Processando o Saber
eISSN 2179-5150
FATEC Praia Grande · fatecpg.edu.br/revista
submetido: Jan/2021 · **aceito**: Mar/2021 · **publicado**: Jun/2021

Segurança da informação nas redes sociais

Information security on social media

Alana Pagani Barros
Fatec Praia Grande
alana.pagani.b@gmail.com

Vagner dos Santos Macedo
Fatec Praia Grande
vagner.macedo2@fatec.sp.gov.br

RESUMO

Este artigo aborda a segurança da informação, nos mostrando como agir perante as redes sociais, a importância da sua utilização nas redes sociais, os riscos corridos em sua utilização, as ameaças sofridas e quem pratica cada tipo de ataque e como se prevenir. As redes sociais vieram como uma facilitação para suprir nossa vontade de compartilhar tudo o que ocorre em nossa vida, essa necessidade pode ser explicada dizendo que isto faz parte de nós desde nossos ancestrais, mas claro que por outros meios. Com esse novo meio que são as redes sociais deve-se ter o discernimento sobre o que se deve postar, em nossas contas pessoais e em contas organizacionais. Será abordado também sobre as diversas ferramentas de monitoramento, gerenciamento e de segurança disponíveis hoje e que podem ser utilizadas por empresas assim reduzindo o seu risco em meio a internet, mas não se tem o mesmo benefício para contas pessoais assim tendo que tomar certos cuidados ao se publicar informações voluntariamente que podem acabar prejudicando. Ademais será falado sobre alguns meios de prevenção para contas pessoais e organizacionais, essenciais a serem seguidos e implementados ao utilizar-se das redes sociais tornando-as mais seguras.

PALAVRAS-CHAVE: Segurança. Tecnologia. Redes Sociais.

ABSTRACT

This article approached about information security, show us how to interact with social networks, the importance of your utilization in the social networks, the risks taken in your utilization, the suffered threats to whom practice every type of attack and how to prevent yourself. The social networks came like a facilitation to supply our need to share everything that happen in your lives, this need can be explain saying that it makes part of our lives since our ancestors, but of caused by other ways. With this new way that is social networks we must have the discernment about what we should and can pots, in our personal accounts and in organizational accounts. It will be approached too about diverse monitoring tools, management and security available today and that can be used by companies that way reducing your risks in the middle of the internet, but we haven't the same benefits for the personal accounts so having to take certain care when publish information voluntarily that could end harming. In addition will be say about some ways to prevention to personal and organizations accounts, essential to be follow and implemented when using social networks making them safer.

KEY-WORDS: *Security. Technology. Social Media.*

INTRODUÇÃO

O objetivo da presente pesquisa é em suma levar conhecimento sobre a segurança da informação nas redes sociais, sendo elas pessoais ou nas organizações, a qualquer leitor que utilize das redes sociais, sem a necessidade de um conhecimento prévio sobre segurança da informação e com isso evitar que erros aconteçam.

A metodologia usada para a pesquisa se caracteriza como uma pesquisa bibliográfica, foi utilizado como base, informações sobre segurança da informação, redes sociais e como elas se relacionam nos ambientes profissionais e pessoas, essa pesquisa foi composta por sites e artigos científicos.

As redes sociais estão sendo usadas com mais frequência por usuários de diferentes faixas etárias, contudo, nem todos entendem como funciona a divulgação dos seus dados pessoais nestas plataformas. Uma grande parcela desses usuários não possui o conhecimento acerca do compartilhamento de suas informações pessoais, bem como profissionais, motivo pelo qual é preciso ter cautela sobre os dados colocados nas redes. Com essas novas formas de armazenamento de dados, informação e comunicação disponíveis hoje, há uma necessidade nítida de se adaptar e ter o discernimento correto sobre quais tipos de dados colocar na rede.

Portanto, tendo em vista a falta de conhecimento e segurança por parte dos usuários em relação ao uso das redes sociais nota-se a importância de meios que transmitam a essas pessoas mecanismos de segurança, para que, assim, não haja problemas futuros relacionados aos dados colocados nas redes.

