# A RELEVÂNCIA DA PREVENÇÃO CONTRA ATAQUES DE ENGENHARIA SOCIAL NO ÂMBITO EMPRESARIAL POR UMA PERSPECTIVA DA LGPD

# THE RELEVANCE OF SOCIAL ENGINEERING ATTACK PREVENTION IN THE BUSINESS ENVIRONMENT FROM AN LGPD PERSPECTIVE

Bruno Vicente de Carvalho[1]
Bruno Henrique Coleto[2]

## RESUMO

Este artigo explora a relevância fundamental de combater de forma eficaz os ataques de engenharia social no ambiente empresarial, com foco na Lei Geral de Proteção de Dados (LGPD). Em uma era digital, onde a informação ganha mais importância, o elemento humano se torna um alvo suscetível a ataques cibernéticos. A engenharia social utiliza manipulação psicológica para ludibriar indivíduos, extraindo informações confidenciais ou obtendo acesso não autorizado a sistemas. A lei, alinhada com os padrões globais de proteção de dados, destaca a necessidade de medidas preventivas robustas para garantir que os dados estejam íntegros e seguros. Este artigo explora como o combate aos prevalentes ataques de engenharia social, incluindo *phishing* e *pretexting*, é de extrema importância para a conformidade com as leis de proteção de dados pessoais. Ao integrar estratégias proativas de prevenção, as organizações não apenas fortalecem seus ativos de dados, mas também se alinham aos princípios da LGPD, promovendo a confiança e segurança entre as partes interessadas no cenário digital em constante evolução.

**Palavras-chave**: engenharia social; LGPD; prevenção; cibersegurança; privacidade.



## ABSTRACT

This article explores the fundamental relevance of effectively combating social engineering attacks in the business environment, with a focus on the LGPD. In a digital age where information is gaining increasing importance, the human element becomes a susceptible target for cyberattacks. Social engineering uses psychological manipulation to deceive individuals, extracting confidential information or gaining unauthorized access to systems. The law, in line with global data protection standards, emphasizes the need for robust preventive measures to ensure data integrity and security. This article explores how combating prevalent social engineering attacks, including phishing and pretexting, is of utmost importance for compliance with personal data protection laws. By integrating proactive prevention strategies, organizations not

[1] Centro Universitário Filadélfia de Londrina - UniFil
[2] Centro Universitário Filadélfia de Londrina - UniFil

only strengthen their data assets but also align with LGPD principles, promoting trust and security among stakeholders in the constantly evolving digital landscape.

**Keywords**: social engineering; LGPD; prevention; cybersecurity; privacy.

## 1 INTRODUÇÃO

Em um mundo onde os negócios estão cada vez mais digitalizados e conectados, a segurança da informação vem se tornando cada vez mais um desafio crescente e estratégico. Um dos focos atuais está na proteção de dados pessoais, cuja confidencialidade e integridade são fundamentais para a reputação da empresa, entretanto, ataques como os de engenharia social vem lançando uma sombra preocupante sobre essa questão crítica de segurança, ameaçando a estabilidade e a reputação das organizações.

A engenharia social é uma estratégia de manipulação psicológica que explora fraquezas humanas para obter informações confidenciais, acesso não autorizado a sistemas e redes corporativas, ou mesmo a realização de ações prejudiciais (Salahdine; Kaabouch, 2019). Nesse contexto, os invasores não se valem apenas de brechas tecnológicas, mas também da capacidade de persuadir e enganar as pessoas.



A Lei Geral de Proteção de Dados (LGPD) visa acrescentar uma camada adicional de preocupação quanto a segurança dos dados no contexto destes ataques.Esta visa estabelecer diretrizes rigorosas para como os dados pessoais serão tratados pelas empresas, não apenas com rigorosidade sobre a coleta, processamento, armazenamento e compartilhamento de dados, mas também reforça a necessidade de medidas preventivas para garantir a segurança dessas informações. (Rapôso *et al*., 2019)

Dentro desse cenário, a prevenção contra ataques de engenharia social se torna um componente crítico da estratégia de segurança de dados em ambientes corporativos. Este artigo busca analisar através de um estudo de caso a importância fundamental da prevenção contra ataques de engenharia social no contexto empresarial, com foco na perspectiva da LGPD. Também será visado elucidar como

a adoção de medidas eficazes de prevenção não apenas protege os ativos e informações empresariais, mas também como isto estaria de acordo com os princípios de privacidade e proteção de dados estabelecidos pela LGPD. Pretende-se evidenciar que a segurança contra a engenharia social não é apenas uma medida de proteção, mas uma exigência legal e ética para as organizações que almejam operar em conformidade com a LGPD.

