões mais recentes
• Aplique todas as atualizações disponíveis.

• Utilize e mantenha atualizados mecanismos de segurança, como AntiSpam, antivírus e firewall pessoal.
• Desconfie de mensagens recebidas, mesmo que tenham sido enviadas por conhecidos.
• Seja cuidadoso ao acessar links reduzidos ➢ Use complementos que permitam que você expanda o link antes de clicar sobre ele.

Fonte: Cartilha de segurança para internet fascículo Redes Sociais de Cert.br adaptação própria

Algumas outras recomendações para o bom uso das Redes sociais:

Quadro 9- Conselhos e boas práticas nas redes sociais.

• Imagens podem ser copiadas e expostas fora de contexto.
• Tente não responder mensagens públicas quando estiver irritado.
• Você não vai concordar com a opinião de todos, lide com isso.
• Respeite pontos de vista contrários ao seu.
• Qualquer pessoa em qualquer lugar poderá ver as suas postagens.
• Tenha em mente que a internet "não esquece nada", qualquer informação mesmo que apagada posteriormente pode ter sido "printada" e pode ser usada contra você.
• Não compartilhe fotos e informações de outras pessoas sem ter a devida permissão

Fonte: Navy Social Media Handbook adaptação própria.

É importante ressaltar que todas essas boas práticas de conduta servem para resguardar a instituição, seus militares e, consequentemente, seus familiares.

É necessário que o militar aos poucos estimule a mentalidade de segurança adequada, sobretudo aos membros mais próximos de sua família, sobre as peculiaridades de sua atividade profissional, que requer que sejam tomadas medidas adicionais de segurança, se comparadas as demais atividades mais comuns no meio civil**.** Pois de nada adiantará toda essa cautela e cuidado por parte dos militares, se os membros da família revelarem informações sensíveis nas redes sociais. Como, por exemplo, dados de missões sensíveis em que seus familiares estejam a par ou qualquer outra informação, que chegue ao conhecimento destes.

Um conselho que pode ser dado nesse sentido, seria também a compartimentação da informação. Não é necessário que a família dos militares saiba todos os detalhes de sua atividade profissional.

Não revelar certas informações sensíveis além de resguardar estas contra divulgação indevida por descuido ou falta de mentalidade de segurança dos membros da família, também resguardará o militar e seus familiares dos danos que poderão causar essa exposição indevida.

10. CONCLUSÃO

O presente trabalho teve como objetivo gerar uma mentalidade de segurança institucional, que atingisse a todos os membros da Marinha do Brasil, no que se refere a segurança de dados expostos nas redes sociais. Objetivo que foi materializado no capítulo 9, com a confecção do guia prático de boas práticas nas redes sociais, que se propõe a nortear o pessoal da instituição, para um bom uso das redes, otimizando os seus fatores positivos, como divulgar as ações e o bom nome da instituição junto a sociedade, fato que pode ser logrado, por exemplo, ao se compartilhar conteúdo dos perfis oficiais da Marinha, como também minimizando os riscos estudados associados ao uso desprevenido destas.

A metodologia adotada consistiu em revisão bibliográfica de conceitos pertinentes a segurança da informação de forma geral, tanto considerando inicialmente o fator técnico, como no fator humano, onde foi dado um enfoque maior neste trabalho, introduzindo os conceitos de engenharia social, e mostrando como dados expostos nas redes sociais, podem servir de fonte de dados abertos (OSINT), seja para empresas de publicidade ou dos mais variados fins, que podem tirar proveito próprio, de alguma forma ,destas informações, ou por agentes adversos mal intencionados, que podem usá-las para prejudicar tanto o usuário como a instituição.

