**SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DOS DADOS: MÉTODOS PARA MANUTENÇÃO E SUA IMPORTÂNCIA NAS CORPORAÇÕES**

Danilo Nogueira Vale \*

Rafael Rodrigues \*

Yuri Lima \*

**RESUMO**

O objetivo deste artigo é elucidar a importância da Segurança da Informação na sociedade, visto que após o advento da tecnologia da informação utilizando computadores, a forma de realização dos empreendimentos econômicos foi alterada significativamente, pois as organizações passaram a criar, manipular e armazenar informações processadas em ambiente computacional. Com a competitividade empresarial, a informação passou a ser essencial para a tomada de decisões e também para a otimização dos resultados, tendo como consequência a criação de normas e procedimentos para garantir os princípios da chamada Segurança da Informação, que são integridade, confiabilidade e disponibilidade, diminuindo assim, os riscos de negócios. O Marco Civil da Internet (Lei nº 12.965/2014) que estabelece os princípios, garantias, direitos e deveres para o uso da Internet no Brasil e a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18 - 13.853/19) que estipula regras e regulamentos para a proteção de dados, são exemplos de regulamentações que visam tentar garantir a segurança da informação. Neste artigo, a metodologia utilizada para reunir informações sobre o assunto, inclui pesquisas bibliográficas, levantamento técnico de *survey* e confecção de Matriz Swot. Como resultado, a empresa do estudo de caso mostrou-se devidamente comprometida com a segurança das suas informações, de acordo com avaliação. Tem-se como conclusão que o maior problema para manter segurança e privacidade de informações é, muitas das vezes, a falta de conscientização do ser humano em realizar as práticas necessárias, sendo negligente a ponto de sofrer ataques de engenharia social.

**Palavras-chave:** Segurança da informação. , Sistemas de informação. , Engenharia social. , LGPD. , Marco Civil da Internet.

**ABSTRACT**

The purpose of this article is to elucidate the importance of Information Security in society, since after the advent of information technology using computers, the way of carrying out economic enterprises has changed significantly, as organizations started

to create, manipulate and store processed information in a computational environment. With business competitiveness, information has become essential for decision making and also for the optimization of results, resulting in the creation of standards and procedures to guarantee the principles of the so-called Information Security, which are integrity, reliability and availability, thereby reducing business risks. The Marco Civil da Internet (Law nº 12.965 / 2014) that establishes the principles, guarantees, rights and duties for the use of the Internet in Brazil and the General Law of Protection of Personal Data (Law nº 13.709 / 18 - 13,853 / 19) that stipulates rules and regulations for data protection, are examples of regulations that aim to try to guarantee information security. In this article, the methodology used to gather information on the subject, includes bibliographic research, technical survey survey and preparation of the Swot Matrix. As a result, the case study company was shown to be properly committed to the security of its information, according to the assessment. It is concluded that the biggest problem to maintain security and privacy of information is, many times, the lack of awareness of the human being in carrying out the necessary practices, being negligent to the point of suffering attacks from social engineering.

**Keywords:** Information security. Information systems. Social engineering. LGPD. Civil Framework of the Internet.

**1 INTRODUÇÃO**

Desde meados do século XX, com a chegada da Terceira Revolução Industrial, ou Revolução Informacional, o advento da tecnologia da informação com o uso dos computadores viria a mudar totalmente a forma como o mundo realiza seu empreendimento econômico. As organizações passaram a criar, manipular e armazenar informações processadas em ambiente computacional e a depender deste para realizarem seus compromissos com a sociedade (REVOLUÇÃO..., 2020).

Atualmente, com a competitividade empresarial, a informação é essencial para a tomada de decisão e otimização de resultados (SILVA; ARAÚJO; AZEVEDO, 2013). A confiabilidade da mesma é de suma importância, assim como sua privacidade. Nas redes sociais, os usuários muitas vezes são surpreendidos com a informação de terem seus dados expostos. Criminosos aproveitam essa exposição para realizarem suas práticas.

Neste contexto, um campo chamado Segurança da Informação foi criado com o intuito de propor ferramentas, normas, regulamentos e políticas que garantam a confiabilidade das informações geradas e processadas pelas empresas. O objetivo principal era minimizar os riscos do negócio, observando o uso dos recursos de informação para o funcionamento da organização, já que a falta de integridade dos dados ou a perda de informação comprometem o funcionamento da empresa e podem resultar em grandes prejuízos (SEGURANÇA..., 2020).

A então denominada Segurança da Informação deve ser interpretada como parte fundamental do cotidiano das empresas, tanto pelos funcionários quanto executivos, para que todos estejam comprometidos e não como um fardo ou responsabilidade extra apenas para os profissionais de TI. Entretanto, muitas vezes essa temática não é tratada com grande relevância, o que acaba comprometendo o mercado e as pessoas que desfrutam dos novos meios de comércio e comunicação. Como exemplo, o caso ocorrido em 2019, onde a rede social Facebook deixou expostos cerca de 540 milhões de dados de usuários[[1]](#footnote-1).