Nos tempos atuais, há uma necessidade de sempre estar compartilhando alguma informação, seja ela profissional ou pessoal. E, em razão disto, o indivíduo se torna vulnerável, podendo, inclusive, ocorrer vazamento de informações, que poderão afetar diretamente o usuário ou quem estiver próximo a ele.

No contexto atual do mundo, as redes sociais são essenciais para a maior parte da população, no entanto, as pessoas não possuem o devido conhecimento acerca da segurança das informações nos dados e informações por elas divulgadas, sendo uma conta empresarial ou pessoal. Com isso o tema se torna extremamente relevante para a sociedade atual, e no contexto pessoal vem se tornando cada vez mais com o passar dos anos. Vem aumentando a quantidade de pessoas adentrando esse meio e totalmente despreocupados com o que postam, além disso a idade para entrar nesse meio vem diminuindo constantemente com a abertura para a internet através dos pais sendo cada vez mais precoce, sendo assim é importantíssimo que este conhecimento seja adquirido e então passado a eles. No meio profissional, é observada elevada

dificuldade em gerir todas as redes, se preocupando não só com o que pode ser publicado, gerando um desastre para a marca, caso uma informação sigilosa seja vazada, mas também gerar uma brecha para *hackers* e golpes com perfis falsos.

1. CONTEXTUALIZAÇÃO

> Ao dar às pessoas o poder de partilhar, estamos tornando o mundo mais transparente (Mark Zuckerberg).

A necessidade de compartilhar informações está em nós desde os tempos antigos, onde nossos ancestrais pintavam e escreviam nas pedras em busca de deixar aquilo registrado para o futuro e mais a frente registrávamos tudo em papel e compartilhávamos cartas onde era bem mais demorado, mas tinham o objetivo de transmitir informações sobre nós ou sobre o que está acontecendo em nossas vidas.

Com a vinda da internet e subsequentemente as redes sociais, foi conquistada uma incrível facilidade de compartilhar dados que passaram a estar expostos a pessoas mal-intencionadas, também. Quando se é visto pelo lado de um perfil pessoal temos dois grupos, os que só observam como as coisas andam e os que compartilham sua vida inteira e nesse segundo grupo é onde mora o perigo, porque isto pode ter se tornado até um vício. “The New York Times, em parceria com a *Latitude Research* – empresa especializada em pesquisas de mercado – fez uma pesquisa quantitativa para responder tais questões. No total, 2.500 participantes *heavy-users* (usuários intensos) de internet participaram. 94% dos usuários, antes de compartilhar algo, consideram cuidadosamente se a informação será útil para o receptor. Já 49% levam em consideração se a informação publicada pode mudar a opinião ou incentivar uma ação prática por parte do receptor (INFRA MAGAZINE 7, 2012).

A pesquisa ainda mostrou que 78% dos entrevistados compartilham informações para manter contato com algumas pessoas com quem, fora da web, não têm um relacionamento e 68% dão “share” (compartilhar) em um conteúdo com a intenção de mostrarem quem são e com o que se importam. Já 84% compartilham porque é uma maneira de apoiar causas ou questões que acham relevantes (MAGIC WEB DESIGN, 2012).

Mesmo os dados sendo relativamente antigos, pode-se ter noção de que compartilhamos pensando no próximo e sua importância para ele. Não é mensurado o quanto se está expondo com isso, estamos totalmente expostos sem ao menos repararmos nisso. No ponto de vista de uma organização é necessário ter uma interação via redes sociais constante, o compartilhamento

é essencial assim como uma boa comunicação com os clientes, mas deve-se estar atento para que essa iteração não deixe brechas para ser manipulada, roubada por *hackers* ou por uma concorrente.

2. A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO

> A segurança da informação é a proteção da informação contra vários tipos de ameaças e é essencial para proteger seus dados e informações sejam pessoais ou organizacionais, ela se sustenta nos em três pilares sendo eles (BENETTI, 2015):

a. **Confidencialidade:** A confidencialidade dos dados consiste em estar disponível somente para as partes que precisam do acesso a esses dados ou que são confiáveis para obterem os mesmos;
b. **Integridade:** A integridade dos dados significa ter à certeza de que os dados não são modificados, destruídos ou corrompidos por pessoas não permitidas. Existem dois momentos ao longo do processo de transmissão onde a integridade dos dados pode ser comprometida estas são durante o carregamento de dados e/ou durante o armazenamento ou coleta do banco de dados;
c. **Disponibilidade:** A disponibilidade dos dados e da informação refere-se a estar disponível quando a mesma for necessária. Para que um sistema tenha disponibilidade, deve possuir um sistema computacional, de controle de segurança e canais de comunicação com um bom funcionamento, a maioria são acessíveis em todos os momentos e tem garantias contra falhas de energia, desastres naturais, falhas de *hardware* e atualizações de sistemas.