Visando a prevenção do vazamento de informações e testando até que ponto este grau de exposição é real e poderia ter efeitos danosos a Marinha do Brasil e seus membros, foi feito um experimento de engenharia social, buscando por esses dados abertos na rede social Facebook, onde foram buscadas informações atinentes, tanto da vida pessoal como da vida profissional destes militares. Com o referido experimento foi logrado êxito, demonstrando que realmente essa exposição ocorre, preocupando mais os dados que podem gerar danos a instituição, como a informação de militares de serviço numa determinada OM, sendo uma informação sensível para instituição e conforme foi visto neste estudo, poderia gerar uma série de problemas ao se tornar pública.

Foi visto como os dados coletados pelas redes sociais, podem ser usados em ferramentas que trabalham com algoritmos de inteligência artificial, para de maneira adequada, estruturar estes dados e agrupá-los de tal forma que se consiga predizer características, por exemplo, sobre aspectos da personalidade de um determinado usuário.

Uma sugestão que se julga pertinente para a instituição, caso não haja ainda ações nesse sentido, seria a criação de uma equipe, que tenha interesse e qualificação técnica na área de Segurança da Informação e Comunicações, para realizar o monitoramento preventivo das redes sociais, utilizando artifícios apropriados para se filtrar informações de interesse da Marinha do

Brasil, e assim prevenir ações danosas quanto ao vazamento de informações sigilosas pelas redes sociais. Esta ação poderia tanto ser feita de forma manual, em que os agentes designados fariam estas buscas utilizando, por exemplo, *hashtags* relacionadas com a instituição, como foi feito no experimento prático deste trabalho, ou de forma mais automatizada, utilizando-se das plataformas de inteligência artificial, como o Watson da IBM, combinadas com outras aplicações próprias, que permitam uma varredura sistemática das redes sociais, buscando por expressões específicas de interesse da instituição.

Também poderia se criar um canal direto deste setor para que pudessem ser feitas denúncias de incidentes nas redes, onde qualquer pessoa poderia reportar conteúdos indevidos e danosos ao bom nome e a reputação da Marinha do Brasil e seus membros junto a sociedade brasileira, nos moldes do que é feito pela Marinha Americana em casos dessa natureza. (NAVY, 2019).

Quanto as ferramentas de inteligência artificial, uma outra aplicação interessante para o uso destas, é a aplicação dessas ferramentas em postagens nas redes sociais de um determinado usuário, permitindo-se através destas se fazer um levantamento do perfil psicológico do mesmo. Isso possibilitaria, por exemplo, o estudo pelo setor de recrutamento de pessoal da Marinha, do perfil de candidatos ao ingresso na força, permitindo uma pré-triagem com base no que há de exposto sobre o candidato armazenado nas redes. Ou determinar se algum militar específico, em que a instituição pensa designar a um cargo sensível ou de comando, tem um perfil compatível com esta função, de acordo com o levantamento do perfil psicológico do indivíduo estudado.

Como sugestão de trabalhos futuros relacionados a esta área de estudo, recomenda-se alguns temas relevantes como:

- Estudo do impacto do uso nas redes sociais pelos perfis oficiais da Marinha do Brasil, na elevação de seu prestígio junto a sociedade.
- Monitoração e medição do alcance e outras características de expressões e temas de interesses da Marinha do Brasil nas redes sociais.
- Uso de ferramentas de mineração de dados aplicadas as redes sociais.

Referências Bibliográficas

ALECRIM, Emerson. **Ataques DoS (Denial of Service) e DDoS (Distributed DoS).** InfoWester. Fev/2012. Disponível em: < https://www.infowester.com/ddos.php>. Acesso em 19/01/2020.

ANDREASI, Diego. O efeito Facebook. Jovem Administrador. Ago/2011. Disponível em: < https://jovemadministrador.com.br/o-efeito-facebook/>. Acesso em 28/12/2019.

AGUIAR, Adriana. Instagram: saiba tudo sobre essa rede social! Rock Content. Set/2019. Disponível em :< https://rockcontent.com/blog/instagram/>. Acesso em 13/10/2019.

ARNOUX, P.A et all. 25 Tweets to Know You: A New Model to Predict Personality with Social Media. Association for the Advancement of Artificial Intelligence, 2017.

