Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Curso Superior de Tecnologia em Segurança da Informação

Bárbara Ianca Zanaqui Ribeiro - RA: 0040971821007

Lucia Helena de Oliveira Casati - RA: 0040971911043

Uma análise da LGPD com foco em Engenharia Social

Americana – SP

2021

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Curso Superior de Tecnologia em Segurança da Informação

Uma análise da LGPD com foco em Engenharia Social

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da informação, sob a orientação do Prof. Especialista Marcus Vinícius Lahr Giraldi

Área de concentração: Segurança da Informação.

Americana – SP

2021

Bárbara Ianca Zanaqui Ribeiro

Lucia Helena de Oliveira Casati

Uma análise da LGPD com foco em Engenharia Social

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação.

Americana, 10 de dezembro de 2021.

Banca Examinadora:

Marcus Vinícius Lahr Giraldi (Presidente)
Especialista
Faculdade de Tecnologia de Americana

Edson Roberto Gaseta (Membro)
Mestre
Faculdade de Tecnologia de Americana

Elton Rafael Mauricio da Silva (Membro)
Mestre
Faculdade de Tecnologia de Americana

AGRADECIMENTOS

Em primeiro lugar, agradecemos a Deus, por nossa vida, pela sabedoria, força e coragem para superar mais uma grande etapa de nossas vidas.

Ao nosso professor Marcus Lahr, que muito nos ensinou e nos orientou para que pudéssemos apresentar um melhor desempenho em nosso processo de formação profissional.

Uma à outra pelo incentivo, apoio e dedicação em colaborar com o desenvolvimento desse trabalho.

As nossas famílias, em especial ao Douglas e a Leila, pela compreensão, paciência e por sempre acreditarem que somos capazes.

Se chegamos ao final desse curso, devemos tudo isso a todos vocês.

RESUMO

Este projeto tem como objetivo demonstrar a importância do fator humano e seu impacto na conscientização das pessoas sobre engenharia social e segurança da informação, principalmente com a aprovação recente da LGPD – Lei Geral de Proteção de Dados, assunto este que está se tornando cada vez mais importante e necessário para todos atualmente. Dentro do tema fator humano, temos a engenharia social, que é uma técnica utilizada para roubo de dados e informações, através da manipulação da confiança das pessoas, utilizando de muita simpatia ou urgência, o engenheiro social consegue explorar brechas de segurança, encontrando assim, pontos frágeis e utiliza tais fragilidades a seu favor, para obter todas as informações pessoais ou mesmo empresariais que necessita. Sendo assim, um bom engenheiro social, habilidoso conseguiria utilizar facilmente suas técnicas para burlar os sistemas de segurança da informação de uma grande empresa através do fator humano, focando seu ataque em funcionários destreinados ou desatentos, conseguindo acesso à informações confidenciais que não deveriam ser de fácil acesso, o que poderia acarretar multas de altíssimo valor a empresa, segundo a nova Lei Geral de Proteção de Dados, além de sanções e severas punições, como também, ocasionar danos a sua reputação, podendo causar até mesmo, em casos extremos, o fechamento da empresa. Abordamos também no trabalho, como a LGPD pode ser explorada por engenheiros sociais, para que eles possam aplicar suas técnicas e conseguir extrair informações confidenciais de terceiros, sejam eles empresas ou pessoas físicas, através da persuasão ou da falta de conhecimentos sobre a lei, conseguindo assim, utilizá-las a seu favor.

Palavras-chave: Engenharia social, LGPD.

ABSTRACT

This project aims to demonstrate the importance of the human factor and its impact on people's awareness of social engineering and information security, especially with the recent approval of the LGPD - General Data Protection Law, a subject that is becoming increasingly important and necessary for everyone today. Within the human factor theme, we have social engineering, which is a technique used to steal data and information, by manipulating people's trust, using a lot of sympathy or urgency, the social engineer can exploit security breaches, thus finding, weak points and uses these weaknesses to your advantage, to obtain all the personal or even business information you need. Thus, a good, skilled social engineer would easily be able to use his techniques to circumvent the information security systems of a large company through the human factor, focusing his attack on untrained or inattentive employees, gaining access to confidential information that he does not collect. easy access, which could result in very high fines for the company, according to the new General Data Protection Law, in addition to sanctions and severe punishments, as well as causing damage to its reputation, which may even cause, in extreme cases, the closing of the company. We also discuss at work, how the LGPD can be exploited by social engineers, so that they can apply their techniques and get information to extract confidential information from third parties, whether companies or individuals, through persuasion or lack of knowledge about the law, in doing so, use them in your favor.

Key words: *Social engineering, LGPD.*

SUMÁRIO

LISTA DE FIGURAS

1. INTRODUÇÃO

Segundo o Dicionário Aurélio (2020), informação, palavra originária do latim *informatio.onis*., tem por significado: “Reunião dos conhecimentos, dos dados sobre um assunto ou pessoa”, Já para o contexto da área de informática, tem-se as seguintes definições para a palavra informação: “Fator qualitativo que designa a posição de um sistema e, eventualmente, o transmite a outro”. E também: “Reunião dos dados que, colocados num computador, são processados, dando resultados para um determinado projeto”.

De acordo com Silva (2015), a informação corresponde ao pilar principal de toda a evolução e desenvolvimento alcançado pelas pessoas, pelas organizações, as cidades, estados e nações. A informação é parte essencial para que os seres humanos e as organizações cheguem a algum lugar. Através da informação, organizações e pessoas podem evoluir, cientista e suas pesquisas progridem, a sociedade como um todo consegue progredir.

Dodt (2019), diz que toda empresa possui um objetivo e para alcançá-los elas utilizam-se de processos, que nada mais é do que informações. A informação é um dado, que quando inserido dentro de um contexto transforma-se na informação, gerando assim o seu valor.

Marcelo e Pereira (2005) acrescentam dizendo que a proporção da informação é indicada conforme com a sua perda, isto é, quanto será perdido pela instituição. O custo indireto da informação pode ser gigantesco, podendo ser contabilizado somente após da sua divulgação ou então depois de ter acontecido.

Dodt (2019) explica ainda sobre a aplicação da informação no gráfico ITIL, sendo composta por quatro etapas, dado, informação, conhecimento e sabedoria. Os dados são considerados diferente da informação, pois nessa etapa eles ainda não estão incluídos em um contexto, sendo assim o entendimento desses dados são ainda muito pequenos. Em seguida é a etapa da informação, onde já está inserido em um contexto, podendo ser identificado o que, quem, quando, onde, isto é, a sua relevância. A próxima fase é constituída pelo conhecimento, que é o como da questão,

ou seja, o seu entendimento adicional. O último estágio é a sabedoria, que é o porquê das coisas, sendo essa etapa provida apenas pelo ser humano.

A informação ainda possui um ciclo de vida segundo Dodt (2019), inicialmente ela é criada, depois armazenada, processada, transmitida, utilizada, atualizada, e logo descartada. É enfatizado ainda a importância de proteger a informação durante todo o seu ciclo e os cuidados adicionais que devem serem tomados ao se vender, doar ou descartar um computador ou *smartphone* antigo, descartando de forma correta todas as informações ali contidas, para que a pessoa que que irá receber o aparelho não consiga restaurar essas informações.

2. O QUE É A SEGURANÇA DA INFORMAÇÃO

A segurança da informação, segundo Sêmola (2015), é uma área destinada para a proteção dos ativos da informação em combate a acessos não autorizados, adulterações impróprias ou que prejudiquem sua disponibilidade. A gestão de riscos de incidentes também pode ser considerada uma prática da segurança da informação, através dos três principais conceitos da segurança, que são: confidencialidade, integridade e disponibilidade da informação.

Marcos (DANTAS, 2011, p.11) diz sobre a norma NBR ISO/IEC 27002:2005 que a segurança da informação é a proteção da informação de múltiplos tipos de ameaças, de forma a assegurar a continuidade do negócio, diminuindo o risco para o negócio, aumentando o retorno sobre o investimento e as oportunidades de negócio. Essa norma estabelece a segurança da informação como a conservação da confidencialidade, da integridade e da disponibilidade da informação. Entre outras virtudes, estão envolvidas a autenticidade, responsabilidade, não repúdio e confiabilidade. Ao tratar de segurança da informação, necessita-se ter apreço pelas qualidades da informação, visto que todo ato que possa afetar qualquer uma dessas qualidades violará contra a sua segurança.