Consequentemente, medidas ao longo do tempo foram tomadas para amplificar a eficácia da Segurança da Informação, algumas sendo bem severas como a intervenção do governo brasileiro na aprovação da Lei nº 13.709/18 - 13.853/19 (Lei Geral de Proteção de Dados Pessoais – LGPD) que estipula regras e regulamentos para a proteção de dados e que foi inspirada na GDPR (*General Data Protection Regulation*) em vigor na União Europeia desde 2018. Da mesma forma, o Marco Civil da Internet (Lei nº 12.965/2014) (MCI) que estabelece os princípios, as garantias, os direitos e os deveres para o uso da Internet no Brasil, além da criação de novas normas, regras e políticas que viabilizem métodos mais compreensíveis de manter a integridade dos dados tão valiosos para as corporações e que possam ser implementados de forma mais natural e rápida.

Portanto este trabalho busca elucidar a importância do tema Segurança da Informação, atrelada a elevação das atuais técnicas elaboradas para garantir a integridade dos dados e informações processadas pelas organizações de uma forma geral, mostrando a importância de cada caso e buscando em campo o grau de utilização, satisfação e relevância das regras de negócio utilizadas por empresas atuais. Será criado e aplicado questionário de pesquisa com intuito de entender quais os impactos das leis citadas, tanto para as empresas quanto para os cidadãos e o quanto mudou no comportamento dos mesmos nos últimos anos.

O questionário de pesquisa será aplicado em uma empresa localizada na macro região de Juiz de fora que oferece consultoria, administração e suporte tanto em software quanto em hardware. Com oito anos de experiência no mercado, apesar de ser atuante em diversos segmentos comerciais, a firma tem foco no ramo hospitalar, prestando serviço a um dos maiores hospitais do estado, sendo este detentor de mais de seiscentos leitos e ocupante de uma vasta área territorial.

Elencado como um dos mais modernos hospitais do país, realiza milhares de atendimentos mensais e conta com tecnologia de ponta, por isso sendo indicado como uma das melhores unidades neonatais do estado de Minas, fatos que ratificam a responsabilidade em resguardar as informações que trafegam no ambiente. A instituição em questão que se assume responsável pelo setor de tecnologia da informação é formada por uma equipe de quinze profissionais, subdivididos entre analistas, técnicos e auxiliares administrativos, escalados de maneira a estarem presentes no hospital sete dias por semana alternando os turnos de operação. A empresa detém servidores e banco de dados físicos armazenados em sala cofre dentro do próprio hospital para garantir maior controle das informações.

O foco principal deste artigo é a adequação dos usuários à utilização de práticas de segurança da informação, observando as leis criadas, para evitar ataques de engenharia social, mantendo assim, a privacidade tanto dos seus dados pessoais como das empresas. Serão analisadas as publicações citadas acima e utilizadas suas informações para auxílio no desenvolvimento deste trabalho.

**2 FUNDAMENTAÇÃO TEÓRICA**

Atualmente, as organizações estão se tornando cada vez mais dependentes dos seus sistemas de informação e acabam preocupadas com o uso adequado das informações, notadamente com privacidade de seus dados pessoais (LYRA, 2015). Dentro deste contexto, cria-se um estudo denominado Segurança da Informação, que nada mais é que o conjunto de orientações, normas, procedimentos, políticas e ferramentas que tem como objetivo proteger o recurso da informação possibilitando que a empresa realize seu objetivo social (FONTES, 2006).

A simples adoção de medidas padronizadas não garante a mitigação dos riscos aos quais as informações estão expostas (DRESNER, 2011). Existe então o entendimento que as decisões sobre a adoção das medidas de Segurança da Informação precisam atender a princípios, requisitos, riscos específicos e objetivos gerais da organização, pois, cada empresa com suas características próprias deve assegurar de adotar técnicas que atendam às suas necessidades (SÊMOLA, 2014).

Contudo, não se deve descartar algumas técnicas básicas para a manutenção dos dados e da sua integridade, tais como a utilização do Termo de Compromisso de cada empresa, que geralmente é renovado periodicamente e busca registrar a responsabilidade que cada funcionário tem de manter sigilo quanto as informações que terá acesso, além de seguir as normas de segurança da informação instituídas (FONTES, 2006).

Outra medida é a utilização de autenticação de usuário, que possui como princípio básico e primordial garantir que o usuário descrito na identificação é verdadeiramente essa pessoa, com uma senha que deve ser bem elaborada, evitando conter nomes e números que possam estar ligados ao usuário ou a empresa, para garantir maior segurança (FONTES, 2006). Existem outras técnicas, como controle de acesso físico aos equipamentos que constituem o ambiente computacional da empresa, programas de treinamento de profissionais de TI, acompanhadas com campanhas de divulgação de regulamentos, políticas de Segurança da Informação da empresa e normas técnicas como a implementação de medidas que diminuam a redundância dos dados e garantam sua transmissão e armazenamento seguro (ALBUQUERQUE *et al*., 2018).

Além disso, também são criadas ferramentas com o objetivo de auxiliar as empresas na tentativa de garantir a segurança de seus dados e informações. Um claro exemplo é a ISO 27.001, uma ferramenta de controle que busca auxiliar corporações a manter a integridade e a segurança dos dados em complacência com a LGPD, auxiliando as organizações para que possam atingir as metas necessárias de adequação de segurança dos dados pessoais dos clientes que foram instituídas pela lei.

Outro ponto, são que questões éticas em sistemas de informação ganharam maior relevância com a ascensão da Internet, desencadeando novas preocupações sobre a utilização das informações dos clientes e à proteção da privacidade das mesmas. A privacidade dos dados na internet hoje está muito comprometida, visto que grandes empresas de publicidade on-line utilizam as informações coletadas para praticar marketing direcionado. As informações são obtidas tanto de buscas efetuadas em sites, como de trajetos percorridos pelos Smartphones. Estudos mostram que pessoas podem ser identificadas por meio de poucas informações básicas. (LAUDON; LAUDON, 2015).

