Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

REVISTA SOCIEDADE CIENTÍFICA, VOLUME 7, NÚMERO 1, ANO 2024

ARTIGO ORIGINAL

A segurança da informação feita em camadas

Erick Neves Martinez[1]

Como Citar:
MARTINEZ, Erick Neves. A segurança da informação feita em camadas. Revista Sociedade Científica, vol.7, n.1, p.1634-1646, 2024.
https://doi.org/10.61411/rsc202414017

DOI:10.61411/rsc202414017

Área do conhecimento: Segurança da Informação.

Sub-área: Engenharia Social

Palavras-chaves: *Oversharenting*; Poder familiar; Conflito de princípios; Direitos Fundamentais.

Publicado: 25 de março de 2024

Resumo

O presente estudo analisa artigos com o tema Segurança da Informação com foco na Engenharia Social e o impacto na vida social dos usuários, bem como medidas de proteção contra ataques cibernéticos. Trata-se de uma pesquisa de revisão bibliográfica, a partir de consultas realizada nas bases de dados do Google Acadêmico e SciELO. Diante do inventário pode-se avaliar as características dos artigos publicados, e assim estabelecer parâmetros para uma melhor visão do objetivo estabelecido. Os resultados mostram que 75% não abordam o assunto alvo da pesquisa, 15% não apresentam informações ou evidenciam os resultados de forma clara e apenas 10% possuem elementos necessários para estudo. As conclusões destacam que grande parte dos artigos são superficiais e não trazem técnicas, formas e modelos atuais de ataques e como estes podem ser abordados dentro de sala de aula. Observado que o tema é pouco aplicado dentro das instituições de ensino e com em sua grande parte com visão apenas para o meio corporativo. Em relação à conclusão deste estudo, destaca-se a margem de pesquisa exploratória de como novas tecnologias podem ajudar no combate e entendimentos de ataques sofisticados.

Information security made in layers

Abstract

The present study analyzes articles on the topic of Information Security with a focus on Social Engineering and the impact on users' social lives, as well as protection measures against cyber attacks. This is a bibliographic review research, based on consultations carried out in the Google Scholar and SciELO databases. Given the inventory, it is possible to evaluate the characteristics of the published articles, and thus establish parameters for a better vision of the established objective. The results show that 75% do not address the target subject of the research, 15% do not present information or clearly highlight the results and only 10% have elements necessary for study. The conclusions highlight that most of the articles are superficial and do not present current techniques,

[1]Universidade Unicarioca – Rio de Janeiro – Brasil ✉

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

forms and models of attacks and how these can be addressed within the classroom. It was noted that the topic is little applied within educational institutions and for the most part with a view only to the corporate environment. In relation to the conclusion of this study, the scope for exploratory research into how new technologies can help combat and understand sophisticated attacks stands out.

Keywords: Social engineering. Hacker. Threat. Information security.

1. Introdução

Nos últimos anos, a segurança da informação vem ganhando mais espaço dentro das instituições de ensino, seja ela pública ou particular e se tornou algo tão importante quanto as demais áreas de estudos, como por exemplo a matemática, português ou história e diante dessa evolução acelerada do mundo globalizado e interconectado, diversos riscos estão surgindo associados a forma como a qual estamos utilizados dispositivos e tecnologias, não tendo a percepção do perigo que isso pode nos gerar. Segundo MORAES (2014), estudos realizados demonstram que a tecnologia possibilitou alterações no modo comportamental de como os usuários buscam facilidades e formas rápidas para executar atividades e resolver problemas ao longo do seu dia, fazendo com que esse novo modo de vida não seja apenas um artigo de luxo, mas sim uma necessidade real no dia a dia e ao mesmo tempo trazendo uma sensação de poder por não necessitar de esforço para executar ações básicas, como ir ao mercado.