Silva, Carvalho e Torres (2003), alegam que o encarregado pela implantação da segurança dos sistemas de informação (SI) na organização tem, como ponto inicial e primordial a realização da garantia sobre a segurança da informação. Esta confirmação é alcançada por meio da aplicação de várias ferramentas, que deverão abranger as diversas áreas da empresa.

2.1. Classificação da Informação

Dantas (2011, p. 15), a classificação da informação colabora com a preservação de suas características principais, ou seja, confidencialidade, integridade e disponibilidade. Para ele a norma ISO 27002:2005, por si só não vai determinar qual a classificação das informações e dados, o que a norma irá fazer é aconselhar que as informações sejam classificadas levando em conta não apenas o seu valor, mas também sua criticidade, sensibilidade e os requisitos legais que as envolvem.

2.2. Princípios da Segurança da Informação

Segundo Dantas (2011), a informação precisa assegurar três propriedades fundamentais: a integridade, a disponibilidade e a confidencialidade, atributos esses que devem ser conservados, pois são os princípios da segurança da informação. Ele cita a norma NBR ISO/IEC 27002:2005, que diz que a integridade é a garantia da veracidade absoluta da informação e dos métodos de processamento. Certificar-se da integridade é garantir que a informação não seja modificada, alterada ou destruída sem autorização, que ela seja legítima e continue coerente. A perda da integridade ocorre quando a informação é adulterada, falsificada, roubada ou destruída. Atestar a integridade é manter a informação no seu estado original.

Ainda de acordo com o autor (DANTAS, 2011), colaboram para a perda da integridade:

> As inserções, substituições ou exclusões de parte do conteúdo da informação; as alterações nos seus elementos de suporte, que podem ocorrer quando são realizadas alterações na estrutura física e lógica onde ela está armazenada, ou quando as configurações de um sistema são alteradas para se ter acesso a informações restritas, bem como são superadas as barreiras de segurança de uma rede de computadores.

Silva, Carvalho e Torres (2003), complementam dizendo que a integridade é um dos pontos essenciais para preservar parcialmente os dados armazenados, processados e transmitidos pela segurança da informação. Todo o valor da informação consiste na sua fiabilidade, onde a inexatidão de uma simples vírgula ou ponto é capaz de prejudicar a integridade de um grande volume de dados, tendo um potencial para causar danos significativos. Deste modo é necessário sistemas para a validação das informações existentes. Este deve levar em conta o grau de importância da informação, podendo ser de forma automática, como regras de validação, ou pode ser primordial realizar processos manuais de validação. A integridade é igualmente indispensável para a recuperação de informações perdidas, visto que a importância das cópias que não apontam garantias de integridade é aproximadamente inexistente. Os autores ainda dizem que a especificação da informação para fins de integridade tende a conciliar os gastos das medidas de proteção ao impacto das perdas esperadas.

2.2.1. Princípio da Disponibilidade

Para Dantas (2011, p.12) a norma NBR ISO/IEC 27002:2005 expõe a disponibilidade como a proteção de que, somente os usuários que são autorizados tenham acesso à informação e aos ativos compatíveis sempre que preciso. O autor ainda diz que, a perda da disponibilidade acontece no momento em que a informação não está disponível para ser desfrutada, isto é, os usuários e destinatários não podem ou não conseguem ter acesso no instante que é necessário usá-las. Sendo assim, garantir a disponibilidade é certificar a conclusão da leitura, do trânsito e do armazenamento da informação.

Dodt (2019), afirma que é necessário garantir que as informações estejam disponíveis, acessíveis e utilizáveis para quem tem o acesso autorizado. Para atestar a disponibilidade controles como redundância e alta disponibilidade, plano de continuidade e recuperação de desastres, cópias de segurança (*backup*) e processos de restauração devem ser implementados.

O acesso dentro do prazo à informação é essencial e a partir dele vai dar o andamento aos objetivos da organização. Dispor da informação necessária, mas não ter a disponibilidade no período apropriado corresponde a não possuir nenhuma informação. A proporção da proteção dos dados carece abranger os pontos que facilitem o acesso aos mesmos. No entanto, deve-se estar apto a realizar a separação dos acessos que são autorizados e dos acessos que não são autorizados. É importante obter o equilíbrio na necessidade dos acessos às informações com o dever de conservar a sua confidencialidade. As proteções empregadas não precisam exibir os dados, possibilitando assim o acesso indevido, e nem impossibilitar ou dificultar consideravelmente o acesso adequado a estes dados. Entretanto, algumas situações podem existir onde a posse e o acesso às informações são mais importantes à instituição do que a preservação da sua segurança (SILVA; CARVALHO; TORRES, 2003).

2.2.2. Princípio da Confidencialidade

Para Dantas (2011), a norma NBR ISO/IEC 27002:2005 alega que o princípio da confidencialidade significa que a informação deve estar disponível somente para

pessoas autorizadas. A ruptura da confidencialidade da informação surge ao se deixar que pessoas não autorizadas tenham acesso aos dados em questão. A perda da confidencialidade é a ausência da privacidade da informação. Proteger a confidencialidade é certificar-se sobre o valor da informação e evitar a sua disseminação indevida.

Segundo Dodt (2019), a confidencialidade consiste na não divulgação de informações para quem não deve ter acesso, ou seja, para quem não tem autorização, sejam elas pessoas, processos ou organizações. Atualmente a lei geral de proteção de dados (LGPD), prevê punições severas e serias para os responsáveis pelo vazamento de dados. Para garantir a confidencialidade é necessário realizar segregação de funções, implementação de criptografia e controles de acesso.

Com o desenvolvimento da área de segurança da informação, é possível notar a preocupação com outros atributos, mais pontualmente no sistema de comunicação, onde a norma NBR ISO/IEC 17799:2001, determinava que a segurança da informação estava responsável pelo cuidado com a confidencialidade, da integridade e da disponibilidade da informação. A norma NBR ISO/IEC 27002:2005 sustenta também esse mesmo conceito, adicionando que outras especificidades possam igualmente estarem inclusas, como a autenticidade, a responsabilidade, o não repúdio e a confiabilidade (DANTAS, 2011).

Silva, Carvalho e Torres (2003) enfatizam ainda a confidencialidade como uma vantagem competitiva das companhias, apoiando-se muitas vezes na informação que possuem e na sua competência para controlar a sua propagação. Necessitando assim que tenham meios para garantir a confidencialidade da informação, mas que não prejudiquem o acesso de pessoas autorizadas à mesma. As formalidades da confidencialidade são nitidamente influenciadas, se não forem definidas e classificadas às informações.

2.2.3. Princípio da Integridade

Dodt (2019), afirma que a integridade é a garantia da informação em se manter integra, exata, verdadeira e completa. Para tanto, existem controles para assegurá-la, como controles de acesso, monitoramento de logs, auditorias e criptografia.

Gran Cursos Online (2019), diz que na integridade só podem ser alteradas dados e informações por quem possui autorização, para não aconteça modificações

indevidas, para isso é preciso garantir um controle de alterações. E é importante que essas informações se encontrem em sua totalidade, completas.

Backup Garantido (2018), completa ainda que o princípio da integridade garante que os aspectos originais da informação, a deixando preservada contra modificações que não foram autorizadas.

2.2.4. Princípio da Autenticidade

A autenticação e o controle de acesso são dois pontos universais da vida e dos sistemas da informação eles são da mesma forma importantes. São eles quem vão garantir que somos quem dizemos ser e quem nos autoriza e concede o que temos direito, seja ele em nível de infraestrutura ou nível aplicacional, por intermédio do fornecimento de credenciais que são de conhecimento exclusivo. (SILVA, CARVALHO E TORRES, 2003).

Para Silva, Carvalho e Torres (2003), o debate sobre quais são os melhores meios para realizar a autenticação e de controle de acessos vem sendo acalorada e tem sido acompanhada pela incorporação de novos componentes, por exemplo, cartões inteligentes *(smart cards*) ou dispositivos de autenticação biométrica, como também o avanço de outros, como os sistemas de gestão de palavras-passe.