Segundo Santos e Catarino (2016), os princípios fundamentais do Marco Civil da Internet são: neutralidade da rede, privacidade e liberdade de expressão. O primeiro, é entendido como obrigação, por parte dos provedores de acesso, do oferecimento de um tráfego sem discriminação de conteúdo ou origem. A liberdade de expressão, seria o direito da manifestação opinativa e informativa, por quaisquer meios utilizados. O controle da disponibilidade de informações de si mesmo é uma definição de privacidade. Um ponto contraditório é que o texto do MCI prevê que o governo possa exigir que provedores não disponibilizem conteúdo e acesso a usuários da internet por decreto de lei, afetando assim, os próprios princípios estabelecidos pelo Marco Civil da Internet. (SANTOS; CATARINO, 2016).

A LGPD foi inspirada em regulamentação da União Europeia, porém, com a inclusão das empresas públicas (BRASIL. SENADO FEDERAL, 2019). De acordo com Rapôso *et al*. (2019), é importante que as empresas adaptem suas tecnologias, além de efetuar treinamento de seus colaboradores, observando princípios éticos para que se adequem ao estabelecido na lei.

**3 TRABALHOS RELACIONADOS**

É notável a importância do tema Segurança da Informação, resultado principalmente da sociedade e das organizações criarem uma extrema dependência do ambiente computacional para a elaboração dos seus negócios (FONTES, 2006). Portanto, a perda ou danificação de dados de uma corporação pode causar sérios danos para as empresas que não realizam um planejamento estratégico para conhecerem qual o grau de importância que essas informações possuem (LYRA, 2015).

Desta forma, diversos estudos, livros e artigos são elaborados atualmente com o intuito de expandir os conhecimentos a respeito da Segurança de Informação, elevando sua importância e elaborando novos métodos e técnicas que possibilitem grandes corporações a atingirem seu objetivo de mercado, mantendo a integridade de suas informações. Como foi abordado por Albuquerque *et al*. (2018), que concluiu em seus estudos que é necessária a utilização de diversos mecanismos para garantir a proteção das informações dos usuários, já que os dados, o bem mais precioso da empresa, com o passar do tempo ficam mais suscetíveis a ataques externos devido à falta de preparo de algumas delas.

Além disso, foi apontado por Pimenta e Quaresma (2016) que a segurança da informação não parte somente de forma unilateral das empresas para os usuários, mas que, atitudes e comportamentos dos usuários nos sistemas de informação podem constituir um risco ou comprometer a proteção destes sistemas. Através de um questionário para coleta de dados, e de um tratamento estatístico simples, chamado de análise de frequências e médias, obteve a conclusão de que, de uma forma geral, boa parte dos usuários respeitam e ajudam na proteção para a segurança dos sistemas de informação das organizações.

Ademais, notamos que a informação possui um papel fundamental em muitas outras bases da sociedade, não só brasileira como mundial, visto que, os dados processados por qualquer organização são fundamentais para elas. Assim como foi levantado em Coimbra (2018), que após elaborar muito bem o grau de relevância dos dados, realizar um levantamento bibliográfico e um questionário, que foi enviado aos utilizadores dos SI desenvolvidos nas Forças Aéreas, concluiu que a adoção de medidas de segurança juntamente com mecanismos de proteção contribui efetivamente para garantir a segurança dos sistemas de informação desenvolvidos internamente nesta área.

Dentro de um contexto da área de saúde, também podemos notar a relevância dos sistemas de informações, como podemos ver em Cavalcante, Silva e Ferreira (2011), que aborda justamente a utilização dos sistemas dentro desta área. Em seu artigo, ele faz o levantamento de possibilidades e desafios para a implantação dos sistemas de informação na área da saúde, visto que este é um setor da sociedade fundamental, onde o cuidado ao ser humano, que é a retórica dos profissionais na área da saúde, precisa ser o centro de uma gestão eficiente. Neste contexto, ocorre o levantamento de vantagens da utilização dos sistemas como apoio à organização administrativa, facilidade na coleta, armazenamento e processamento de dados, auxílio no diagnóstico a prescrição dos medicamentos, além de ter um papel fundamental no processo decisório colaborando para as tomadas de decisão. Por outro lado, aborda também os desafios para adição dos sistemas, como a resistência de algumas unidades de saúde em modernizar seus processos, a exigência de um suporte para os profissionais que irão utilizar o sistema, a necessidade de um planejamento independentemente de quais serão os setores ou processos a serem contemplados pelo sistema para que este consiga corresponder as reais necessidades impostas. Outro fator de extrema importância é a segurança dos dados que serão captados e processados, sendo necessário um controle de acesso ao usuário somado a criação de normas e diretrizes que visem garantir a integridade das informações.