Ficamos anestesiados pela facilidade e comodidade, mas não somos informados ou notificados sobre os perigos do mundo digital, pois ninguém vende uma tecnologia, como por exemplo o celular (smartphone) e diz que se utilizamos de maneira incorreta isso poderá trazer algum tipo de infelicidade, esse marketing não é lucrativo e muita das vezes os próprios vendedores não possuem noção ou conhecimento de quais serão esses riscos e como devemos agir caso sejamos o alvo do dia. Segundo DANTAS (2011), refere que a Segurança da Informação necessita assegurar os três pilares essenciais,

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

trazendo a Confidencialidade, Integridade e Disponibilidade, também conhecida como a tríade CID, dos dados obtidos ou armazenados, pois são os principais fundamentos da Segurança da Informação.

Com a crescente expansão do uso da Internet nos últimos anos, as empresas de telecomunicações têm aumentado suas ofertas de serviços ligados à conectividade. A pandemia de COVID-19 acelerou ainda mais a transformação digital em todo o mundo, tornando a conectividade ainda mais vital para a vida pessoal e profissional das pessoas. VIEIRA; DIAN (2023).

Como dizem, a educação vem de casa, mas e quando ele não está presente em nossas famílias e amigos, como e onde poderemos obter o conhecimento ou tirar dúvidas? O que devo fazer? Quem devo notificar? Essas e outras perguntas são frequentemente feitas quando somos deparados com alguma ocorrência, como por exemplo: roubo de Facebook, vazamento de dados, clonagem de celular, essas e outras ataques vem aumentando e ganhando os noticiários das TV's e rádios no nosso país.

Juntamente com as vantagens da tecnologia e do uso da internet, criminosos e oportunistas podem se apropriarem de informações confidenciais e da privacidade os usuários (OLIVEIRA; FILGUEIRAS 2022).

Diante do exposto, esse estudo faz uma revisão bibliográfica sistemática de diversos artigos publicados nas plataformas digitais em um período fixado entre os anos de 2019 e 2023, buscando artigos publicados com o tema segurança da informação com ênfase em educação, os quais visam identificar como os artigos podem ser utilizados dentro de uma instituição de ensino.

2. Pesquisa e metodologia

A palavra pesquisa pode ser considerada um ato de buscar respostas para boas perguntas, geradas por diversas questões pessoais ou profissionais, com o propósito de não apenas descobrir a verdade, mas sim fundamentar e estruturar o resultado final.

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

Segundo GOLDENBERG (2009, p. 21), pesquisar é juntar dados não tratados, para assim serem processados e gerar valor, neste sentido virar informação para localizar respostas para uma pergunta, com o intuito de resolver um determinado problema.

> Na condição de princípio científico, pesquisa apresenta-se como a instrumentação teórico-metodológica para construir conhecimento. Como princípio educativo, pesquisa perfaz um dos esteios essenciais da educação emancipatória, que é o questionamento sistemático crítico e criativo. Neste sentido, educar e construir conhecimento podem aproximar-se, e, em alguns momentos, mesmo coincidir, desde que não se mistifique a construção de conhecimento, que é apenas meio. A educação possui, ademais, a relação com fins, valores, afetos e sentimentos, cidadania e direitos humanos, aos quais os meios deverão servir (DEMO, 2009, p.33).

A metodologia pode ser descrita como um meio de ordenar, estruturar a lógica à pesquisa que será construída pelo pesquisador, orientando e direcionando o caminho que ele deve seguir. Para o autor GOLDENBERG (2009), compreende que a metodologia orienta o pesquisador a observar e ter um senso crítico e científico, buscando assim desenvolver no mesmo uma estrutura sólida, inovadora, limpa e crítico.

De acordo com Lakatos e Marconi (1987) evocam que a deliberação da metodologia é crucial, pois elucida diversos pontos da pesquisa: “como?, com quê?, onde?, quanto?” (LAKATOS e MARCONI, 1987, p.105).

O método utilizado é revisão bibliográfica sobre o tema de segurança da informação na educação. Método científico pode ser definido como um conjunto de etapas e instrumentos pelo qual o pesquisador científico, direciona seu projeto de trabalho com critérios de caráter científico para alcançar dados que suportam ou não sua teoria inicial (CIRIBELLI, 2003).

Diante deste contexto, os objetivos desta pesquisa são:

[1] Identificar artigos publicados contendo Segurança da Informação com foco no ataque de Engenharia Social.

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

[2] Avaliar se os artigos possuem informações que possam ajudar outros usuários.