Os autores dizem ainda que, a grande dúvida diante deste debate é, sobretudo, encontrar qual é a forma mais correta e preferível para poder autenticar e de certificar que só quem for autorizado tenha acesso aos recursos disponibilizados. (SILVA, CARVALHO E TORRES, 2003, p. 80 e 81).

Dantas (2011, p. 14), complementa que a autenticidade é a salvaguarda de que a informação é procedente da fonte que lhe é atribuída e criada por quem tem autoridade para tal.

2.2.5. Princípio da Confiabilidade

Dantas (2011), diz que a confiabilidade é a segurança de que a informação é confiável, originária de uma fonte autêntica e que expõe uma mensagem verídica. O autor afirma também que a autenticidade e confiabilidade estão conectadas. A autenticidade dizendo a respeito da credibilidade da origem. Onde a verificação de autenticidade da procedência pode ser feita a partir da sua seriedade. E a prova da

confiabilidade pode ser feita em associação ao seu conteúdo, tal como uma confirmação por meio de fontes diversas.

2.2.6. Não Repúdio

O não repúdio tem a intenção de garantir que a informação chegará ao destino certo e não será desprezada (DANTAS, 2011).

Para a equipe pedagógica da plataforma Gran Cursos Online (2019), o não repudio é a garantia que o autor de tal informação seja ele mesmo, ou seja, não possui meios de negar a sua autoria.

Santiago (2018), completa ao dizer que é de extrema importância aos *e-commerces* garantir o não repudio, pois é um método que garante que posteriormente o cliente que realizou a transação não negue ou conteste tal ato.

2.2.7. Responsabilidade

Para Dantas (2011, p.15), “a responsabilidade diz respeito aos deveres e proibições entre remetente e destinatário”.

Segundo o site da empresa Backup Garantido (2018), o princípio da responsabilidade é o dever de se responsabilizar pelos atos nos tratamentos de dados seja uma modificação, perca ou vazamento por exemplo. Este princípio é essencial para preservar a proteção e integridade da informação e fundamental para a gestão de organizações e equipes de tecnologia da informação.

3. FATOR HUMANO

Segundo Simon e Mitnick (2006, p. 10 e 11), é instintivo se sentir protegido e por conta disso tanta gente acaba tendo uma ideia enganosa da segurança. O fator humano é considerado o ponto mais enfraquecido da segurança, pois com periodicidade a segurança é meramente ilusão, que em muitas ocasiões tem o agravamento da inocência, credulidade e ignorância. Os ataques de engenharia social conseguem ter êxito no momento da estupidez humana ou quando ignoram ou desconhecem as boas práticas da segurança.

Para Marcelo e Pereira (2005), nenhuma empresa, por mais segurança que tenha, é de toda segura, pois o ser humano pode desestabilizá-la. Conhecendo isso os engenheiros sociais se beneficiam utilizando das fraquezas e até mesmo gostos pessoais tentando se aproximarem para obter a informação. Pode-se dizer que secretárias principalmente de diretores e presidentes são as vítimas favoritas dos atacantes, pois são consideradas fáceis de se aproximar, através de técnicas de sedução conseguem arrancar delas informações importantes e até senhas.

Simon e Mitnick (2006) complementam, quando se trata da proteção muitos responsáveis pelo setor de tecnologia da informação (TI), preservam um conceito errôneo de como proteger a empresa, pensado que mecanismos de segurança padrão como *firewall*, *softwares* de detecção de intrusos, ou sistemas de autenticação são suficientes. Pensar que somente esses produtos sozinhos proporcionam uma proteção efetiva é o mesmo que estar condenado ao fracasso. Onde a qualquer momento irão se tornar vítimas de algum ataque. Diz ainda que a segurança não é impasse apenas para a tecnologia, mas sim para a direção e as pessoas.

Marcelo e Pereira (2005) dizem que por meio da exploração de sentimentos de amizade e carência, os engenheiros sociais têm resultados incríveis para eles, porém assombrosos para as instituições. Agindo sem caráter os criminosos utilizam dessas técnicas de forma indefinida e descontrolada. A forma principal de explorar suas vítimas é agir aos poucos, dando um passo de cada vez, ganhando a sua confiança até chegar ao objetivo. O criminoso mais refinado e com mais artifícios consegue adulterar a situação ou narrar um problema que comova a vítima conseguindo comover e conquistar a sua confiança.

Simon e Mitnick (2006) acrescentam que conforme as autoridades no assunto colaboram com o avanço das tecnologias de segurança, mais árduo se torna a exploração das vulnerabilidades técnicas, voltando assim o foco dos ataques para a exploração humana, onde conseguir acesso a informações se tornam mais fáceis e exigem nenhum capital a não ser o gasto com algumas ligações telefônicas, tendo assim um risco insignificante.

Para Marcelo e Pereira (2005) vale citar que os casos de sucesso para os engenheiros sociais foram denominados como excesso de confiança, isto é, sempre se mostravam como pessoas educadas, prestativas e sofisticadas. O modo de se vestir, utilizar de frases de efeito e demonstrar confiança, funciona de maneira a impressionar a vítima.

Um dos maiores exemplos de sucesso da engenharia social pode-se dizer que é Goebbels, um antigo ministro das propagandas nazistas, que conseguiu tornar em políticos e heróis, quem antes eram criminosos, carrascos e tantos outros degenerados, transformando assim a mentira em verdade absoluta, mostrando somente o que as pessoas desejam ouvir e ver. Os autores concluem ainda que o ser humano é o mais explorado quando se trata de ataques de engenheiros sociais, sendo considerado o mais frágil na cadeia da segurança da informação, isto é, a parte mais vulnerável do sistema. (MARCELO E PEREIRA, 2005, p. 9).

3.1. Engenharia Social

Marcelo e Pereira (2005), a engenharia social é o método que consegue se beneficiar através de pontos como egocentrismo, vaidade e humildade, através da habilidade de cultivar as pessoas, conseguindo assim coletar informações sobre uma instituição ou pessoa.

A engenharia social precisa da vulnerabilidade humana para conseguir explorar a Segurança da Informação, pois quando o atacante foca seus ataques diretamente nos usuários faz com que essas investidas se tornem mais difíceis de se proteger, pois sistemas de segurança de *hardware* e *software* não funcionam. Dito isso, é de extrema importância a conscientização do usuário final, pois apesar de muitas vezes

ser considerado um método simples de prevenção, ele é o mais eficaz contra os ataques de engenharia social. (BAKHSHI, 2017).

Torres, Carvalho e Silva (2003, p. 129), complementam que a engenharia social pode ainda ser um simples grupo de tentativas, como meio para conseguir as informações desejadas, essas tentativas podem ser realizadas via contato telefônico, ou meio de ações mais complicadas, como por exemplo, tentar entrar nas instalações.

Para Bakhshi (2017), o engenheiro social utiliza-se de técnicas de manipulação humana como a urgência, autoridade, persuasão, pedidos de ajuda, personificação, entre outros métodos, para conseguir alcançar o ponto fraco humano e fazer com que o outro atenda suas solicitações.

3.2. Engenheiro Social

Marcelo e Pereira (2005, p. 4 e 5), o engenheiro social é uma espécie de malandro usufruindo da boa vontade do próximo e conquistando a sua confiança. Pode-se falar que existe dois tipos de engenheiros sociais os notórios-saber e os formados. Os formados são conhecidos como policiais, detetives e espiões, são especializados, tendo passado por treinamentos ou formação técnica.

Notório-saber geralmente possuem uma perspectiva e olhar diferente em relação a situações, em que a maioria tem um pensamento mais lógico, o notório-saber busca e pensa de maneira ilógica, sendo para ele o melhor jeito de resolver as situações e problemas. Vale lembrar que por não ser um profissional cadastrado é difícil de localizar, sendo assim considerado alguém perigoso. Quase sempre ele nasce de situações de necessidade. (MARCELO e PEREIRA, 2005, p. 6).

Ainda segundo os autores, Marcelo, Pereira (2005), o engenheiro social pode ser descrito como alguém que é detalhista e curioso, que tem a capacidade de investigar e aprender sobre a sua vítima, sempre em busca de pequenos detalhes e vulnerabilidades, que possa o levar a conquistar as informações desejadas.