## 2 ESTADO DA ARTE

A engenharia social, um método sofisticado de manipulação psicológica, tem se destacado como uma ameaça significativa no panorama da segurança da informação. Com a ascensão da era digital e o aumento na dependência de sistemas de informação, a engenharia social aparece como um desafio. Nesse contexto, a Lei Geral de Proteção de Dados (LGPD) representa um marco crucial. Essa legislação visa estabelecer diretrizes rígidas para o tratamento de dados pessoais, impulsionando a necessidade de estratégias proativas de prevenção e conscientização contra as artimanhas desses ataques para assegurar a privacidade e integridade de dados.



### 2.1 Ataques Cibernéticos

Nos dias atuais onde quase todo tipo de negócio possui uma parte ou se concentra exclusivamente no meio digital, as plataformas e recursos que concentram as informações e dados destas empresas são cada dia mais visadas para ataques que podem possuir diversos motivos e razões.

Segundo Rai e Mandoria (2019), as principais motivações de ataques cibernéticos atualmente são:

- **Crimes cibernéticos**: Esses ataques têm como principal objetivo a obtenção do recurso digital que está sendo atacado por meio de phishing, hacking ou spamming. Entre as razões para esse crime estão o acesso de informações de segredos comerciais ou dados pessoais e a realização de ações pelo recurso atacado se passando pelo real proprietário deste recurso;

- **Espionagem cibernética**: É a prática de obter informações confidenciais e sigilosas de sistemas de computador ou redes por meios não autorizados, muitas vezes conduzida por governos, organizações ou indivíduos com o objetivo de obter vantagens políticas, econômicas ou estratégicas;
- **Guerra cibernética**: Uso de operações cibernéticas para infligir danos a sistemas de computador, redes, infraestruturas críticas e ativos digitais de um adversário, com o objetivo de causar interrupções, destruição ou comprometimento da capacidade do adversário de conduzir operações normais. É uma forma de conflito que envolve ataques cibernéticos como parte de uma estratégia militar ou política;
- **Hacktivismo**: É uma forma de ativismo político ou social que envolve o uso de habilidades de hacking e tecnologia da informação para promover causas, divulgar informações, protestar ou causar interrupções online em nome de uma causa política, social ou ética.

### 2.1.1 Engenharia Social



A Engenharia Social é uma prática maliciosa que se baseia na manipulação de aspectos psicológicos e sociais dos indivíduos para obter informações confidenciais, realizar ações não autorizadas ou induzir a vítima a tomar decisões prejudiciais. Esses ataques visam explorar a confiança e a natureza muitas vezes previsível do comportamento humano em situações sociais ou online (Ariza *et al.*, 2022).

A definição destes ataques abrange uma variedade de técnicas enganosas e manipulativas, mas, em sua essência, envolve a exploração de interações sociais para alcançar objetivos maliciosos (Aldawood; Skinner, 2019). Isso pode incluir enganar uma pessoa para conseguir o acesso a informações como senhas, dados pessoais ou informações financeiras.

Abaixo a Figura 1 nos trás uma melhor visualização de um ciclo de vida deste tipo de ataque.

**Figura 1 –** Ciclo de um ataque de Engenharia Social


**Fonte**: Adaptado de Fortifirewall (2023)



Segundo Hijji; Alam (2021), o ciclo demonstrado na Figura 1 pode ser compreendido da seguinte forma:

- **Investigação**: Nesta primeira fase do ciclo de vida da engenharia social, o atacante identifica a vítima, coleta informações sobre o alvo e elabora estratégias para selecionar o método de ataque;
- **Ganho da Confiança**: É uma estratégia em que o atacante realiza tentativas de obter a confiança da vítima, tentando convencê-la de realizar ações acreditando na autenticidade do atacante. É nessa fase onde se procura assumir o controle da interação à medida em que a vítima é envolvida;
- **Ação**: Após conquistar a confiança da vítima, o atacante aproveita os recursos disponíveis e executa o ataque para acessar as informações de forma oportuna;
- **Saída**: A saída é a etapa final do ciclo de vida da Engenharia Social, na qual o invasor conclui a interação sem gerar desconfiança, eliminando todas as evidências do ataque e cobrindo seus rastros.