Além do exemplo anterior, também podemos citar Lima *et al.* (2009), que teve como objetivo avaliar as dimensões de qualidade dos dados e os métodos aplicados na avaliação dos sistemas de informação em saúde (SIS). Este abordou em seu artigo a importância de se garantir uma informação de qualidade, sendo este fator uma condição essencial para a análise objetiva da situação sanitária, para a tomada de decisões baseadas em evidências e para a programação de ações de saúde. Visto que, no Brasil o monitoramento da qualidade dos dados dos SIS não segue um plano regular de avaliações, normatizado pelo Ministério da Saúde, resultando em iniciativas não sistemáticas e isoladas. Com este objetivo em mente, foi elaborada uma metodologia que visava encontrar artigos, dissertações e teses que avaliassem a qualidade dos dados dos SIS de âmbito nacional do Brasil, através de uma pesquisa que teve como exemplos de alguns descritores: “avaliação e sistemas de informação”, “confiabilidade e agravos”, “confiabilidade e internação e hospitalar”, “confiabilidade e sistemas de informação”, “confiabilidade e validade”, e outra série de itens de busca para que a pesquisa tornasse o mais sensível possível.

Com esta consulta, obteve-se como resultado cerca de 375 artigos, onde após serem classificados, revisados e avaliados, foram selecionados cerca de 78 que seriam objeto principal do estudo. Estes selecionados através de uma série de tópicos de uma dimensão de qualidade tais como, por exemplo: “acessibilidade”, “clareza metodológica”, “cobertura”, “completitude”, “confiabilidade”, “consistência”, “não duplicidade”, “oportunidade” e “validade”. O resultado, foi que existe no Brasil uma carência muito grande em relação a qualidade dos dados e as informações associadas a estes no âmbito da saúde, visto que muitos estudos não explicitam suas medições para avaliações e que muitos destes ocorreram somente em grandes regiões brasileiras, o que corrobora com a necessidade de se implantar uma avaliação sistemática de âmbito nacional. Como conclusão, obteve-se a concepção de que a importância de informações com boa qualidade indica a necessidade de que se institua no Brasil uma política de avaliação formal e regular, liderada pelo Ministério da Saúde. A elaboração de uma política deste porte deverá considerar os diversos aspectos que influenciam a qualidade das informações, para que possa apontar medidas para seu aprimoramento.

Também podemos abordar os estudos de Pereira *et al.* (2012), voltados para a utilização dos sistemas de informação na gestão hospitalar, onde apresentou uma visão com o objetivo de incentivar a busca pela excelência em sistemas nessa gestão em todos os níveis desde o operacional ao estratégico. Para isso, apresenta uma série de vantagens para a implementação de um sistema nessa área tal como a redução de custos com orçamentos operacionais logísticos, com materiais, equipamentos e com os funcionários contratados. Para que isso seja possível, primeiramente torna-se necessário a implantação de um ERP (*Enterprise resource planning*), um sistema integrado de gestão empresarial, que se utilizado com outros sistemas integrados pode melhorar consideravelmente os processos dentro de um hospital além de fornecer um planejamento avançado, uma sincronização e colaboração entre os fabricantes e distribuidores de insumos hospitalares, fatores que geralmente não são encontrados nos hospitais e que tornam-se além de um diferencial competitivo de mercado uma necessidade. Além disso, é relatado que muitas das vezes, um hospital tende a iniciar seu plano de implantação de sistemas informatizados pelos sistemas logísticos, neste processo o foco ocorre na gestão do fluxo de atividades, com objetivo de atender as necessidades dos clientes e da organização, contudo este processo inicia-se sem uma avaliação da realidade existente no hospital e das suas reais necessidades.

A partir deste ponto, ocorre a abordagem de quais fatores são essenciais para o sucesso na implantação de um sistema na área hospitalar, sendo um destes a necessidade do comprometimento com o caso de todos os níveis de colaboradores da corporação desde o estratégico até o operacional, além da capacidade de sensibilização dos usuários e gestores para os benefícios na implantação do sistema. Além disso, são relatados que outros fatores críticos de sucesso estão relacionados as questões relativas aos recursos humanos, já que um sistema envolve mudanças nos processos de negócios, na cultura organizacional e no treinamento da equipe, refletindo em toda a estrutura organizacional. Por fim, vale ressaltar a necessidade de se garantir a segurança e a integridade das informações disponibilizadas, que devem estar sempre acessíveis para as pessoas autorizadas, corretas e atualizadas em tempo real para a tomada de decisão, sendo preciso para isso a adoção de uma política da valorização da qualidade da segurança do sistema (PEREIRA *et al.*, 2012).

Portanto, partimos de um conceito inegável sobre a relevância da Segurança da Informação e buscamos neste estudo, relatar o porquê da sua importância, implantando os métodos, técnicas, estudos e normas que instituem esta área, buscando realçar quais estratégias são melhores e quais são implementadas atualmente por profissionais da área de TI e por algumas corporações realçando a sua importância e sua real efetividade.

Citando parte do procedimento efetuado durante a pesquisa bibliográfica, seguem exemplos das buscas efetuadas. Em pesquisas realizadas com a *string* de busca: "segurança da informação nas redes sociais", sem filtro de datas, foi encontrado um artigo utilizado como base de avaliação: “Engenharia social nas redes sociais online: um estudo de caso sobre a exposição de informações pessoais e a necessidade de estratégias de segurança da informação”. Ao utilizar a mesma *string*, mas filtrando apenas o que foi publicado desde 2015, foram obtidos outros artigos como “Um estudo sobre a confiança em segurança da informação focado na prevenção a ataques de engenharia social nas comunicações digitais” e “Engenharia social e segurança da informação no ambiente corporativo: um estudo de caso em uma cooperativa de crédito localizada no sul de Santa Catarina”.

Nas pesquisas com a *string* "marco civil da internet”, desde 2015, foram encontrados: “Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet” e “25 anos da web e o marco civil da internet: apontamentos sobre o livre acesso à informação, a liberdade de expressão e a privacidade”.