AVAST. Avast. Avast, 2020. Disponivel em: <https://www.avast.com/pt-br/c-spoofing>. Acesso em: 19 jan. 2020.

BÁRBARA, Fernandes. **Facebook faz 14 anos: veja curiosidades sobre a história da rede social.** Tectudo. Fev/2018.
Disponível em: < https://www.techtudo.com.br/noticias/2018/02/facebook-faz-14-anos-veja-curiosidades-sobre-a-historia-da-rede-social.ghtml> Acesso em 28/12/2019.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Marco civil da internet,** Brasília, DF, abr 2014

BRASIL. Lei nº 13.709, de 14 de agosto de 2018**. Lei geral de proteção de dados,** Brasília, DF, abr 2018.

CERT.BR. Cartilha de Segurança para a internet. **Fascículo Redes Sociais**, Março 2017.

COSTA, Thais. **Quais são as redes sociais mais usadas no Brasil em 2019?** Rockcontent. Out/2019. Disponível em: < https://rockcontent.com/blog/redes-sociais-mais-usadas-no-brasil/>. Acesso em 16/11/2019.

DAVENPORT, Thomas H; PRUSAK, Laurence. Conhecimento empresarial: como as organizações gerenciam o seu capital intelectual. 11. ed. Rio de Janeiro: Campus, 1998.

DE SOUZA, D.A et all. Segurança da Informação nas Redes Sociais. Out/ 2018. Disponível em: <https://singep.org.br/7singep/resultado/345.pdf >. Acesso em 06/10/2019.

FACEBOOK admite uso indevido de dados de 87 milhões de usuários, 443 mil no Brasil**. BBC news Brasil,** 2018. Disponível em: <https://www.bbc.com/portuguese/geral-43646687>. Acesso em: 24 de abr. de 2019.

FERREIRA, Fernando Nicolau Freitas. Segurança da informação. Rio de Janeiro: Ciência Moderna, 2003.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. Política de Segurança da Informação: guia prático e implementação. Rio de Janeiro: Ciência Moderna, 2006.

FONTES, Edison. **Praticando a Segurança da Informação**. Rio de Janeiro: Brasport, 2008.

FONTES, Edison. **Segurança da Informação: o usuário faz a diferença.** São Paulo: Editora Saraiva, 2006.

GABARDO, Ademir C. Análise de Redes Sociais. São Paulo-SP: Novatec, 2015. 143 p.

IBM, Cloud. Pernonality insights Introduction. Dez/2019. Disponível em: < https://cloud.ibm.com/apidocs/personality-insights>. Acesso em: 30/12/ 2019.

INFORMATION, N. O. O. U.S. **Navy Social Media Handbook for Navy leaders, communicators, Sailors, families, ombudsmen and civilians.** Washington, D.C.: [s.n.], 2019.

IMME, Amanda. **Ranking das redes sociais: as mais usadas no Brasil e no mundo, insights**. PTI. Jan/2020. Disponível em: <https://www.profissionaisti.com.br/2017/06/redes-sociais-e-seu-impacto-no-comportamento-humano/>. Acesso em 25/01/2020.

KASPERSKY. **Kaspersky**, 2020. Disponivel em: <https://www.kaspersky.com.br/resource-center/definitions/what-is-ransomware>. Acesso em: 08 fevereiro 2020.

KLEIN, Soeli Claudete. **Engenharia Social na Área da Tecnologia da Informação**. 2004. 63 pág. Monografia (trabalho de conclusão de curso). Instituto de Ciências Exatas e Tecnológicas, Centro Universitário Feevale. Novo Hamburgo, RS.

KLEINA, Nilton. **A história do Facebook. A maior rede social do mundo**. Tecnomundo. Ago/ 2018. Disponível em: < https://www.tecmundo.com.br/mercado/132485-historia-facebook-maior-rede-social-do-mundo-video.htm >. Acesso em 06/10/2019.