### *2.1.1.1 Phishing*

O *phishing* é uma técnica prevalente de engenharia social que visa enganar as vítimas, levando-as a revelar informações pessoais, financeiras ou credenciais de login, muitas vezes por meio de mensagens eletrônicas fraudulentas (Jain; Gupta, 2022). Essas mensagens frequentemente se passam por comunicações legítimas de instituições confiáveis, como bancos, lojas online, serviços de e-mail e redes sociais.

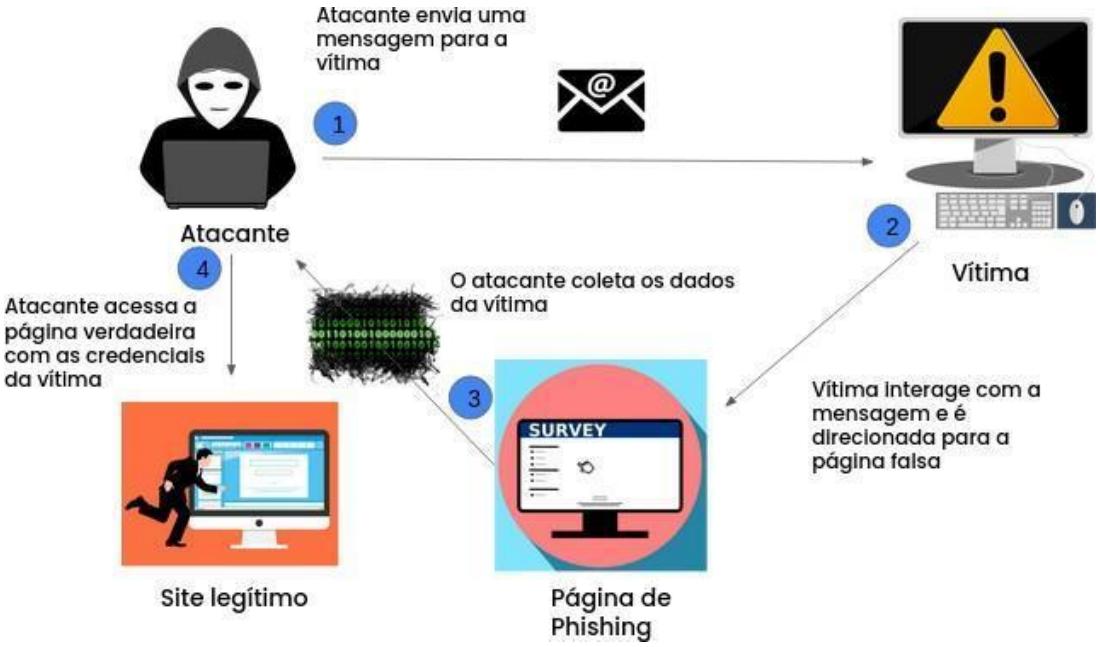
Segundo Alkhalil *et al.* (2021), entre as técnicas mais comuns de *phishing* estão:

- ***Phishing* por E-mail**: Mensagens de e-mail fraudulentas, muitas vezes contendo links ou anexos maliciosos, são enviadas para as vítimas;
- ***Phishing* por telefone (*Vishing* ou *Smishing*)**: Quando realizado através de mensagens de texto fraudulentas são enviadas para dispositivos móveis, este é denominado por *smishing*, onde é caracterizado pela tentativa de induzir a vítima a fornecer informações confidenciais ou a clicar em links prejudiciais. Já quando os atacantes usam chamadas telefônicas para se passar por organizações confiáveis, este é denominado de *vishing*;
- ***Phishing* por redes sociais (*Soshing*)**: Atacantes utilizam de redes sociais para enganar as vítimas e as direcionam para páginas falsas.



Na Figura 2 nos apresenta um exemplo da sequência de passos de um ataque de *phishing*.