A prática da segurança tem por objetivo reduzir as vulnerabilidades que algo ou alguém estejam sujeitas, com esse intuito de proteger é preciso reduzir os riscos corridos e então com esse propósito foram criados procedimentos para serem seguidos

A segurança da informação compõe um grupo de procedimentos e precauções que visa proteger as informações, sejam elas armazenadas em servidores, trafegadas em uma rede, comentada no interior ou exterior de uma organização ou de uma residência, comentários publicados em redes sociais, entre inúmeros outros casos possíveis onde as informações podem ser obtidas ou transmitidas.

3. REDES SOCIAIS E ACESSOS INAPROPRIADOS VIA LOGIN E DEMAIS *MALWARES*

> (Em sites como o Facebook). Nós temos o banco de dados mais abrangente sobre pessoas, seus relacionamentos, nomes, endereços, localização e as conversas entre elas, seus parentes, tudo à disposição dos serviços de inteligência americanos (JULIAN ASSANGE, 2011).

O poder representado pelas redes sociais é enorme e está em constante crescimento, são diversas redes sociais existentes atualmente, as mais utilizadas atualmente são o Facebook (plataforma de compartilhamento desenvolvida por Mark Zuckerberg em 2004), Youtube (plataforma de compartilhamento de vídeos desenvolvida por Chad Hurley, Steve Chen e Jawed Karim em 2005) e WhatsApp (aplicativo multiplataforma de mensagens instantâneas e chamadas de voz desenvolvida por Jan Koun e Brian Acton em 2009).

3.1 CONTA PESSOAL

> As redes sociais são muito úteis, oferecem serviços muito prazerosos, mas são uma armadilha (ZYGMUNT BAUMAN, 2015).

Na perspectiva de uma conta pessoal tem-se várias informações compartilhadas que contém risco, nem se imagina que aquele pequeno dado pode abrir brechas. Alguns exemplos de dados simples que podem ocasionar um problema são: divulgar seu aniversário, cidade de onde nasceu ou onde mora, nome do seu animal de estimação, o nome da sua mãe entre outros. Estas informações podem ser usadas para invadir suas contas sociais, e-mail ou contas de banco por meio do “esqueceu sua senha” onde utiliza-se estas respostas para suas perguntas de segurança.

Deve-se preocupar-se também com fotos e vídeos íntimos que são enviados por chat, mas que podem ser facilmente divulgados. Divulgar onde você vai estar assim como o horário, check-in, lugares habituais que você frequenta e reclamações sobre o trabalho, pode ocasionar terríveis consequências como sequestros e *stalkers* (perseguidor). É preocupante pensar que estes dados são divulgados por adultos, sendo assim o que pensar das crianças utilizando as redes sociais, crianças cada vez mais jovens possuem contas nas redes sociais e sem ter o devido conhecimento do que elas podem ou não divulgar.

3.2 CONTAS ORGANIZACIONAIS

A dificuldade em controlar os meios de comunicação e conseguir administrar as informações nas redes é imensa. Quando o conteúdo é publicado por uma empresa, existe um controle e acompanhamento de tudo que está sendo é postado. O responsável pela função de publicar em uma empresa precisa ter noção das consequências de tudo que é publicado.

É importante salientar a importância da troca de informações entre o responsável pelas redes sociais e a área marketing, já que são eles que definem o que está adequado para ser publicado e quando é o momento adequado. A oposição das empresas para entrarem nas redes sociais vem diminuindo progressivamente, mas continua sendo comum. Não ter adentrado à esse mundo, onde a facilidade com que pode se comunicar com clientes, futuros clientes e divulgar sua empresa ou produto é gigantesca, se deve muitas vezes a sua área de atuação, valores, visão, público-alvo, entre outros.