Assim, as perguntas de pesquisa levantadas foram:

1. Qual o conteúdo publicado a respeito do ataque de Engenharia Social?
2. Quais as formas que são apresentadas para identificar, combater e mitigar esse tipo de ataque cibernético?

2.1 A proposta de revisão bibliográfica

O presente estudo tem sua metodologia estabelecida na revisão bibliográfica em consultas realizadas em plataformas que possuem repositórios com artigos indexados, como o Google Acadêmico e SciELO, consulta está realizada entre as datas de 01 de novembro de 2023 até o dia 09 de dezembro de 2023. A pesquisa apresentada tem como objetivo quantitativa pois manifesta um levantamento do conteúdo de medidas e contra medidas para mitigar ataques de Engenharia Social, mas não tratando o resultado final.

O artigo utiliza a metodologia fundamentada na leitura e na revisão bibliográfica de diversos artigos publicados, com o tema segurança da informação, mas com foco no ataque de Engenharia Social, disponibilizadas em diversas plataformas virtuais, com o objetivo principal de quantificar, visto que o ataque em destaque está cada dia mais sendo utilizado em diversos meios, seja ele físico ou digital.

A investigação quantitativa atua em níveis de realidade e tem como objetivo trazer à luz dados, indicadores e tendências observáveis. A investigação qualitativa, ao contrário, trabalha com valores, crenças, representações, hábitos, atitudes e opiniões (MINAYO e SANCHES, 1993).

Após definir as palavras chaves e submeter nas consultas nas plataformas online, obteve o seguinte resultado de artigos publicados por ano.

Tabela 1 Resultado de pesquisa em plataformas digitais.

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

	ARQUIVOS LOCALIZADOS		POR ANO				
	TOTAL	BRASIL	2019	2020	2021	2022	2023
SciELO	191	80	22	18	18	13	9
Google Academyc	256	251	60	55	62	49	31

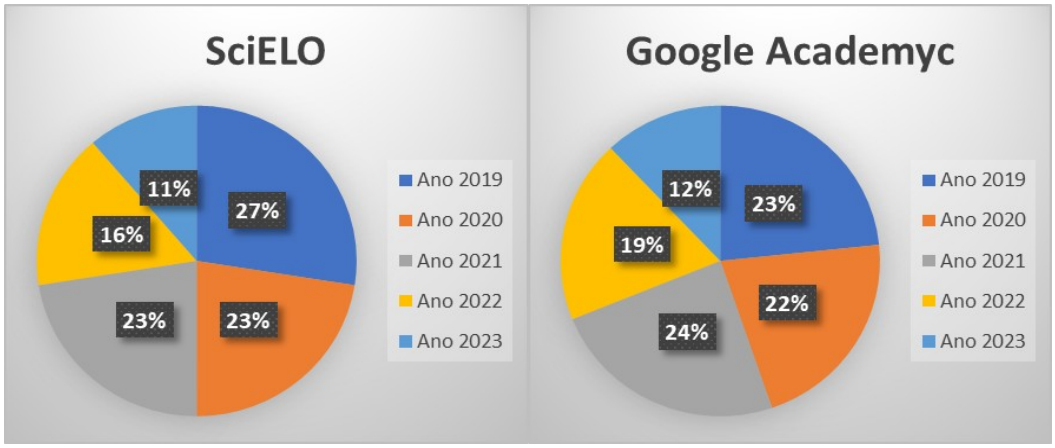

Figura 1 Analise por ano de publicação.

2.2 Vulnerabilidades e ameaças

Podemos definir vulnerabilidade como uma falha em um sistema que permite a um atacante usá-lo de uma forma não prevista pelo projetista (ANLEY, 2007), sendo assim, a vulnerabilidade possibilita que usuários não autorizados possam acessar de forma ilícita o sistema e por conta da falha acaba gerando uma ameaça ao ambiente.

Segundo PEREIRA; VICENTE; RIZO (2022), a ameaça pode ser descrita como um caminho que levam a possibilidade de um ataque ou acesso não autorizado em dispositivos ou recursos, podendo ser acarretada de forma indireta ou indireta, com o objetivo de causar problemas ao seu alvo.

