U.PORTO

MASTER
IN ECONOMICS OF BUSINESS AND STRATEGY

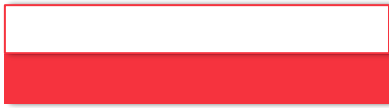
The Re-Launch of NOS Safe Net: A Cybersecurity Service by NOS Communications S.A.

José Francisco Martins Aguiar

M

2023

FACULDADE DE **ECONOMIA**



U.PORTO

FEP FACULDADE DE ECONOMIA
UNIVERSIDADE DO PORTO

The Re-Launch of NOS Safe Net: A Cybersecurity Service by NOS Communications S.A.

José Francisco Martins Aguiar

Internship Report

Master's in Economics of Business and Strategy

Supervised by
Pedro Luís Silva

2023

Acknowledgments

I want to express my sincere gratefulness to everyone who has supported and encouraged me throughout my internship journey over the past few months.

First of all, I would like to share my gratitude to my supervisor **Pedro Luís Silva** for his continuous guidance, support, and availability throughout the master's internship. Thank you for all your valuable attention, comments, and recommendations, which were crucial to developing this internship report.

I would also like to thank **Dr. Kellan Nguyen**, a lecturer at the School of Business at the Middlesex University of London, for his generosity and great advice.

I am humbled by my **family** and **girlfriend**'s unconditional support and encouragement during my studies, especially during the completion of the current master's program. Thank you for never stop believing in me and inspiring me to keep pushing the barriers forward.

Last but definitely not least, I express my immense gratitude to NOS Communications S.A. for the remarkable opportunity to complete my studies in such an enriching business environment. Thanks to the Internet product management team for welcoming me and offering valuable insights. A special thanks to **João Ceriz**, team leader and internship supervisor, for granting me the necessary resources to explore the theme and providing fundamental comments and recommendations. Mainly, I am profoundly grateful to **Isabel Aroso** for her exceptional and unceasing mentorship during my internship. Her wise counsel and constructive feedback have impacted my progress and the quality of the present work, and I am grateful to have had such an extraordinary mentor.

To all the mentioned and non-mentioned, my sincere gratefulness. Your kindness and support mean the world to me.

Abstract

The present work was elaborated in the context of an academic internship at NOS Communications (NOS) regarding the conclusion of the Master's in Economics of Business and Strategy at the School of Economics and Management, University of Porto. The identified problem was the small customer base and negligible growth of NOS Safe Net, while a recently introduced DNS solution – NOS Safe Browsing – had already surpassed twenty times its thousand customer base. The envisioned action plan was revitalizing the End-Point offer – NOS Safe Net. Therefore, the study intends to evaluate the suitability of NOS' intention to re-launch and re-brand NOS Safe Net to exploit its full potential.

A comprehensive market analysis was conducted, examining Telecommunications and Cybersecurity industries. A benchmark compared international and national telecommunications operators' (Telcos) cybersecurity offers and Strategic Groups' positioning. A macro-environment analysis (PESTEL) considered external factors impacting NOS. The research was sustained by data from Telcos' websites, government and regulators publications, statistical institutions, industry reports, and news articles. A similar study was directed at NOS based on internal information and studies. Further, an STP and a Marketing Mix analysis were developed, sustaining the assessment of the strategy's economic viability founded on NOS' internal data.

The study evidences the opportunity value-added cybersecurity services represent for Telcos to differentiate from competitors and strengthen revenue. The macro-environment emphasizes it and suggests the need to promote customer retention. The internal examination evidence that competitors outclass NOS' End-Point solution. NOS' partnerships reveal crucial for NOS Safe Net's value proposition and respective marketing advancement. Finally, the economic evaluation provided positive support to the strategy.

Overall, NOS should pursue its revitalization strategy. Reflecting on the lack of research on re-launching and re-branding products and services, the study expands existing concepts' practical applications. Future studies should be conducted to promote the advancement of practical applications.

Keywords: Re-Launch, Re-Branding, Telecommunications, Cybersecurity, Value-Added Services, NOS Communications

Resumo

O presente trabalho foi elaborado durante um estágio curricular na NOS Comunicações (NOS), no âmbito da conclusão do Mestrado em Economia da Empresa e da Estratégia da Faculdade de Economia da Universidade do Porto. O problema identificado consiste na pequena base de clientes e crescimento insignificante do NOS Safe Net, enquanto uma solução DNS recentemente introduzida - Navegação Segura - ultrapassou vinte vezes a sua base de clientes. Portanto, o estudo avalia a intenção de relançar e reformular a solução End-Point - NOS Safe Net.

Foi realizada uma análise de mercado, examinando as indústrias de Telecomunicações e Cibersegurança. Uma avaliação comparativa considerou as ofertas de cibersegurança de operadores internacionais e nacionais e o seu posicionamento. Uma exploração do macro ambiente (PESTEL) considerou fatores externos que impactam a NOS. A pesquisa foi sustentada em dados de sites de operadores, publicações governamentais e regulatórias, instituições estatísticas, relatórios do setor e artigos de notícias. Um estudo semelhante foi direcionado à NOS baseado em informações e estudos internos. Adicionalmente, foi desenvolvida uma análise STP e Marketing Mix, sustentando a avaliação da viabilidade económica da estratégia.

O estudo evidenciou a oportunidade que os serviços de cibersegurança com valor acrescentado representam para os operadores se diferenciarem dos concorrentes. A PESTEL enfatiza a necessidade de promover a retenção de clientes. A análise revelou que os concorrentes superam a solução End-Point da NOS. As parcerias da NOS revelaram-se cruciais para o progresso da proposta de valor do NOS Safe Net e da estratégia de marketing. Finalmente, a avaliação económica proporcionou suporte positivo à estratégia.

Concluindo, a NOS deve seguir a estratégia de revitalização. Considerando a falta de pesquisa sobre relançamento e reformulação de produtos e serviços, o estudo amplia as aplicações práticas dos conceitos existentes. No futuro, estudos devem ser conduzidos para promover o desenvolvimento de aplicações práticas.

Palavras-chave: Relançamento, Reformulação de Marca, Telecomunicações, Cibersegurança, Serviços de Valor Acrescentado, NOS Comunicações

Table of Contents

Table of Figures

1 Executive Summary

Companies and end-users look forward to protection from online threats in the context of increasing cybercrime. In this sense, the Portuguese Telco – NOS – launched a simple cybersecurity (DNS) service that delivers online protection to NOS' mobile and fixed networks clients – NOS Safe Browsing – in May 2022. Considering the DNS solution success, and the stagnant customer base of NOS Safe Net, a complete End-Point service from its cybersecurity portfolio, NOS intends to promote the re-branding and re-launch of NOS Safe Net. Therefore, the present study aims to assess NOS' strategy to evaluate whether NOS should re-launch "NOS Safe Net." Considering the lack of research on re-launch and re-branding products and services, particularly in the Telecommunications Industry, the study contributes to expanding existing concepts' practical applications.

To evaluate NOS' intention's suitability, a market analysis was conducted. It involved an examination of the related industries, a benchmark of international and national Telcos, and a macro-environment study. To achieve that, Telcos' websites, relevant government, statistical institutions', and regulators' publications, as well as industry reports and news articles, were considered. Furthermore, a similar study was directed at the case study's company based on its internal information. From a sustained base analysis and considering NOS' prior experience, a marketing and communication plan was developed to support the re-launch and re-branding, as well as an analysis of the strategy's economic viability.

The examination evidences the opportunity the commercialization of value-added cybersecurity services represents for Telcos to differentiate from competitors and reinforce revenue streams. Further, the favorable macro-environment emphasizes the opportunity and suggests the need to promote customer retention. Additionally, the internal analysis revealed that NOS' End-Point solution is outdated among the national offers, suggesting a need for a modification. In this sense, partnering with F-Secure and Centili revealed crucial for reinforcing NOS Safe Net's value proposition and respective marketing strategy. Finally, the economic evaluation provided crucial insights to answer the research question.

The study comprises a description of the internship at NOS, a clarification of the research problem, a literature review, and an explanation of the methodology before delving into the external and internal analysis, followed by the marketing and communication plan and economic evaluation. Finally, a conclusion will be provided.

2 The Internship at NOS Communications S.A.

The academic internship started on January 30, 2023, with the integration of NOS Communications' Internet Product Management team, and concluded on June 30, 2023, to complete the Master's in Economics of Business and Strategy cycle of studies at the School of Economics and Management (FEP), University of Porto. Such a team manages the internet services directed to the final consumer, a crucial market segment for NOS, which controls over a third of the national market (Anacom, 2023a). At the beginning of the internship, with its technological leadership vision, NOS had already decided to promote the re-launch of NOS Safe Net. In this sense, the internship entailed the analysis of the suitability of the strategic re-launch and re-branding decision, supporting its operationalization, developing a marketing and communication plan for the online safety portfolio, and accessing its business sustainability.

The strategic analysis involved a national and international telecommunications industry benchmark regarding their offers and communications best practices, complemented by a cybersecurity industry overview and a macro environment evaluation. The analysis, developed in section 6, allowed the reinforcement of NOS re-launch intentions and provided substantial support to answer the research question. Further, the operationalization support entailed assisting the contributions of NOS and its partners (F-Secure and Centili) to develop and market the new service, which was crucial for the strategy's viability. Moreover, the internship envisioned assessing the new service's target market and developing a marketing and communication plan. Also, it implied the development of internal information materials and an external communication plan for the new service. It was designed throughout section 8 and was valuable in assisting NOS' re-launch initiatives and providing fundamental insights into developing the following section's matter. Finally, the new service's business sustainability was assessed in section 9 by identifying the target market dimension, the envisioned sales, and entailed costs. The business sustainability evaluation was essential to strengthen the re-launch strategy and offered substantial funding to the research topic.

To conclude, the internship period at NOS revealed crucial for the throughout comprehension of the company's goals and the development of inherent activities. Moreover, it provided a solid basis for developing the present work by accessing crucial information and experiencing the business environment.

3 Research Problem

There is a broad literature on enterprise re-launch and re-branding. However, a gap in the study of a product or service re-launch and re-branding can be identified. That is an essential field of study, considering the competitive market economy constantly challenging businesses to revitalize their offers, as argued by Partanen (2021). In this sense, addressing the topic expands existing concepts' practical applications.

NOS is established in the Portuguese market as the best mobile internet services provider (NOS, n.d.-a; Marketeer, 2023). It aims to expand its leadership to fixed services and elevate its position by providing the best and safest internet services, taking advantage of the growing social concern regarding digital safety. Currently, NOS offers two cybersecurity services with different characteristics. **NOS Safe Net** is a complete offer that provides browsing safety at the device level, Antivirus, and Parental Controls. At the same time, **NOS Safe Browsing** is a simpler, more affordable solution offering cybersecurity while browsing through NOS' mobile and fixed networks. Since the first registered negligible growth and a small subscriber base, NOS decided to re-launch it to exploit its envisioned potential and progressively establish a reputation as the safest internet provider in Portugal. Such a decision entails the development of 1) a more differentiated offer, including new features; 2) a re-branding of the service; 3) its commercial and communication channels exploitation; and 4) more versatile subscription methods to make it available to non-clients.

The internship context favored exploring the research topics and the development of the present thesis, which aims to answer the question: **Should NOS pursue the Re-launch of NOS Safe Net?** That is a relevant research topic as it widens the practical applications of the re-launch and re-branding knowledge, particularly in the Telecommunications Industry context. Moreover, it is significant for NOS by providing essential insights regarding its market positioning and reinforcing its strategy's reasoning.

Finally, the present study is motivated by the United Nations' 2030 Agenda and the European Union's initiatives, considering it envisions expanding cybersecurity services' availability. The ninth Sustainable Development Goal encourages the development of secure and resilient information and communication technologies infrastructure, which is critical for cybersecurity and protecting against cyber threats (OECD, n.d.; United Nations, 2022). Likewise, the European Union is conducting various initiatives to foster cybersecurity resilience (European Commission, 2022; European Commission, 2023).

4 Literature Review

The present section explores relevant literature to provide a sustained basis for analyzing NOS' strategic decision. Since it intends to re-brand an existing cybersecurity service and re-launch it, it is fundamental to address the Brand concept and the strategy's implications on it. Further, as it intends to promote a re-launch, it is important to properly understand a Product's Life Cycle and dive into methods that companies may use to keep their offers up to date, which is important to address the evolution of cybersecurity services. Finally, it is crucial to dive into re-branding and re-launch literature to fully understand the theoretical basis that sustains the pursuit of such a strategy.

4.1 Branding

There is no consensus in the literature on the concept of Brand. However, it is commonly accepted that it combines several elements that allow consumers and sellers to identify a product or service a company provides from its competition offers (Quang, 2022; Partanen, 2021; Kotler & Armstrong, 2019). According to Partanen (2021), a brand entails the "tangible and intangible, the functional and emotional aspects of an organization" (Partanen, 2021, pg.13). On the one hand, it comprehends its visual identity through elements such as brand name, term, sign, symbol, design (Quang, 2022), logo, characters, slogans, and packages (Partanen, 2021). On the other hand, it involves corporate identity and personality, which translate into customer emotions, spokespeople, brand associations, and awareness (Partanen, 2021). Kotler & Armstrong (2019) reinforced such a vision arguing that brands are more than their products' visual attributes - "brands have meaning" (Kotler & Armstrong, 2019, pg.231). Therefore, brand elements must be carefully selected (Partanen, 2021) as they constitute the foundation of a brand (Alnabhan, 2018) and are combined to form one of the most critical assets of a company (Peterson et al., 2015). Alnabhan (2018) proposed that such elements dictate a business's success and play essential roles in a company.

A brand is a crucial aspect of a company as it benefits buyers and sellers. The brand allows consumers to differentiate a product or service in the market. Peterson et al. (2015) argued that its elements make the brand recognizable and remembered by clients, which helps them distinguish similar products and services (Partanen, 2021; Alnabhan, 2018). Further, Quang (2022) pointed out that customers have a strong attachment to brands and their names, affecting their purchase decisions. Additionally, brands convey information and

evidence about the consistency and quality of products (Kotler & Armstrong, 2019), granting customers time savings and safer purchasing decisions (Partanen, 2021; Alnabhan, 2018; Quang, 2022). Moreover, it benefits the company and sellers by creating a foundation for connecting and establishing lasting client relationships. By communicating through brand associations (Partanen, 2021), companies can build a positive brand image and reputation (Alnabhan, 2018; Quang, 2022). Since most consumers base their purchases on brand trust and familiarity, sellers face lower commercialization risks (Alnabhan, 2018; Quang, 2022). Furthermore, brand names and trademarks legally protect unique product attributes that rivals may otherwise imitate (Kotler & Armstrong, 2019). Therefore, the brand of a product or service translates into a higher value for both consumers and companies/sellers.

A strong brand can enhance the perceived value of a product or service to a customer and generate higher value for a company. According to Kotler & Armstrong (2019), consumers establish close connections with brands, considering such attributes an essential product element. As a result, consumers' willingness to pay for products from specific bands can be higher, as branding can increase a product's value (Alnabhan, 2018). From a company's perspective, a vital brand grants a company more leverage in bargaining with resellers (Kotler & Armstrong, 2019), has a favorable differentiating effect from other players (Alnabhan, 2018), and can increase some companies' share values by 5 to 7% (Todor, 2014). Moreover, it improves the efficacy of marketing campaigns and promotes a company by cultivating brand loyalty among customers (Partanen, 2021). Further, a brand's success can be leveraged to launch additional products or related brands, with reduced advertising costs and ease of gaining consumer confidence (Quang, 2022; Todor, 2014). Such aspects are described as "Brand Equity" (Alnabhan, 2018), and a company is considered to have a positive one when consumers respond more favorably to its brand than they do to a generic version of the same goods (Kotler & Armstrong, 2019). That occurs because a brand is far more than a logo, name, or slogan. It comprises a consistency and quality promise, a position in the customer's mind, and several advantages and qualities (Quang, 2022). In this sense, it is detrimental to a company to maintain its brand image.

A large part of managing a brand image lies in keeping up with its promises and meeting clients' expectations. It is fundamental for a company to deliver its promises regarding the quality, consistency, and features of its goods since it contributes to building brand equity. Ultimately, it translates into customers perceiving extra value in a brand to

which they become loyal, contributing to sustained competitive advantage and marketing power (Nyambane & Makori, 2013; Quang, 2022). Therefore, it is crucial to maintain a close connection with customers by listening and engaging with them (Partanen, 2021) to meet their needs unceasingly, which helps build a positive brand image (Alnabhan, 2018). As Partanen (2021) elucidated, a brand does not exist in a vacuum but rather in a dynamic environment. As a result, a brand ought to be "managed, refreshed, rethought and revised periodically" (Partanen, 2021, pg12). Therefore, brands must know their product's life cycle.

4.2 Product Life Cycle

A product's success lies in paying close attention to every stage of its lifecycle. Businesses aspire to have good market penetration and a consistent, long-term revenue stream for the items they launch to maximize their return on product development and launch investment (Kotler & Armstrong, 2019). However, as Kotler & Armstrong (2019) pointed out, there are only a few exceptions to the fact that products will not continue to be demanded indefinitely. Therefore, organizations must be aware of each product's life cycle, which involves five stages, whose configuration is uncertain beforehand.

Such stages include product development, market introduction, sales growth, maturity, and decline. Easingwood & Harrington (2002) proposed that to be successful, the subsequent phases of product introduction must be prepared with the same level of care as the launch stage. For the aim of this thesis, it is sufficient to delve into the maturity and decline stages, which help access the re-launch of NOS Safe Net. As sales growth slows and stability is attained, a maturity stage is reached. At this point, companies commercializing successful goods or services take on market, product, and marketing mix modification (Kotler & Armstrong, 2019). By doing so, businesses can provide customers with new or improved services so that products remain relevant, attract potential customers, and encourage usage. It entails changing characteristics like quality, features, style, and packaging (Kotler & Armstrong, 2019). However, most sales revenue inevitably decreases gradually to reach the decline stage. That is because of technological advancements, changes in consumer preferences, and heightened competition. Organizations either step out of the market, cut their cost structures, or revitalize their products. Kotler & Armstrong (2019) advocated that a company may take the last path to return the product to the growth stage.

Furthermore, Easingwood & Harrington (2002) contended that there is an opportunity for a re-launch when a period of transition during which momentum is lost

occurs – a "chasm" (Easingwood & Harrington, 2002, pg1). Thus, the re-launch method can steer a high-tech product or service toward the mainstream in an introductory or growth stage that is losing sales traction early. Kotler & Armstrong (2019) reinforced this perspective, arguing that some products cycle from decline to growth through marketing or re-branding. In addition, introducing a product with a fresh design frequently occurs during the decline stage (Bissdorf, 2016). Maintaining a close watch on the product life cycle is fundamental to developing suitable marketing strategies and communicating effectively. In this sense, businesses must constantly innovate and evolve their images to remain viable.