Os autores dizem ainda que o livro “Mitnick: A arte de enganar” de Kevin Mitnick e Willian Simon, apesar de interessante, seus casos não se enquadram no Brasil, pois apesar do Brasil correr atrás para tirar o atraso tecnológico, ainda se encontra em defasagem. Para eles, Mitnick além de ser um dos maiores engenheiros sociais, foi

quem criou as primeiras metodologias que utilizam como ferramenta a tecnologia, para apoiar os ataques. Mesmo tendo desenvolvido a sua metodologia própria e sendo um engenheiro social engenhoso, ele caiu em sua própria armadilha ao ter a sua vaidade desafiada. Comprovando assim, que o homem cai em suas fraquezas e que essas falhas acabam sendo a sua ruína. (MARCELO E PEREIRA, 2005, p.12).

3.3. Modo de Agir do Engenheiro Social

Para Marcelo e Pereira (2005), é necessário primeiramente criar disfarce, para assim poder ter os primeiros contatos com a vítima. Existe três principais técnicas, contato telefônico, *e-mail* ou engenharia *on the fly*, que são utilizadas para roubos de informações e até mesmo dinheiro.

Contato Telefônico: Esse tipo de contato geralmente é feito para realizar o levantamento das primeiras informações necessárias. Onde deve-se tomar algumas precauções como utilização de telefones públicos, buscar identificar o cargo de cada pessoa na empresa e não ser reconhecido por ninguém, por exemplo. Sendo assim o telefone considerado um dos principais instrumentos para o ataque, pois com ele é possível realizar toda a sondagem das informações. (MARCELO e PEREIRA, 2005, p. 7).

Contato por *e-mail:* Segundo Marcelo e Pereira (2005), a partir do crescimento da Internet, muitas das atividades e troca de informações passaram a ser realizadas por *e-mail*, incluindo troca de dados importantes. Com isso o engenheiro social se aproveita para se passar por outra pessoa ou empresa, para que consiga pegar informações e até mesmo instalar programas que o auxiliem nessa busca de dados. É tida como uma categoria perigosa, conhecida como *phishing* que está fazendo vítimas em especial de forma bancária.

Segundo Yuge (2018), em um período próximo as eleições de 2018, foi ligada à Justiça Eleitoral um *e-mail* falso. Nesse *e-mail* havia uma convocação de um treinamento obrigatório para os mesários, utilizada de forma a chamar atenção. No corpo do *e-mail* dizia ainda que a pessoa foi convocada para trabalhar nas eleições de 2018 e pedia para ele comparecer ao fórum da sua cidade, e logo após sugere que a vítima faça um *download* do formulário anexo, caso ele não possa comparecer. Este

arquivo era malicioso, onde foi relatado que era instalado um vírus que podia roubar os dados bancários de usuários do sistema operacional *Windows*. A forma de urgência e de até mesmo da possibilidade de ter o CPF suspenso, levou as vítimas a caírem nesse tipo de golpe.

Engenharia Social *On The Fly:* Marcelo e Pereira (2005, p. 8), pode-se dizer que esse tipo de ataque é o mais arriscado e destemido, pois precisa ser feito pessoalmente. Geralmente o engenheiro social já está se passando por outra pessoa nesse momento, a procura de informações. Usualmente esse ato não é feito por novatos e exige que o atacante tenha experiência e já tenha algumas informações necessárias.

3.4. Engenharia Social no Brasil

O regime militar causou uma lacuna no desenvolvimento tecnológico no Brasil, onde se gerou uma geração de alienados e em seguida governos caóticos e corruptos. Saindo da década de 80 onde o país se encontrava em um abismo tecnológico, a década de 90 trouxe ao Brasil primeiramente as telecomunicações, seguida da informática e por último a Internet, só então as pessoas começaram a opor-se de alguns modelos existentes. (MARCELO E PEREIRA, 2005, p.13).

Marcelo e Pereira (2005), contam que os primeiros *hackers* brasileiros possuíam como objetivo primário invadir os provedores para adquirir os arquivos de senhas para Internet gratuita e então usar como se fosse uma ponte para ataques mais ousados. Podendo então considerar suas ações como anarquistas e a certeza de que estariam impunes de seus atos. Nessa época aconteceu uma série de coisas interessantes e a execução das primeiras operações de atacantes que agiam para roubar informações e dados de contas bancárias, cartões de crédito ou sites de movimentações bancárias, este ataque é conhecido como *“carding”*, esses ataques ocorreram contra alguns sites da época, como a *Amazon* que estava no seu início e a *CD World*. Entre o período considerado como a grande bolha (1996-1999), muitos crimes virtuais aconteceram, foi quando o *hacking* chegou ao conhecimento do povo, ao mesmo tempo muitos *hackers* ficaram conhecidos. Conforme o movimento foi se tornando popular, os *hackers* antigos foram sumindo e dando espaço para uma

geração nova, que passou a utilizar o termo *hacker* de uma forma errônea para tentar a autopromoção em cima dos antigos.

Com isso os antigos *hackers* ao se retirarem, começam a se tornar especialistas em segurança, e alguns criam empresas de informática. Entretanto, alguns poucos continuam com o *hacking*, criando assim um ângulo novo, onde uma nova geração surgira, os engenheiros sociais. Estes primeiros engenheiros sociais eram *carders*, isto é, pessoas que realizavam compras com o cartão de crédito dos outros. Todavia, muitos acabaram por levar uma vida no crime, pois não souberam a hora de parar. (MARCELO E PEREIRA, 2005, p. 14).

Marcelo e Pereira (2005) afirmam ainda que, atualmente esse grupo de criminosos causam preocupação para investigadores, devido à alta dos crimes cometidos e dos prejuízos que vem causando aos *e-commerce*. Apesar da luta contra esses delitos, são poucas as medidas que realmente funcionam, mesmo tendo um grande empenho da polícia.

4. LEGISLAÇÃO NO BRASIL E NO MUNDO

Para Dodt (2019), conformidade é o método para garantir de que as regulamentações e as leis, como também as diretrizes e políticas que foram estabelecidas na empresa, sejam cumpridas de forma satisfatória. Para que assim possa se certificar de que possíveis desvios e inconformidades que venham a ocorrer sejam evitados, detectados e tratados de forma correta, durante um prazo razoável. Diz ainda que de acordo com a ISO 27001, que para tal é indispensável esquivar-se de qualquer violação, seja ela de obrigações legais, regulamentares, estatuarias ou até mesmo contratuais que estejam associadas a segurança da informação.

Ainda segundo Dodt (2019), é preciso entender e saber quais são os danos que a violação de conformidade pode acarretar, podendo ser desde um prejuízo financeiro, impacto operacional, ações legais e a própria reputação da empresa. Para estar de acordo com a conformidade é preciso seguir um modelo de passos:

1. Entender os requisitos – Necessidade de saber sobre as leis e regulamentações ou obrigações contratuais se aplica a empresa. Quem é o responsável pelos requisitos. Os requisitos *compliance* devem estar identificados, documentados e atualizados.
2. Criar políticas internas – Percurso a ser seguido para atingir a conformidade. Declarar de forma categórica como deve ser cumprida a legislação nacional, internacional (se aplicável) e os regulamentos que o negócio está sujeito.
3. Analisar riscos – Realizar a identificação da probabilidade e de qual impacto uma violação ao *compliance* pode acarretar. Planejar o controle que deve ser realizado para garantir que seja cumprido todos os pontos da conformidade.
4. Documentar resultados – Precisa ser documentado todos os atos associados a conformidade, em especial as normas, procedimentos e política.
5. Tratar desvios – Desvios podem acontecer, mas é necessário que sejam tratados. Precisa ter controles para evitar que os mesmos aconteçam e que sejam detectados e tratados. É necessário que seja

> realizada a documentação de qualquer desvio que aconteça. (DODT, 2019).

Dodt (2019) complementa ainda que a conformidade é considerada um processo contínuo, onde cada uma dessas etapas será repetida.

4.1. General Data Protection Regulation (GDPR).

Segundo a Conube (2021), *General Data Protection Regulation* (GDPR), em português, Regulamentação Geral de Proteção de Dados, é uma lei da União Europeia (UE) voltada para a proteção de dados. Apesar de ter sido proposta no ano de 2016 ela somente entrou em vigor no ano de 2018.