**Figura 2 –** Sequência de um ataque de *phishing*




**Fonte**: Adaptado de Cloudfare (2023).



Conforme apresentado na Figura 2 podemos entender o passo a passo de como esses ataques funcionam da seguinte maneira:

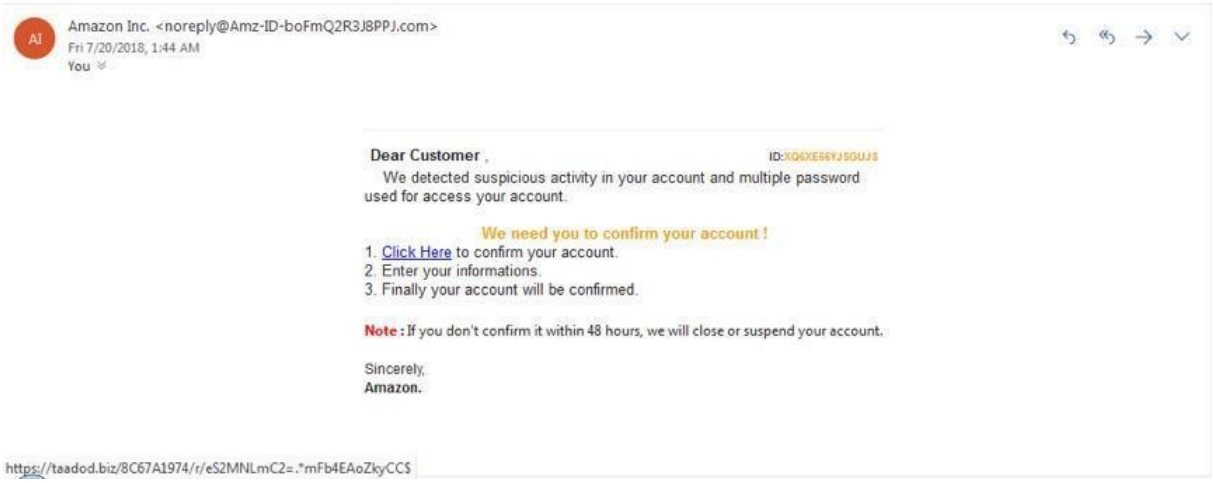
O atacante identifica potenciais vítimas ou organizações, frequentemente pesquisando redes sociais e vulnerabilidades específicas. Em seguida, cria uma mensagem convincente, muitas vezes se passando por uma entidade confiável.

Uma vez que a vítima interage com a mensagem, pode ser redirecionada para um site falso ou ter malware instalado em seu dispositivo. O invasor utiliza técnicas psicológicas para aumentar a probabilidade de sucesso na obtenção de informações cruciais, como senhas e números de cartão de crédito. As informações obtidas são usadas para acessar contas online, cometer fraudes financeiras ou serem vendidas.

Este esquema sequencial oferece uma visão simplificada das etapas que compõem um ataque de *phishing*, desde a seleção do alvo até a exploração das informações adquiridas. Compreender essas etapas é essencial para desenvolver estratégias eficazes de prevenção e conscientização contra esse tipo de ameaça.

A figura 3 nos trás um exemplo de um e-mail de uma tentativa de *phishing* onde o atacante se passa por uma organização confiável, neste caso a Amazon, para conseguir obter informações da vítima.

**Figura 3 –** Exemplo de um ataque de *phishing*




**Fonte**: Malwarebytes (2023)



Na figura 3 podemos notar com clareza a utilização de técnicas de manipulação psicológica da vítima, uma vez que o atacante realiza a criação de um senso de urgência ao ameaçar a suspensão da conta no caso que a vítima não tome providências no prazo de 48 horas.

### *2.1.1.2 Pretexting*

O *pretexting* é uma forma de engenharia social em que um atacante cria uma narrativa falsa ou pretexto para obter informações confidenciais. Esse pretexto muitas vezes envolve a criação de uma situação falsa e convincente que justifique a necessidade das informações solicitadas (Salahdine; Kaabouch, 2019).

O *pretexting* explora a natureza humana, incluindo a vontade de ajudar, a crença na autoridade, a simpatia e a relutância em questionar. As interações humanas são usadas como uma ferramenta para coletar informações sem suspeitas.

A conscientização e o treinamento são vitais para combater o *pretexting*. Os indivíduos devem ser educados sobre os riscos associados ao compartilhamento indiscriminado de informações, mesmo em situações que parecem legítimas. A

validação das solicitações de informações por meio de canais oficiais é uma prática fundamental.