4.3 Enterprise Design Thinking

Businesses must be as adaptable as possible, considering the rapid technological, environmental, and societal change that has become the *status quo*. To achieve such business responsiveness, "Design Thinking" can be employed to support organizations facing changing environments, understand users and their problems, and concentrate on their experience (Sharpe, 2020). Such a framework focuses on understanding people's needs, generating ideas, experimenting, and improving solutions in a closed and continuous path of evolution (Sharpe, 2020).

IBM points out that in an uncertain environment, "The Loop" provides a guide for action. It consists of an enterprise design thinking method that fosters an uninterrupted observation, reflection, and action cycle. The Loop promotes the consciousness of the present and the projection of the future by cultivating multidisciplinary cooperation that focuses on the customers' needs on an ongoing cycle of revitalization (IBM, 2018).

The Design Council introduced the "Double Diamond" (Design Council, n.d.; Val et al., 2017). The two diamonds reflect the process of engaging in more extensive analysis by promoting divergent thinking (discover and develop stages), followed by narrowing the course of action by fostering convergent thinking (define and deliver) (Design Council, n.d.; Val et al., 2017). According to Elmansy (2021), such a framework entails problem identification through the discovery and defining stages and solution elaboration over the development and delivery phases.

Overall, there are similarities between the various design thinking models. Firstly, they contend that organizations must put people first, engaging with them to understand their needs properly (Sharpe, 2020; Design Council, n.d.). Secondly, the frameworks foster a

broad awareness and understanding of the identified problems and developed ideas in the organization (Design Council, n.d.; IBM, 2018). Thirdly, it cultivates multidisciplinary cooperation to promote divergent thinking (IBM, 2018; Val et al., 2017). Fourthly, the models incentivize ongoing experimentation, development, and improvement of solutions (Sharpe, 2020; IBM, 2018; Design Council, n.d.). Finally, a crucial aspect of supporting organizations dealing with the ever-changing environment consists of the notion of continuity and dynamism in a loop-shaped process (IBM, 2018).

4.4 Re-Branding

Companies must continuously restore their brands because the market is a dynamic environment. As the market and time progress, ensuring the quality of goods or services is no longer sufficient to safeguard a company's success (Todor, 2014). Thus, re-branding must be continuous and iterative for a brand to maintain relevance and competitiveness (Partanen, 2021). Such a process entails replacing the brand name, adjusting the design, or repositioning the brand (Goi & Goi, 2011; Singh et al., 2013). That intends to foster a more contemporary appearance, remain relevant (Bryant, 2013), and influence a change in consumer attitudes, perceptions, and conduct to produce positive market growth (Singh et al., 2013). Peterson et al. (2015) pointed out that re-branding can be applied to products and companies (Bryant, 2013) and that there is a need to conduct balanced rejuvenation while preserving the heritage of the brand (Peterson et al., 2015). Such a strategy can adopt distinct forms.

There are several variations of the re-branding process. Keller (2000) proposed that re-branding can occur at the corporate, business, and product levels. Moreover, according to Opuni et al. (2013) and Quang (2022), it can consist of an evolutionary or revolutionary process. On the one hand, evolutionary re-branding entails a few organizational modifications that occur so gradually that they are barely noticed (Opuni et al., 2013). Further, it can range from mere revamp to restyling or rejuvenating a brand and typically takes only slight adjustments to the slogan or logo (Nyambane & Makori, 2013). On the other hand, changing a brand's name is considered a more revolutionary move (Peterson et al., 2015). Such a re-branding style may also entail corporate value changes in addition to evolutionary changes (Nyambane & Makori, 2013). It consists of a more significant and visible modification in the company's positioning and image that essentially reshapes it (Nyambane & Makori, 2013; Opuni et al., 2013). Consequently, depending on their

motivations, one can conduct subtle or more drastic changes in a company's brand, business unit, or product elements.

Organizations adopt re-branding strategies to stay relevant and competitive. According to Goi & Goi (2011), they are motivated by internal or external drivers. From a firm's perspective, a new emerging focus or vision may be driving changes in corporate strategy. Thus, a brand's revitalization signals a mission, purpose, attitude, or strategy change (Goi & Goi, 2011) as organizations look forward to being viewed as evolving and up-to-date businesses (Peterson et al., 2015). Moreover, brand adjustments may be pursued to block competitors' initiatives and rejuvenate a company's profitability and consumers' confidence (Goi & Goi, 2011). According to Partanen (2021), such a movement can be followed to enter new markets and expand business and profits since underperformance is a common stimulus for corporate or product re-branding (Opuni et al., 2013). Additionally, re-branding can occur due to a change in the ownership structure (Nyambane & Makori, 2013), namely through an M&A process (Kyriaki, 2019). From a market environment perspective, companies might react to a shift in marketplace dynamics, such as increased price competitiveness (Goi & Goi, 2011; Kyriaki, 2019). Furthermore, organizations adopt re-branding to meet ever-changing consumer needs (Goi & Goi, 2011; Quang, 2022). Therefore, the implementation of such a strategy may be imposed by market dynamics or internally motivated by the organization. Whatever the rationale for re-banding is, businesses must cautiously implement such a strategy.

The re-branding process can be risky if not conducted properly. Consumers may disapprove of the brand's heritage change or no longer distinguish it (Bryant, 2013). In this sense, it is fundamental for a brand to establish trust with its customers, as they are more likely to react positively to change, despite Collange & Bonache (2015) finding that 50 percent of consumers respond negatively. To conduct a successful re-branding, an organization must identify an opportunity and conduct a throughout and continuous market analysis (Goi & Goi, 2011; Partanen, 2021). In addition, it must communicate effectively, both internally and externally. According to Todor (2014), a successful re-branding strategy starts by repairing various internal problems and restoring the inner brand vision among collaborators (Opuni et al., 2013) as an inside-out-oriented process.

Further, it is fundamental to adequately communicate the change to prevent confusion and misleading customers (Todor, 2014). Collange & Bonache (2015) proposes

that companies should inform consumers about the product or brand name change and explain the need for such a move to prevent negative emotions and attitudes and foster customer trust. Although organizations must progress their brand to stay relevant and address new market segments at the re-branding strategy level, they must continue fulfilling existing clients' needs and maintain part of their identity (Opuni et al., 2013). Companies must evolve their offer characteristics and brand image based on customer feedback and competition moves (Kyriaki, 2019; Peterson et al., 2015). However, (Collange & Bonache, 2015; Bryant, 2013) advocates that re-branding actions should be simple to avoid confusing consumers. The authors contend that organizations must avoid making additional modifications during re-branding, such as improving the marketing mix, as this leads to enhanced customer confusion. Although loyalty to the original brand is essential for consumer items, it is not critical for services (Collange, 2015). Therefore, service re-branding must concentrate on place attachment. Finally, Goi & Goi (2011) pointed out the need to evaluate the entire strategy to assess its viability. Also, Singh et al. (2013) contended that timing plays an essential role in the re-branding process, arguing that some businesses rebrand "prematurely or unnecessarily" (Singh et al., 2013, pg.96). The pursuit of a successful re-branding tactic entails several vital aspects that businesses must consider. Companies must be aware of the impacts the pursuit of such a tactic involves.

The re-branding process has consequences for several corporations. Such a process impacts its internal perception as a company by promoting a shift in employees' attitudes and enhancing the connection with the company (Goi & Goi, 2011). Moreover, re-branding stimulates improved communication with stakeholders. According to Goi & Goi (2011), a change in brand name conveys higher standards in the service sector. That contributes to a brand's continuity and consistency (Singh et al., 2013). When conducting revolutionary re-branding, a company risks losing its brand name awareness (Kyriaki, 2019). However, Bryant (2013) argues that organizations incur such a risk because of the potential for even greater profit. This process has distinct effects on well-established and emerging corporations. Roy & Sarkar (2015) found that upon re-branding news, the customer-based brand equity of an established brand will decline, whereas that of a less established brand is expected to increase. In addition, re-branding promotes the awareness of a less-known brand, and customers seem to be more engaged with the revolutionary re-branding style. Although brand loyalty may weaken if modifications are implemented in the company's fundamental principles and advantages, loyal consumers are more receptive to evolutionary changes (Nyambane &

Makori, 2013; Peterson et al., 2015). However, more revolutionary evolutions, such as name or logo changes, promote more pessimistic reactions and modify customers' perceptions.

In contrast, less-loyal customers are more favorable to revolutionary changes (Peterson et al., 2015). However, logo change favors client loyalty and business performance (Peterson et al., 2015). Additionally, a brand's revitalization strategy affects its valuation and financial position. Despite not granting success, re-branding enhanced a company's income (Singh et al., 2013). Re-branding impacts how a company is perceived internally and externally and affects its financial situation. Another essential dimension when considering revitalizing a brand or product is its re-launch.

4.5 Launching & Re-Launching

A product launch follows the beginning of the product life cycle in the market. The market introduction of a technological product requires significant planning and is mainly based on consumer understanding of the technology (Easingwood & Harrington, 2002). Although the launch strategy for a well-known technology concentrates on building a brand name and competitive advantage, that of an emerging technology focuses on the product's benefits. Further, the authors contended that a chasm following the launch is anticipated, especially for emerging technology products, providing a chance for a later re-launch to reach the mainstream. However, re-launch is not only associated with a period of chasm. Saunders & Jobber (1988) argued that most products in the maturity or decline stage are typically discontinued and replaced with new or improved variants. Re-launching is regarded as the modification of an existing product to satisfy changing consumer needs (Bissdorf, 2016), and there are a few types.

Several marketing strategies are connected to a product's re-launch. As neither invention nor removal of a product has occurred, Bissdorf (2016) advocates that product re-launch must be classified as a component of product modification. It entails three distinct types of re-launches. First, product modification refers to replacing a product on the market with one that displays changes to some characteristics (Bissdorf, 2016), which is the most common (Saunders & Jobber, 1988). Second, differentiation involves pairing an additional and improved product with one already on the market. Also known as line or brand extensions, they effectively address different market segments. Third, product variation consists of substituting an earlier version as an ongoing process over a product's lifespan,

implying minimal changes to the current offer (Bissdorf, 2016). Such approaches serve different business purposes and have been pursued for various reasons.

Several aspects motivate organizations to promote the re-launch of existing products or services. Companies need to keep their products and services portfolios simple and profitable. Thus, promoting a modification or variation re-launch avoids introducing complexity to current portfolios and confusing customers (Gottfredson & Aspinall, 2005; Saunders & Jobber, 1988). Quelch & Kenny (1994) reinforced this perspective by advocating that any business introducing a new product or service must discontinue one that already exists from its portfolio. That intends to redirect free resources to advertise profitable new products.

Moreover, companies pursue re-launching strategies to increase their likelihood of mainstream popularity. Therefore, the launch strategy must be implemented at two distinct moments. The first step is to launch a product to an early market composed of "Visionaries" (Easingwood & Harrington, 2002, pg1) or early adopters of technology before adjusting and reintroducing it to more mainstream customers (Easingwood & Harrington, 2002; Frattini et al., 2013). Additionally, it presents advantages by requiring less time and money to develop products because it leverages existing markets and technologies (Saunders & Jobber, 1988; Bissdorf, 2016). Further, it offers logistical advantages because substitutes can build on existing distribution channels and, by doing so, ease the challenge of obtaining store space (Saunders & Jobber, 1988; Quelch & Kenny, 1994).

Further, revitalizing an existing product or service benefits from prior awareness requires lower promotion investments and benefits from a reignited sales force. In addition, it represents a lower risk for customers because the newly introduced product is related to a well-established old version (Saunders & Jobber, 1988). Finally, owing to high competition intensity, fast technological progress, and changing needs, businesses strive to evolve their offers. Thus, re-branding is the most popular method because it is less risky than product innovation (Bissdorf, 2016). Corporations have numerous incentives to rebrand their portfolios and must strategically plan them.

The re-launch journey must be conducted as carefully as the initial launch. To reach the mainstream market, it is fundamental to follow several steps. First, businesses must adjust their initial offers based on analytical tools and customer feedback (Rust et al., 2006;

Easingwood & Harrington, 2002). Companies should make their offers as simple as possible by incorporating the appropriate features and ensuring their products fulfill their primary purposes (Rust et al., 2006). Second, organizations would benefit from preparing a re-launch both internally and externally. It is imperative that the business successfully informs its staff of the rationale behind the change and the market advantages and features of the new product for the target markets. The same applies to its customers, as it is crucial to communicate with mainstream added features, such as compatibility with industry standards. Third, the re-launch requires targeting followers, who are generally more conservative (Easingwood & Harrington, 2002). In this regard, it is crucial to target specific consumer or industry segments that will adopt and endorse the refreshed solution and improve the chances of an imitation response (Easingwood & Harrington, 2002; Frattini et al., 2013). Further, Easingwood & Harrington (2002) argued that companies must leverage re-launch to target rival clients.

Fourth, adequate product and company positioning is essential to reach mass consumers. The product or service must be positioned as an effective solution to a particular problem that the target customer has, and the company must be regarded as a strong and credible provider of such an offer. Fifth, timing is the most critical component of any effective market movement. A company ought to quickly spread its reputation to fulfill customers' needs (Easingwood & Harrington, 2002). Additionally, Saunders & Jobber (1988) pointed out parallel selling as the most frequent tactic by offering old and new products concurrently for a while. The re-launching of an offer must be considered the launch of a new product or service (Bissdorf, 2016). Therefore, firms must plan adequately while taking all stages into account.

To conclude, the study of branding, product life cycle, and enterprise design thinking has been conducted throughout, providing a robust basis for developing the current work. However, the concepts of re-branding and re-lunch have yet to be sufficiently explored. Furthermore, the literature that addresses such topics often focuses on a company's re-brand or re-launch. Oppositely, there is little literature regarding products or services re-brand or re-launch, which is a topic of great interest in a market economy. Furthermore, no studies were conducted to access telecommunications services' re-brand or re-launch, nor to evaluate the suitability of telecommunications operators' commercialization of cybersecurity services.

5 Methodology

The present work required extensive research, covering the concepts discussed in the previous section, to provide a complete and sustained theoretical foundation for developing the current strategic analysis.

Additionally, the present work focuses on qualitative analysis to produce a robust basis to answer the research question: **Should NOS pursue the Re-launch of NOS Safe Net?** An extensive external investigation of the Telecommunications and Cybersecurity industries and an internal analysis of the company at hand – NOS – were fundamental to evaluating NOS' strategic decision. Furthermore, a marketing and communication plan was developed to sustain the new service's business sustainability analysis. Therefore, besides concentrating on the strategic analysis, considering the market environment and NOS characteristics, the study also entailed a quantitative evaluation to assess the strategy's viability. The present section delves into the methodologies specific to each analysis.

The primary data source for this study was Telcos' websites, which were systematically reviewed to collect data on cybersecurity services offered by international and national Telcos. Secondary data from industry reports, academic articles, government publications, national industry regulator (Anacom) periodicals, and relevant publications specific to the sector were also used to supplement the analysis. Finally, internal data and studies provided by NOS were considered as well.

5.1 External Analysis

The external analysis examined the telecommunications, cybersecurity, and telecom cybersecurity industries. Detailed research explored market trends, industry reports, and publications specific to the sector. Moreover, a cybersecurity panorama and a macro environment analysis were conducted sustained on relevant government, statistical institutions, and regulators publications, as well as on industry reports and news articles. Further, the study addressed national and international Telcos' cybersecurity offers directed to final consumers (B2C) based on their websites. All national Telcos offering a cybersecurity service were considered. The selection of the addressed international players was based on three criteria: belonging to a group related to national players, such as the Vodafone Group; operating in a country similar to Portugal in socioeconomic and sociocultural terms, such as Spain and Italy; and operating in well-developed nations, as Norway and the United

Kingdom. A strategic groups analysis was conducted from the benchmark, enabling to accessing competitors' cybersecurity positioning.

This analysis provides an understanding of the current state of the telecommunications and cybersecurity industries, their growth prospects, and the opportunity for Telcos to deliver cybersecurity services. Further, the social analysis provides important insights regarding cybersecurity needs, and the benchmark evaluation identifies the competitors' offers' best practices and positioning.

5.2 Internal Analysis

A contextualization of NOS Communications was conducted, and its current cybersecurity portfolio was analyzed following the same approach. Additionally, the newly envisioned service was described, its positioning was accessed and entailed partnerships considered. Such analysis was based on the company's website and internal data provided by NOS and the partners' websites. It offered essential insights regarding NOS' vision, learnings from its existing portfolio, and its intentions to revitalize its End-Point service.

5.3 Marketing & Communication Plan and Economic Evaluation

To assess the business strategy's sustainability, it was necessary to define the new service target market and how it would be marketed. Thus, a marketing and communication plan was elaborated through a Segmentation, Targeting, and Positioning analysis and a Marketing Mix. The economic viability of the strategy was assessed by estimating envisioned revenue and entailed costs in a cost-benefit approach. Such evaluations were based on literature, relevant statistical institutions' publications, and NOS' internal data (a national market segmentation analysis and a cybersecurity market assessment study). It contributed to a better understanding of the market segment dimension and attractiveness.

5.4 Limitations & Disclaimer

The data from NOS used in this thesis is from 2017 and is therefore outdated, not entirely accurate, having been collected for research purposes only to protect the company's privacy. While every effort was made to ensure that the findings and conclusions reflect a real-world scenario, the results of this study may be affected by the fact that the data could be completer and more accurate. Moreover, the presented projections are by the author and independent of NOS. Finally, by the time of the present work conclusion, the new service's name was yet to be defined. Consequently, "NOS Antivirus Total" is merely illustrative.

6 Market Analysis

6.1 The Telecommunications Industry

The telecommunications industry has its roots in the success of the telegraph industry and the rising electrical manufacturing businesses in the 1830s (Vonage, n.d.; TechnoFunc, 2012). The industry's products have progressed significantly since the 19th century to the contemporary exchange of audio, video, and text content across multiple wireless infrastructures. The telecommunications market registered substantial advancements in data speeds, leading to the current commercialization of Fifth Generation (5G) networks (Grand View Research, 2021b).

Telecommunications operators are substantially raising data speeds as the telecommunications industry matures worldwide. However, connectivity services are no longer differentiators (Garcia, 2020). Telcos must prioritize offering unparalleled services that customers demand if they want to differentiate themselves from their rivals, engage with new clients, and sustain growth (Garcia, 2020). In a competitive market like the telecommunications industry, operators are moving from traditional voice and data bundles to over-the-top services (Garcia, 2020). These value-added services (VAS) provide an opportunity to attract and offer customers more, which is essential when considering that customers' needs continue to evolve and change. Moreover, Mahabir (2021) argued that customers are generally more attracted to telecommunications companies that offer VAS.

The Global Telecommunications market, estimated at USD 1,805.61 billion in 2022, is anticipated to grow at a 6.2% compound annual growth rate (CAGR) from 2023 to 2030 (Grand View Research, 2021b). Such prospects result from the proliferation of smartphones worldwide, exceeding 8 billion mobile subscribers globally in 2020, boosting demand for high-speed data connectivity and the growing need for VAS (Grand View Research, 2021b). The industry's growth is also driven by the effects of the pandemic that led to a shift among the masses to remote working, enhancing the demand for network connectivity and infrastructure, as such practices came to stay, with the increasing number of companies worldwide adopting hybrid work models (Grand View Research, 2021b).