Analisando como o público jovem consome publicidade, como se comunica, e o que assiste é possível ter uma ideia de como as coisas serão no futuro. Não se vê mais jovens em sua grande maioria assistindo televisão, efetuando telefonemas para comprar produtos, entre outras diversas coisas.

A preferência sempre são compras *online*, consumir publicidades em anúncios nas redes sociais ou *streaming* (transmissão), quando deseja saber mais sobre uma marca ou estabelecimento procura sobre ele nas principais redes sociais, procura atendimento por meio de mensagens, entre outras diversas mudanças no perfil dos jovens que deve ser levado em consideração.

3.3 MONITORAMENTO E GERENCIAMENTO DAS REDES SOCIAIS

Como dito anteriormente, quando se trata de uma empresa monitorar as redes sociais não é uma tarefa fácil e as organizações tendem a ter uma enorme dificuldade em gerenciá-las, para solucionar este problema podemos utilizar ferramentas de monitoramento. Dentro da variedade de ferramentas no mercado, algumas são gratuitas e outras pagas, como na maioria das ferramentas gratuitas disponíveis em diversos segmentos, são limitadas e não conseguem abranger muitas redes sociais simultaneamente, por outro lado, as pagas e ainda dispõem de outros benefícios como da criação de relatórios e gráficos estatísticos (INFRA MAGAZINE 7, 2012).

3.3.1 Ferramentas Gratuitas

- *PeerIndex*: Não atende muitas redes sociais. Realiza uma análise onde o resultado é fundamentado em três componentes sendo eles a autoridade, audiência e atividade (PEERINDEX, 2009);
- *Whos Talkin*: Faz uma análise sobre o assunto de interesse do usuário, retornando uma lista de opiniões ou diálogos em torno do assunto pesquisado, podendo ainda ser filtrado por tipo de mídia social;
- *Socialmention*: Funciona como buscador e como ferramenta de análise agregando conteúdo gerado pelo usuário em um fluxo único de dados. Possibilita em tempo real a realização de filtros por palavras-chave ou frases, onde o usuário pode escolher qual tipo de busca deseja realizar, que pode ser por vídeos, imagens, entre outras opções, ou ainda todas as opções de busca disponíveis ao mesmo tempo. Ele consegue monitorar mais de 100 redes sociais (SOCIALMENTION s/d);
- *Google Trends*: Ele permite analisar termos mais buscados e mais populares em um determinado período. Os assuntos mais buscados refletem nas redes sociais, assim sendo uma ferramenta ideal para saber a tendência dos assuntos nas redes (GOOGLE 2006);
- *TweetDeck*: Possui um painel de controle simplificado onde é possível monitorar conversas, publicar em diversas contas simultaneamente, gerenciar várias contas, agendar posts, monitorar interações, *hashtags*, pesquisar por palavras-chave entre outros recursos (TWITTER, 2008).

3.3.2 Ferramentas Pagas

Dentre as ferramentas pagas a maioria permite a realização de um teste gratuito por um certo período de dias ou uma análise entrando em contato com a ferramenta. É recomendável sempre testar a ferramenta a fim de saber se é essa mesmo a que melhor soluciona seu problema.

- *HootSuite*: Permite acompanhar as redes sociais em tempo real, possui opções de agendamento para postagens com datas e horários ajustáveis. Ademais pode criar relatórios personalizados para compartilhar com clientes. Possui painel para iPhone (smartphone da marca Apple desenvolvido por Steve Jobs em 2007), *iPad* (*tablet* da marca Apple desenvolvido por Steve Jobs em 2010), BlackBerry (linha de smartphones e *tablets* desenvolvida por Mike Lazaridis, Douglas Fregin em 2013) e

Android (sistema operacional baseado no núcleo Linux desenvolvida por Andy Rubin, Rich Miner e Nick Sears em 2008) (HOLMES, 2008);