Resultando de pesquisas efetuadas com a *string* "Lei Geral de Proteção de Dados Pessoais", tanto em site de busca acadêmico quanto busca comum, obteve-se: “O Brasil não está pronto para a Lei Geral de Proteção de dados. ”, “País deve se preparar para Lei de Proteção de Dados Pessoais, aponta debate” e “LGPD-LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS EM TECNOLOGIA DA INFORMAÇÃO: Revisão Sistemática”.

Em cada trabalho encontrado existem peculiaridades, mas muitas informações são úteis em conjunto para análise do conteúdo dos artigos. Segue um breve resumo de cada um.

Rapôso *et al*. (2019) cita problemas com empresas fornecerem dados pessoais de seus clientes. Informa que as empresas devem adaptar seus princípios éticos e sua tecnologia e é necessário treinamento dos colaboradores. Entende que existem poucos trabalhos relacionando à aplicabilidade da LGPD em sistemas de informação e que são necessários mais artigos para esclarecimentos à população.

A LGPD foi tema de debate no Senado. O promotor do debate, Presidente do Instituto Iluminante de Inovação Tecnológica e Impacto Social, Gilberto Lima, entende que a lei não tem caráter punitivo, seu objetivo é disciplinar e moralizar o uso dos dados pessoais. (BRASIL. SENADO FEDERAL, 2019).

De acordo com Moura (2019), muitas empresas brasileiras não entenderam ainda o problema por completo. Entendem que atender a esse tipo de legislação requer discussão de princípios, mudança cultural e de procedimentos na empresa inteira e informam que existem empresas analisando o custo do descumprimento e outras mapeando seus fluxos para justificarem as solicitações de dados, ao invés de se adequarem para manter a privacidade desses dados.

Em Costa (2018) foi feita pesquisa sobre segurança da informação com ênfase no conceito de Engenharia Social, analisando atitudes dos colaboradores de uma Cooperativa de Crédito. Os resultados revelaram que parcela significativa ainda não segue rigorosamente as normas adequadas.

O artigo de Fernandes e Souza (2016) é inserido no debate sobre aspectos objetivos e subjetivos para estabelecimento da confiança entre as pessoas de uma organização. A violação das propriedades de segurança por abuso da confiança causa prejuízo organizacional. Identificados potenciais alvos para ataques de engenharia social.

Em Santos e Catarino (2016), entende-se que com o princípio de que todos devem ser capazes de comunicar-se livremente com todos os outros e gratuitamente, a Internet expandiu-se espantosamente e a primeira lei sobre ela é aprovada com vinte e cinco anos de sua existência. O Marco Civil da Internet estabelece direitos e deveres de usuários e provedores. O objetivo desse estudo foi a análise das iniciativas para a liberdade de expressão, privacidade e livre acesso de informação na Internet. Como resultado da lei, temos avanços e brechas para o controle e vigilância dos cidadãos.

O artigo de Teffé e Moraes (2017) visa examinar os mecanismos criados pela Lei do Marco Civil da Internet para amparar os direitos da personalidade nas redes sociais virtuais. Quanto à privacidade, considera-se que o controle e a autodeterminação de informações para os usuários da rede foram observados de modo positivo na lei. A conclusão é que a lei criou instrumentos, mas foram insuficientes.

De acordo com Silva, Araújo e Azevedo (2013), percebe-se que o desenvolvimento de sites de redes sociais fez surgir um fenômeno que aumenta a exposição de informações pessoais na Internet, aumentando os riscos associados a elas, principalmente, com utilização de engenharia social. O objetivo do trabalho é examinar o grau de exposição das informações de pessoas físicas acessíveis na Internet. De acordo com pesquisa realizada, nenhum dos entrevistados apresentou baixo grau de exposição, o que indica a facilidade para encontrar informações referentes a um usuário na Internet, subsidiando ataques de engenharia social.

**4 METODOLOGIA**

A questão de investigação deste trabalho é baseada em realizar pesquisa e análise sobre as possíveis alterações no comportamento das pessoas quanto à manutenção da privacidade de seus dados, levando em conta a Lei Geral de Proteção de Dados Pessoais e o amadurecimento das pessoas quanto ao uso e compartilhamento de informações nas empresas. A proposta é levantar informações sobre os impactos dessas leis nas empresas e nos cidadãos.

A metodologia utilizada para reunir informações sobre o assunto consiste em uma pesquisa aplicada, focada em gerar conhecimentos de aplicações práticas onde é possível visualizar quais técnicas de segurança da informação realmente são pertinentes para garantir a segurança dos dados. Além disso, será feita uma abordagem mista sobre os dados reunidos para que possa ser feita a classificação destes, sua interpretação e uma comparação entre as informações para elevarmos quais são de maior importância.

Serão realizadas principalmente pesquisas bibliográficas, buscando artigos e livros relacionados ao assunto e que possam integrar maior domínio do tema, além de um levantamento técnico de *survey,* pois é de suma importância que informações sobre as técnicas utilizadas atualmente no mercado das corporações sejam esclarecidas pelos próprios profissionais da área, que possuem conhecimento no assunto e realizam o procedimento técnico diariamente em suas ocupações.

Será realizada análise dos resultados obtidos da aplicação de questionário para levantamento de questões relacionadas à exposição de dados, utilizando como auxílio a Lei Geral de Proteção de Dados Pessoais, para análise do comportamento e percepção das empresas a respeito desses assuntos.