The Portuguese telecommunications market was valued at USD 5.4 billion in 2021 and is expected to grow at a slower rate (less than 1% during the forecast period (2021-26)) than the global telecommunications industry (Global Data, 2023).

6.2 The Cybersecurity Industry

Over the years, the development of the internet, paired with the wide adoption of devices with intelligent and IoT technologies, enhanced users´ exposure to cybercrime (Technavio, 2023). The need for cybersecurity is continually increasing as more functions and elements in critical infrastructure depend on computer-based systems and the Internet (F-Secure, n.d.). Cybersecurity regards the procedures involved in safeguarding networks, computer systems, and internet-connected devices to preserve online information and resources' availability, confidentiality, and integrity (F-Secure, n.d.; Schatz et al., 2017; Johansen, 2022). It intends to preserve private information against unintentional access, harmful online attacks, and malware such as trojans, spyware, and ransomware programs (F-Secure, n.d.; Johansen, 2022; Farrier, 2022). Companies fearing the consequences of data breaches, such as losing their intellectual property, trade secrets, and customer base information, commonly started adopting cybersecurity solutions (EFTMG, 2018).

According to Grand View Research (2022), implementing the remote working practice enhanced organizations' exposure and led to a growing demand for cybersecurity solutions, especially from SMEs, which were generally less protected (Aiyer et al., 2022; EFTMG, 2018). An organization's average cost of data breaches amounted to USD 4.87 million in 2021 (Grand View Research, 2022). Therefore, the sector faced higher demand from businesses that looked forward to preventing cyberattacks, which demand increased mainly due to the Covid-19 pandemic in 2020.

Cybercrime is evolving at a fast rate (Aiyer et al., 2022) and requires companies and end-users to adopt updated solutions. Organizations have become more cautious in the last few years as cyberattacks gained traction (Grand View Research, 2022), adopting high-end technologies (Yosifovich et al., 2023). As a result, cybercriminals are shifting their attention to the home user because they are perceived as weaker targets. Work-from-home and hybrid practices have become common, and hackers target end-users who grant less secure access to organizations' networks (Wooden, 2022; Yosifovich et al., 2023). Besides, as the number of connected devices in the home context and mobile banking usage is growing, households face the need for cybersecurity solutions (Yosifovich et al., 2023).

Overall, households and companies, through remote employees, are highly exposed to cyber threats nowadays. Companies have been adopting cybersecurity solutions and are

expected to keep investing (Grand View Research, 2022; Fortune Business Insights, 2022; Aiyer et al., 2022; EFTMG, 2018) while end-users are getting aware of the risks.

6.3 International & National Cybersecurity Market Panorama

The rising usage of mobile devices, including smartphones, tablets, and computers (Technavio, 2023), the emergence of e-commerce activities, and the proliferation of Cloud solutions fuel the growth of cybercrime (Grand View Research, 2022). Such a trajectory promotes the evolution of the cybersecurity market in the same direction. It evolved substantially with the pandemic, as malware attacks increased by 358% (Griffiths, 2023), which translated into a rise of 7.7% in the global market exhibited in 2020 compared to 2019 (Fortune Business Insights, 2022). In 2022, the cybersecurity industry was estimated to be worth USD 202.72 billion. Further, it was anticipated to evolve positively at a 12.3% compound annual growth rate from 2023 to 2030 (Grand View Research, 2022), as businesses and individuals will keep being threatened and are expected to invest more in their online safety (Technavio, 2023).

At the Portuguese market level, there has been a growing trend in the use of internet services, in the last few years, with a relevant contribution of the pandemic (Anacom, 2022d; SecurityMagazine, 2021), having reached 82% of the population, in 2021 (Centro Nacional de Cibersegurança Portugal, 2022). The increased use of smartphones and the growing internet adoption significantly fuel the demand for cybersecurity nationally (Mordor Intelligence, 2023). According to CNCS (Centro Nacional de Cibersegurança Portugal, 2022; SecurityMagazine, 2021), there was a 79% increase in cybercrime in 2020 and a 26% increase in 2021, which translated into 46 327 reported incidents in 2021, evidencing the growing trend of such issue. As a result, cyber threats awareness also evolved positively (Centro Nacional de Cibersegurança Portugal, 2022), as searches for "Cybersecurity" increased substantially in 2020 and kept high in 2022 (Centro Nacional de Cibersegurança Portugal, 2022). Furthermore, Portugal ranked third among the European nations with the highest number of cyberattack occurrences in 2022, as reported by IBM (Calado, 2023). In 2021, Portugal's cybersecurity market was estimated to be worth €165 million (Cruz et al., 2022). Those trends are expected to promote the growth of the Portuguese cybersecurity market at a 7.7% compound annual growth rate from 2023 to 2028 (Mordor Intelligence, 2023; IDC, 2020).

6.4 Telecommunications Operators on Cybersecurity

The telecommunications industry is undergoing significant change. Consumers' habits, technologies, and threats to the sector are evolving at a fast rate, creating new cybersecurity challenges and risks. Therefore, Telcos must pioneer emerging technologies to face increasing regulatory demands and retain clients' trust (Rica et al., 2019).

The provision of VAS allows Telcos to differentiate from competitors. That effectively addresses evolving customer needs, increases customer satisfaction and loyalty, reduces churn (Annex 1), and enables upselling of goods and services to customers (Mahabir, 2021). VAS offers excellent chances to enhance the customer experience while going beyond being a mere connectivity supplier (Garcia, 2020). Telcos may grow their customer bases, generate new revenue, and establish vital alliances by concentrating on these services.

Regulators are focused on the cyber agenda. As a result of the rise of significant cyber incidents (including interruption of business, loss of intellectual property, and reputational damage), authorities are pressuring Telcos to build robust cybersecurity systems and cyber incident response capabilities (Rica et al., 2019).

Cybersecurity can have a significant impact on Telcos' credibility. Since operators are responsible for managing the crucial infrastructure required to transmit and store substantial quantities of sensitive data, Telcos constitute a significant target for cybercriminals (Slijkerman & Nijboer, 2022). Therefore, they must protect their operations from cyberattacks, which they often accomplish by partnering with the cybersecurity industry and equipment providers. As they develop capabilities and partnerships to improve their internal security resilience, Telcos can approach the rise in cybercrime as an opportunity to commercialize differentiated services that engage customers (Slijkerman & Nijboer, 2022). According to Nielsen et al. (2022), customers intend to purchase additional services from their telecommunications provider, especially device insurance and cybersecurity services. Despite imposing a significant threat to their reputation, Telcos can leverage cybercrime to earn customers' trust by providing better security and privacy protection. Moreover, Telcos' proximity to a broad customer base grants them an advantage to profit by offering cybersecurity solutions (Rica et al., 2019).

According to Allot, nowadays, cybersecurity is required by telecommunications consumers. With over 20 years of experience, Allot is a major network intelligence and

security solutions provider. Its cutting-edge technologies make the networks of more than 500 Telcos and businesses smarter, enabling 20 million users to be more secure (Allot, n.d.). In a more informed society aware of the cyber threats on their mobile devices, cybersecurity is not considered a luxury but a must-have. In an inquiry Allot conducted, 62% of respondents believe that secure connectivity is an essential feature they expect from mobile service providers. Furthermore, 75% of participants trust their mobile provider to shield them from online dangers, and 68% of all surveyed are willing to subscribe to a cybersecurity solution from their mobile service provider, which promotes higher customer loyalty. Additionally, Allot found that mobile security protection is the biggest concern among consumers (54%), surpassing entertainment (13%) and equipment insurance (12%). Moreover, 80% and 62% of consumers considered switching to an operator that offers a security service and a superior offer, respectively. Further, over 90% of the enquired were willing to pay for cyber protection (Allot, 2022). MacKinney (2020) reinforces such trends, pointing out that rising concern over cyberattacks translates into a higher willingness to pay for security from telecommunications operators.

In 2021, the IT and Telecom Cybersecurity market was estimated to be worth USD 30.18 billion, and it is projected to grow by a compound annual growth rate of 12.1% over the next decade (Grand View Research, 2021a). Hence, cybersecurity creates a significant opportunity for Telcos services and revenue growth as consumers seek integrated security software and services (Slijkerman & Nijboer, 2022). Thus, operators can bundle such services by partnering with cybersecurity providers, enhancing customer loyalty (Sujata et al., 2015).

In this sense, the following sections aim to understand the current state of the telecommunications industry, internationally and at the Portuguese market level, regarding B2C cybersecurity offers. To achieve that, a benchmark of leading global Telcos' offers will be conducted, followed by an analysis of the national market and a positioning analysis. Finally, a PESTEL evaluation will take place to explore the environment NOS operates.

6.5 International Players' Offers

In the international market, some players stand out due to their offers regarding cybersecurity services. In this sense, the services provided by some of the leading telecommunications operators globally were analyzed and summarized in Annex 2. Thus, the present section will overview international players' offers and best practices regarding their packages and features (explained in Annex 1).

From the evidence of leading international operators, it is possible to conclude that, excluding O2 (UK), all analyzed players provide solutions regarding the growing online safety concern. O2 (UK) only includes in their broadband services age restrict content to protect the youngest. A fundamental aspect concerning cybersecurity services is how they are provided. There are currently two technologies: DNS and End-Point (Annex 1). The End-Point solution is the most common, with over 75% of players providing it. However, providing both is not. Telenor (Norway) is an excellent example of an operator offering a complete portfolio, providing both individually, and TIM (Italy) goes further, offering both in a bundle. Such a topic will be further developed in section 6.7.1. Moreover, Real-Time protection and Antivirus (Annex 1) are standard features across all End-Point services. Over 75% of the telecommunications operators analyzed offer Parental Control features in their online security services. Players such as Telenor (Norway), TIM (Italy), and Sunrise (Switzerland) include those services on their packages oriented to the youngest. Although Sunrise (Switzerland) stands out regarding its parental control service – "Kaspersky Safe Kids," as it provides child location, social networks management, and real-time alerts in case of suspicious behavior, it consists of an extra service not included in the cybersecurity services. Additionally, a few operators offer find-device or anti-theft tools that make it possible to locate devices in the event of loss or theft and remotely delete user data.

All cybersecurity services intend to protect consumers' personal information. Some new features are emerging in Telcos' offers, such as VPN, Identity Protection, and Password Manager (Annex 1), which are only offered in End-Point protection packages. VPN and Password Manager have become more common, with 25% and 35% of the addressed operators providing in their offers, respectively, allowing more robust services and addressing customers´ needs. However, some services are more powerful, with more than 60% of End-Point service providers looking forward to avoiding personal data breaches with Identity Protection features. TELUS (Canada) stands out by providing the most complete Identity Protection service in partnership with Norton. Besides protecting users from personal data exposure, its "Online Security" services conduct dark web monitoring, continuously searching for users´ information online (clients' usernames, passwords, and credit card information) and notifying them when a data breach is found.

Cybersecurity services are generally compatible with all operative systems (OS). Despite some incompatibilities with iOS regarding Antivirus features, online safety services

are compatible with Android and iOS smartphones and tablets, as well as with Desktops and Macs. Provisioning users with a platform to manage their features as Parental Controls and monitor the threats they were protected from enhances the envisioned benefits the services generate. The services provided at the End-Point level tend to provide an App/software where users can monitor their features, such as Proximus (Belgium), Orange (France), and DNA (Finland). Alternatively, operators such as TELUS (Canada), TIM (Brazil), and Telenor (Norway) provide reports on usage by SMS or Email or have an online portal where customers can access the service tools.

Online safety services are provided on a single-license or multiple-license basis. Operators offer alternative packages besides providing single-license subscriptions, which are more common in DNS services. The most common End-Point packages include three and five licenses, but companies like DNA (Finland) and TELUS (Canada) have plans for up to 25 devices. Moreover, it is a common practice to offer "Family" packages, which generally allow five devices in End-Point services and unlimited devices when the service is provided through operators' home networks (DNS). Further, offering family-oriented packages with Parental Controls, such as Vivo (Brazil) and TIM (Italy), is a great practice. Besides offering online safety services in packages, some operators also provide those in bundles. For instance, TIM (Italy) provides – "TIM Safe Navigation 360", which includes mobile network (DNS) and End-Point protection for up to five devices. Moreover, it combines "TIM Safe Navigation" on its telecommunications subscriptions for children – "TIM Junior," a common practice among operators. For instance, Sunrise (Switzerland) includes its "Surf Protect" and "Surf Protect Home" services in mobile and internet subscriptions. Regarding pricing, some companies, such as Virgin Media (UK) and SKY (UK), provide online security services for free. It is important to note that those offered for free are DNS services. In section 6.7, prices will be further explored.

A few players' packages include additional features like Cloud and Cyber Insurance (Annex 1). Two operators offer subscription-based services, and companies like Telenor (Norway) and Movistar include unlimited Cloud storage on their online safety services. With a different value proposition, Sunrise (Switzerland) and TIM (Italy) have game clouds available for the youngest, which intends to deliver games adapted to the user's age. Further, some Telcos include Cyber Insurance services in their packages. That is the case for operators like TELUS (Canada) and Telenor (Norway), which offer insurance services covering identity

and data theft damages. However, TELUS (Canada) stands out by providing identity restoration from specialists, and Telenor (Norway) offers psychological or legal help.

To conclude, it is possible to access Telcos' wide adoption of online safety services offers. They provide different services, with a few standard features and emerging new ones, such as VPN and Password Manager. Additionally, they deliver essential solutions to more complete ones, targeting different customers and household dimensions.

6.6 National Competitors' Offers

The Portuguese Telecommunications industry comprises a few strong operators, such as MEO (Altice), Vodafone, and NOS, and some small and new entrants, such as NOWO, Lycamobile, and DiGi. The national offers are synthesized in Annex 3.

National Telcos provide both DNS and End-Point online safety services. Vodafone and MEO offer mobile DNS solutions, which provide Real-Time threat protection. Additionally, MEO's solution comprises an age-restricting content feature. Further, MEO and NOWO commercialize End-Point solutions containing Real-Time threat protection, Antivirus, and Parental Controls, in partnership with Panda and F-Secure. Regarding emerging features, MEO is the only operator offering Password Manager and Identity Protection. Moreover, the End-Point offers include an App to monitor the features. However, such solutions evidence some limitations in operative systems compatibilities and are provided in packages with fewer licenses than international services. Overall, diverse online safety solutions are offered by Telcos in Portugal.

National competitors' communication focus is an important dimension to consider. MEO centers on the users' protection from malicious websites and their devices' security. Vodafone communicates its service differently, focusing on browsing risk-free and family safety. Finally, NOWO focuses its message on the safe browsing experience it provides. Such a dimension will be further explored in section 6.7.1.

Besides the offers from Telcos in the national market, it is critical to consider indirect competitors. Technology, insurance, and banking players also offer cybersecurity solutions. Technology companies like FNAC, Worten, and MediaMarkt provide online safety services from well-known cybersecurity providers such as Norton, McAfee, Kaspersky, and Panda (FNAC, n.d.-b; Worten, n.d.; MediaMarkt, n.d.). Further, in partnership with F-Secure, FNAC offers "Fnac Total," which combines device insurance and cloud with online safety

features, such as password manager and identity protection under its brand name (FNAC, n.d.-a). Moreover, it is important to note that numerous global cybersecurity providers, such as the ones mentioned above, offer their services digitally through website commercialization, enlarging the national competitive environment. Furthermore, insurance companies like Fidelidade and Ageas Seguros provide Cyber Insurance services directed to final consumers (Fidelidade, n.d.; Ageas Seguros, n.d.). Finally, national banking players, such as Santander Totta and Millennium BCP, offer Cyber Insurance services to businesses (Santander, n.d.; Millennium BCP, n.d.). Hence, it is possible to access that other players offer services that international Telcos include in their cybersecurity plans.

To conclude, national Telcos address online safety concerns by providing DNS and End-Point solutions (Annex 3). MEO stands out by providing the most complete offer. However, none offer VPN, Cloud, or Cyber Insurance in their plans, lagging behind the international offers. Also, it is worth noting that indirect rivals offer solutions from well-known providers and are introducing Cloud and Cyber Insurance services.

6.7 Competitors' Positioning

6.7.1 Competitors' Business Positioning

In addition to understanding competitors' offerings, it is fundamental to assess their positioning. Strategic groups analysis aims to identify the critical strategic dimensions that differentiate firms within an industry and to understand how those differences affect their competitive behavior and performance (Johnson et al., 1984/2017, pp. 81–84).

There are crucial dimensions for Telcos regarding the supply of cybersecurity services impacting their positioning. On the one hand, the suppliers they partner with will influence their decision regarding their branding strategies. Operators seek to establish partnerships with strong cybersecurity players with strong brand awareness and services, to benefit from their reputation and service reliability. Thus, two different strategies arise. Some Telcos provide services under their partner's brand, leveraging their reputation and incurring lower reputational concerns. Oppositely, other operators establish partnerships with less-known players and commercialize their services under their brand name. Such a path implies enhanced marketing efforts, despite benefiting from higher revenue share.

Additionally, the services' technology conveys a strategic dimension. By providing online safety services through their (mobile and fixed) networks (DNS), Telcos look forward

to delivering more straightforward solutions. In contrast, by providing End-Point solutions, operators offer more advanced services, targeting different customers. Figure 12-5 (Annex 4) summarizes the Telcos' positioning regarding such dimensions. It is possible to acknowledge that most operators adopt their brand to place their online safety offers. By partnering with less-known players, such as Allot, F-Secure, and Kaspersky (NOS, 2021), operators are subject to higher reputational implications. Companies that employ their providers' brands establish partnerships with well-known players, such as Norton, Panda, and McAfee (NOS, 2021). Also, those only provide End-Point services, which are generally preferred. There is a parity between DNS and End-Point services regarding white-label offers at the international and national levels. Moreover, it is essential to note that national operators tend to provide cybersecurity services under their branding. However, MEO offers two services placed oppositely on the map, providing an End-Point service from Panda. The strategic duality End-Point versus DNS services leads to other dimensions.

On the other hand, the services' role for the operator and its business model are also important aspects to consider. The last refers to the service being included for free or offered as a value-added service. A service is deemed to have a strategic role in case online safety is a crucial aspect of the operator's positioning regarding internet services. Moreover, a tactic role occurs when an operator looks forward to adding value through commercial conditions. Therefore, operators' positioning can be defined in four categories, according to their goals and business model. Figure 12-6 (Annex 4) synthesizes the national and international operators' safety positioning. It shows that most players provide cybersecurity services as a VAS to improve their revenues, even though national players (MEO and NOWO) place those offers as a crucial feature in their internet services (strategic role). Additionally, it is worth noting that the direct competition NOS faces promotes its offers as value-added services, not directly threatening NOS initiatives' business viability.

To conclude, there is a dominance of international white-label commercialization and End-Point services. Moreover, cybersecurity services are commonly provided as VAS, taking on a tactic role internationally and a strategic position in the Portuguese market.