- *Agorapulse*: A pulse tem como proposta de monitoramento concentrar tudo em um lugar só. O painel principal mostra mensagens, menções e comentários da rede social escolhida, ela oferece mais recursos, mas como principal o monitoramento como agendamento de postagens e análise de relatórios. Ela oferece suporte para Facebook, *Instagram*, *Twitter*, *YouTube* e *LinkedIn*. Gratuita para teste por 28 dias (AGORAPULSE, s/d);
- *Audiense*: Auxilia a gerenciar, explorar e analisar contas do Twitter. Realiza análises de interações em tempo real, armazena um histórico com todos os dados mais relevantes sobre os perfis e realiza pesquisas cruzando diversos dados através de hashtags, menções e palavras-chave. Possui versão grátis onde limita 5.000 interações (BURÓN, 2011);
- *Zoho Social*: Analisa o desempenho dos perfis das redes sociais através de estatísticas do relatório e agenda os conteúdos da semana e permite a interação em tempo real, suporta *Twitter, Facebook* (página e grupo), *Instagram, LinkedIn* (perfil e página de empresa) e *Google* 'Meu Negócio' (ZOHO SOCIAL, 2013).

O *software* mais adequado depende das suas necessidades e quanto gostaria de investir. Nota-se que os serviços pagos têm bem mais recursos em relação aos gratuitos, mas no geral tanto gratuitos como pagos conseguem transmitir como anda a saúde da organização nas redes sociais.

3.4 TIPOS DE HACKERS

> Se você colocar uma chave debaixo do tapete permitirá que um ladrão encontre-a. Os cibercriminosos estão usando todas as ferramentas da tecnologia à sua disposição para hackear contas das pessoas. Se eles sabem que há uma chave escondida em algum lugar, eles farão de tudo para encontrá-la (TIM COOK, 2015).

Hacker foi o termo genérico dado ao se referir as pessoas que fazem ataques as informações, embora seja associado a palavra *hacker* (ciberpirata) ao criminoso virtual, essa não é a definição mais adequada, já que qualquer um que se dedique intensamente em alguma área específica da computação e descobre utilidades além das previstas nas especificações originais pode ser considerado um *hacker*.

Quando se tratando de ataques específicos esse termo sofre variações, quando motivados a roubo de informação tanto em meio profissional como pessoal, são eles os (INFRA MAGAZINE 7, 2012):

- *Script kiddies* (garoto dos scripts) –Amadores, rejeitam algumas premissas mantidas por *hackers* profissionais. Geralmente utilizam-se de programas escritos por outros por não possuir habilidades para fazer os próprios, focam seus ataques em sistemas e redes e sites;
- *Cyberpunks* (punk cibernético) – Mais velhos e antissociais. Motivados muitas vezes pelo desafio e diversão, em geral grandes conhecedores de segurança e obcecados pela mesma;
- *Insiders* (de dentro) – Colaboradores insatisfeitos com sua organização. São o tipo mais comum encontrado;
- *Coders* (codificadores)– Gostam de comentar suas conquistas como um atacante. Em geral gostam de compartilhar seus conhecimentos;
- *White hat* (chapéu branco) – São *hackers* éticos. É uma categoria onde há pesquisadores e operadores de segurança com objetivo de rastrear e monitorar ameaças de forma ativa. Quando encontradas, notificam as empresas sobre vulnerabilidades, mas sem levá-las ao público;
- *Black hat* (chapéu preto) – Essa categoria tem conhecimento sobre como invadir redes, ignorar os protocolos de segurança e em escrever malwares. A principal motivação é ganho pessoal ou financeiro, além da espionagem cibernética;
- *Gray hat* (chapéu cinza) – Explora uma determinada falha de segurança que há em um sistema ou produto com o propósito de chamar a atenção da organização. Age com o objetivo de aperfeiçoar a segurança do sistema e/ou da rede. diferente do *White Hat*, essa categoria divulga publicamente essas brechas, o que pode permitir que criminosos explorem isso.