Os 2 tipos que podem ser classificados a palavra ameaçam interna ou também cunhada como insider:

> "Internas: geralmente os responsáveis por danos causados internamente são funcionários insatisfeitos, que querem prejudicar o desenvolvimento do trabalho ou

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

> tirar vantagens financeiras. Outros responsáveis são prestadores de serviços e funcionários terceirizados. Como exemplo de ameaças internas destacam-se o roubo de informações, a alteração ou destruição de informações, os danos físicos a hardware e alteração de configurações e danos lógicos à rede." (GABBAY, 2003, p. 24).

3 Resultados e considerações

Após realizar pesquisas e a leitura dos diversos artigos foi utilizado o método de exclusão seguindo as seguintes premissas:

- Não aborda o tema em sala de aula.
- Não possui elementos claros sobre segurança da informação na educação.
- Aborda de forma genérica o tema, trazendo apenas informações sobre o significado, mas não o como pode mitigado ou utilizado na sala de aula.

O resultado obtido com o levantamento realizado aponta que grande parte das publicações com o tema Segurança da Informação, não abordam o tema Engenharia Social de forma clara, objetiva e com exemplos de como o mesmo pode ocorrer dentro ou fora de instituições de ensino ou corporativo, bem como as ações para mitigar ou educar os seus usuários.

A Engenharia social de acordo com BERTI e ROGERS (2004), descreve:

> "As tentativas bem-sucedidas ou fracassadas para influenciar uma pessoa a revelar qualquer informação ou agir de uma forma que possa resultar em acesso não autorizado, uso não autorizado de, ou divulgação não autorizada de um sistema de informação, de uma rede ou de dados."

Para MITNICK e SIMON (2003), a ator de ameaça que se declara um engenheiro social, é um usuário que realiza ações maliciosas através de manipulação com o objetivo de conquistar informações privadas a respeito de seu alvo, enganando-o, com propósito de lesar de forma material e psicológicos.

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

O Brasil registrou uma redução de ataques cibernéticos ao longo do ano de 2023, segundo o estudo realizado pelo Instituto Information Management, onde registrou uma queda em algumas áreas e um aumento em outras.

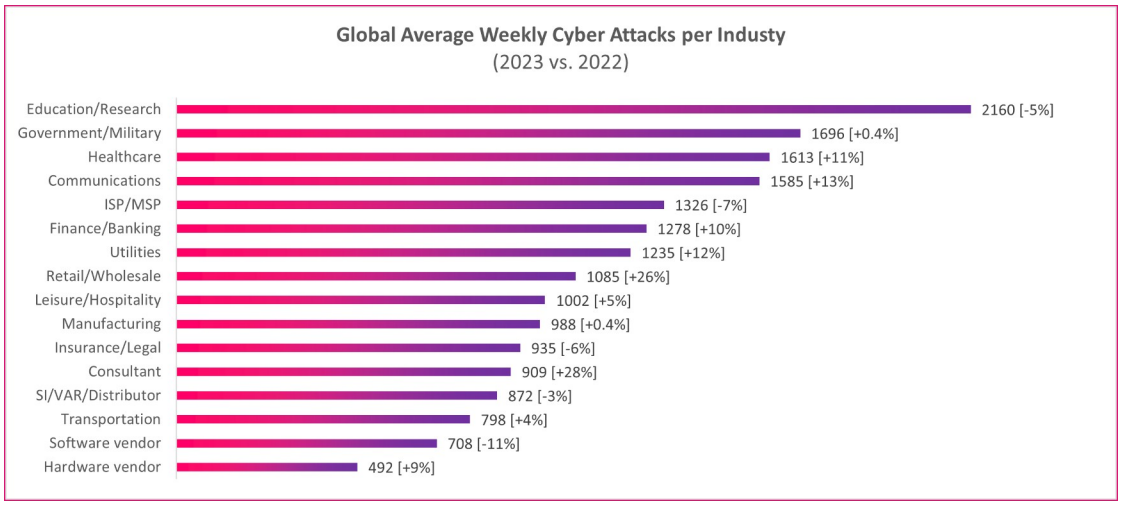

Figura 2 Ataques por tipo de indústria. Fonte:https://docmanagement.com.br/11/08/2023/brasil-registra-queda-de-ataques-ciberneticos-nos-primeiros-tres-trimestres-de-2023/ (Acessado em 29 nov. 2023).