6.7.2 Competitors' Positioning towards Customers

Regarding Telcos´ positioning toward their customers, there are essential aspects to consider. As consumers have identified a need, they start searching for solutions. When conducting their purchase decisions, the first aspect customers compare over the offers they

face in the market is the features they include (APM, 2022). Some clients have more standard needs, such as Antivirus and Real-Time protection features, while others have more advanced ones, like VPN and Identity Monitoring. Additionally, device compatibility with operating systems is a core aspect when considering subscribing to a cybersecurity service. In this sense, the criteria "Nº of Features" (Annex 2 and Annex 3) is considered in Figure 12-7 (Annex 4), comprising the total amount of features and compatible operative systems.

Every customer has different motivations when choosing an online safety service. Apart from the services' features, customers also consider their prices (APM, 2022; Wagner, 2019). That happens when the products' perceived characteristics are somewhat indistinguishable, especially during a period of purchasing power loss (section 6.8). Moreover, they care about the number of licenses, i.e., the number of devices the service can protect. Therefore, Figure 12-7, which intends to summarize national and international players positioning, refers to the "Price p/License" to address such vital dimensions. It represents every offer from the national operators. However, the average price per license and the total number of features was computed for each international player's offers to simplify the analysis.

Customers want to subscribe to the best value offers (First Insight, 2023; Kraus, 2019). Thus, they aim to find products that offer maximum benefits for the lowest price. As Figure 12-7 evidence, there are two major approaches toward customers. The first consists of a lower-value segment, which offers fewer features for a lower price. The second consists of a higher-value one that entails more advanced features on top of the basic ones for a higher price point. From Figure 12-7 is possible to access that most operators provide lower-value services. The national competitors are included in such a conclusion except for MEO, which provides a high-value service from Panda.

6.8 External Environment Analysis

The PESTEL analysis is a vital technique for examining the whole macro-environment of a business, essential for developing a corporate strategy (Johnson et al., 1984/2017, pp. 34-48). In this sense, an analysis will be conducted at the Portuguese level regarding political, economic, social, technological, environmental, and legal dimensions.

At the **Political** dimension, several factors can be pointed out that are external to NOS but can affect its operations. Firstly, the government and the National

Communications Authority – Anacom - promoted an initiative that imposed telecommunications operators to provide internet services for low-income or socially disadvantaged families (Anacom, 2022a). Further, the government is committed to fostering national cohesion and connectivity by investing in developing telecommunications networks in less-covered areas (Rodrigues, 2021). Finally, the national minimum wage will be revised by 7,8% to reflect the inflation evolution (Portuguese Government, 2022).

From an **Economic** point of view, the minimum wage increase, despite being substantial, did not translate into the maintenance of the national purchasing power, which translated to families experiencing an actual decrease of 2% in their purchasing power (Idealista, 2023). Moreover, to counteract the inflation path, BCE carried through 2022 a series of raises on interest rates, leading to families´ purchasing power loss (Idealista, 2022; Idealista, 2023). In addition, as inflation is still far from the desired level, BCE is expected to keep such measures in 2023 (Idealista, 2022). Finally, in 2022, unemployment decreased, reaching 6%, the lowest value since 2002, pointing to a strong dynamism in the national economy (Portuguese Government, 2023; INE & Pordata, 2023).

The **Social** environment in Portugal got characterized by the general perception of the "Internet" as an essential service. Such a perspective resulted mainly from the pandemic experience, which led to unprecedented levels of teleworking and distance learning, causing significant growth in the use of communications services (Anacom, 2022b), namely the increase in broadband traffic by 36% in 2020 (Anacom, 2021). Further, such practices have become a new standard, as employees have preferred remote (Eco, 2022b) and hybrid work models (Nova SBE Education, 2022). Moreover, according to Anacom, Portugal registered a shift in consumption behaviors, as residential internet connectivity is currently at 87%, compared to 92% in the EU, and the usage of over-the-top services surpasses the EU (Anacom, 2022b). Consequently, as mentioned in section 6.3, the rising cybercrime trend leads to increased social awareness (Coelho Dias, 2022). Finally, the most technological generation - Generation Z, which prefers digitally enabled experiences and on-demand convenience, is just beginning its purchasing power ascent (Smurygina et al., 2022).

Technology consists of a detrimental aspect of today's society, especially for companies operating in the telecommunications industry. Consumers' behaviors constantly evolve and become more demanding, requiring continuous connectivity and internet accessibility (Perrin, 2022; Oliveira, 2014; Cruz, 2023; Anacom, 2021; Nagel, 2020).

Operators must keep track of technological evolvements to sustain and enhance their position in such a competitive industry. Hence, introducing 5G technology at its full potential is essential (Marr, 2022), despite being expected to convey new security concerns and challenges (Wood, 2022; Vonage, n.d.). Moreover, cybersecurity has become a significant concern recently and consists of a fast-evolving technology (Chukwube, 2023). Deploying artificial intelligence and machine learning tools is vital to address such an issue and improve businesses' operations (Marr, 2022; Smurygina et al., 2022).

There are **Environmental** aspects that also impact the telecommunications sector. The environmental crisis is acknowledged by Europeans, especially by Portuguese people, as the second-most significant global concern (Neves, 2022; Green Savers, 2021). Such strong environmental consciousness (Gromicho, 2020) impacts their purchasing behaviors, as many consumers value and favor companies with ethical or environmentally friendly practices and offers (Correia, 2021; Archer, Cromwell, & Fenech, 2022). Finally, consumers are taking essential steps towards a sustainable lifestyle, considering producing sustainable packaging and products as a crucial sustainable practice (Archer, Cromwell, & Fenech, 2022), especially regarding technological products (Correia, 2021).

From a **Legal** perspective, the telecommunications industry is regulated by Anacom in Portugal. As mentioned above, new laws are being introduced to support low-income families during economic constraints. A recent law enables early contract termination without penalty for those unemployed, suffering from severe sickness, or moving abroad. In case there is no legal coverage, consumers can also terminate their contracts for 50% or less of the expenses (Eco, 2022a; Anacom, 2022c) to promote enhanced competition to counteract the positive evolutions of prices driven by inflation (Abreu, 2023). Further, new legislation stipulates that firms must support employees' operational expenses in work-from-home scenarios (Sacadura, 2021; IT Insight, 2022; Eco, 2023). In addition, the national regulator introduced new legislation that requires examining operators' network hardware to look for potential security holes in the nation based on security standards that align with EU regulations, stipulating that operators can only use audited and approved equipment (Rodrigues, 2022). Moreover, the sector's regulation comprises laws that protect consumers from data breaches and privacy invasions (Procuradoria-Geral Distrital de Lisboa, 2022).

Several relevant factors regarding the external environment in which NOS operates were pointed out. Such insights allow NOS to tailor better and sustain its re-launch strategy.

7 NOS Analysis

7.1 NOS Group

In 2014, ZON and Optimus, two of the largest communications companies in Portugal, merged to form NOS Communications S.A. (NOS, 2023a). ZON was a market leader in Portugal, leading the nation's Pay-Tv industry, placing second among Internet service providers, and dominating the national market for movie theatres. Optimus was a national telecommunications disruptor, emerging with the introduction of mobile and fixed services and mobile broadband internet. At the time, there was an industry trend toward consolidation, as operators intended to present integrated offers (David, 2015).

NOS Group comprises sixteen companies, including NOS Communications (Annex 5). Currently, NOS Group is the biggest telecommunications and entertainment group in Portugal. It conducts operations in the telecommunications sector, cinema, audiovisuals, advertisement, and brand placement. It is committed to the quality of its services and customer satisfaction, driven by ideals of responsibility and technological advancement.

NOS Group was established in the Portuguese telecom market with cutting-edge services that enabled the operator to record a 37,2% market share in Pay-Tv in 2022, 65% of the Cinema exhibitions industry, and more than 50% of the content distribution market in 2021. The consolidation enabled NOS to market more robust offers by developing its business portfolio, and delivering its consumers better value, translating into the conquer of several awards over the years, especially the Product of the Year award, Fastest Mobile Network, and Best Mobile Network Coverage awards, in 2022.

7.2 NOS Communications Positioning

Although NOS Group operates various businesses, the current analysis will concentrate on NOS Communications, the telecommunications operator. NOS provides various telecommunication services, namely fixed and mobile telephone services, pay-tv signal distribution services, and internet access services at fixed and mobile locations.

NOS emerged in the Portuguese Telecommunications market with the introduction of innovative services. It aspires to promote Portugal's development into a better society by expanding all connections and incorporating the most advanced technologies to deliver customers the best experience. NOS is dedicated to fostering ambition and attitudes toward challenging and transforming the present, with the future as an inspiration to employ the

most innovative technologies to create value for society. Accordingly, NOS launched over the years several cutting-edge services. It introduced the first Pay-Tv – "Iris," in Portugal, and an on-demand content service – "N Play," which enabled the operator to reach a 37,2% market share in the segment in the third quarter of 2022 (Anacom, 2023b).

The present work is focused on NOS' internet services. It brought internet cable services to Portugal, adopted the first wireless internet service – "Kanguru," and released the first fixed internet service with immediate installation – "wÖw." In 2021, NOS improved its Power Wi-Fi offer, contributing to the operator capturing 34.1% of the fixed broadband Internet services market in the third quarter of 2022 (Anacom, 2023a), awarded Product of the Year in 2022. Additionally, in February 2023, it launched Wi-Fi Total 6e, intended to enhance residential consumers' internet experience, evidencing its commitment to innovate. Further, NOS pioneered the adoption of 4G technologies in 2012, registering a 28.1% share of mobile services and 31.0% of mobile broadband Internet subscriptions in the third quarter of 2022. It recently introduced 5G, which made NOS' mobile network nationally recognized as the fastest (NOS, n.d.-a) and best mobile broadband (NOS, n.d.-a; Marketeer, 2023).

In this sense, NOS aims to position itself in the Portuguese market as the operator that provides the best and safest internet services. Therefore, since 2010, it has offered mobile and fixed network customers (B2C) online safety services to enhance its visibility and improve market awareness as a safe internet provider.

7.3 NOS Cybersecurity Portfolio

7.3.1 NOS Safe Net

NOS introduced its first cybersecurity service for consumers – "Internet Protection," in 2010. Maintaining the partnership with F-Secure (technology provider), the service evolved into the current NOS Safe Net in 2017. The service consists of End-Point protection, which offers Real-Time safety while browsing, Antivirus, and Parental Controls, covering up to 10 devices. Such service, provided under NOS branding, is available for all NOS mobile customers and is compatible across iOS, Android, PC, and Mac devices.

NOS Safe Net is available in three different monthly subscription plans, including the same features, differing by the number of devices included (2, 5, and 10) (Annex 6). It is commercialized through the operator´s website and communicated to its client base via SMS and email. The service is also bundled with mobile plans, particularly kids' plans. Moreover,

NOS deployed Forum NOS and its internal information system to spread the word about the service externally and internally. Finally, in 2017, NOS counted on Centili's cooperation to successfully bill and charge for the service.

Focus message: "Safety for the entire family."

7.3.2 Navegação Segura – NOS Safe Browsing

In the context of growing cybercrime in Portugal, promoted by the pandemic, NOS launched NOS Safe Browsing in May 2022. The service was intended to provide NOS customers with a simple solution that offers a first line of defense against online threats. In partnership with Cisco, NOS provides the service under its branding, which blocks access to dangerous and malicious websites. It is available on NOS' fixed and mobile networks (DNS) and compatible with any device. Therefore, it is commercialized in two plans, respectively.

The commercialization of NOS Safe Browsing is conducted through outbound initiatives, inbound, website, and NOS App, as well as in the operator´s retail stores. Moreover, the company's external communication strategies entail the introduction of banners on the website and envision the usage of SMS and Email with tailored messages to welcome new clients and provide newsletters, usage tips, and retention strategies. Also, NOS communicated its new service through its information system internally and enhanced service available information through Forum NOS.

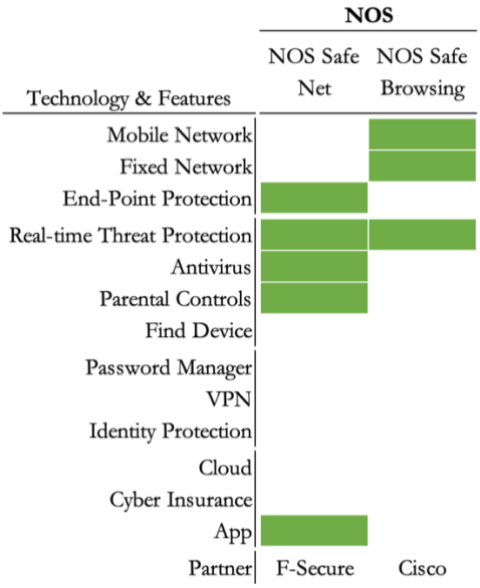


Figure 7-1: NOS Current Cybersecurity Portfolio
Source: Author's Elaboration

Figure 7-1 and Annex 6 synthesize the current cybersecurity portfolio's characteristics.

Focus message: "Immediate protection against malicious websites indoors and outdoors."

7.3.3 NOS Cybersecurity Portfolio – Key Takeaways

NOS' cybersecurity portfolio is one of the most complete nationally (Annex 3 and Annex 6). The DNS solution provides fixed and mobile protection. Further, the operator also offers an End-Point service, despite offering fewer benefits than other national offers. The success of NOS Safe Browsing is notable (Annex 7), reaching 20 times more clients in less than a year compared to the stagnant NOS Safe Net subscriber base. On the one hand,

the Safe Browsing launch in 2022 benefited from enhanced awareness regarding cybercrime threats and consequences. Additionally, it was introduced at a low price point, was available in more commercial channels, and its sale was promoted internally through retail sales commissioning. On the other hand, NOS Safe Net was only available on the website and communicated via SMS and Email to its customers. It was limited to mobile clients, with no commercial incentives in place. Moreover, it was launched with lower cybercrime awareness and at a higher price point. Despite the less favorable commercialization environment, the service registered very positive customer satisfaction. Therefore, leveraging the cybercrime panorama and developing a more robust marketing plan to promote the re-launch is crucial.

7.4 NOS Antivirus Total – The New Service

NOS has been conducting initiatives to address its customer´s online safety concerns and capture the business opportunity it represents. Considering the knowledge gained from its existing portfolio, NOS intends to improve its service launched in 2017. This includes enhancing NOS Safe Net's value proposition and implementing a re-branding and re-launching strategy to maximize its potential fully.

NOS Antivirus Total consists of an improved version of NOS Safe Net. It is an all-in-one End-Point online protection solution with features that make the product more advanced and distinct. It addresses a demanding audience willing to pay more for robust security products. The service, offered in partnership with F-Secure, adds features including VPN, Identity Monitoring, and Password Manager, which can be controlled via an App (Figure 7-2). According to the national and international benchmark and "Estudo de Opinião: Segurança Digital" (NOS, 2021) (Annex 8), these are the most prominent features. Additionally, according to the same study, the average number of internet-connected devices per household did not exceed five (NOS, 2021). Further, NOS Safe Net subscriptions evidenced that the average number of licenses active per subscription never surpassed four. Thus, despite being more robust, NOS intends to simplify its new offer by providing a single subscription plan, including five licenses.

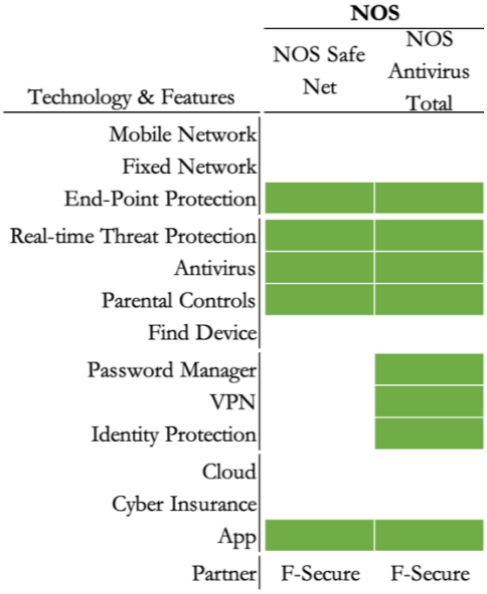


Figure 7-2: NOS Safe Net evlovution to NOS Antivirus Total

Source: Author's Elaboration

7.4.1 NOS Antivirus Total – Business Positioning

NOS Antivirus Total consists of an End-Point cybersecurity service, and despite being provided by F-Secure, it is commercialized under NOS branding. Therefore, it is positioned in the first quadrant (Figure 7-3), regarding the Service Branding Strategic Groups' map, competing directly with NOWO in such a segment. Further, the analysis of the international players evidences a trend toward Telcos providing End-Point protection services. Thus, the re-launch of NOS Safe Net reinforces the operator's cybersecurity portfolio by providing both DNS and End-point protection, as Telenor (Norway) and TIM (Italy) do. According to Allot (2022), that represents an opportunity for NOS to enhance its visibility as a safe-net provider, increase average revenue per client and attract new ones.