## 2.2 Lei Geral de Proteção de Dados

A Lei Geral de Proteção de Dados (LGPD), possui como seu principal objetivo tratar sobre a proteção e a privacidade de dados no Brasil, estabelecendo princípios e diretrizes rigorosas para o tratamento de dados pessoais, com o objetivo de garantir a segurança e um tratamento adequado no uso dessas informações. (Rapôso *et al*., 2019).

Dados pessoais podem ser entendidos como informações relacionadas a uma pessoa identificada ou identificável através desses dados, incluindo assim qualquer informação que possa, direta ou indiretamente, identificar um indivíduo, como nome, endereço, e-mail, CPF, RG, dados de localização, orientação religiosa, entre outros. (Teffé; Viola, 2020).



As penalidades por não conformidade são substanciais, incluindo multas significativas e outras sanções administrativas. Isso ressalta a importância de as organizações não apenas adotarem práticas preventivas contra ataques cibernéticos, mas também garantir a conformidade com os princípios e requisitos estabelecidos. (Martin, 2020).

### 2.2.1 Agentes de Tratamento de Dados

A LGPD estabelece os agentes de tratamento de dados e suas responsabilidades, distinguindo controladores e operadores com base nas finalidades do tratamento. O controlador define quais são os objetivos e as formas de tratamento. Enquanto o operador executa conforme o estabelecido pelo controlador, cabendo a este realizar todas as medidas de natureza técnica ou administrativa, podendo decidir qual seria o sistema, o método e as ferramentas utilizadas para tal. (Fernandes; Nuzzi, 2022).

## 3 METODOLOGIA

O tema da Engenharia Social é discutido há décadas, sendo reconhecido como um desafio significativo. Nos últimos anos, com a crescente dependência e relevância dos dados pessoais na era digital, a prevenção contra esses ataques tornou-se crucial. A ascendente adoção de sistemas de informação em nossa rotina destaca a necessidade de programas de conscientização e defesa contra as táticas persuasivas destes ataques.

Empresas renomadas no âmbito da segurança cibernética disponibilizam, de forma periódica, análises detalhadas que evidenciam métricas relativas aos incidentes de segurança e de vazamentos de dados que estão ocorrendo na atualidade.

Neste trabalho, foi realizado um estudo de caso de um reporte que abrange os incidentes e vazamentos de dados ocorridos entre novembro de 2021 e outubro de 2022, trazendo uma visão sobre 16.312 incidentes de segurança nos quais 5.199 se transformaram em vazamentos de dados comprovados. (Verizon, 2023)



A Figura 4 nos traz em detalhes maiores os números a respeito da seção focada em números sobre Engenharia Social do Verizon Data Breach Investigations Report.

**Figura 4 –** Detalhes do relatório anual da Verizon sobre Engenharia Social

| | |
|---|---|
| **Frequency** | 1,700 incidents, 928 with confirmed data disclosure |
| **Threat actors** | External (100%), Multiple (2%), Internal (1%), Partner (1%) (breaches) |
| **Actor motives** | Financial (89%), Espionage (11%) (breaches) |
| **Data compromised** | Credentials (76%), Internal (28%), Other (27%), Personal (26%) (breaches) |

**Fonte**: Verizon (2023)

Através da Figura 4 podemos realizar algumas constatações sobre os ataques realizados através de Engenharia Social analisados no relatório:

- Dos 16.312 incidentes analisados no relatório, 1700 foram relacionados a Engenharia Social, correspondendo a 10,4% dos incidentes
- Dos 5.199 dos vazamentos de dados analisados no relatório, 928 foram relacionados a Engenharia Social, correspondendo a 17,8% dos vazamentos de dados.
- Os tipos de dados vazados foram: 76% foram relatados a roubos de credenciais, 28% foram informações internas comprometedoras das empresas, 26% foram dados pessoais e 27% foram outros tipos de dados.
- Através do item acima, podemos constatar que, em média, a cada 4 vazamentos em ataques de Engenharia Social, 1 estaria envolvendo dados pessoais.

Também de acordo ao reporte, a figura 5 nos traz dados sobre as estratégias adotadas pelos atacantes e a quantidade em porcentagem dos 1696 incidentes analisados.