Para Pinheiro (2020) a manifestação para o nascimento das regulamentações de proteção de dados pessoais, vem se firmando desde os anos 90, estando conectado de maneira direta com o crescimento da economia, principalmente quando as empresas passaram a aumentar o fluxo de bases de dados que transitam internacionalmente. Com isso surge a necessidade de reaver o comprometimento das organizações com os cidadãos, garantindo um dos direitos fundamentais que é assegurado pela Declaração Universal dos Direitos Humanos de 1948, que garante a privacidade.

Para o *High Security Center* (HSC) 2019, a GDPR tem como finalidade dar às pessoas o comando sobre os seus próprios dados pessoais, que acabam por transitar na Internet, sejam por meio de atividades em redes sociais ou por empresas que possuem essas informações do indivíduo. Sendo assim, o proprietário da informação passa a decidir se essa movimentação que acontece com os seus dados pessoais através de empresas pode continuar sendo feita. Onde as organizações passam também a seguir uma série de normas, ao manusear os dados para atender às exigências da lei.

Com o objetivo principal de intensificar a precisão da proteção de dados pessoais dos europeus. O que, por consequência, acaba afetando qualquer organização que tenha uma plataforma *online*, desde redes sociais, *e-commerce* e serviços bancários por exemplo. (CONUBE, 2021).

DocuSign (2018), diz ainda que a GDPR está associada diretamente às normas de segurança de dados das pessoas que fazem o uso da Internet, isso faz com que a regulamentação reflita sobre as atividades do mercado.

Conube (2021), afirma ainda que antes da GDPR já existia um grupo de regras e leis desde o ano de 1995, entretanto, devido aos avanços da tecnologia fez com que muitos serviços *online* fossem criados ou migrados para a plataforma *online*, o que ocasionou o surgimento da GDPR.

4.2. Lei Geral De Proteção de Dados (LGPD)

Dodt (2019), diz que a privacidade é um direito primordial do ser humano e que está prescrito na Declaração Universal dos Direitos Humanos, mais precisamente no artigo 12°, onde se declara que ninguém poderá sofrer de maneira autoritária intromissões em sua vida pessoal, familiar ou correspondências, da mesma forma o cidadão não poderá sofrer de ataques contra a sua honra e que para tais atos a pessoa pode contar com o direito a proteção da lei.

De acordo com o Serviço Federal de Processamento de Dados - SERPRO (2020), a Lei Geral de Proteção de Dados (LGPD) irá impactar diversos setores e serviços. A lei n° 13.709, mas conhecida como LGPD, foi sancionada em agosto de 2018 e com validade a partir de agosto de 2020. De forma clara a lei já diz que se trata de dados pessoais, determina que alguns desses dados devem ser cuidados de uma maneira mais especifica, como os dados de crianças e adolescentes, que são considerados sensíveis, e quaisquer outros dados tratados, sejam eles de maneira digital ou física, estarão suscetíveis a regulamentação.

Para Dodt (2019), a Lei Geral Brasileira de Proteção de Dados determina sobre como deve ser realizado o tratamento de dados, principalmente nos meios digitais e com isso muda o Marco Civil da Internet. A LGPD é aplicável à coleta de dados pessoais de indivíduos situados no Brasil, para o tratamento de dados realizado no Brasil, para oferta de serviços e bens para cidadãos no Brasil. Entretanto, ela não é aplicável em algumas situações, como: dados provenientes e/ou destinados a outros países, que estão apenas sendo transitados no Brasil, e a utilização pessoal, não comercial, para fins jornalísticos, artísticos ou acadêmicos e a segurança pública,

onde é até de certa forma controverso, devendo ser muito bem definido e realizado por especialistas em direito digital e direitos relacionados à informação.

É importante ressaltar que a LGPD serve para sedes de centros de dados e organizações em localidades nacionais ou estrangeiras, que tratam de dados de pessoas brasileiras e demais que se localizam no território do Brasil. (SERPRO, 2020).

Dodt (2019) aponta que existem quatro tipos de classificação de dados, os anonimizados, os pseudonimizados, pessoais e sensíveis, sendo assim as punições e sanções e os requisitos de proteção estão alinhados ao nível de privacidade. Dados sensíveis podem ser considerados convicções religiosas, opiniões políticas, orientação sexual, dados médicos e outros. Para esses tipos de dados a LGPD exige um nível de proteção maior e requisitos de segurança, consequentemente as sanções e punições serão maiores.

4.3. LGPD e o que motivou a sua criação

Após o surgimento da GDPR, que veio com o propósito de levar proteção dos dados pessoais para os cidadãos europeus, criou-se então uma ação em cadeia, pois com ela veio a exigência de que países e empresas que quisessem manter ou começar a ter relações comerciais com a União Europeia criassem uma regulamentação que mantivessem o padrão da GDPR (PINHEIRO, 2020).

O site *High Security Center* (HSC) (2019), completa dizendo que para que as organizações estrangeiras que possuem algum vínculo com empresas da UE e que manuseiam dados pessoais de cidadãos europeus, elas também precisam possuir uma regulamentação que corresponda as imposições propostas pela GDPR. Sendo influenciada pela Lei Europeia, o Brasil passa a ter a sua própria regulamentação para proteção de dados pessoais a LGPD, onde estabelece que quaisquer dados pessoais só podem ser coletados e tratados com o expresso consentimento do indivíduo proprietário dessas informações.

4.4. Explorando a legislação

Mesmo com a existência de leis que visam proteger os dados de usuários, como por exemplo, a GDPR, citada anteriormente, atacantes estão encontrando brechas na própria lei, como demonstrado por Robyns e Di Martino et. al (2019), no artigo *Personal Information Leakage by Abusing the GDPR "Right of Access",* em português Vazamento de Informações Pessoais Por Abuso do "Direito de Acesso" da GDPR. Com autorização das pessoas envolvidas, eles primeiro perguntaram a elas suas informações pessoais: nome completo da pessoa, uma lista com as organizações das quais eles sabiam que possuíam informações pessoais sobre eles, o link para um perfil público de mídia social dos participantes e o endereço residencial e de *e-mail* dos indivíduos. Em seguida, realizaram uma pesquisa onde obtiveram informações pessoais, através de fontes públicas, como por exemplo: mídias sociais ou registros do governo. Ao final dessa pesquisa, quase todas as informações passadas pelos participantes do estudo foram obtidas facilmente, com exceção do endereço residencial, que não descoberto.

4.4.1. Vazamento de dados explorando a GDPR

Para Kelion (2019), a GDPR pode ser explorada por atacantes para conseguirem acesso a dados pessoais de terceiros. Um especialista realizou uma pesquisa com algumas empresas com sedes locais nos Estados Unidos e Reino Unido, buscando ter acesso a informações feitas em nome de uma terceira pessoa, no caso de sua noiva, que estava ciente da pesquisa e o autorizou a realizá-la. Ele pôde chegar à conclusão de que em média, grandes organizações foram bem diante as solicitações, não entregando os dados. Já as organizações pequenas, costumavam o ignorar, talvez pela falta de conhecimento da lei. Mas as médias empresas como sabiam da existência da GDPR e talvez por não possuir um procedimento específico para tal, acabavam falhando e informando dados como: registro de diárias de sua noiva no hotel, registros de viajem realizadas por ela por determinadas empresas ferroviárias, antecedentes criminais, notas do ensino médio e até mesmo informações de cartão de crédito e previdência social.

Por ser uma lei relativamente nova, muitas empresas não possuem o conhecimento necessário e nem ao menos sabem muitas das vezes como fazê-lo de maneira correta, como a GDPR diminui o tempo hábil que uma organização possui

para atender as solicitações e inseriu juntamente uma penalidade para quem não o cumprir, isso acabou levando consequentemente ao erro de muitas empresas. (KELION, 2019).