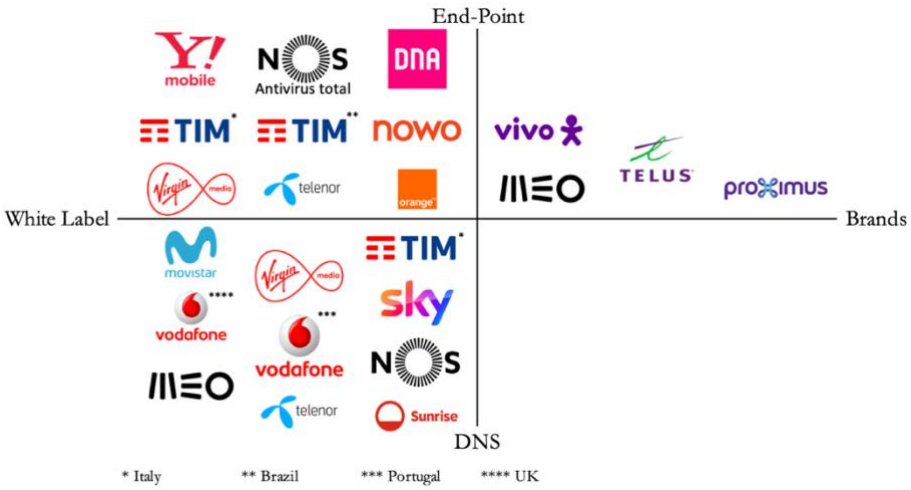


Figure 7-3: NOS Service Branding Strategic Groups Map *Source: Author's Elaboration*

As mentioned in section 7.2, NOS aspires to distinguish itself as the Portuguese market's best and most secure internet services provider. Moreover, it intends to

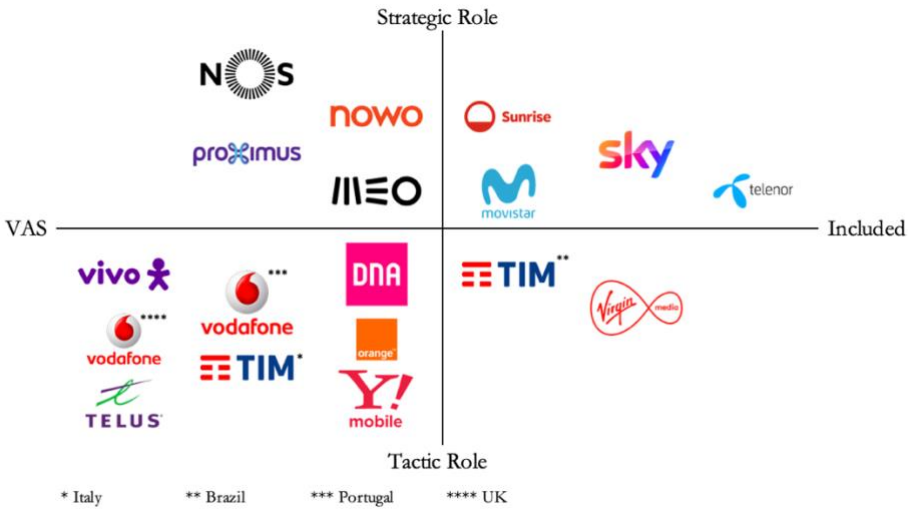
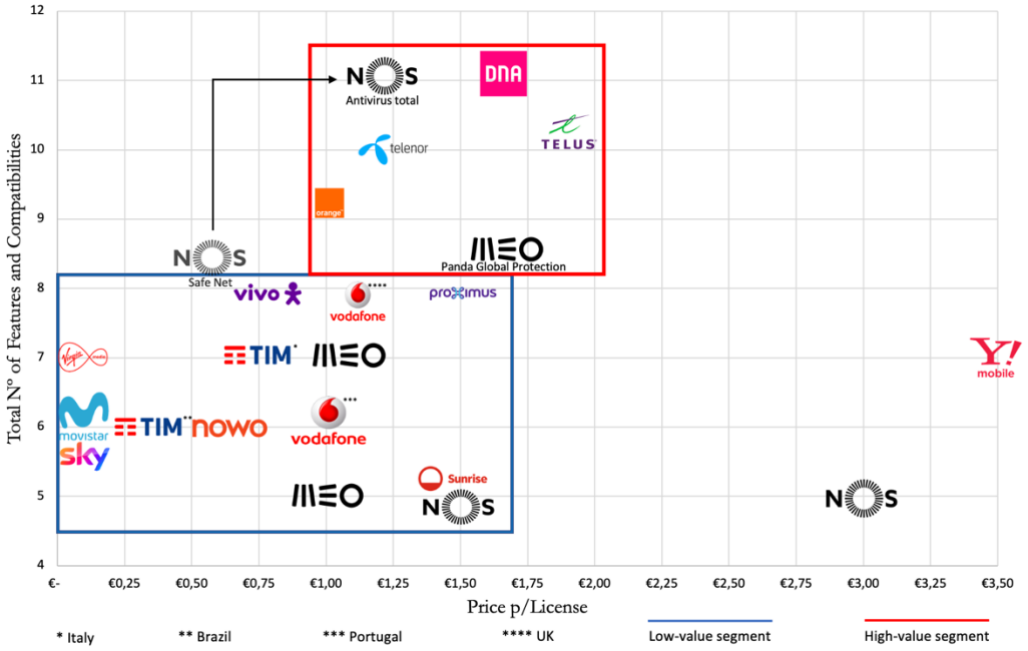


Figure 7-4: NOS Safety Positioning Strategic Groups Map *Source: Author's Elaboration*

commercialize NOS Antivirus Total as a value-added service in line with the ancestor - NOS Safe Net. In this sense, within the Safety Positioning Strategic Groups developed regarding the national and international competitors, NOS' cybersecurity portfolio, particularly the new service, is positioned in the first quadrant (Figure 7-4), i.e., it plays a strategic role for the operator and is provided as a value-added service.

7.4.2 NOS Antivirus Total – Positioning toward Customers

The improved service NOS intends to re-launch is placed in the high-value segment of the competitors' positioning towards its customers (Figure 7-5). Its predecessor – NOS Safe Net – was already placed above the low-value segment. However, it reaches the high-value section by providing extra advanced features at a competitive price. Moreover, as per Figure 7-5, it further allows NOS to enhance its competitive price advantage over MEO's offer. Consequently, NOS reinforces its portfolio by improving its End-Point offer. Therefore, the operator provides a robust portfolio with a simpler solution – "Safe Browsing," competing in the low-value segment, and a highly complete one – "NOS Antivirus Total," competing in the high-value segment.



Note: Y!mobile Price per License is €4,5;

Figure 7-5: NOS Antivirus Total – Positioning toward Customers *Source: Author's Elaboration*

7.4.3 Partners Architecture

NOS Antivirus Total is offered in association with F-Secure and counts on Centili's support to be available to clients and harmonize partners' systems.

F-Secure was established in the cybersecurity industry in 1988. It has followed cybercrime evolvement throughout the years and conducted industry-leading innovation to neutralize such threats. By developing award-winning services and partnering with over 170 service providers, such as communication service providers, retailers, banks, and insurance companies, F-Secure protects millions of customers worldwide (F-Secure, 2023). The maintenance of the partnership lies in the robustness of F-Secure service, the fact that it allows NOS to personalize the App, commercializing it under its branding, and the fact that it fortifies a long-term alliance, exploiting its reliability and avoiding further operational costs.

With cutting-edge features, mobile payment options, and an effortless user experience, Centili makes it possible to monetize digital content and services (Centili Limited, 2023). It aims to increase engagement and expenditure in digital platforms. Since its launch in 2011, Centili has grown to serve more than 4 billion mobile consumers across 80 countries, and its services are recognized as the top direct carrier billing services for 2021 (Infobip Limited, 2023). The billing phase of the customer's subscription process is where Centili contributes. Contrary to NOS Safe Browsing, which is fully integrated with NOS operations, NOS Safe Net required an extra partner regarding the billing process, enabling the harmonization of NOS and F-Secure systems. Furthermore, Centili's platform will allow more versatile payment methods that enable non-clients to subscribe to the service and compete with non-Telcos. Therefore, the maintenance of the partnership will expand the service's availability and reinforce NOS's competitive positioning nationally.

NOS manages to provide a cybersecurity service with the best technology in the market and a great subscription experience for its clients by partnering with F-Secure and Centili. NOS will make F-Secure's technology available in its online and retail stores, and customers will be able to subscribe online through Centili's payment platform, available on the service's landing page on the NOS website. As clients complete the subscription journey, Centili signals F-Secure to provide the licenses to subscribers and NOS to charge customers through the selected payment methods. Finally, NOS credits F-Secure and Centili for their respective revenue share. Annex 9 synthetizes the entailed customer experience.

Overall, the maintenance of such relationships is due to the excellent established reputation of the partners in their industry, which ensures service reliability and availability, avoiding increased costs related to integration procedures with new partners or internal IT and operational developments.

8 Marketing & Communication Plan

The present section intends to develop a marketing and communication plan to re-launch NOS Safe Net into the new NOS Antivirus Total. A Segmentation, Targeting, and Positioning analysis and a Marketing Mix will be developed to accomplish that.

8.1 STP Analysis

Developing a marketing and communication plan is essential to promoting the introduction of a product or service in the market (Kotler & Armstrong, 2019). Due to the market's diversity of users and their preferences, Kotler & Keller (2012) outline the importance of businesses concentrating on the clients they most likely satisfy to compete more effectively. To adequately address those customers, the authors argue that companies must organize potential consumers into different segments regarding their general characteristics and demand to target the most attractive ones. Then, to communicate more effectively, organizations must determine how they want to position themselves in the market to launch tailored marketing campaigns for each segment (Kotler & Keller, 2012). In this sense, a Segmentation, Targeting, and Positioning (STP) analysis will be conducted.

8.1.1 Segmentation

The first stage of an STP analysis consists of market segmentation. According to Kotler & Keller (2012), it consists of partitioning a market with diverse demand into smaller segments with similar needs. The segmentation process will be conducted for this analysis based on different consumer characteristics (Kotler & Keller, 2012).

NOS Antivirus Total target market comprises Portuguese households. Thus, it is detrimental to define the criteria to segment it. The first criterion is going to be the **Family Dimension**. It entails three categories: small, to address small families without children or dependents; and medium and large, regarding families with children or dependents. That is relevant since the family context is fundamental for Telcos' business (NOS, 2023b, p.8), and the new service offers five licenses envisioned for households and familiar environments, as pointed out in section 7.4.

The second is **Customer´s Technologies Dominance**. It consists of a significant aspect when offering a cybersecurity service affecting consumers' interest in such an offer. It considers three levels of technology dominance: no or low internet usage and dominance, medium and high, to represent consumers who use the internet and those with higher

dominance over technologies. Thus, the identified segments are small, medium, and large households whose inhabitants have no to high internet dominance, as per Figure 8-1.

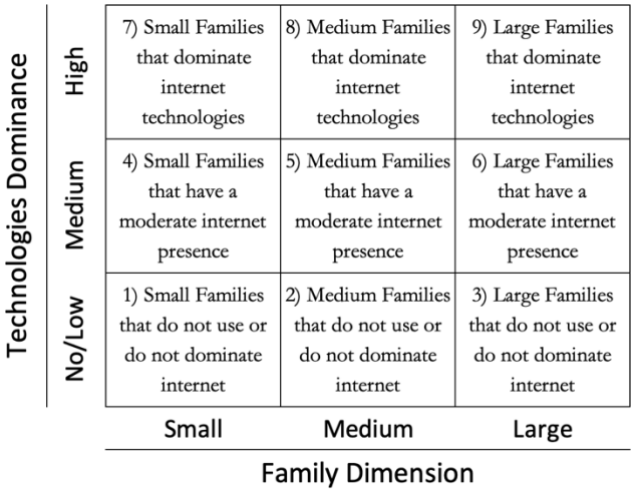


Figure 8-1: STP Analysis, Segmentation *Source: Author's Elaboration*

8.1.2 Targeting

As the market segments are identified, the next step is selecting which the company will target. Following Kotler & Armstrong (2019), not all identified segments are attractive from a size and profitability point of view. Additionally, the authors contend that the selected market segments must match the company's objectives and resources (Kotler & Armstrong, 2019). Thus, targeting requires determining the most appealing segments to serve.

The marketing and communication plan must direct initiatives to the core customer target to successfully promote the service's re-launch. NOS Antivirus Total is envisioned to serve a technological and more demanding audience aware of the available market solutions and already uses solutions such as Antivirus. Therefore, the segments that do not use the internet daily or barely dominate it should not be addressed, as they do not use it sufficiently to be willing to pay for a powerful cybersecurity service. NOS Safe Browsing addresses such a market segment, which provides a simple solution for less technological customers. Thus, targeting those customers, represented in the bottom row in Figure 8-1, would result in a marketing overlap and confuse customers.

According to a study NOS conducted to assess national online safety market feasibility, in 2021, families with children comprised 64% of the families, and the average household entailed three members. Moreover, the average household contained 2,5 elements who were 12 years old or older and were internet users, and the average number of internet-connected devices per household was 4,8 (NOS, 2021). Those insights evidence the

attractiveness of segments numbered four to nine (Figure 8-1) due to their market size (section 9.1) and alignment with the company's goals – provide technological clients with the safest internet experience. Figure 12-14 (Annex 10) illustrates the selected segments to target.

Additional criteria will be considered as the household' representative generational cohort (Dimock, 2019) and average income to conduct further segment selection within the attractive ones. According to Karadal & Abubakar (2021), generation Z (Gen Z) was born in a digitalized and connected world, and Generation Y (Gen Y) are "digital natives." Thus, Figure 8-2 synthesizes the cross-section analysis, evidencing that Gen Z and Gen Y have similar IoT skills, being placed as the ones with the highest dominance over IoT (Karadal & Abubakar, 2021). Moreover, Generation X (Gen X) are considered digital immigrants, having inferior IoT skills compared to Gen Y and Gen Z but superior to Boomers. Thus, Gen X and Boomers are categorized with medium and no to very low technology dominance. Furthermore, it is fundamental to consider consumers' income to access the most willing to subscribe. According to INE (2023), Banco de Portugal (2023), and Ferreira et al. (2021), the national average income evidences a growth trend with age. However, there is no substantial difference between Gen X and Boomers (Banco de Portugal, 2023), as represented in Figure 8-2. Consequently, it makes more sense to target older generations of consumers.

It is important to note that the present analysis considers the generational cohorts of the household members responsible for purchasing decisions, notwithstanding that other generations may live in the same household and influence it. Based on the additional criteria, segments four to six are considered the most attractive due to the higher average annual income of Gen X compared to Gen Y (Annex 10). Within such market segments, customers are more likely to find the new service suitable to their household environment due to the number of licenses it includes and the Parental Controls. Consequently, segment four is less attractive than the fifth and sixth, as those consist of medium and large families. The second more attractive segments are 7, 8, and 9 due to their higher IoT skills, despite Gen Y and

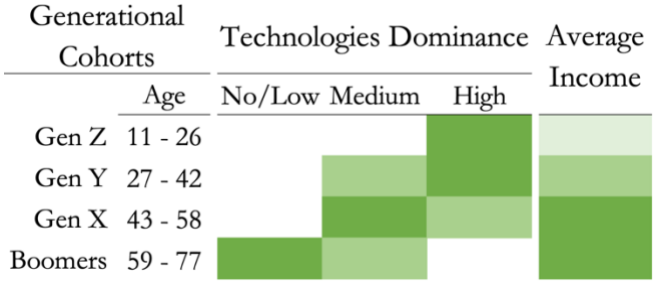


Figure 8-2: STP Analysis, Targeting Criteria *Source: Author's Elaboration*

Gen Z's lower income since they are more aware of the online dangers. Moreover, Gen Z looks forward to digitally enabled experiences (Smurygina et al., 2022). In this sense, the most attractive segments are illustrated in Annex 10 by generational cohorts.

Revella (2015) argued that it is essential to develop buyer personas to promote effective marketing strategies. That is because it provides companies with a better understanding of their customers' characteristics, needs, and preferences. As a result, it allows companies to align their marketing initiatives with the target customers' expectations, improving communications and engagement (Revella, 2015).

In this sense, three target personas can be defined from the most attractive market segments to simplify communication and marketing initiatives, based on NOS (2017). The first and most attractive target – "The Classical Parents" – is represented in Figure 8-3 and consists of medium and large families that use the internet daily, despite not dominating it completely. They are between 43 and 58 years old and present concerns regarding online safety, mainly online banking, shopping, and child protection. The second target – "The Technological Parents" – is similar to the previous one, differentiating because consumers belong to a younger generation (27 to 42 years old), with higher IoT skills and being more aware of online threats. Thus, they are more demanding regarding the features the new service includes. Finally, the third – "The Independents" – consists of small households with high technological capabilities with different interests, aged between 18 and 42. For instance, they do not benefit from Parental Controls and are more interested in features like VPN and Identity Monitoring. In this sense, the three target segments, synthesized in Figure 8-3, must be addressed individually, focusing on each one's specificities to enhance communication and marketing initiatives effectiveness.

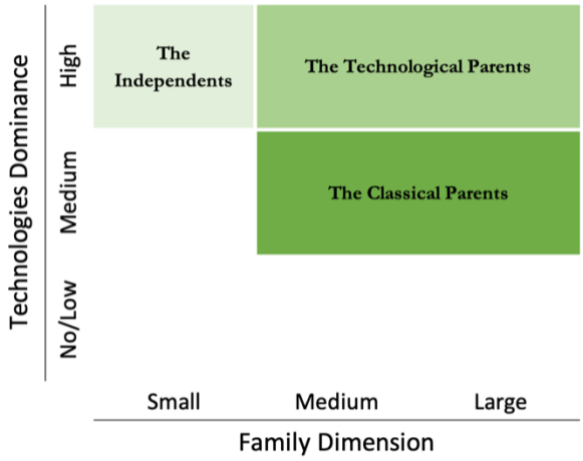


Figure 8-3: STP Analysis, Targeting *Source: Author's Elaboration*

8.1.3 Positioning

According to Kotler & Armstrong (2019), the final step is developing a differentiated image for the product in the minds of the target customers. NOS Antivirus Total is intended to provide NOS clients and non-clients with the safest online experience and stand out as the Telco that provides the completest cybersecurity service under its brand in Portugal.

The new service is directed to the most technological customers that demand more than the standard online safety technologies (such as Antivirus and Parental Controls). The target customers look forward to additional benefits, such as preserving their online browsing and location privacy (VPN). In this sense, NOS Antivirus Total aims to take over a relatively unexplored market segment, taking it as an advantage to address the most technological telecommunications customers and differentiate from the competition. The new service is intended to provide households with the ultimate cybersecurity service, by including highly valued benefits at a price point in line with the international practice for similar services, despite being higher than national offers. Thus, NOS intends to differentiate itself from its competitors by providing an advanced package in partnership with a credible provider (F-Secure) that offers more value to its customers. Further, the operator intends to leverage the re-launch to target Competitors' clients, as Easingwood & Harrington (2002) suggested.

Additionally, the re-branding entails a name and visual shift. The new service involves several changes that intend to convey a fresh identity to the ancestor service and portfolio through a new name, design, and logotype. At the time of the present work's conclusion, such aspects were yet to be defined by NOS. Thus, suggestions regarding re-branding will be devised. The success of NOS Safe Browsing would make it advantageous to name the new service after it, benefiting from its existing market awareness. Moreover, it could enhance the perception that the re-launch is a portfolio extension. Thus, it should be named "Safe Browsing Total," taking F-Secure's branding into account, or "Safe Browsing 360°," as Tim Italy does to promote a sense of a completer solution. Further, the current service's visual identity could be combined with the well-known NOS wheel, re-shaping it into a shield (Annex 11). Such evolution intends to reinforce the market association of NOS as a cybersecurity services provider. Moreover, it aims to enhance NOS brand visual identity association with safety, strengthening its positioning as a safe telecommunications operator.

Overall, NOS Antivirus Total is envisioned to enhance the operator's visibility as a safe internet and telecommunications provider and serve more demanding customers with a

higher willingness to pay. In this sense, the communication and marketing elements for the re-launch will be devised in the next section while considering the STP analysis findings.

8.2 Marketing Mix

The development of a marketing mix takes place as the organization has identified its target market and defined how it intends to position itself. From a buyer's perspective, the development of a marketing mix must encompass which problems the service will solve, the costs it entails, the convenience of its availability, and communication interactivity (Kotler & Armstrong, 2019). Thus, it consists of aspects NOS should articulate to promote successful market acceptance.

8.2.1 Product

As mentioned in section 7.4, the new service will be provided in a single configuration. That is to promote product simplicity and avoid confusing customers with various offers. NOS Antivirus Total prevents access to phishing websites and known harmful links that may attempt to infect devices with malware (Real-Time browsing safety). Additionally, it continuously scans devices' files and programs to identify and eliminate dangerous malware in real-time (Antivirus). Parents can restrict their children's access to potentially harmful applications, block access to inappropriate websites, and establish time limits for internet use (Parental Controls). Moreover, NOS Antivirus Total preserves online browsing and location privacy, preventing websites and advertisers from tracking users' online activities (VPN). Furthermore, the new service protects customers´ online identity by continuously monitoring the internet for their personal information (Identity Monitoring). It enables securely storing passwords and logging in with just one click (Password Manager). NOS Antivirus Total will provide five licenses per plan, including all the mentioned benefits.