**Figura 5 –** Estratégias adotadas em ataques de Engenharia Social



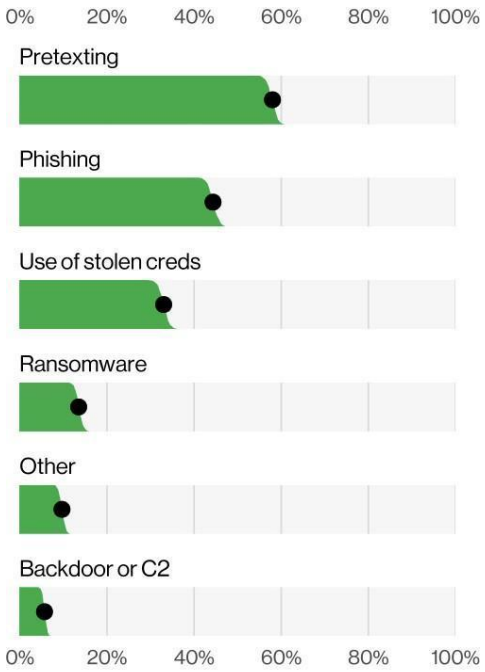


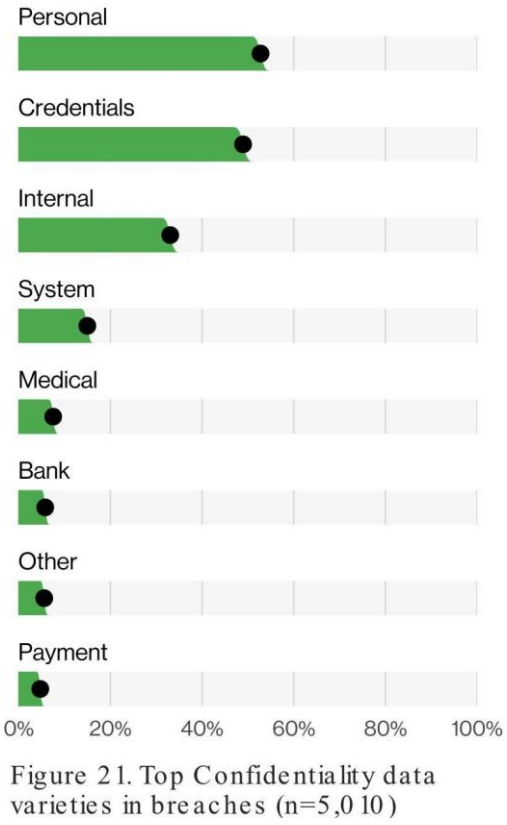

Figure 35. Action varieties in Social Engineering incidents (n=1,696)

**Fonte**: Verizon (2023)

Através da figura 5 podemos destacar os ataques utilizando as estratégias de *pretexting* e *phishing*, estando presentes respectivamente em aproximadamente 60% e 40% dos ataques de engenharia social analisados no relatório.

A figura 6, presente no relatório também nos trás uma visão detalhada sobre os tipos de dados presentes nos vazamentos de dados analisados no relatório.

**Figura 6 –** Tipos de dados presentes em vazamentos de dados




**Fonte**: Verizon (2023)

De acordo com o demonstrado na figura 6, podemos notar que dentre os ataques analisados, os dados pessoais estão liderando como o principal tipo de dado visados em vazamentos de dados, seguidos de credenciais de acesso e informações internas de empresas. Isso enfatiza a atual necessidade das empresas em focar cada vez mais seus esforços na proteção desse tipo de dados e também para conseguir cumprir com as regulamentações e leis ligadas à privacidade.

A LGPD deixa claro que dentre as responsabilidades dos agentes de tratamento, está a adoção de medidas técnicas e administrativas para que possam assegurar que os dados pessoais estejam protegidos de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qual- quer outra forma de tratamento inadequado ou ilícito, como também garantir que os dados pessoais estejam seguros mesmo após o fim do tratamento realizado (Costa, 2022).