Observando ataques por região global, notou-se que algumas tiveram um aumento significativo, como por exemplo a APAC e outras sofreram uma redução mínima em comparação as demais regiões. Já no Brasil, nos três primeiros trimestres do ano de 2023, foi registrado uma pequena redução de 3% nos ataques digitais.

Região	Média de ataques semanais por organização	Mudança Ano a Ano
África	1.987	6%
APAC	1.963	15%
América Latina	1.663	+0.4%
Europa	966	-1%
América do Norte	939	5%

Figura 3 Ataques cibernéticos por região. Fonte:https://docmanagement.com.br/11/08/2023/brasil-registra-queda-de-ataques-ciberneticos-nos-primeiros-tres-trimestres-de-2023/ (Acessado em 29 nov. 2023).

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

Observado que na região das Américas houve uma na média de ataques semanais por organização, tendo como o Chile com um aumento forte de 13% e um destaque positivo para o Canadá onde a redução foi de -20% ano a ano.

Região	País	Média de ataques semanais por organização	Mudança Ano a Ano
Américas	Argentina	880	0%
	Brasil	747	-3%
	Canadá	335	-20%
	Chile	639	13%
	Colômbia	1.184	0%
	México	825	-5%
	Estados Unidos	443	4%

Figura 4- Ataques cibernéticos por região das Américas.
Fonte:https://docmanagement.com.br/11/08/2023/brasil-registra-queda-de-ataques-ciberneticos-nos-primeiros-tres-trimestres-de-2023/ (Acessado em 29 nov. 2023).

Diante dos gráficos apresentados, a tecnologia vem abrindo diversas portas e a evolução destas acabam criando novas formas de ataques digitais, causando insegurança aos que utilizam. Uma vez que há este risco, a preocupação de como as informações são manipuladas entre os usuários em uma rede, torna necessário tomada de medidas que visam a segurança da informação (COELHO;RASMA;MORALES, 2013).

4. Considerações finais

O objetivo desta pesquisa foi analisar a produção de outros artigos científicos a respeito de segurança da informação aplicada em sala de aula utilizando como base de consultas o SciELO e Google Acadêmico, na linguagem brasileira. O foco da pesquisa

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

tem como artigos publicados nos últimos 5 anos, entre 2018 e 2023, tendo possível identificar oportunidades de pesquisa em segurança da informação.

Os principais pontos de destaque para a construção deste artigo são os critérios de seleção e filtro para “segurança da informação” e “educação escolar” no título dos artigos. Dentre os 40 artigos selecionados para a confecção deste trabalho, 25 não abordavam de forma clara e objetiva o uso da segurança da informação dentro de sala de aula e 10 não continham informações relevantes que pudessem ajuda na formação ou instrução dos docentes e discentes, restando apenas 5 que tiveram dados suficientes para seguir no processo até o final. Verificou-se que grande parte dos artigos relacionados a segurança da informações publicadas tem como objetivo dissertar a respeito de pontos básicos ou pontos únicos da segurança da informação, como por exemplo o ataque de engenharia social, mas deixando lacunas de como os usuários podem identificar e se proteger contra.

Logo, a construção deste artigo, a partir de ensaio exploratório, ajudou para observar que os artigos relacionados a segurança da informação são rasos e não apresentam formas e técnicas de ataques atuais e como se defender, como, por exemplo, hardware hacking, possibilitando assim a criação de outros documentos ou dissertações a respeito do mesmo.