8.2.2 Price

NOS Antivirus Total will be provided in two subscription plans. The monthly plan will be commercialized at €5,99 after a free monthly trial, promoting the service experimentation and accessibility for more price-sensitive customers (Becker, 2020). Clients can subscribe to the annual plan for €59,99 to promote retention by including two free months (Campbell, 2016; Harmon, 2018). Further, a three-month trial will be bundled with telecommunications package upgrades to promote its commercialization and awareness. That is due to the predomination of convergent clients within the target market (NOS, 2017).

Attracting competitors' clients is challenging in a saturated market like national telecommunications. However, it is one of the few ways to expand revenue. To attract non-clients, it is crucial to offer discounts and promotions (Kesten, 2022). Thus, conditions like those envisioned for NOS convergent clients would be ideal for addressing such clients.

NOS intends to promote a subtle transition for the existing NOS Safe Net clients. To achieve that, the operator will offer a one-year subscription to the new service for the same price point as their subscription. Additionally, since the new service entails the removal of the ten licenses subscription plan (Annex 6), it would be suitable to promote its bundling with NOS Safe Browsing (mobile or fixed), as TIM Italy does (section 6.5, Annex 2). That addresses households that may require more than five licenses or were subscribers of the ten licenses NOS Safe Net plan (Opuni et al., 2013). Such bundles should be priced considering MEO's End-Point offer, which provides a monthly license extension for €0,79 (Annex 12).

Such price points align with the End-Point solutions' prices that national and international Telcos offer (Annex 12) while providing additional features (Figure 7-5). It is noteworthy that free trial periods consist of the author's recommendation, as NOS had only determined price points as of the conclusion of the present study. NOS' pricing strategy positions the new service as the premium offer of the portfolio, being offered at a much higher price than NOS Safe Browsing. In addition to the convenience of the two subscription plans, the service does not entail a binding period. Further, Centili will grant the new service more versatile payment methods, such as MB Way and credit cards.

8.2.3 Place

The re-launch will be conducted in two steps. The first entails the availability of the new service for online subscription through the NOS website (monthly and annual plans). Although the target market, as mentioned in section 7.1, consists of people with medium and high technological dominance, most consumers still prefer to subscribe to services in-store (Tybus et al., 2023; NOS, 2017). Therefore, the second step intends to expand the NOS Antivirus Total market availability by offering annual subscription cards at the NOS stores. That consists of a significant step since it allows for promoting commercialization via commissioning, which proved effective with NOS Safe Browsing. Despite being available, door-to-door sales and Telemarketing are unsuitable channels as they do not allow targeting specific segments and entail high costs. Thus, NOS Antivirus Total will be available online and retail to expand convenience, availability, and market awareness.

8.2.4 Promotion

Even though consumers still prefer in-store purchases, digital marketing is a fundamental tool nowadays to interact with potential clients online (Chaffey, 2023). Such a marketing path promotes the reinforcement of Telcos' customer experience (Righini, 2020) due to the wide adoption of smartphones and internet usage, as mentioned in section 6.4.

In this sense, the new service must be promoted online through the website and digital marketing (SMS and Email) in the first re-launch step. BeeCreative (2021) argued that creating quality content is fundamental to attracting, engaging, and retaining customers. Thus, promoting the re-launch through the website provides customers with accessible information. Additionally, BeeCreative (2021), Righini (2020), and Chaffey (2023) contend that content marketing is a valuable tool for telecommunications companies to establish themselves as credible and pertinent sources of information for their audience. Forum NOS offers trustworthy educational content, enhancing NOS's brand positioning (Righini, 2020).

Furthermore, the exploitation of SMS and Email marketing allows direct contact with the target customers (BeeCreative, 2021; Righini, 2020). Such tools are among the most prevalent promotional techniques (Goworek, 2022) and crucial for non-mass market products. Despite the higher conversion rates of SMS marketing, those channels are complementary marketing strategies as SMS allows for short interactions, and Email enables completer and more dynamic exchanges (Goworek, 2022; Dmitrieva, 2023). Moreover, it will allow engaging with non-clients by recontacting old clients (Lesonsky, 2020). Thus, considering the STP analysis, it is possible to address consumers with tailored communications.

As per NOS (2017), customers favor in-store campaigns, followed by SMS and Email marketing as the primary methods of receiving marketing communications. Thus, the new service's in-store promotion should occur in the second stage.

8.2.4.1 The Re-Launch Communication

As pointed out in sections 4.4 and 4.5, properly communicating the re-branding and re-launch strategy is fundamental. Despite the current small customer base of NOS Safe Net, it is crucial to elucidate the reasons for such a move to foster positive reactions. Moreover, NOS must inform existing customers of the new service's changes and its implications on their subscription conditions. To promote such initiatives, SMS and Email marketing are

suitable channels. That is because SMS allows for an alert regarding the changes in their service subscription, referring to the website and Forum NOS. Email supports sharing additional contextualization for change, special subscription conditions, and raising awareness for new features. Further, NOS should consider communicating the re-branding by promoting messages through the NOS Safe Net app (Perplies, 2018; McCloskey, n.d.).

Similar methods will take place to address the target market NOS Antivirus Total intends to serve. As noted in section 4.5, a re-launch must be considered as the launch of a new offer (Bissdorf, 2016). Therefore, the new service must be communicated to the target segments through the website and digital marketing. To enhance the effectiveness of communications initiatives, NOS should tailor their messages and shared content to the characteristics of the different segments. For instance, when interacting with an "Independent" consumer (section 8.1), it must focus on the functionalities the new service offers that are the most relevant, such as VPN, and neglect its Parental Controls features.

The interactions with potential clients must place the new service as a viable solution to the target consumer's specific problem and NOS as a credible provider, as argued in section 4.4. Further, it is crucial to convey a superior value proposition when interacting with non-clients and to make it possible to compare offerings (Taylor, 2021). Thus, NOS must focus its communications on the benefits of such features for consumers (section 8.2.1), as well as on its brand name (NOS) and the credibility of its partner (F-Secure), to enhance the perceived quality of the new service. The operator conducted a test that proved that including the partner's brand name in SMS marketing enhanced engagement (NOS, 2022). In this sense, the new service's focus message could be "The Safest Internet Experience for the Entire Family." Furthermore, NOS should pursue a continuous communication plan to promote bilateral interactions and superior engagement with clients (Matthews, 2021). Additionally, by targeting "The Independents," NOS will take advantage of a target less likely to subscribe (section 8.1.2) but with a higher probability of influencing the other segments' buying decisions, as suggested in section 4.5.

Finally, despite being a VAS and not being promoted through mass media (TV, outdoors, and social media), NOS should promote a marketing campaign that does not focus on NOS Antivirus Total but refers to it through such channels. To reinforce its visibility and awareness as the safest operator, NOS could advertise its physical (NOS Alarms) and cybersecurity safety services, exploiting the proposed cybersecurity portfolio's new image.

9 Market Dimension and Economic Viability Analysis

9.1 Market Dimension

Once the target market has been identified through the STP analysis, it is crucial to evaluate its size. According to IGNOU (2017), any economic research should begin with a projection of total market potential. However, since the present analysis intends to access a Telco's B2C cybersecurity market dimension, the present section will focus on such market segments. A market segmentation study conducted by NOS (2017) on the Portuguese consumer market will sustain the analysis.

The new product's target market is national households. According to the study, there are around 4,1 million households in Portugal. The Independents, Classical Parents, and Technological Parents segments represent approximately 38%. Therefore, considering that NOS Antivirus Total is directed to NOS clients and non-clients, its market comprises over **one and a half million families** nationally (Annex 13).

9.2 Forecast Revenue

When planning the launch of a product, it is essential to assess its market dimension but also its envisioned sales (Business Queensland, 2022). There are various ways to estimate it, among them forecasting having market awareness, product trial, repeat purchase, and intent to buy indicators into account. Additionally, a company must consider its market share, product price, and market growth rate when estimating a product's revenue (IGNOU, 2017).

The target market for NOS Antivirus Total comprises over 1,5 million households. The service targets NOS clients and non-clients within the identified STP segments and is offered to NOS convergent clients. Three criteria were used to estimate how many people from the target segments would buy the product, based on "NOS Estudo de Opinião: Segurança Digital" (NOS, 2021). The first was the level of **cyber threats awareness**, considering the most worried customers about their online safety (13%) as the most likely to purchase. Second, the inquiries that **already had an Antivirus solution** were considered, representing 83% of the sample. The third criterion was customers' **willingness to pay** for a cybersecurity solution from a Telco, with the study evidencing that different segments have different purchasing intentions (NOS, 2021). Hence, the NOS clients' target market is predicted to be **13 thousand** households (Annex 14).

An additional criterion was considered regarding non-clients. According to Allot (2022), consumers are willing to switch to providers that offer cybersecurity services (80%), and 62% are considering changing to access greater offers. Switching providers in the Portuguese telecommunications market is disincentivized through contractual conditions, translating into 51% of consumers never having changed operators (Autoridade da Concorrência, 2020), and only 33% have changed in the last five years (Marktest, 2021). However, it is important to note that the new service will not require switching operators and that 48% of the target segments are clients of more than one Telco (NOS, 2017). Further, national competitors have cybersecurity offers serving part of such a market. Therefore, it is considered that 40% of non-clients are **willing to subscribe** to a service from a different Telco, making the non-clients target consisting of over **12 thousand** households (Annex 15).

In addition to the addressed target segments, NOS is targeting the new service to its convergent customers with internet services in their packages when they intend to change or renew their services. According to previous experience, as with Safe Browsing, NOS expects a 1% conversion rate after the free trial period by commissioning such sales. Thus, by addressing convergent customers, NOS expands the new service target by approximately **10 thousand** customers (Annex 16).

The estimated customer base is expected to be gathered throughout the first two years from the product re-launch. From the third year onwards, the product's customer base is anticipated to follow market growth. The Telecom Cybersecurity global market is predicted to grow at a compound annual growth rate (CAGR) of over 12% until 2030 (section 6.3). However, the Portuguese cybersecurity market is expected to evolve at a slower 7,7% rate (section 6.4), and the National Telecommunications industry is envisioned to expand at an under 1% CAGR from 2021 to 2026 (section 6.1). In this sense, the revenue projection for the first three years can be estimated, considering a market growth rate of 7% (Annex 17).

The conditions for directly targeted, convergent, and NOS Safe Net clients and non-clients must be considered (section 8.2.2). That is because they entail different prices or trial periods, leading to adjustments in the subscription income. Further, an assumption is considered regarding the distribution of subscription plans. Considering the national economic panorama of purchasing power loss, section 6.8, and according to Kodali (2023), it is considered that 70% of clients are monthly subscribers. Additionally, the analysis predicts

a 1% churn rate (Annex 1) as a standard rate for VAS, according to past data and F-Secure experience with over 200 Telcos. Finally, the estimation does not include value-added tax.

9.3 Cost Structure & Profit Projection

The new service's cost structure entails revenue share and sales commissioning. As pointed out in section 7.4.3., NOS Antivirus Total is offered in partnership with F-Secure and Centili. Such partnerships entail a revenue share distribution among the three players (Tymchuk, 2022). Centili assists with billing, taking a small per-transaction fee (CFI, 2022), while NOS and F-Secure share most of the revenue. F-Secure provides the technology, and NOS brings in its customer base, marketing channels, and strong, established brand (Nielsen et al., 2022). As a result, both contributions are essential for the service to become commercially viable. Therefore, a 50% revenue share for NOS is considered (Saxena, 2012). Thus, partners' revenue share may be considered as a cost. Moreover, by offering the re-launched service in their stores, NOS also incurs costs related to promoting service sales through sales commissioning. Such commissions consist of a month's revenue per annual plan sale, as NOS Safe Browsing. In this sense, the operational costs can be estimated, and the envisioned profits can be accessed in Figure 9-1.

	Year 0	Year 1	Year 2	Year 3
Total Customer Base	1 000	17 610	32 320	34 600
Revenue	**€ 36 000**	**€ 363 000**	**€ 1 249 000**	**€ 1 922 000**
Operational costs		€ 282 000	€ 714 000	€ 961 000
Commisioning		€ 23 000	€ 23 000	€ 3 000
Communication		€ -	€ -	€ -
Total Costs		€ 305 000	€ 737 000	€ 964 000
Operational Margin		**€ 58 000**	**€ 512 000**	**€ 958 000**

Figure 9-1: NOS Antivirus Total – Customer Base, Revenue, Costs, and Margin Projection
Source: Author's Elaboration base on NOS (2017) and NOS (2021)

Such projections evidence the attractiveness of such a market segment and its potential to expand NOS' income. It consists of a robust market, and the re-launch of NOS Safe Net is expected to drive the current €36 000 revenue (Year 0) to over €1,9 million by the third year. Despite not considering expenses with communication initiatives, NOS Antivirus Total is anticipated to generate over €1,5 million accumulated operational margin over the first three years, representing 0,002% of NOS' EBITDA in 2022 (NOS, 2023b). Since the commercialization of the new service does not require capital expenditure and the operational costs are tied to sales, the re-launch is sustainable independently of the customer base. Overall, such projections support the re-launch strategy.

10 Conclusions and Limitations

The present work seeks to evaluate NOS' strategy to promote the re-launch and re-branding of a cybersecurity service that has struggled to attract new customers for several years. NOS Safe Net was launched in 2017, and its customer base remained stagnant due to a lack of commercial availability and incentives and lower cyber threat awareness at the time. As a result, the service has remained in the maturity stage. Therefore, the study's objective is to evaluate whether NOS should undertake the re-launch of NOS Safe Net.

A broad market analysis addressed the research problem, providing crucial insights. The study of the involved industries evidenced the maturity of national telecommunications and the envisioned growth of Portugal's Cybersecurity and Telecom Cybersecurity markets. In such a scenario, the commercialization of VAS can be employed to retain and attract new customers to expand a Telco´s revenue. Moreover, the study suggests that Telcos face favorable conditions to exploit the opportunity the growing cybersecurity market trends represent by offering value-added cybersecurity services. The national and international benchmarks evidence Telcos' wide adoption of the commercialization of online safety services, with End-Point services being the most prevalent. Additionally, the national offers are less sophisticated when compared with the completer international solutions, which include emerging and advanced features, such as VPN and Cyber Insurance. In the national market, Telcos offer DNS and End-Point solutions under their brand, except for MEO, which commercializes an End-Point solution under its partner's brand name. Further, national competitors position their online safety offers as a crucial aspect of internet services, except for Vodafone, while offering them as VAS. The national macro-environment evidences the government's support for the access to and development of telecommunications services, translating into internet services being widely available and used, and considered an essential service. Further, it is crucial to note the enhanced awareness of cybersecurity issues and the introduction of laws favoring early contract termination and raising competitiveness in the national telecoms market.

By closely examining the Telco at study, NOS's innovative vision and commitment to delivering customers the best experience by incorporating the most advanced technologies is clear. And online safety is no exception. The operator strives to provide the best and safest internet services and experience nationally. NOS is the national Telco offering the most complete online safety portfolio comprising End-Point and DNS (fixed and mobile) services.

However, the current End-Point solution – NOS Safe Net – has a small and stagnant customer base. Further, it delivers fewer benefits than national competitors' services and is considerably weaker than international offers.

Therefore, considering the national telecommunications industry's negligible growth, it becomes harder for Telcos to enlarge their customer base and revenue. Moreover, as a new law enhanced competitive dynamics, retaining and attracting new customers challenges heightened. In such an environment, Telcos look for growth opportunities, and providing VAS stands out as a viable method to improve average revenue per customer and loyalty, reduce churn, and attract new clients. Additionally, as cybercrime rises and awareness expands, providing online safety VAS is anticipated to be a valuable opportunity. According to Saunders & Jobber (1988) and Bissdorf (2016), re-launch an existing offer presents advantages over developing a new one. In this sense, NOS would most likely benefit from revitalizing its cybersecurity portfolio by re-launching NOS Safe Net.

The new NOS Antivirus Total reinforces NOS' End-Point value proposition by considering the best international practices and findings of NOS (2021). It is intended to strengthen NOS´ safety strategic positioning, positively impacting revenue. Further, it places NOS' End-Point offer as the best value in the national telecommunications market (Figure 7-5). Additionally, the maintenance of the partnerships with F-Secure and Centili reveal vital for the re-launch, enabling the commercialization of a strong service available for any client, regardless of its Telco provider. Therefore, NOS reinforces its position as a credible cybersecurity services provider, managing to compete with non-Telcos, such as Fnac and Worten. Moreover, reflecting the learnings from its cybersecurity portfolio on NOS Antivirus Total marketing plan, NOS is re-launching a service to over one and a half million household target market, expected to generate €1,5 million accumulated operational margin throughout the first three years.

According to Singh et al. (2013), timing is crucial when implementing a re-branding strategy. NOS Safe Net is currently outdated among the national offers since its last value proposition modification was in 2017. Considering the success of NOS Safe Browsing, and the growing cybercrime trends, one may consider it the right time to pursue such a strategy.

Consequently, the re-launch and re-branding of NOS Safe Net reinforce NOS's cybersecurity portfolio, promotes customers' loyalty, resonate on average revenue per user,

and allow it to attract non-clients. Furthermore, it is cost-effective and contributes favorably to NOS' positioning and image in the national market.

The envisioned "NOS Antivirus Total" incorporates most international best practices, making it a high-value service. However, NOS must address the emergence of Cloud solutions to keep the portfolio attractive and competitive, either by introducing it in "NOS Antivirus Total" or by expanding the portfolio with a new value proposition, as Vivo (Brazil) with its "Safe Connect" VPN solution. Moreover, the mentioned trend among other national industries into offering Cyber Insurance poses an opportunity for NOS to reinforce its cybersecurity portfolio and lead such a market segment. Such prospects sustain the promotion of bundles within the portfolio and upsell of services.

The present work aimed to understand the foundation for the decision pursued by NOS. To achieve it, a telecommunications industry benchmark was conducted regarding cybersecurity offers based on players' website data, which may be incomplete and potentially lead to inaccurate conclusions. Further, the new service's market and economics assessment was based on NOS' outdated internal information and market surveys, which may not reflect an accurate forecast and compromise inferences. However, the study provides a robust basis to support NOS' strategic decision on the re-launch and re-branding of NOS Safe Net into "NOS Antivirus Total" and offers valuable insights on how to market it.

The study contributes to a practical understanding of the application of important theories and models in supporting decision-making. Additionally, despite the rich literature on corporate re-launch and re-branding, there needs to be more work developed on products and services and their application to real case studies. In this sense, the present study delves into a relatively underexplored application of a research topic, expanding the body of knowledge and enlightening future re-launch and re-branding initiatives by analyzing a real-world case study and offering valuable insights. Future research should be undertaken to encourage the evolvement of practical applications and the dissemination of best practices.