**5 RESULTADOS ESPERADOS**

Com o levantamento de diversos estudos sobre o que foi apresentado com relação a Segurança da Informação, buscamos ressaltar a importância do assunto, destacando o grau de relevância de diversas técnicas na manutenção da segurança dos dados para o planejamento e execução do objetivo social de cada corporação ou empresa.

De acordo com os resultados da aplicação do questionário de pesquisa, espera-se compreender os impactos das leis e regras no comportamento das empresas, no que diz respeito a Segurança da informação.

**6 ESTUDO DE CASO**

**6.1 Coleta dos Dados**

Foi efetuada a aplicação de questionário na empresa citada para obtenção de informações específicas sobre a utilização da segurança da informação para preservação dos princípios de integridade, confidencialidade e disponibilidade sobre os dados da empresa.

**6. 2 Resultados**

Elaboramos o questionário com diversas perguntas bem abrangentes e obtemos como resultados muitas respostas bem genéricas, visto que esta é uma área bem sensível da empresa e também tentamos ser menos invasivos possível. Contudo, obtermos informações muito produtivas que demonstram que a empresa em questão está devidamente comprometida com a segurança das suas informações e processos.

Podemos relatar acerca do posicionamento da empresa mediante a vulnerabilidade existente no Brasil devido ao alto número de ataques registrados e também como a empresa se portou mediante a LGPD, que a organização mostrou-se estar totalmente atenta aos riscos mediantes a falta de barreiras na Internet, atrelada a uma divulgação de ferramentas que exploram a vulnerabilidade, além de reconhecer que não existe sistema de segurança que seja absolutamente seguro. Contudo, ao reconhecer estes riscos, se esforçam para detê-los e utilizam de várias tecnologias para minimizá-los. Além disso, a empresa está de acordo com todas as diretrizes da LGPD possuindo também um Plano Diretor de Tecnologia da Informação, que é revisado de forma periódica e estratégica para se manter sempre atualizado de acordo com o planejamento institucional.

Além disso, foi constatado que a empresa em questão está totalmente calcada nos pilares da segurança da informação, sendo estes confiabilidade, integridade e disponibilidade, e buscam sempre elencar suas ações, seus domínios e sua política de segurança da informação nestes pilares. Atrelado a estes, a empresa também se preocupa em realizar treinamentos introdutórios a seus funcionários e colaboradores, bem como ditar regras e listas com boas e más ações para conseguir sempre ofertar os serviços certos, para as pessoas certas e no momento certo sem correr o risco do fator humano se tornar uma vulnerabilidade.

Também vale ressaltar que a empresa apresenta um suporte voltado para a proteção da rede, muito bem elaborado. A começar pelo fato de que as redes sem fio da organização possuem infraestrutura distinta da rede administrativa, esta que é cabeada e os colaborados que fazem o uso desta possuem acesso restrito a funcionalidades corporativas. Ademais, todo o tráfego da rede é monitorado em tempo real, sendo assim, existem rotinas que permitem mapear os horários de pico em uso de banda e os transportes de pacotes, tudo isso atrelado a um antivírus corporativo que também fornece uma camada de firewall com um monitoramento de portas bem como a possível abertura indevida das mesmas. Além de tudo isso para manter a segurança da rede, também é levado em consideração as sete camadas de proteção, sendo elas DNS, Firewall, Rede, Dispositivos, Usuários, Aplicações e Dados, que são verificadas e atualizadas em diferentes prazos sendo em algumas destas necessária a utilização de um ambiente de homologação, buscando mitigar e corrigir possíveis vulnerabilidades antes de qualquer atualização.

Foi inclusive questionado sobre qual a imposição da empresa sobre um possível ataque envolvendo sequestro de dados e qual seriam as atitudes perante a isso. As soluções apresentadas pela corporação foram que mesmo reconhecendo o possível risco de um ataque, já que um cenário de segurança perfeita é inalcançável, a empresa conta com várias ferramentas de prevenção, como as já citadas camadas de proteção, além de realizarem backups em nuvem e também utilizarem fita magnética, para caso venha ocorrer uma perda de informações o retorno dos dados fosse facilitado. Valendo ressaltar também, que visando a confidencialidade das informações, a empresa apresenta por padrão deixar todas as saídas USB dos equipamentos bloqueadas, tentando reduzir ao máximo a probabilidade de vazamento de dados, tendo em vista que tratam de um ambiente hospitalar. Contudo reconhecem a necessidade de alguns cargos estratégicos necessitarem da liberação destas portas e, portanto, a concedem com a devida autorização assinada pela diretoria.

Por último, foram levantadas as informações sobre a infraestrutura da empresa, indicando quais maquinários e equipamentos eles apresentam. Com isso obtemos as informações que a organização possui uma sala cofre para armazenar os servidores e demais equipamentos de rede devidamente refrigerada com dois aparelhos de ar-condicionado, além de contar com um sugador de oxigênio para caso de altas temperaturas que podem resultar em incêndio, o piso é elevado para o isolamento dos equipamentos além de facilitar as acomodações e estruturações dos cabeamentos. Além disso, possuem ferramentas de monitoramento destes servidores e dos equipamentos de nobreak também presentes.