4.4.2. Possíveis ataques que podem ocorrer no Brasil

Segundo Marl (2021), uma quantidade de aproximadamente 1,5 bilhões de informações confidenciais vazaram de um prestador de serviços eletrônicos que trabalha com algumas das maiores empresas de compras *online* no Brasil. A organização *Hariexpress*, localizada em São Paulo, trabalha atendendo clientes como *Amazon*, Mercado Livre, Magazine Luiza, BMW Digital e os Correios, visando aperfeiçoar a capacidade operacional e eficiência dos seus clientes.

O vazamento da *Hariexpress*, foi descoberto em julho de 2021, pelo pesquisador de segurança, Anurag Sen da *Safety Detectives*, onde segundo ele ocorreu devido a um problema de má configuração de um servidor que se encontrava desprotegido. Sendo divulgados mais de 610 GB de dados pessoais, apesar de informações bancárias dos clientes não serem divulgadas, dados como nome completo, *e-mails*, número de previdência social, endereço residencial e comercial, credenciais de *login* e detalhes de compras estavam entre os dados vazados. (MARL, 2021).

Marl (2021), enfatiza ainda a preocupação dos especialistas em segurança, onde os clientes podem sofrer não apenas com possíveis ataques de engenharia social e *phishing*, mas também de assaltos residências, comerciais e extorsão. Vale ressaltar que ANPD do Brasil, não comentou o caso até o momento.

5. PESQUISA SOBRE PERCEPÇÃO DO USUÁRIO

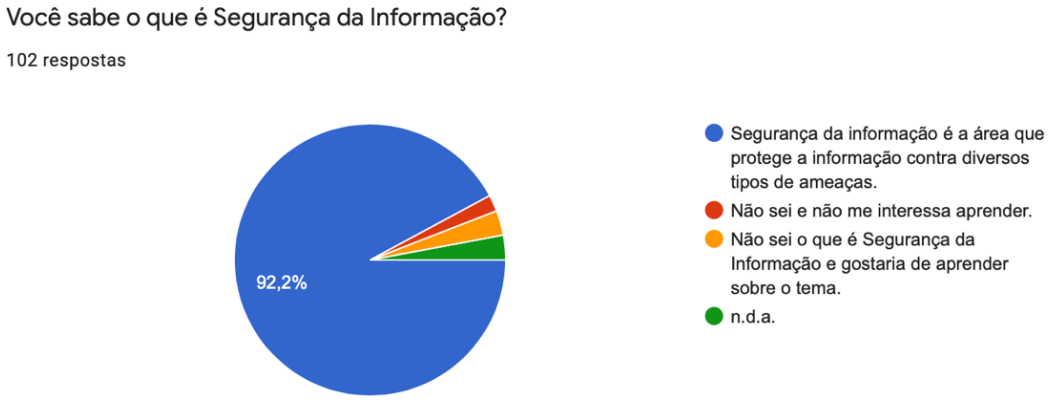
Ao longo do trabalho, desenvolvemos um questionário utilizando a ferramenta Formulários Google (que pode ser acessada através do link: https://www.google.com/intl/pt-BR/forms/about/), onde o objetivo deste questionário foi medir o nível de conhecimento dos participantes com questões relacionadas a Segurança da Informação, Engenharia Social e LGPD.

Tivemos um total de 102 respostas, sendo 39 participantes do sexo masculino e o restante (63 pessoas) do sexo feminino, onde a grande maioria 55,9%, possui a faixa etária de 18 a 27 anos, seguido pela faixa etária entre 28 a 37 anos (25,5%), sendo 13,7% com a idade de 38 a 47 anos.

Também perguntamos no questionário qual a escolaridade dos participantes e tivemos como resposta que a maior parte dos participantes estão cursando/são formados no ensino superior e/ou possuem pós-graduação.

Sabendo disso, questionamos se todos sabiam o que é segurança da informação. Pudemos então observar na Figura 1, que a grande maioria dos participantes, aproximadamente 92% conhecem o que é segurança da informação.

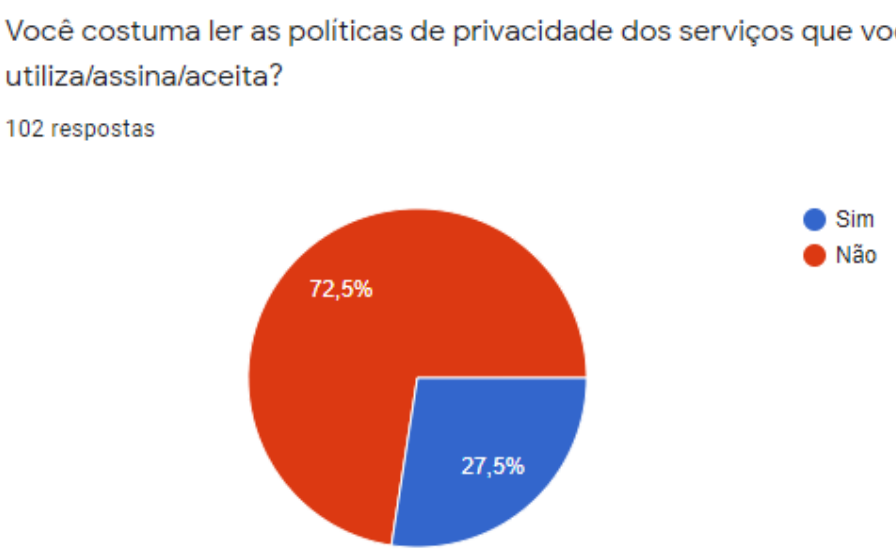
Figura 1 - Segurança da Informação



Fonte: Elaborado pelas autoras

Ao questionar se os participantes se preocupam com a proteção de seus dados pessoais praticamente todos, 99% responderam que sim, mas conforme Figura 2 apenas 27% possuem o costume de ler as políticas de privacidade dos serviços que utilizam.

Figura 2 – Políticas de privacidade



Fonte: Elaborado pelas autoras

Quando abordamos o tema se as pessoas têm conhecimento sobre qual a finalidade do tratamento e uso de seus dados pessoais pelas organizações e empresas apenas 7% responderam que tem conhecimento da finalidade, como pode ser observado na Figura 3. Pois, é importantíssimo saber qual o objetivo, para qual intuito seu dado pessoal será utilizado, para que não haja desvios de conduta por parte da empresa que realizou a coleta dos dados do usuário.

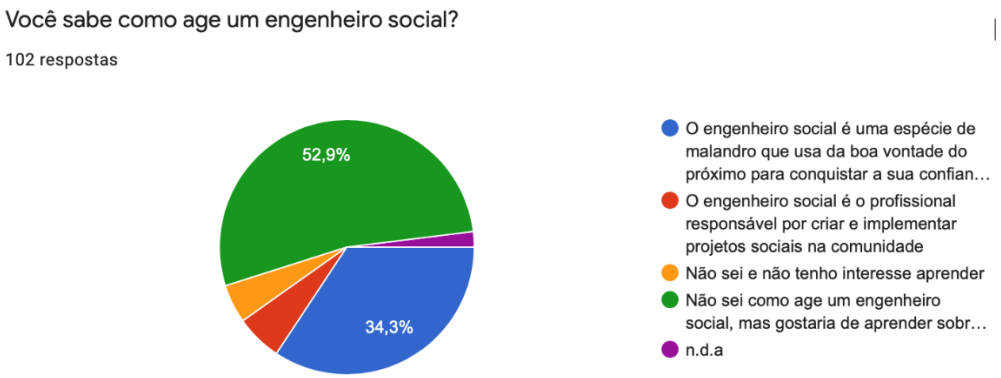
Figura 3 – Finalidade do tratamento de dados

Fonte: Elaborado pelas autoras

Quando questionados se possuem conhecimentos sobre diferentes tipos de ataques para roubo de dados pessoais, 95,1% afirmaram que sim. Mas, apenas 41,2% responderam corretamente à questão “Você sabe o que é engenharia social?” O que é menos da metade dos entrevistados, sendo um resultado alarmante.