11 References

Abreu, S. (2023, February). *Anacom propõe reduzir prazo das fidelizações para baixar preços das telecomunicações*. Www.jornaldenegocios.pt. https://www.jornaldenegocios.pt/empresas/telecomunicacoes/detalhe/anacom-propoe-reduzir-prazo-das-fidelizacoes-para-baixar-precos-das-telecomunicacoes

Ageas Seguros. (n.d.). *Seguro Habitação - Casa Segura*. Ageas Seguros. https://www.ageas.pt/particulares/produtos/casa/casa-segura/

Aiyer, B., Caso, J., Russell, P., & Sorel, M. (2022). *New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers | McKinsey*. Www.mckinsey.com. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers

Allot. (n.d.). *Corporate // About Allot*. ALLOT. Retrieved June 13, 2023, from https://www.allot.com/corporate/about/

Allot. (2022, February). *ALLOT | Telco Security Trends H1 2022*. Info.allot.com. https://info.allot.com/TelcoSecurityTrendsH122_ContentDownloadLP.html

Alnabhan, O. (2018). *The Brand Effect*. Www.odayalnabhan.com. https://www.odayalnabhan.com/research-papers/the-brand-effect

ANACOM. (2021, March 11). *Pandemia de COVID-19 - Impacto na utilização dos serviços de comunicações em 2020*. Www.anacom.pt. https://www.anacom.pt/render.jsp?contentId=1603793

ANACOM. (2022a, February 21). *Tarifa social de Internet já pode ser subscrita*. Www.anacom.pt. https://www.anacom.pt/render.jsp?contentId=1716901

ANACOM. (2022b, May 15). *O estado das telecomunicações em Portugal e na UE numa imagem*. Anacom.pt. https://anacom.pt/render.jsp?contentId=1721924

ANACOM. (2022c, November 28). *Lei n.º 16/2022, de 16 de agosto*. Www.anacom.pt. https://www.anacom.pt/render.jsp?categoryId=324016

ANACOM. (2023a, January 6). *Internet access service at a fixed location - 3rd quarter 2022*. Www.anacom.pt. https://www.anacom.pt/render.jsp?contentId=1736254

ANACOM. (2023b, January 6). *Pay-TV signal distribution service - 3rd quarter 2022*. Www.anacom.pt. https://www.anacom.pt/render.jsp?contentId=1736244

APM. (2022, January 17). *How A Customer Decides What To Buy: A Step By Step Guide*. Apex pro Media. https://apexpromedia.com/how-a-customer-decides-what-to-buy-a-step-by-step-guide/

Archer, T., Cromwell, E., & Fenech, C. (2022). *How consumers are embracing sustainability*. Deloitte. https://www2.deloitte.com/uk/en/pages/consumer-business/articles/sustainable-consumer.html

Autoridade da Concorrência . (2020). *A fidelização nos serviços de telecomunicações*. https://www.concorrencia.pt/sites/default/files/processos_e_decisoes/epr/2020/As%2520Fideliza%C3%A7%C3%B5es%2520nos%2520Servi%C3%A7os%2520de%2520Telecomunica%C3%A7%C3%B5es%2520-%2520vers%C3%A3o%2520final.pdf

Banco de Portugal. (2023). *Boletim Económico - Tema em Destaque* (pp. 10–11). https://www.bportugal.pt/sites/default/files/be_mar2023_p_ted.pdf

Becker, F. (2020, May 29). *Monthly vs Annual Subscription: What's Best For You As a Customer*. Synder Blog. https://synder.com/blog/monthly-vs-annual-subscription/

BeeCreative. (2021, December 17). *Understand the role of digital marketing strategies for the telecom industry*. Bee Creative. https://beecreative.com.br/en/understand-the-role-of-digital-marketing-strategies-for-the-telecom-industry/

Bispo, D. (2023, May 16). *Vivo Protege: Saiba como proteger seus dados sendo cliente da Vivo!* Melhor Plano. https://melhorplano.net/vivo/vivo-protege

Bissdorf, J. (2016). *Success Factors of the Product Relaunch The Influence of the Advertising Strategy on the Success of Product Relaunch Campaigns* (pp. 1–11) [Master Thesis]. http://hh.diva-portal.org/smash/get/diva2:954176/FULLTEXT02.pdf

Bryant, M. (2013). *A Study on Rebranding Strategies*. https://digitalcommons.calpoly.edu/cgi/viewcontent.cgi?article=1106&context=grcsp

Business Queensland. (2022, December 8). *New Product Development*. Www.business.qld.gov.au. https://www.business.qld.gov.au/running-business/growing-business/new-product-development#-business-analysis-of-new-products-

Calado, D. (2023, February 24). *Cibercrime: Portugal no topo dos países europeus mais afetados em 2022*. Revista Líder. https://lidermagazine.sapo.pt/cibercrime-portugal-no-topo-dos-paises-europeus-mais-afetados-em-2022/

Campbell, P. (2016, October 31). *Why Annual Plans Are Crucial for Reducing Your Churn*. Www.profitwell.com. https://www.profitwell.com/recur/all/why-annual-plans-are-crucial-for-reducing-your-churn

Centili Limited. (2023). *Centili - About us - Global Digital Monetisation Company - Centili*. Www.centili.com. https://www.centili.com/about

Centro Nacional de Cibersegurança Portugal . (2022). Cibersegurança em Portugal - Riscos & Conflitos. In *Centro Nacional de Cibersegurança Portugal*.

https://www.anacom.pt/Nyron/Library/catalogo/winlibimg.aspx?skey=2753FD797E33438C8AFA4D43A392688E&doc=13748&img=20097

CFI. (2022, December 21). *Payment Processing Fees*. Corporate Finance Institute. https://corporatefinanceinstitute.com/resources/accounting/payment-processing-fees/

Chaffey, D. (2023, March 7). *10 reasons you need a digital marketing strategy in 2019 | Smart Insights*. Smart Insights. https://www.smartinsights.com/digital-marketing-strategy/digital-strategy-development/10-reasons-for-digital-marketing-strategy/

Chukwube, M. (2023, January 9). *5 Major Technology Trends to Observe in 2023*. ReadWrite. https://readwrite.com/major-technology-trends-to-observe-in-2023/

Coelho Dias, M. (2022, December 20). *Poder de compra: Seis em cada dez portugueses estão a viver pior do que em 2021*. Dinheiro Vivo. https://www.dinheirovivo.pt/economia/nacional/poder-de-compra-seis-em-cada-dez-portugueses-estao-a-viver-pior-do-que-em-2021-15514993.html

Collange, V. (2015). Consumer reaction to service rebranding. *Journal of Retailing and Consumer Services*, *22*, 178–186. Elsevier. https://doi.org/10.1016/j.jretconser.2014.07.003

Collange, V., & Bonache, A. (2015). Overcoming resistance to product rebranding. *Journal of Product & Brand Management*, *24*(6), 621–632. Emerald Group Publishing Limited. https://doi.org/10.1108/jpbm-10-2014-0730

Correia, R. (2021, June 17). *52% dos consumidores portugueses já compram produtos sustentáveis*. Distribuição Hoje. https://www.distribuicaohoje.com/consumo/52-dos-consumidores-portugueses-ja-compram-produtos-sustentaveis/

Cruz, F., Cerejeira, J., & Esteves, R. (2022). *Cibersegurança em Portugal*. CNCS. https://www.cncs.gov.pt/docs/relatorio-economia2022-obciber-cncs.pdf

Cruz, J. J. (2023, January 25). *Castelo Branco: Transportes públicos com internet gratuita*. Www.reconquista.pt. https://www.reconquista.pt/articles/castelo-branco-transportes-publicos-com-internet-gratuita

David, P. B. S. (2015). *ZON-OPTIMUS Merger: The Rise Of A Major Player In The Portuguese Telecom/Media Market* [Master's Thesis]. https://run.unl.pt/bitstream/10362/15420/1/David_2015.pdf

Design Council. (n.d.). *Framework for Innovation - Design Council*. Www.designcouncil.org.uk. Retrieved May 12, 2023, from https://www.designcouncil.org.uk/our-resources/framework-for-innovation/

Dimock, M. (2019, January 17). *Defining generations: Where Millennials End and Generation Z Begins*. Pew Research Center. https://www.pewresearch.org/fact-tank/2019/01/17/where-millennials-end-and-generation-z-begins/

Dmitrieva, I. (2023, February 2). *Comparing text messages and emails: a comprehensive guide to choose the right marketing channel*. Selzy. https://selzy.com/en/blog/sms-marketing-vs-email-marketing/

DNA. (2023). *Protect your online identity*. DNA. https://www.dna.fi/tietoturva/identiteettisuoja

Easingwood, C., & Harrington, S. (2002). Launching and re-launching high technology products. *Technovation*, *22*(11), 657–666. https://doi.org/10.1016/s0166-4972(02)00097-4

ECO. (2022a, August 16). *Publicada nova lei das telecomunicações. Saiba o que muda*. ECO. https://eco.sapo.pt/2022/08/16/publicada-nova-lei-das-telecomunicacoes-saiba-o-que-muda/

ECO. (2022b, December 20). *Trabalho híbrido e remoto representa, no máximo, 30% das vagas*. ECO. https://eco.sapo.pt/2022/12/20/trabalho-hibrido-e-remoto-representa-no-maximo-30-das-vagas/

ECO. (2023, February 10). *Parlamento aprova alterações à lei do trabalho. Saiba o que muda*. ECO. https://eco.sapo.pt/2023/02/10/novo-codigo-do-trabalho-vai-hoje-a-votos-saiba-o-que-muda/

EFTMG. (2018). *Cybersecurity Industry Overview*. Etfmg.com. https://etfmg.com/wp-content/uploads/2019/03/26-Prime-Indexes-CyberSecurity-Industry-Review-14112019.pdf

Elmansy, R. (2021, September 1). *The Double Diamond Design Thinking Process and How to Use it*. Designorate. https://www.designorate.com/the-double-diamond-design-thinking-process-and-how-to-use-it/

European Commission. (2022, June 7). *Cybersecurity Strategy | Shaping Europe's digital future*. Digital-Strategy.ec.europa.eu. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

European Commission. (2023, April 18). *Cybersecurity Act | Shaping Europe's digital future*. Digital-Strategy.ec.europa.eu. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

F-Secure. (n.d.). *What is cyber security?* Www.f-Secure.com. Retrieved May 10, 2023, from https://www.f-secure.com/us-en/articles/what-is-cyber-security

F-Secure. (2023). *Company | F-Secure*. Company.f-Secure.com. https://company.f-secure.com/en

Farrier, E. (2022, June 9). *What is cybersecurity?* Avast.com. https://www.avast.com/c-b-what-is-cybersecurity

Ferreira, P., Lopes, M., & Tavares, L. (2021). O Salário Médio em Portugal. In *Gulbenkian* (pp. 12–15). https://gulbenkian.pt/wp-content/uploads/2022/08/3_FF_SumarioExecutivo_SalarioMedio_pt.pdf

Fidelidade. (n.d.). *Fidelidade Cyber Famílias*. Fidelidade. Retrieved May 19, 2023, from https://www.fidelidade.pt/PT/particulares/Paginas/cyber-familias.aspx

First Insight. (2023, January 26). *Price vs Quality: What Matters Most to Consumers?* Www.firstinsight.com. https://www.firstinsight.com/blog/price-vs-quality-what-matters-most-to-consumers

FNAC. (n.d.-a). *Proteção FNAC - Planos*. FNAC. Retrieved May 19, 2023, from https://www.fnac.pt/planos-protecao

FNAC. (n.d.-b). *Serviços de Informática - Antivírus*. FNAC. Retrieved April 12, 2023, from https://www.fnac.pt/SearchResult/ResultList.aspx?SCat=8!1&SDM=list&Search=antivirus&sft=1

Fortune Business Insights. (2022, February). *Cyber Security Market Size, Share, Growth - Industry Analysis, 2026*. Fortunebusinessinsights.com. https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165

Frattini, F., Bianchi, M., De Massis, A., & Sikimic, U. (2013). The Role of Early Adopters in the Diffusion of New Products: Differences between Platform and Nonplatform Innovations. *Journal of Product Innovation Management*, *31*(3), 466–488. https://doi.org/10.1111/jpim.12108

Garcia, R. (2020, December 1). *The Role of Value-Added Services in Telecom Digital Transformation*. XpertAI. https://xpertai.com/blog/the-role-of-value-added-services-in-telecom-digital-transformation/

Global Data. (2023, March 9). *Portugal Telecom Services Market Size and Analysis by Service Revenue, Penetration, Subscription, ARPU's (Mobile, Fixed and Pay-TV by Segments and Technology), Competitive Landscape and Forecast, 2022-2027*. Market Research Reports & Consulting | GlobalData UK Ltd. https://www.globaldata.com/store/report/portugal-telecom-operators-market-analysis/

Goi, C.-L., & Goi, M.-T. (2011). Review on Models and Reasons of Rebranding. *International Conference on Social Science and Humanity*, *5*. IACSIT Press, Singapore. https://www.academia.edu/39004142/Review_on_Models_and_Reasons_of_Rebranding

Gottfredson, M., & Aspinall, K. (2005, November). *Innovation Versus Complexity: What Is Too Much of a Good Thing?* Harvard Business Review. https://hbr.org/2005/11/innovation-versus-complexity-what-is-too-much-of-a-good-thing

Goworek, K. (2022, August 12). *SMS marketing is still very effective (2022 update)*. TASIL. https://tasil.com/insights/sms-marketing-2022/

Grand View Research. (2021a). *IT & Telecom Cyber Security Market Size Report, 2022-2030*. Www.grandviewresearch.com. https://www.grandviewresearch.com/industry-analysis/it-telecom-cyber-security-market-report

Grand View Research. (2021b, April). *Global Telecom Services Market Size & Share Report, 2020-2027*. Www.grandviewresearch.com. https://www.grandviewresearch.com/industry-analysis/global-telecom-services-market

Grand View Research. (2022). *Cyber Security Market Size and Share | Industry Report, 2019-2025*. Grandviewresearch.com. https://www.grandviewresearch.com/industry-analysis/cyber-security-market

Green Savers. (2021, October 27). *Novo estudo indica que jovens portugueses têm grandes preocupações ambientais*. Green Savers. https://greensavers.sapo.pt/novo-estudo-indica-que-jovens-portugueses-tem-grandes-preocupacoes-ambientais/

Griffiths, C. (2023, March 6). *The Latest 2022 Cyber Crime Statistics (updated December 2022) | AAG IT Support*. Aag-It.com. https://aag-it.com/the-latest-cyber-crime-statistics/

Gromicho, I. (2020, December 16). *Inquérito revela que portugueses estão mais preocupados com problemas ambientais*. Ambiente Magazine. https://www.ambientemagazine.com/inquerito-revela-que-portugueses-estao-mais-preocupados-com-problemas-ambientais/

Harmon, A. (2018, October 10). *Monthly vs. Annual Subscription Pricing Analysis | Recurly*. Recurly, Inc. https://recurly.com/blog/monthly-vs-yearly-pricing-an-analysis/

IBM. (2018). *Learn the Enterprise Design Thinking Framework - Enterprise Design Thinking*. Ibm.com. https://www.ibm.com/design/thinking/page/framework/loop

IDC. (2020). *Visão 360° do Mercado TIC e Digital em Portugal*. https://www.idcdx.pt/insights/insights-up/uploads/2020/09/idc_360_pt.pdf

Idealista. (2022, December 30). *Subida de juros e inflação tornam créditos habitação mais caros — idealista/news*. Www.idealista.pt. https://www.idealista.pt/news/financas/credito-a-habitacao/2022/12/30/55883-inflacao-e-juros-altos-em-2022-encarecem-credito-habitacao-em-portugal

Idealista. (2023, January 24). *Salários Vs inflação – impacto do aumento no poder de compra por país — idealista/news*. Www.idealista.pt. https://www.idealista.pt/news/financas/economia/2023/01/24/56452-salarios-vs-inflacao-impacto-do-aumento-no-poder-de-compra-por-pais

IGNOU. (2017). New Product Development - Economic Analysis. In *eGyanKosh*. IGNOU. https://egyankosh.ac.in/bitstream/123456789/10230/1/Unit-14.pdf

INE. (2023, April 12). *Remuneração Bruta Mensal Média Por Trabalhador*. Www.ine.pt. https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=606765498&DESTAQUESmodo=2

INE, & PORDATA. (2023, February 22). *PORDATA - Taxa de desemprego: total e por sexo (%)*. Www.pordata.pt. https://www.pordata.pt/Portugal/Taxa+de+desemprego+total+e+por+sexo+(percentagem)-550

Infobip Limited. (2023). *Your business. Just more of it.* Partners.infobip.com. https://partners.infobip.com/centili

IT Insight. (2022, November 16). *IT Insight - As tendências que vão moldar o trabalho em 2023*. IT Insight. https://www.itinsight.pt/news/mobilidade/as-tendencias-que-vao-moldar-o-trabalho-em-2023

Johansen, A. (2022, April 28). *What is cyber security?* Us.norton.com. https://us.norton.com/blog/malware/what-is-cybersecurity-what-you-need-to-know#

Johnson, G., Scholes, K., Angwin, D., Regnér, P., & Whittington, R. (2017). *Exploring Strategy: Text and Cases* (11th ed., pp. 34–48; 81-84). Pearson. (Original work published 1984)

Karadal, H., & Abubakar, A. M. (2021). Internet of things skills and needs satisfaction: do generational cohorts' variations matter? *Online Information Review*, *45*(5). https://doi.org/10.1108/oir-04-2020-0144

Keller, K. (2000). Building and Managing Corporate Brand Equity. In M. Schultz, M. Hatch, & M. Larsen (Eds.), *The Expressive Organization* (pp. 115–137). Oxford University Press.