De acordo com o (GOV.BR, 2023) caso ocorra um incidente de segurança e estejam presentes dados pessoais, é de dever do controlador realizar a comunicação aos titulares dos dados envolvidos, tendo como tempo recomendado para realização o prazo de 2 dias úteis após a ciência do fato. Além disto, o incidente passará por uma avaliação onde será determinado se a empresa sofrerá as sanções previstas pela LGPD, que poderão ser aplicadas nos casos de:

1. Não comunicar a Agência Nacional de Proteção de Dados ou os titulares de dados no tempo estabelecido.
2. Não realizar a adoção de medidas de segurança de acordo com o risco das atividades realizadas.



O art. 52 da LGPD menciona, entre outros pontos, as sanções que poderão ser aplicadas por infringir as medidas técnicas para prevenção de incidentes, contendo:

- Advertências, com indicações de prazos para adoção de medidas de segurança necessárias.
- Multas de até 2% do valor do faturamento anual da empresa ou de R$50.000.000,00 por infração.
- Publicação da infração.
- Bloqueio dos dados pessoais que estiverem presentes no incidente.
- Eliminação dos dados pessoais que estiverem presentes no incidente.
- Suspensão do banco de dados onde estão presentes os dados pessoais por um tempo limite de 6 meses e passível de extensão.

- Proibição das atividades relacionadas ao tratamento de dados pessoais.

Considerando as sanções estabelecidas pela LGPD para possíveis infrações nos tratamentos de dados realizados pelas empresas, ressalta-se a relevância da implementação de medidas preventivas tanto durante o tratamento de dados nas atividades quanto na defesa contra ataques de engenharia social. A adequada adoção dessas medidas não apenas alinha-se com as diretrizes da legislação, mas também fortalece a proteção dos dados e contribui para a promoção de um ambiente digital seguro e confiável da empresa.

Segundo Syafitri *et al*. (2022), dentre as medidas cabíveis de prevenção a ataques de engenharia social que podem ser utilizados, estão os seguintes items:

- Investir em treinamentos para os colaboradores, proporcionando conhecimento sobre as técnicas de engenharia social e sua identificação.
- Utilizar tecnologias de segurança, tais como filtros de spam, firewalls e autenticação multifatorial, fortalecendo a proteção dos sistemas.
- Implementar procedimentos organizacionais.Possíveis medidas seriam a adoção de políticas de senhas robustas e o controle rigoroso de acesso a informações confidenciais.
- Conscientizar os funcionários e usar ferramentas de filtragem de *phishing*.
- Utilizar da análise de comportamento para identificar atividades suspeitas que podem indicar um ataque.



## 4 RESULTADOS

Foi demonstrado neste artigo a importância da prevenção contra ataques de engenharia social no contexto empresarial, com foco na perspectiva da LGPD. Para isso, foi realizado um estudo de caso onde foram explorados números estatísticos de um reporte anual de incidentes de segurança de uma empresa de segurança da informação e então foram relacionados à proteção de dados pessoais, mostrando assim a importância de estratégias e práticas para prevenção ataques de engenharia social.

Os resultados indicam que os ataques de engenharia social são uma ameaça significativa para a segurança da informação no ambiente empresarial. De acordo com

o estudo apresentado, os ataques de engenharia social correspondem a 10,4% dos incidentes de segurança da informação nas empresas analisadas, sendo os ataques de *phishing* e de *pretexting* os mais comuns e representam uma ameaça significativa para a privacidade e a segurança dos dados pessoais.

O combate a esses ataques se mostra como um foco necessário com uma adoção de uma abordagem que envolva medidas técnicas e educacionais. As empresas devem implementar políticas de segurança da informação, treinar constantemente seus funcionários, usar ferramentas de detecção de *phishing* e de autenticação de usuários, entre outras estratégias. Além disso, esse combate se mostrou uma estratégia fundamental para que as empresas se mantenham atualizadas sobre as regulamentações da LGPD e também de se adequem às suas exigências para evitar possíveis sanções e prejuízos financeiros.

## 5 CONCLUSÃO



Este trabalho visou realizar um estudo de caso sobre como os ataques de engenharia social podem estar ligados a incidentes de dados pessoais e sobre como a importância da conscientização e prevenção destes ataques se mostra como uma estratégia crítica da segurança da informação no ambiente empresarial, especialmente no contexto da LGPD.

Concluímos que é necessário o envolvimento de medidas técnicas e educacionais, como treinamentos, adoção de políticas e adoção de medidas técnicas, incluindo a conscientização de seus funcionários dos riscos associados aos ataques de engenharia social e saibam como realizar a identificação desses ataques.