Na questão seguinte, perguntamos se as pessoas conhecem o modo de agir de um engenheiro social. E como vimos na questão anterior a maior parte respondeu que não sabe/conhece, conforme mostra o gráfico da Figura 4

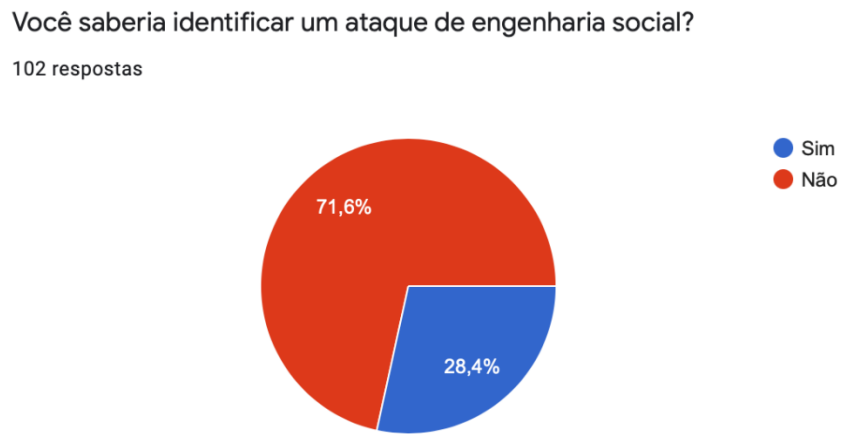
Figura 4 - Como age um engenheiro social



Fonte: Elaborado pelas autoras

Quando questionados se saberiam identificar um ataque de engenharia social, penas 28,4% responderam que sim, conforme Figura 5:

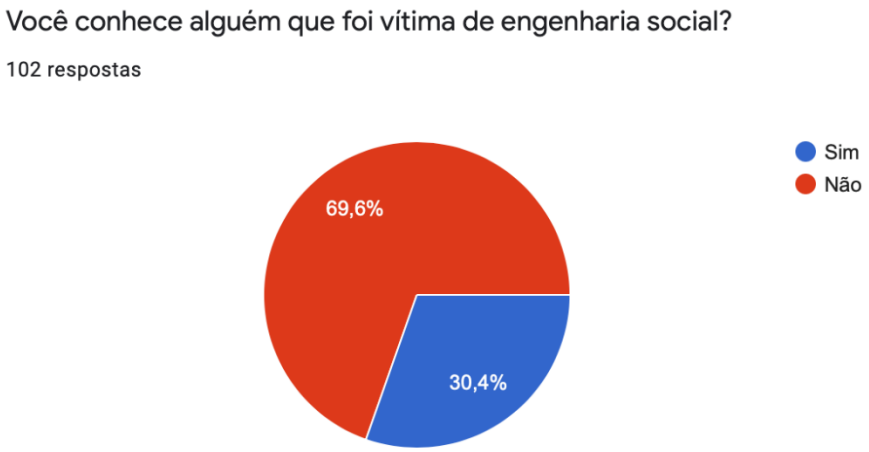
Figura 5 - Identificando um ataque de engenharia social



Fonte: Elaborado pelas autoras

Observamos que uma porcentagem um pouco maior, 30,4% dos participantes, conhece alguém que foi vítima de engenharia social, como pode ser observado na Figura 6:

Figura 6 - Vítimas de engenharia social

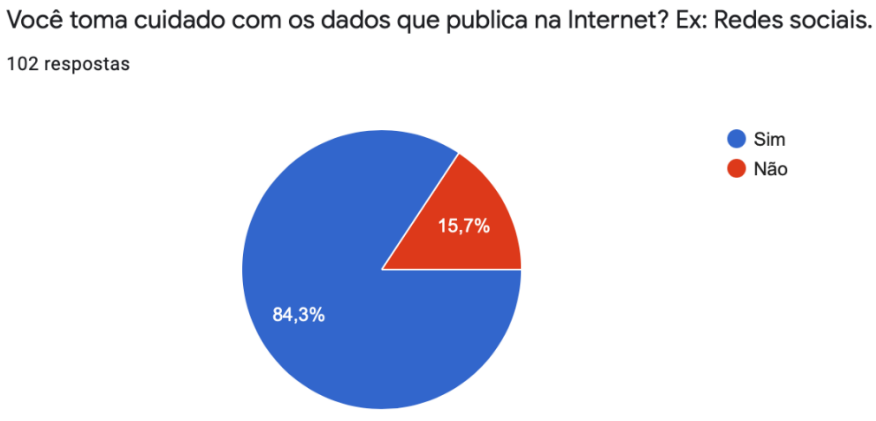


Fonte: Elaborado pelas autoras

Consideramos preocupante a pequena porcentagem de participantes que mesmo conhecendo um pouco sobre segurança da informação, conforme ilustra a Figura 1, poucos saberiam distinguir um ataque de engenharia social, não sabendo se proteger deste ataque ou não sabendo orientar familiares sobre as consequências de um ataque desse tipo.

Ao mesmo tempo, grande parte dos usuários, cerca de 84% responderam que tomam cuidado com os dados que publicam na Internet, conforme Figura 7

Figura 7 - Cuidados com redes sociais

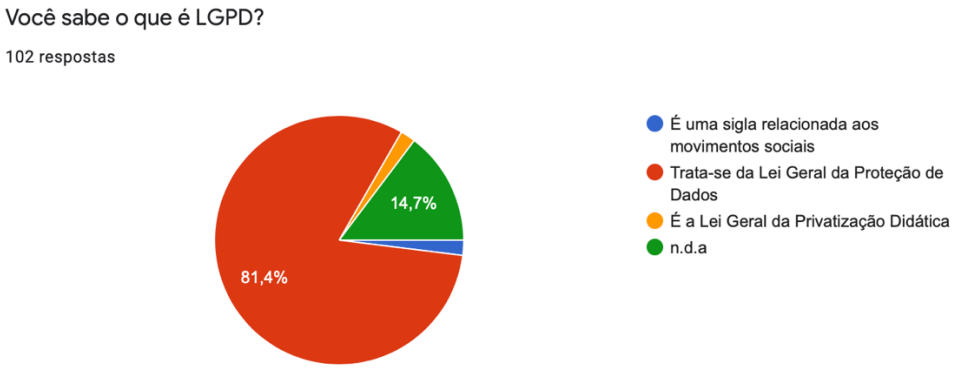


Fonte: Elaborado pelas autoras

Consideramos uma boa prática os cuidados com os dados publicados em redes sociais, pois isso limita a quantidade de informação que um engenheiro social pode obter para aplicar um ataque nesta pessoa.

Entrando no assunto de legislação, perguntamos se os colaboradores da pesquisa sabem o que é LGPD e grande maioria 81,4% acertaram a resposta correta, conforme Figura 8. Ao serem questionados se sentem-se seguros com a proteção dos seus dados pessoais, apenas 15,7% responderam que sim, como ilustra a Figura 9

Figura 8 - O que é LGPD



Fonte: Elaborado pelas autoras

Figura 9 - Proteção dos dados pessoais

Fonte: Elaborado pelas autoras

E quando questionados se já tiveram os seus dados pessoais vazados, 16,7% afirmam que infelizmente já vivenciaram essa situação e 27,5% desconfiam que já passaram pela mesma condição, conforme a Figura 10 aponta:

Figura 10 – Vazamento de dados pessoais

Fonte: Elaborado pelas autoras

6. CONCLUSÃO

Após ter sido realizado todo o levantamento bibliográfico, foi possível perceber o quanto o fator humano é um tema importante, ainda que não seja recente, continua sendo muito atual e necessário nos dias de hoje, pois, a cada dia que passa, a informação se torna o bem mais precioso, tanto para empresas quanto para pessoas e garantir que ela esteja segura está diretamente relacionado ao fator humano, já que as tecnologias para proteger as redes e os computadores estão cada vez mais avançadas e seguras, o elo mais fraco da segurança da informação se tornou o fator humano.

Cada vez mais as pessoas e até empresas tem utilizado técnicas de engenharia social para atingir seus objetivos, para tirar vantagens de terceiros, sendo eles pessoas comuns ou empresas. Este fator adjacente a recente aprovação da Lei Geral de Proteção de Dados (LGPD), nos coloca em um possível cenário futuro catastrófico, caso as organizações não deem a atenção devida ao tema e comecem a trabalhar em projetos de conscientização e treinamento de seus colaboradores.