Com base nos dados obtidos e com conversas internas realizadas com o analista de rede e segurança, foi possível elaborar uma matriz Swot com objetivo de analisar todos os ambientes da organização, sejam eles internos e externos a fim de otimizar as áreas. Com a matriz Swot podemos elencar o que devemos manter e progredir com os pontos fortes bem como as fraquezas, ameaças e oportunidades. A matriz em questão não é de uso exclusivo do setor de TI, sendo aplicada amplamente em diversas empresas e repartições.

Tabela 1 – Matriz Swot

|  |  |
| --- | --- |
| **Fatores internos da empresa** | **Fatores externos da empresa** |
| **Fraquezas (-)** | **Ameaças (-)** |
| Poucos Analistas | Empresas concorrentes com necessidade de profissionais |
| Acesso irrestrito a sala cofre para a TI | Fracasso em implementações por falta de conhecimento específico |
| Pouca organização na distribuição das funções | Colaboradores insatisfeitos com a empresa |
| Pouca comunicação | - |
| Gestão externa de BD | - |

|  |  |
| --- | --- |
| **Forças (+)** | **Oportunidades (+)** |
| PDTI Atualizado com frequência | Ampliação do quadro de profissionais |
| Contingência de riscos | Investimento no setor de RH |
| Implantação de Permissões | Acomodação do setor de BD |
| Sólido conhecimento hospitalar | Maior frequência de auditorias externas |
| Comprometimento na resolução de problemas | Acreditações de qualidade |
| Equipe qualificada | - |
| Rápida resposta de chamados | - |

Fonte: Elaborado pelos autores do artigo.

**7 CONCLUSÕES**

Com o resultado obtido através da análise do questionário e a entrevista realizada, foi possível observar que a empresa do estudo em questão mostrou-se devidamente comprometida com a segurança das suas informações, apresentando assim excelente embasamento e conhecimento prático nos procedimentos e normas atreladas a segurança da informação. Tem-se como conclusão que o maior problema para manter a segurança e a privacidade das informações é, muitas das vezes, a falta de conscientização dos usuários em seguir as devidas orientações. Agindo com um simples gesto de confidencialidade, de modo a não absorver possíveis impasses pessoais gerados no interior da instituição e consequentemente se tornar vulnerável a um ataque muito difundido atualmente, que consiste na engenharia social, o usuário dificulta que a empresa se veja exposta por uma negligência de sua equipe.

**8 CONSIDERAÇÕES FINAIS**

Interessante perceber que talvez o maior problema para manter segurança e privacidade de informações, seja conscientizar as pessoas sobre suas atitudes, tanto em empresas quanto na vida pessoal.

Apesar do Marco Civil da Internet não ter estabelecido parâmetros com exatidão absoluta para funcionamento pleno, a LGPD pode auxiliar na melhoria da possibilidade de garantia da manutenção de informações seguras e privadas.

Com a adequação das empresas às leis, regras e metodologias de segurança da informação, e os próprios usuários de sistemas empresariais, particulares e de redes sociais acostumarem-se com os procedimentos necessários para a garantia dos pilares dessa segurança, espera-se uma eventual evolução no comportamento humano para que os problemas de privacidade de dados sejam minimizados.

# REFERÊNCIAS

ALBUQUERQUE JUNIOR, A. E.; SANTOS, E. M.; OLIVEIRA, R. C. R.; SILVA, A. S. R.; ALMEIDA, L. M. A Adopção de Medidas Formais, Informais e Técnicas de Segurança da Informação e sua Relação com as Pressões do Ambiente Institucional. **Revista lbérica de Sistemas e Tecnologias de Informação.** Portugal, n. 30, p. 17-33, dez. 2018. ISSN 1646-9895. Disponível em: <http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1646-98952018000500003>.

BRASIL. Senado Federal. País deve se preparar para Lei de Proteção de Dados Pessoais, aponta debate. **Senado Notícias**, ago. 2019. Disponível em: <https://www12.senado.leg.br/noticias/materias/2019/08/08/pais-deve-se-preparar-para-lei-de-protecao-de-dados-pessoais-aponta-debate>. Acesso em 22 nov. 2019.

CAVALCANTE, R. B.; SILVA, P. C.; FERREIRA, M. N. Sistemas de informação em saúde: possibilidades e desafios. **Revista de Enfermagem da UFSM.** Santa Maria, v. 1, n. 2, p. 290-299, mai. 2011. Disponível em: <https://periodicos.ufsm.br/reufsm/article/view/2580>.

COIMBRA, S. A. M. P. **Ameaças e vulnerabilidades à segurança da informação dos sistemas de informação da força aérea. Política de segurança e prevenção.** Orientador: TCOR/ADMAER Pedro Dinis Capinha Maio. 2018. 60 f. Trabalho de Investigação Individual do Curso de Promoção a Oficial Superior - Instituto Universitário Militar [IUM], Lisboa. Disponível em: <http://comum.rcaap.pt/handle/10400.26/24931>.

COSTA, J.E. **Engenharia social e segurança da informação no ambiente corporativo:** um estudo de caso em uma cooperativa de crédito localizada no sul de Santa Catarina. Orientador: Prof. Dr. Paulo César Leite Esteves. 2018. 72 f. Trabalho de Conclusão do Curso de Graduação em Tecnologias da Informação e Comunicação - Campus Araranguá da Universidade Federal de Santa Catarina. Disponível em: <http://150.162.242.35/handle/123456789/187348>. Acesso em: 10 nov. 2019.

DRESNER, D. G. **A study of standards and the mitigation of risk in information systems.** 2011. 276 f. Tese de Doutoramento - The University of Manchester, Reino Unido.