5. Declaração de direitos

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

6. Referências

1. ANLEY, C. The shellcoder's Handbook: discovering and exploring Security holes. 2ª.ed. Editora Wiley. Data de publicação: 2007. ISBN 9780470080238.
2. BERTI, John; ROGERS, Marcus. Social engineering: The forgotten risk, in Information Security Management Handbook. vol. 3, H. F. Tipton and M. Krause, 4 ed, New York: Auerbach. Data de publicação: 2004. ISBN 0849374952.
3. COELHO, Cristiano Farias; RASMA, Eline Tourinho; MORALES, Gudelia. Engenharia Social: uma ameaça à sociedade da informação. Exatas & Engenharias. Campos dos Goytacazes, v. 3. Data de publicação: 2013. ISSN 2236-885. Disponível em: https://ojs3.perspectivasonline.com.br/exatas_e_engenharia/article/view/87/59. Acesso em: 12/12/2023.
4. CIRIBELLI, Marilda Corrêa. Como elaborar uma dissertação de Mestrado através da pesquisa científica. Marilda Ciribelli Corrêa, Rio de Janeiro: 7 Letras, 2003. ISBN 85-7577-081-0.
5. DANTAS, Marcus Leal. Segurança da Informação - Uma Abordagem Focada em gestão de Riscos. Olinda. Livro Rápido. Data de publicação: 2011. ISBN 97885406004781.
6. DEMO, Pedro. Metodologia do Conhecimento Científico. São Paulo: Editora Atlas. Data de publicação: 2009. ISBN: 9788522426478.
7. GABBAY, Max Simon. Fatores influenciadores da implementação de ações de Gestão de Segurança da Informação: um estudo com Executivos e Gerentes de Tecnologia da Informação em empresas do Rio Grande do Norte. Data de publicação: 2003. Disponível em: https://repositorio.ufrn.br/bitstream/123456789/14985/1/Max%20Simon%20Gabbay.pdf. Acesso em 28 nov. 2023.

Scientific Society Journal
ISSN: 2595-8402
Journal DOI: 10.61411/rsc31879

8. GOLDENBERG, Mirian. A Arte de Pesquisar. 17ª Ed. Rio de Janeiro: Editora Record. Data de publicação: 2009. ISBN: 8501049654.
9. LAKATOS, Eva Maria e MARCONI, Marina de Andrade. Metodologia do Trabalho científico. 2 ed. São Paulo: Editora Atlas. Data de publicação: 1987. ISBN: 8597026537.
10. MORAES, Dulcimara Carvalho. A internet como ferramenta tecnológica e as consequências de seu uso: aspectos positivos e negativos. Revista Científica Semana Acadêmica. ISSN 2236-6717. Data de publicação: 2014. Disponível em: https://semanaacademica.org.br/artigo/internet-como-ferramenta-tecnologica-e-consequencias-de-seu-uso-aspectos-positivos-e. Acesso em 28 nov. 2023.
11. MITNICK, Kevin; SIMON, William. A Arte de Enganar: Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. Editora Pearson. Data de publicação: 2003. ISBN: 8534615160.
12. MINAYO, Maria Cecilia; SANCHES, Odécio. O Quantitativo-qualitativo: oposição ou complementaridade?. Caderno de Saúde Pública. Data de publicação: 1993. Disponível em: https://www.academia.edu/26132359/Quantitativo_Qualitativo_Oposi%C3%A7%C3%A3o_ou_Complementari_dade. ISSN: 239-262. Acesso em 29 nov. 2023.
13. OLIVEIRA, Eliane Vendramini; FILGUEIRAS, Rodrigo. A importância da segurança da informação para as organizações. Revista Científica Alomorfia. Data de publicação: 2022. ISSN 2594-5637. Disponível em: https://www.alomorfia.com.br/index.php/alomorfia/article/view/137/63. Acesso em: 28 nov. 2023.
14. PEREIRA, Lucas Avanci de Souza; VICENTE, Augusto Luciano; RIZO, Andre Castro. Impactos da Engenharia Social na Segurança da Informação. Data de

publicação: 2022. ISSN: 2675-1828. Disponível em: https://www.fateccampinas.com.br/rbti/index.php/fatec/article/download/75/34. Acessado em 13 dez. 2023.

15. VIEIRA, Gustavo; DIAN, Mauricio de Oliveira. Impacto e crescimento da internet nos últimos anos. Revista Interface Tecnológica. Data de publicação: 2023. ISSN 2447-0864. Disponível em: https://revista.fatectq.edu.br/interfacetecnologica/article/view/1656/891. Acesso em 28 nov. 2023.