Pode-se considerar a Lei Geral de Proteção Dados atualmente como uma das leis mais importantes existentes no país, uma lei que veio agregar onde a sua influência vai além de ser somente em meios tecnológicos e/ou *online*, ela é aplicável também para meios físicos, o que torna a sua abrangência muito maior, tornando o nível de responsabilidade para os que as detêm muito superior e consequentemente, espera-se que o grau de consciência ao se manusear essas informações cresça igualmente.

A LGPD tornou-se necessária devido ao cenário atual da nossa sociedade como um todo, onde a informação é o bem mais precioso, sendo utilizada até mesmo como moeda de troca em algumas situações. Assim sendo, a LGPD foi criada muito mais do que para apenas multar e aplicar punições nas organizações, ela veio para ajudar na organização dos dados que as empresas possuem, mostrando o valor de cada uma e qual a real necessidade da posse e do tratamento dos dados.

Mesmo tendo algumas garantias de proteção de seus dados, os usuários não podem confiar cegamente na LGPD e não tomarem conta de seus dados, passando

mais informações do que o essencial para as empresas e estabelecimentos. Também é de vital importância que os usuários tomem cuidado com as informações postadas por eles em redes sociais.

REFERÊNCIAS

BAKHSHI, Taimur. **Social engineering**: Revisiting end-user awareness and susceptibility to classic attack vectors. 2017 13th International Conference on Emerging Technologies (ICET), [S. l.], p. 1-6, 28 dez. 2017.

BRASIL, High Security Center. **O que é GDPR e o que muda para as empresas e os brasileiros?** 2019. Disponível em: https://www.hscbrasil.com.br/gdpr/. Acesso em: 04 out. 2021.

CONUBE. **O que é GDPR e como você e sua empresa podem ser impactados?** 2021. Disponível em: https://conube.com.br/blog/o-que-e-gdpr/. Acesso em: 16 nov. 2021.

CURSOS, Gran. **Informática**: Segurança da Informação. 2019. Gran Cursos Online. Disponível em: https://www.grancursosonline.com.br/download-demonstrativo/download-aula-pdf-demo/codigo/1cuh1IBdWfQ%3D#:~:text=Princ%C3%ADpios%20B%C3%A1sicos%20de%20Seguran%C3%A7a%20da%20Informa%C3%A7%C3%A3o,-Vou%20come%C3%A7ar%20falando&text=Eles%20norteiam%20as%20pol%C3%ADticas%20de,quanto%20a%20ambientes%20n%C3%A3o%20computacionais. Acesso em: 18 nov. 2021

DANTAS, Marcus Leal. **Segurança da informação:** uma abordagem focada em gestão de riscos. Olinda: Livro Rápido, 2011.

DICIO, Dicionário Aurélio *online*. **Significado de Informação**. Disponível em: https://www.dicio.com.br/informacao/. Acesso em: 20 nov. 2020.

DOCUSIGN. **GDPR**: entenda o que é o regulamento geral de proteção de dados. Disponível em: https://www.docusign.com.br/blog/gdpr-entenda-o-que-e-o-regulamento-geral-de-protecao-de-dados. Acesso em: 16 nov. 2021.

DODT, Claudio**. ISO 27001:** Curso completo para certificação EXIN ISFS!. (68. Legislação e regulamentação – segurança e conformidade). UDEMY. Disponível em: https://www.udemy.com/course/isfs-iso27001/learn/lecture/12324760#overview Acesso em: 25/11/2020.

DODT, Claudio. **ISO 27001:** Curso completo para certificação EXIN ISFS!. (71. Proteção e privacidade de informações pessoais - 01). UDEMY. Disponível em: https://www.udemy.com/course/isfs-iso27001/learn/lecture/12324760#overview Acesso em: 27 nov 2020.

DODT, Claudio. **ISO 27001:** Curso completo para certificação EXIN ISFS!. (71. Proteção e privacidade de informações pessoais - 02). UDEMY. Disponível em: https://www.udemy.com/course/isfs-iso27001/learn/lecture/13330936#overview Acesso em: 28 nov. 2020.

DODT, Claudio. **ISO 27001:** Curso completo para certificação EXIN ISFS!. (3. O conceito de informação). UDEMY. Disponível em: https://www.udemy.com/course/isfs-iso27001/learn/lecture/12246742#overview Acesso em: 28 nov. 2020.

DODT, Claudio. **ISO 27001**: Curso completo para certificação EXIN ISFS!. (4. Valor da informação). UDEMY. Disponível em: https://www.udemy.com/course/isfs-iso27001/learn/lecture/12246748#overview Acesso em: 28 nov. 2020.

DODT, Claudio. **ISO 27001:** Curso completo para certificação EXIN ISFS!. (5. Aspectos de confiabilidade). UDEMY. Disponível em: https://www.udemy.com/course/isfs-iso27001/learn/lecture/12246752#overview Acesso em: 06 nov. 2020.

GARANTIDO, Backup. **Quais são os pilares da segurança da informação e como colocá-los em prática?** 2018. Disponível em: https://backupgarantido.com.br/blog/pilares-da-seguranca-da-informacao/. Acesso em: 18 nov. 2021.

KELION, Leo. **Black Hat:** GDPR privacy law exploited to reveal personal data. BBC News, 2019. Disponível em https://www.bbc.com/news/technology-49252501 Acesso em 03/10/2021.

MARL, Angelica. **Brazilian e-commerce firm Hariexpress leaks 1.75 billion sensitive files.** 2021. ZDNet. Disponível em: https://www.zdnet.com/article/brazilian-e-commerce-firm-hariexpress-leaks-1-75-billion-sensitive-files/. Acesso em: 24 out. 2021.

MARTINO, Mariano di; ROBYNS, Pieter; et all. **Personal Information Leakage by Abusing the GDPR "Right of Access"**: this paper is included in the proceedings of the fifteenth symposium on usable privacy and security. 2019. 16 f. Tese (Doutorado) - Curso de Law Faculty, Usenix Association, Santa Clara, Ca, Usa, 2019. Disponível em: https://www.usenix.org/system/files/soups2019-di_martino.pdf. Acesso em: 22 nov. 2021.

MERCELO, Antônio; PEREIRA, Marcos. **A Arte de Hackear Pessoas:** Um guia para conhecer a Engenharia Social, os crimes digitais, os ataques de phishing e de como os novos criminosos estão atacando na Internet. Rio de Janeiro: Brasport, 2005.

NBR ISO/IEC 27002, Associação Brasileira de Normas Técnicas. **Tecnologia da informação:** Técnicas de segurança — Código de prática para controles de segurança da informação. 2. ed. Rio de Janeiro: ABNT, 2013.

PINHEIRO, Patricia Peck. **PROTEÇÃO DE DADOS PESSOAIS COMENTARIOS A LEI N 13.709/2018.** Editora Saraiva, 2020. Diponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=oXPWDwAAQBAJ&oi=fnd&pg=PT13&dq=dados+pessoais&ots=k8-mHqIM-P&sig=j2u_N1wEv_GSQJsh_9fJLGcgwcI#v=onepage&q=dados%20pessoais&f=false Acesso em 03/10/2021.

SANTIAGO, Christopher. **Você sabe o que significa não repúdio?** descubra neste post! 2018. Solutiresponde. Disponível em: https://solutiresponde.com.br/voce-sabe-o-que-significa-nao-repudio-descubra-neste-post/. Acesso em: 18 nov. 2021.

SÊMOLA, Marcos. **Gestão da Segurança da Informação:** uma visão executiva. 2. ed. Rio de Janeiro: Elsevier, 2014.

SERPRO, Serviço Federal de Processamento de Dados. **O Que Muda com a LGPD**. Disponível em: https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd. Acesso em: 26 nov. 2020.

SIMON, Willian; MITNICK, Kevin. **Mitnick:** A Arte de Enganar. São Paulo: Pearson Makron Books, 2006.

TORRES, Catarina; CARVALHO, Hugo; SILVA, Pedro. **Segurança dos Sistemas de Informação:** Gestão Estratégica da Segurança Empresarial. Lisboa: Editora Centro Atlântico, 2003.

YUGE, Claudio. **Cuidado com o phishing:** email falso da justiça eleitoral vem com vírus. 2018. Disponível em: https://www.tecmundo.com.br/seguranca/135507-cuidado-phishing-email-falso-justica-eleitoral-vem-com-virus.htm. Acesso em: 20 mar. 2021.