FERNANDES, J. H. C.; SOUZA, R. C. Um estudo sobre a confiança em segurança da informação focado na prevenção a ataques de engenharia social nas comunicações digitais. **Brazilian Journal of Information Studies: Research Trend.** Brasília, v. 10, n. 1, p. 63-75, 2016. Disponível em: <http://www2.marilia.unesp.br/revistas/index.php/bjis/article/view/5088/3976>. Acesso em: 10 nov. 2019.

FONTES, E. L. G. **Segurança da Informação:** o usuário faz a diferença. 1. ed. Brasil: Ed. Saraiva, 2006. 172 p.

LAUDON, K. C.; LAUDON, J. P. **Sistemas De Informação Gerenciais**. 11ª. ed. São Paulo: Pearson, 2015.

LIMA, C. R. A.; SCHRAMM, J. M. A.; COELI, C. M.; SILVA, M. E. M. Revisão das dimensões de qualidade dos dados e métodos aplicados na avaliação dos sistemas de informação em saúde. **Cadernos de Saúde Pública.** Rio de Janeiro, v. 25, n. 10, p. 2095-2109, out. 2009. Disponível em: <https://www.scielo.br/scielo.php?pid=S0102-311X2009001000002&script=sci_arttext>.

LYRA, M. R. Governança da Segurança da Informação**. Amazon- eBook Kindle**. Brasil, v.1, p.1-173, 2015.

MOURA, M. **O Brasil não está pronto para a Lei Geral de Proteção de dados**. Revista Época Negócios, nov. 2019. Disponível em: <https://epocanegocios.globo.com/Empresa/noticia/2019/11/o-brasil-nao-esta-pronto-para-lei-geral-de-protecao-de-dados.html>. Acesso em: 22 nov. 2019.

PEREIRA, S. R.; PAIVA, P. B.; SOUZA, P. R. S.; SIQUEIRA, G.; PEREIRA, A. R. Sistemas de Informação para Gestão Hospitalar. **Jounal of Health Informatics.** São Paulo, v. 4, n. 4, p. 170-5, 2012. Disponível em: <http://www.jhi-sbis.saude.ws/ojs-jhi/index.php/jhi-sbis/article/view/206>.

PIMENTA, A. M. S.; QUARESMA, R. F. C. A segurança dos sistemas de informação e o comportamento dos usuários. **Revista de Gestão da Tecnologia e Sistemas de Informação.** São Paulo, v. 13, n. 3, p. 533-552, set. 2016. Disponível em: <https://www.scielo.br/scielo.php?script=sci_arttext&pid=S1807-17752016000300533&lng=en&nrm=iso&tlng=pt>.

RAPÔSO, C. F. L.; LIMA, H. M.; OLIVEIRA JUNIOR, W. F.; SILVA, P. A. F.; BARROS, E. S**.  LGPD-LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS EM TECNOLOGIA DA INFORMAÇÃO:**Revisão Sistemática. **RACE- Revista de Administração do Cesmac.** Brasil, v. 4, p. 58-67, 2019. Disponível em: <https://revistas.cesmac.edu.br/index.php/administracao/article/view/1035>. Acesso em: 22 nov. 2019.

REVOLUÇÃO DIGITAL. *In*: **WIKIPÉDIA**, a enciclopédia livre. Flórida: Wikimedia Foundation, 2020. Disponível em: <https://pt.wikipedia.org/w/index.php?title=Revolu%C3%A7%C3%A3o_digital&oldid=59381069>. Acesso em: 17 dez. 2020.

SANTOS, M. C. F.; CATARINO, M. E. 25 anos da web e o marco civil da internet: o livre acesso à informação, a liberdade de expressão e a privacidade. **Comunicação & Informação.** Goiás, v. 19, n. 1, p. 05-19, out. 2016. Disponível em: <https://www.revistas.ufg.br/ci/article/view/31855>. Acesso em: 10 nov. 2019.

SEGURANÇA DA INFORMAÇÃO. *In*: **WIKIPÉDIA**, a enciclopédia livre. Flórida: Wikimedia Foundation, 2020. Disponível em: <https://pt.wikipedia.org/w/index.php?title=Seguran%C3%A7a_da_informa%C3%A7%C3%A3o&oldid=59353085>. Acesso em: 17 dez. 2020.

SÊMOLA, M. **Gestão da segurança da informação:** uma visão executiva. 2. ed. Rio de Janeiro: Campus, 2014.

SILVA, N. B. X.; ARAÚJO, W. J.; AZEVEDO, P. M. Engenharia social nas redes sociais online: um estudo de caso sobre a exposição de informações pessoais e a necessidade de estratégias de segurança da informação. **Revista Ibero-Americana de Ciência da Informação.** Brasília, v. 6, n. 2, p. 37-55, 2013. Disponível em: <http://eprints.rclis.org/23215/>. Acesso em: 30 set. 2019.

TEFFÉ, C. S.; MORAES, M.C.B. Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. **Revista Pensar**. Fortaleza, v. 22, n. 1, pp. 108-146, 2017. Disponível em: <https://periodicos.unifor.br/rpen/article/view/6272>. Acesso em: 10 nov. 2019.

1. 540 milhões de dados de usuários do Facebook ficam expostos em servidores da Amazon. G1, 2019. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2019/04/04/dados-de-540-milhoes-de-usuarios-do-facebook-ficam-expostos-em-servidor.ghtml. [↑](#footnote-ref-1)