4. RISCOS CONSTATADOS NAS REDES SOCIAIS

Riscos representam a probabilidade de que as ameaças explorem as vulnerabilidades causando impacto. Não existem risco zero sempre haverá um risco. Sabe-se que existem diversos riscos na internet, dentre eles alguns ocorrem facilmente utilizando as mídias sociais, que é onde passamos grande parte do nosso dia a dia por meio de smartphones (um celular que combina recursos de computadores pessoais desenvolvido pela IBM em 1992), computadores (conjunto de componentes eletrônicos capaz de executar variados tipos de algoritmos e tratamento de informações desenvolvido por Konrad Zuse em 1936), *tablets* (dispositivo pessoal em formato de prancheta que pode ser usado para acesso à Internet criado por Grid Systems em 1989) etc. É essencial ter conhecimento sobre quais são os principais riscos a fim de poder evitá-los, tanto em contas pessoais como de empresas, alguns deles são (INFRA MAGAZINE 7, 2012):

- Perseguição: Quando se possui informações, fotos ou vídeo visíveis para todos nas redes sociais, corre-se o risco de ser vítima de um perseguidor. Se não houver uma configuração das privacidades nas redes sociais, qualquer um pode acessar tudo o que é publicado, o que pode se tornar um problema e um risco para nossa integridade;
- Sequestro: Quando compartilhados lugares onde se frequenta, horários de compromissos, eventos, entrada/saída em trabalho etc. assim como fotos contendo local;
- Roubo de informações: Publicação de informações confidenciais como telefones, locais, vídeos privados que podem ser compartilhados, fotos em redes sociais etc. Tais incidentes levam ao roubo de informações, um exemplo são usuários que postam fotos de seus passaportes e/ou cartões de embarque publicamente em seus perfis, como uma forma de contar sobre sua viagem, não sabendo que o código de barras ou código QR (*Quick Response*) da passagem que pode ser identificado na imagem ou vídeo é uma fonte de informação caso haja acesso à Internet;
- Perfis Falsos: Com esses dados roubados pode acontecer de algum cyber (cibernética) criminosos criam perfis falsos para então acessarem pessoas você ou pessoas próximas a você e atacarem de algum modo;

- Golpistas: Um perfil falso que invade a página de mídia social, explora as *hashtags* (símbolo #) e lança um golpe disfarçado de uma promoção imperdível. Para obter o desconto, cliente liga para um número de telefone, onde é induzido a fornecer informações do seu cartão de crédito;
- Colaboradores descuidados: Quando um colaborador comete algum erro por meio das redes sociais no perfil da empresa;
- Erros ao enviar mensagens: Muitas vezes temos várias janelas abertas, por isso não é raro quando ocorre o envio de uma mensagem para um lugar errado, sendo mensagens, documentos, imagens entre outros dados e informações. Isto pode acarretar consequências sérias. Por exemplo, pode ser disponibilizado para todos os dados pessoais de clientes que acabam sendo divulgados através de um envio em massa.

5. PREVENÇÃO

A maioria das empresas ou pessoas que estão no mundo das redes sociais e principalmente, as que vão migrar, não estão preparadas para os riscos que podem correr, as ameaças que estão expostos e consequências de seus atos. Para evitar que tais coisas ocorram, a melhor opção é a prevenção. Sendo assim será listado algumas dicas de como prevenir sua conta pessoal e organizacional, levando em conta que existem outros meios, não somente esses (CYBERFLY, s/d).

5.1 PERFIS PESSOAIS

- Configurar suas redes sociais para que apenas seus amigos vejam suas mensagens assim evitando que pessoas más intencionadas e estranhas tomem conhecimento de suas informações. Caso seu perfil esteja aberto fique atento a quaisquer irregularidades e reporte contas falsas;
- Mantenha o mínimo de informações pessoais em seu perfil;
- Se divulgar fotos, use as que não facilitem seu reconhecimento, nem endereço ou nome da escola;

- Não adicione estranhos, mesmo que algum amigo tenha em seu perfil, somente pessoas que você conheça;
- Troque sua senha periodicamente, lembrando sempre de deixá-la o menos simples possível com uso de números, caracteres e letras maiúsculas e minúsculas;