LOFRANO, F. https://www.contabeis.com.br/. **Contábeis**, 2017. Disponivel em: <https://www.contabeis.com.br/artigos/4078/as-organizacoes-e-o-valor-da-informacao/>. Acesso em: 02 Fevereiro 2020.

MARINHA DO BRASIL, **Diretoria Geral do Material da Marinha -0540.** Normas De Tecnologia Da Informação Da Marinha, 2019.

MARINHA DO BRASIL, **Diretoria de Comunicações e Tecnologia da Informação da Marinha. DCTIMARINST Nº30-08A**. Uso Institucional e não Institucional de mídias e redes sociais extra-MB pelo pessoal da MB, 2015.

MCCRAE, R. R., and John, O. P. 1992. An introduction to the fivefactor model and its applications. Journal of personality 60(2):175-215.

MITNICK. Kevin D, (1963) MITNICK - A arte de enganar/ Kevin D. Mitnick; William L. Simon; Tradução: Kátia Aparecida Roque; revisão técnica: Olavo José Anchieschi Gomes Título original: The art of deception: controlling the human element of security.

NEIL, Patel. **Como usar o Instagram: O guia definitivo**. Out/2019. Disponível em: < https://neilpatel.com/br/blog/instagram/>. Acesso em: 29/12/ 2019.

NOGUEIRA, Josicleido. **O que são Redes Sociais?** Administradores. Jun/ 2010. Disponível em: < https://administradores.com.br/artigos/o-que-sao-redes-sociais >. Acesso em 06/10/2019.
RECUERO, Raquel. Redes Sociais na Internet. Porto Alegre: Sulina, 2009. 191 p.

PAKZAD, Roya. **Human Rights Implications of IBM Watson's 'Personality Insights' Tool.** Ago/2019. Disponível em: < https://medium.com/taraaz/https-medium-com-taraaz-human-rights-implications-of-ibm-watsons-personality-insights-942413e81117>. Acesso em 29/12/2019.

PRESTES, Vladimir. **Fator humano: o principal componente da segurança da informação**. Computerworld. Jun/2018. Disponível em: < https://computerworld.com.br/2018/06/06/fator-humano-o-principal-componente-da-seguranca-da-informacao/> . Acesso em: 08/01/ 2020.

SÊMOLA, Marcos. Gestão da Segurança da Informação: uma visão executiva da segurança da informação. Rio de Janeiro: Elsevier, 2003.

SILVA, A. D. O. E. ENGENHARIA SOCIAL: O FATOR HUMANO NA SEGURANÇA DA INFORMAÇÃO. **Revista do Exército Brasileiro**, agosto 2011.

SOARES, D. G. Aplicação da análise de redes complexas em apoio ao planejamento e emprego da inteligência militar. Centro de Instrução de Guerra eletrônica, Brasília, 2018.

SMAAL, Beatriz. A história do Twitter. Tecnomundo. Fev/2010. Disponível em:
< https://www.tecmundo.com.br/rede-social/3667-a-historia-do-twitter.htm >. Acesso em 13/10/2019.

TAUSCZIK Y, PENNEBAKER J (2010) **The psychological meaning of words: Liwc and computerized text analysis methods**. Journal of Language and Social Psychology 29: 24–54.

TOFFLER, Alvin. A Terceira Onda. Rio de Janeiro: Record, 1980.

TORRES, G. AVG. AVG, 2018. Disponivel em: <https://www.avg.com/pt/signal/man-in-the-middle-attack>. Acesso em: 08 FEVEREIRO 2020.

VASQUEZ, Vladimir. **LAS APLICACIONES de Facebook roban informacíon**. El Nuevo Diario, 2018. Disponível em: <https://www.elnuevodiario.com.ni/suplementos/tecnologia/456245-aplicacionesfacebook-roban-informacion/>. Acesso em: 01 de mai. de 2019.