Garantir a segurança no que se trata de ataques de engenharia social pode ser entendido assim como fundamental para estar de acordo com a LGPD, assim as empresas devem estar cientes das exigências de medidas para conseguir prevenir a ocorrência deste tipo de ataque. A não adoção dessas medidas pode ser entendida como uma não conformidade com a LGPD resultando assim em sanções administrativas e financeiras, podendo até mesmo causar danos à reputação da empresa.

Para trabalhos futuros, poderão ser estudadas as sanções aplicadas pela

Agência Nacional de Proteção de Dados em incidentes relacionados à engenharia social no Brasil e como a ANPD se comportará nesses casos.

Por fim, é importante destacar que a prevenção contra ataques de engenharia social é um processo contínuo e que além de medidas técnicas, também exige a colaboração de todos os membros da empresa.

## REFERÊNCIAS

ALDAWOOD, H.; SKINNER, G. Contemporary cyber security social engineering solutions, measures, policies, tools and applications: A critical appraisal. **International Journal of Security** (IJS), v. 10, n. 1, p. 1, 2019.

ALKHALIL, Z. *et al.* Phishing attacks: A recent comprehensive study and a new anatomy. **Frontiers in Computer Science, Frontiers Media SA**, v. 3, p. 563060, 2021.

ARIZA, M. *et al*. Ataques automatizados de engenharia social com o uso de bots em redes sociais profissionais. *In*: SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS, 22., 2022. **Anais** [...]. [S.l.]: SBC, 2022. p. 153–166.

CLOUDFARE. **O que é um ataque de phishing?** 2023. Disponível em: https://www.cloudflare.com/pt-br/learning/access-management/ phishing-attack/. Acesso em: 23 out. 2023.

COSTA, R. B. **A lei geral de proteção de dados pessoais aplicada à internet das coisas**: uma revisão sistemática. 2022.

FERNANDES, M. E.; NUZZI, A. P. E. Fundamentos da lei geral de proteção de dados (lgpd): Uma revisão narrativa. **Research, Society and Development**, v. 11, n. 12, p. e310111234247–e310111234247, 2022.

FORTIFIREWALL. 2023. Disponível em: https://fortifirewall. com.br/Blog/O-Que-E-Engenharia-Social/b/47/. Acesso em: 30 out. 2023.

GOV.BR. **Comunicação de incidente de segurança.** 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/ agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acesso em: 10 out. 2023.

HIJJI, M.; ALAM, G. A multivocal literature review on growing social engineering based cyber-attacks/threats during the covid-19 pandemic: challenges and prospective solutions. **Ieee Access**, IEEE, v. 9, p. 7152-7169, 2021.

JAIN, A. K.; GUPTA, B. A survey of phishing attack techniques, defence mechanisms

and open research challenges. **Enterprise Information Systems**, Taylor & Francis, v. 16, n. 4, p. 527–565, 2022.

MALWAREBYTES. **Tudo sobre phishing**. 2023. Disponível em: https://br.malwarebytes.com/phishing/. Acesso em: 25 out. 2023.

MARTIN, B. Aplicação das penalidades da lei geral de proteção de dados. **Conhecimento Interativo**, v. 14, n. 2, 2020.

RAI, M.; MANDORIA, H. A study on cyber crimes cyber criminals and major security breaches. **Int. Res. J. Eng. Technol**, v. 6, n. 7, p. 1–8, 2019.

RAPÔSO, C. F. L. et al. Lgpd-lei geral de proteção de dados pessoais em tecnologia da informação: Revisão sistemática. **RACE-Revista de Administração do Cesmac**, v. 4, p. 58–67, 2019.

SALAHDINE, F.; KAABOUCH, N. Social engineering attacks: A survey. **Future internet, MDPI**, v. 11, n. 4, p. 89, 2019.

SYAFITRI, W. et al. Social engineering attacks prevention: A systematic literature review. **IEEE Access**, IEEE, v. 10, p. 39325–39343, 2022.

TEFFÉ, C. S. de; VIOLA, M. Tratamento de dados pessoais na lgpd: estudo sobre as bases legais. **Civilistica. com**, v. 9, n. 1, p. 1–38, 2020.

VERIZON. **Verizon Data Breach Investigations Report**. [S.l.], 2023.