5.2 PERFIS ORGANIZACIONAIS

- Ter uma equipe especializada que tenha visão crítica e pensamento estratégico, levando a sério a importância das redes sociais. Contar com a parceria de uma agência digital pode ser uma ótima solução, já que conta com profissionais em tudo que uma boa rede social precisa assim não correndo riscos;
- Implementar uma política corporativa para mídias sociais, estabelecendo um conjunto de processos e protocolos para seus canais de comunicação;
- Educar e treinar todos os colaboradores mesmos quando não houver interação com o perfil organizacional;
- Dificultar o acesso às contas sociais além de senhas complexas, duas camadas de *login*, gerenciadores de senhas e *single sign on* (mesma senha para todas as aplicações corporativas);
- Estabelecer um fluxo para aprovação de postagens sociais para que não ocorra uma postagem com dados ou informações sigilosas;
- Monitorar e gerenciar continuamente a atividade nas redes sociais;
- Caso algo de errado ocorra ter um plano de contingência é essencial;
- Para evitar que mensagens sejam enviadas erroneamente, existem ferramentas de bloqueio. Os documentos que deve se manter sigilo são marcados com inscrições especiais e o envio externo é barrado. Ao ser enviado um documento com esta marcação, ele então é colocado em quarentena e sem a verificação do serviço de segurança, ele não é enviado;
- É de extrema importância que as organizações tomem consciência do riscos e conduzam periodicamente treinamentos de Segurança da Informação entre seus colaboradores;
- Uma boa prática seria a criação de uma conta nova conta para trabalho, caso as redes sociais sejam necessárias para as tarefas de trabalho;

- Possuir um sistema de proteção contra vazamentos de informações (DLP). Data *loss prevention* (prevenção de perda de dados) é uma medida de segurança essencial, ele rastreia automaticamente qualquer atividade realizadas pela conta nas redes sociais no computador da empresa e salva todo o histórico de mensagens, sem diferenciação de contas. Assim, o empregador garante a segurança de seus dados e informações;
- Os colaboradores, no entanto, precisam ter conhecimento sobre a medida de segurança da informação implantada para que assim possam manter a privacidade de suas conversas pessoais e não as faça usando os equipamentos da empresa (LEADCOMM, 2019).

6. CONSIDERAÇÕES FINAIS

Sabe-se que a presença da população nas redes sociais crescerá exponencialmente. Pode-se afirmar que é imprescindível se obter conhecimento sobre segurança da informação para ser aplicado ao uso das redes sociais e que existem sim, diversos riscos tanto para perfis organizacionais como pessoais e que não se deve subestimar estes riscos de forma alguma e sim, se utilizar do conhecimento obtido para se tomar medidas contra.

Organizações são as que mais possuem meios de tomar medidas para se proteger, tendo disponível diversas ferramentas de monitoramento, gerenciamento e de segurança contra vários tipos de *hackers* e vazamentos de informações, sendo elas de graça e pagas. Além de medidas educativas a serem aplicadas nos colaboradores e preventivas que são executadas através dos colaboradores da organização que são essenciais.

Perfis Pessoais onde se é postado, voluntariamente nossos dados e informações importantes é onde mais devemos nos preocupar em aplicar a segurança da informação, já que não se tem acesso aos mecanismos de segurança disponíveis às organizações e não se possui o conhecimento de como pode ser perigoso. Com o conhecimento passado podemos reduzir esse risco e passar a postar somente o que não causará ataques ou vazamentos importantes que podem comprometer nossa vida.

As prevenções podem ser feitas tomando as medidas citadas no artigo, além de diversas outras disponíveis, saber quem pode querer nossos dados e informações e com que objetivo se é alvo deles é de essencial e o primeiro passo quando falamos de segurança, a importância de se estar preparado contra ameaças e riscos é imensa e pode fazer toda a diferença.

Portanto, se conclui que devemos estar atentos aos riscos e ameaças decorridos nas redes sociais, tomando assim cautela ao se utilizar, sendo por parte de colaboradores de uma organização ou sua conta pessoal, identificando o que pode ou não ser publicado e tomando as devidas prevenções e medidas contra qualquer risco que se possa correr.

REFERÊNCIAS

AGORAPULSE. **Agora Pulse.** s/d. Disponível em: https://www.agorapulse.com/. Acesso em: 01/05/2021.

ASSANGE. **WikiLeaks: Facebook, a mais apavorante máquina de espionagem já inventada**. Vio Mundo, 2011. Disponível em: https://www.viomundo.com.br/denuncias/assange-do-wikileaks-facebook-a-mais-apavorante-maquina-de-espionagem-ja-inventada.html. Acesso em: 02/09/2020.

BAUMAN, Zygmunt: **As redes sociais são uma armadilha**, 2016. Disponível em: https://brasil.elpais.com/brasil/2015/12/30/cultura/1451504427_675885.html. Acesso em: 02/09/2020.

BENETTI, Ticiano: **Segurança da Informação – Confidencialidade, Integridade e Disponibilidade** (CID). Profissionais TI, 2015. Disponível em:https://www.profissionaisti.com.br/seguranca-da-informacao-confidencialidade-integridade-e-disponibilidade-cid/#:~:text=Confidencialidade%20significa%20garantir%20que%20a,n%C3%A3o%20estejam%20autorizadas%20para%20tal.&text=Integridade%2C%20por%20sua%20vez%2C%20significa,corretamente%20para%20quem%20a%20consulta. Acesso em:10/05/2021.

BURÓN, Javier. **Audiense**, 2011 Disponível em: https://audiense.com/. Acesso em: 01/05/2021.

COSTA SANTOS DIAS, Juliana**. As 10 melhores frases de Tim Cook sobre privacidade e segurança**, kaspersky daily, 2015.

CYBERFLY: **Segurança na internet: Cuidados necessários nas redes sociais**. Cyberfly s/d. Disponível em: https://www.cyberfly.com.br/seguranca-na-internet-cuidados-necessarios-nas-redes-sociais/. Acesso em: 04/09/2020.

INFRA MAGAZINE 7: **Segurança da informação x redes sociais.** DevMedia, 2012. Disponível em: https://www.devmedia.com.br/seguranca-da-informacao-x-redes-sociais-revista-infra-magazine-7/25678. Acesso em: 15/08/2020.

GOOGLE. **Google Trends**, 2006. Disponível em: https://trends.google.com.br/trends/?geo=BR. Acesso em: 01/05/2021.

HAMMERSCHMIDT, Roberto. **Oversharing: quando o compartilhamento de dados foge do controle**. TecMundo, 2015. Disponível em: https://www.tecmundo.com.br/redes-sociais/73167-oversharing-compartilhamento-dados-foge-controle.htm. Acesso em: 08/09/2020;

HOLMES, Ryan. **HootSuite**, 2008. Disponível em: https://www.hootsuite.com/. Acesso em: 01/05/2021.

IBERDROLA: **Dependência das redes sociais: principais causas e sintomas**. Disponível em: https://www.iberdrola.com/compromisso-social/como-redes-sociais-afetam-jovens. Acesso em: 05/09/2020.

LEADCOMM: **O acesso a mídias sociais em dispositivos corporativos apresenta riscos à segurança**. Leadcomm, 2019. Disponível em: https://leadcomm.com.br/2019/01/10/o-acesso-a-midias-sociais-em-dispositivos-corporativos-apresenta-riscos-de-seguranca/. Acesso em: 04/09/2020.

MAGIC WEB DESIGN: **Por que compartilhamos?** Magic Web Design, 2012. Disponível em: https://www.magicwebdesign.com.br/blog/redes-sociais/por-que-compartilhamos/. Acesso em: 08/09/2020.

ZOHO SOCIAL. **A maneira mais fácil de gerenciar suas marcas nas mídias sociais**, 2013. Disponível em: https://www.zoho.com/pt-br/social. Acesso em: 01/05/2021.

PEERINDEX, 2009. **Peer Index.** Disponível em: https://www.brandwatch.com/p/peerindex-and-brandwatch/. Acesso em: 01/05/2021.

ROCKCONTENT: **As 45 melhores ferramentas gratuitas para monitoramento de redes sociais**. Rockcontent, 2015. Disponível em: https://rockcontent.com/br/blog/ferramentas-gratuitas-para-monitoramento-de-redes-sociais/. Acesso em: 01/05/2021.

SOCIALMENTION. **Social Mention.** s/d. Disponível em: http://www.socialmention.com/. Acesso em: 01/05/2021.

TWITTER. **Tweetdeck**. 2008. Disponível em: https://tweetdeck.twitter.com/. Acesso em: 01/05/2021.