Kesten, G. (2022, September 1). *7 Excellent Ways to Get New Customers*. Business Trends and Insights; American Express. https://www.americanexpress.com/en-us/business/trends-and-insights/articles/7-excellent-ways-to-attract-new-customers/

Kodali, S. (2023, February 8). *What Consumers Like — And Detest — About Subscriptions*. Forrester. https://www.forrester.com/blogs/what-consumers-like-and-detest-about-subscriptions/

Kotler, P., & Armstrong, G. (2019). *Principles of marketing* (17th ed.). Pearson Higher Education. https://nit-edu.org/wp-content/uploads/2021/09/Principles-of-Marketing-Kotler-Armstrong.pdf

Kotler, P., & Keller, K. L. (2012). *Marketing management* (14th ed.). Upper Saddle River, Nj Prentice Hall. https://cdn.website-editor.net/25dd89c80efb48d88c2c233155dfc479/files/uploaded/Kotler_keller_-_marketing_management_14th_edition.pdf

Kraus, E. (2019, April 22). *Do Customers Want the Best Price – or the Best Deal?* The Marketing Desks. https://marketingdesks.com/best-deal-marketing-2

Kyriaki, G. (2019, April 11). *Rebranding an industrial product with marketing strategies* . International Hellenic University Repository. https://repository.ihu.edu.gr//xmlui/handle/11544/29326

Lesonsky, R. (2020, February 28). *10 Great Ways To Attract New Customers To Your Small Business*. Forbes. https://www.forbes.com/sites/allbusiness/2020/02/28/attract-new-customers-small-business-tips/?sh=2fb166934d1a

MacKinney, N. (2020, July 7). *New research shows consumers want cybersecurity from service providers*. Cisco Umbrella. https://umbrella.cisco.com/blog/new-research-shows-consumers-want-cybersecurity-from-service-providers

Mahabir, H. (2021, September 10). *Value Added Services* . AdaptIT. https://telecoms.adaptit.tech/blog/value-added-services/

Marketeer. (2023, January 25). *Deco Proteste distingue NOS como a operadora com melhor internet móvel – Marketeer*. Marketeer. https://marketeer.sapo.pt/deco-proteste-distingue-nos-como-a-operadora-com-melhor-internet-movel/

Marktest. (2021). *Estudo de Fidelização e Pacotização*. http://apritel.org/assets/media/media-s3/original/20210629_152414Uja.pdf

Marr, B. (2022, December 9). *The Top 4 Telecom Trends In 2023*. Forbes. https://www.forbes.com/sites/bernardmarr/2022/12/09/the-top-4-telecom-trends-in-2023/?sh=61b8b098514f

Matthews, R. (2021, July 2). *8 Essential Steps for Communicating Your Rebrand | Tamarindo*. Www.tamarindo.global. https://www.tamarindo.global/articles/8-essential-steps-for-communicating-your-rebrand

McCloskey, H. (n.d.). *How to Communicate Product Changes To Your Users*. Uservoice.com. Retrieved May 3, 2023, from https://uservoice.com/blog/communicate-product-changes

MediaMarkt. (n.d.). *Software de Segurança PC*. MediaMarkt. Retrieved April 12, 2023, from https://mediamarkt.pt/collections/software-de-seguranca-pc

MEO. (n.d.-a). *MEO Net Segura – Navega online em segurança com o teu telemóvel*. MEO. Retrieved February 12, 2023, from https://www.meo.pt/net-segura

MEO. (n.d.-b). *Navega em segurança na Internet com soluções Panda*. MEO. Retrieved February 12, 2023, from https://www.meo.pt/servicos/antivirus#eab7d860-949c-4e54-ad10-05a0e6a09c5d

Millennium BCP. (n.d.). *Seguro Cyber Risk - Millennium bcp*. Millennium BCP. Retrieved May 19, 2023, from https://ind.millenniumbcp.pt/pt/negocios/seguros/Pages/Seguro-Cyber-Risk-Empresas.aspx

Mordor Intelligence. (2023). *Portugal Cybersecurity Market Size & Share Analysis - Industry Research Report - Growth Trends*. Www.mordorintelligence.com. https://www.mordorintelligence.com/industry-reports/portugal-cybersecurity-market

Movistar. (n.d.-a). *Conexión Segura: Navega por Internet sin Riesgo - Movistar*. Www.movistar.es. Retrieved February 2, 2023, from https://www.movistar.es/particulares/conexion-segura

Movistar. (n.d.-b). *Movistar Cloud: Almacenamiento Ilimitado en la nube*. Www.movistar.es. Retrieved February 2, 2023, from https://www.movistar.es/particulares/tienda/servicios-digitales/cloud

Nagel, L. (2020). The influence of the COVID-19 pandemic on the digital transformation of work. *International Journal of Sociology and Social Policy*, *40*(9/10), 861–875. https://doi.org/10.1108/ijssp-07-2020-0323

Neves, C. (2022, September 4). *Portugueses são os mais preocupados com a destruição das florestas*. Www.dn.pt. https://www.dn.pt/sociedade/portugueses-sao-os-mais-preocupados-com-a-destruicao-das-florestas-15137669.html

Nielsen, L., Joseph, T., Leonardo, J., & Vanderspar, B. (2022, November 15). *Thinking like a "ServCo": How telcos can drive B2C growth | McKinsey*. Www.mckinsey.com. https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/thinking-like-a-servco-how-telcos-can-drive-b2c-growth

NOS. (n.d.-a). *Móvel: Prémios Rede Móvel*. Nos. Retrieved May 15, 2023, from https://www.nos.pt/movel/premios-rede-movel

NOS. (n.d.-b). *Navegação Segura na Internet e NOS Safe Net*. Nos. Retrieved June 12, 2023, from https://www.nos.pt/net/seguranca

NOS. (2017). *Segmentação Mercado Consumidor - Famílias*. Internal Data.

NOS. (2021). *Estudo de Opinião: Segurança Digital*. Internal Data.

NOS. (2022). *Product naming - NOS versus F-Secure*. Internal Data.

NOS. (2023a). *NOS - About us | NOS Institutional*. Nos. https://www.nos.pt/institucional/EN/nos/about-us/Pages/about-us.aspx

NOS. (2023b, March 8). *Results Presentation 4Q22*. Nos.pt. https://www.nos.pt/en/institutional/investors/results-and-presentations/results

NOVA SBE Education. (2022, September 15). *CEMS study at Nova SBE and BNP Paribas concludes that most workers prefer hybrid working model | Business Room*. En.blog.exed.novasbe.pt. https://en.blog.exed.novasbe.pt/articles/study-by-nova-sbe-and-bnp-paribas-concludes-that-most-workers-prefer-the-hybrid-work-model

NOWO. (n.d.). *Antivírus NetSecure | Solução Completa de Segurança* . Www.nowo.pt. Retrieved February 12, 2023, from https://www.nowo.pt/servicos/internet/antivirus-netsecure/

Nyambane, M., & Makori, E. (2013). The Relationship between Rebranding and Customer Loyalty: The Case of Kenya Power. *International Journal of Science and Research* , *4*(3). https://doi.org/10.13140/RG.2.1.2030.2325

O2. (n.d.). *Know your child's net | Hot Topics | Inspiration | O2*. Www.o2.Co.uk. Retrieved February 2, 2023, from https://www.o2.co.uk/inspiration/hot-topics/know-your-childs-net

OECD. (n.d.). *OECD and the Sustainable Development Goals: Delivering on universal goals and targets - OECD*. Www.oecd.org. Retrieved May 10, 2023, from https://www.oecd.org/dac/sustainable-development-goals.htm

Oliveira, T. (2014, November 10). *A Internet Wi-Fi dos autocarros do Porto*. Jornal Expresso. https://expresso.pt/iniciativaseprodutos/CidadesdoFuturo/a-internet-wi-fi-dos-autocarros-do-porto=f897442

Opuni, F., Baffoe, M., & Adusei, E. (2013). The Effectiveness of Rebranding as a comparative study of Ghanaian Business Using the Principles of Corporate Rebranding . *Journal of Marketing and Management*, *4*(2), 69–77. ResearchGate. https://www.researchgate.net/publication/334575886_The_Effectiveness_of_Rebranding_as_a_Comparative_Study_of_Ghanaian_Business_Using_the_Principles_of_Corporate_Rebranding

Orange. (n.d.). *Option Suite Sécurité, protégez vos données - Orange*. Boutique.orange.fr. Retrieved February 6, 2023, from https://boutique.orange.fr/options/suite-securite?thematic=internet

Partanen, J. P. (2021). *Rebranding to enter new markets: Designing a competitive brand strategy through service design process*. https://www.theseus.fi/bitstream/handle/10024/507430/Partanen_Jukka-Pekka.pdf?sequence=2

Perplies, V. (2018, November 14). *How to Successfully Communicate to Customers That You're Rebranding*. Medium. https://medium.com/aleph-vc/how-to-successfully-communicate-to-customers-that-youre-rebranding-43db305891e3

Perrin, A. (2022, March 14). *How Telcos Need To Adapt for the Consumer of the Future*. Telecoms.adaptit.tech. https://telecoms.adaptit.tech/blog/how-the-telecommunication-industry-needs-to-adapt-for-the-consumer-of-the-future/

Peterson, M., AlShebil, S., & Bishop, M. (2015). Cognitive and emotional processing of brand logo changes. *Journal of Product & Brand Management*, *24*(7), 745–757. https://doi.org/10.1108/jpbm-03-2015-0823

Portuguese Government. (2022, December 15). *Novo apoio extraordinário de 240 euros abrange um milhão de famílias*. Www.portugal.gov.pt. https://www.portugal.gov.pt/pt/gc23/comunicacao/noticia?i=novo-apoio-extraordinario-de-240-euros-abrange-um-milhao-de-familias

Portuguese Government. (2023, February 8). *Desemprego diminui para 6% e população empregada atinge máximo histórico em 2022*. Www.portugal.gov.pt. https://www.portugal.gov.pt/pt/gc23/comunicacao/noticia?i=desemprego-diminui-para-6-e-populacao-empregada-atinge-maximo-historico-em-2022

Procuradoria-Geral Distrital de Lisboa . (2022, August 16). *Protecção de Dados Pessoais e Privacidade nas Telecomunicações* . Www.pgdlisboa.pt. https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=707&tabela=leis&so_miolo=

Proximus. (n.d.-a). *Cloud storage space*. Www.proximus.be. Retrieved February 2, 2023, from https://www.proximus.be/en/id_cr_cloud/p ersonal/internet-subscriptions-for-all/choose-your-option/cloud.html

Proximus. (n.d.-b). *Norton Security – Protection antivirus*. Www.proximus.be. Retrieved February 2, 2023, from https://www.proximus.be/en/id_cr_intsecurity/personal/internet-subscriptions-for-all/choose-your-option/norton-security.html

Quang, H. (2022). The Effects of Rebranding on Customer's Perspective [Bachelor's thesis]. In *www.theseus.fi*. https://www.theseus.fi/handle/10024/783907

Quelch, J., & Kenny, D. (1994, September 1). *Extend Profits, Not Product Lines*. Harvard Business Review. https://hbr.org/1994/09/extend-profits-not-product-lines

Revella, A. (2015). *Buyer personas how to gain insight into your customer's expectations, align your marketing strategies, and win more business*. Hoboken, Nj Wiley C.

Rica, F., Verbree, M., Michaux, D., & Gupta, A. (2019). Global Perspectives on Cyber Security in Telco: A roundtable discussion on the state of cyber security management in the telco sector. In *KPMG*. https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2019/02/global-perspectives-on-cyber-security-in-telco.pdf

Righini, E. (2020, March 12). *Digital marketing in the telecommunication industry: the right strategy to start growing again*. Doxee. https://www.doxee.com/blog/digital-marketing/digital-marketing-in-the-telecommunication-industry/

Rodrigues, J. (2021, May 13). *Governo vai avançar com investimento em redes de telecomunicações onde os operadores privados não chegam | O Jornal Económico*. Jornaleconomico.pt. https://jornaleconomico.pt/noticias/governo-vai-avancar-com-investimento-em-redes-de-telecomunicacoes-onde-os-operadores-privados-nao-chegam-738558

Rodrigues, J. (2022, December 3). *Operadores obrigados a retirar antenas que ponham em risco as comunicações*. Dinheiro Vivo. https://www.dinheirovivo.pt/empresas/telecomunicacoes/operadores-obrigados-a-retirar-antenas-que-ponham-em-risco-as-comunicacoes-15419984.html

Roy, S., & Sarkar, S. (2015). To brand or to rebrand: Investigating the effects of rebranding on brand equity and consumer attitudes. *Journal of Brand Management*, *22*(4), 340–360. https://doi.org/10.1057/bm.2015.21

Rust, R., Thompson, D. V., & Hamilton, R. (2006, February 1). *Defeating Feature Fatigue*. Harvard Business Review. https://hbr.org/2006/02/defeating-feature-fatigue

Sacadura, P. (2021, July 29). *O teletrabalho veio para ficar?* Euronews. https://pt.euronews.com/my-europe/2021/07/29/o-teletrabalho-veio-para-ficar

Santander. (n.d.). *Seguro Proteção Empresas Cyber*. Santander. Retrieved May 19, 2023, from https://www.santander.pt/empresas/seguros/seguro-protecao-empresas-cyber

Saunders, J., & Jobber, D. (1988). An exploratory study of the management of product replacement. *Journal of Marketing Management*, *3*(3), 344–351. https://doi.org/10.1080/0267257x.1988.9964051

Saxena, R. (2012, December 30). *Mobile VAS firms turn to global markets for survival*. Mint. https://www.livemint.com/Industry/Ftm64F0VLsMXWTcnfDDnGI/Mobile-VAS-companies-turn-to-global-markets-for-survival.html

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *The Journal of Digital Forensics, Security and Law*, *12*. https://doi.org/10.15394/jdfsl.2017.1476

SecurityMagazine. (2021, May 17). *Centro Nacional de Cibersegurança lança relatório Riscos & Conflitos 2021*. Security Magazine. https://www.securitymagazine.pt/2021/05/17/centro-nacional-de-ciberseguranca-lanca-relatorio-riscos-conflitos-2021/

Sharpe, K. (2020, April 20). *Insights - The Design Thinking Process - How does it work?* MAQE. https://www.maqe.com/insight/the-design-thinking-process-how-does-it-work/

Singh, A., Tripathi, V., & Yadav, P. (2013). Rebranding and Organisational Performance- Some Issues of Relevance. *American Journal of Sociological Research*, *2*(5), 90–97. https://doi.org/10.5923/j.sociology.20120205.01

SKY. (n.d.). *Safety and security on your Sky products* . Www.sky.com. Retrieved February 7, 2023, from https://www.sky.com/help/articles/safety-and-security-on-your-sky-products

Slijkerman, J. F., & Nijboer, F. (2022, January 28). *Telecom Outlook: Rising cyber threats a cause for concern, as well as a source of success*. ING Think. https://think.ing.com/articles/rising-cyber-threats-cause-for-concern-and-source-of-success

Smurygina, O., Hung Chong, C., Tjhin, D., Stemberger, S., Luisada, F., & Elbert, V. (2022, November 23). *What Five Trends Mean for Telcos*. BCG Global. https://www.bcg.com/publications/2022/telco-trends

Sujata, J., Sohag, S., Tanu, D., Chintan, D., Shubham, P., & Sumit, G. (2015). Impact of Over the Top (OTT) Services on Telecom Service Providers. *Indian Journal of Science and Technology*, *8*(S4), 145. https://doi.org/10.17485/ijst/2015/v8is4/62238

Sunrise. (n.d.-a). *Kaspersky Safe kids option (mobile)*. Retrieved February 2, 2023, from https://www.sunrise.ch/medias/sys_master/Factsheets/Factsheets/hfe/hc7/8831389532190/Factsheet-Kaspersky-safe-kids-option-EN.pdf

Sunrise. (n.d.-b). *Sunrise Game Cloud Option*. Www.sunrise.ch. Retrieved February 2, 2023, from https://www.sunrise.ch/content/dam/sunrise/residential/hilfe/sonstigehilfe/factsheets-all-languages/options-for-abos/M51_Factsheet_Sunrise%20Game%20Cloud_EN_22.pdf

Sunrise. (n.d.-c). *Surf protect options (mobile & home) Option for mobile and Internet subscriptions*. Retrieved February 2, 2023, from https://www.sunrise.ch/medias/sys_master/Factsheets/Factsheets/heb/hea/9252656578590/M42-Factsheet-surf-protect-EN.pdf

Taylor, R. (2021, July 15). *10 Ways to Win Your Competitors' Customers*. Fleximize. https://fleximize.com/articles/001027/10-steps-to-attracting-customers-away-from-your-competitors

Technavio. (2023, January). *Artificial Intelligence-based Cybersecurity Market by End-user, Deployment, and Geography - Forecast and Analysis 2023-2027*. Technavio. https://www.technavio.com/report/artificial-intelligence-based-cybersecurity-market-industry-analysis?nowebphttps://www.technavio.com/report/artificial-intelligence-based-cybersecurity-market-industry-analysis?nowebp

TechnoFunc. (2012, June 23). *History of Telecommunications Industry*. Www.technofunc.com. https://www.technofunc.com/index.php/domain-knowledge/telecom-industry/item/history-of-telecommunications-industry

Telenor. (n.d.-a). *SAFE – Safety online, and help if you need it*. Www.telenor.no. Retrieved February 7, 2023, from https://www.telenor.no/sikkerhet/din-trygghet/safe/

Telenor. (n.d.-b). *This is how Telenor's Network protects you*. Www.telenor.no. Retrieved February 7, 2023, from https://www.telenor.no/privat/artikler/sikkerhet/slik-beskytter-telenors-nettvern-deg.jsp

TELUS. (n.d.). *TELUS Online Security Plans*. TELUS. Retrieved February 2, 2023, from https://www.telus.com/en/online-security/plans?intcmp=tcom_tos_chevron_ffh_overview_toplans

TIM. (n.d.-a). *Cloud games: scopri il catalogo online TIMGAMES*. Www.tim.it. Retrieved February 3, 2023, from https://www.tim.it/offerte-tv/timgames

TIM. (n.d.-b). *Servizi digitali per clienti di rete fissa e mobile*. Www.tim.it. Retrieved February 3, 2023, from https://www.tim.it/fisso-e-mobile/mobile/servizi#casa-e-famiglia

TIM. (n.d.-c). *TIM Junior Pack: Sim e offerte mobile per bambini*. Www.tim.it. Retrieved February 3, 2023, from https://www.tim.it/fisso-e-mobile/mobile/tim-junior-mese

TIM. (2023a). *TIM Protect*. Timsegurancadigital.com.br. https://www.timsegurancadigital.com.br/produtos/protect-essencial

TIM. (2023b). *TIM Protect BACKUP*. Timsegurancadigital.com.br. https://www.timsegurancadigital.com.br/produtos/protect-backup

Todor, R. D. (2014). The Importance of Branding and Rebranding for strategic Marketing. *Bulletin of the Transilvania University of Braşov* , *Vol. 7 (56)*(No. 2). http://rs.unitbv.ro/BU2014/Series%20V/BULETIN%20V/I-08_TODOR%20Raluca.pdf

Tybus, M., Hoppe, L., & Burgstaller, T. (2023, January 25). *Why haven't telcos cracked the code on shifting to digital channels?* Kearney. https://www.kearney.com/telecommunications/article/-/insights/why-havent-telcos-cracked-the-code-on-shifting-to-digital-channels

Tymchuk, S. (2022, November 5). *The Outsourcing Revenue Share Model Can Enhance Profitability*. Computools. https://computools.com/outsourcing-revenue-share-model/

United Nations. (2022). *Goal 9 | Department of Economic and Social Affairs*. Sdgs.un.org; United Nations. https://sdgs.un.org/goals/goal9

Val, E., Gonzalez, I., Iriarte, I., Beitia, A., Lasa, G., & Elkoro, M. (2017). A Design Thinking approach to introduce entrepreneurship education in European school curricula. *The Design Journal*, *20*(sup1), S754–S766. https://doi.org/10.1080/14606925.2017.1353022

Virgin Media. (n.d.). *Online Safety*. My.virginmedia.com. Retrieved February 2, 2023, from https://my.virginmedia.com/customer-news/articles/online-safety.html

VIVO. (n.d.). *Proteja-se das Ameaças Digitais*. Www.vivo.com.br. Retrieved February 2, 2023, from https://www.vivo.com.br/para-voce/produtos-e-servicos/servicos-digitais/apps-no-plano-de-celular/aplicativo-mc-afee?q=proteo%20digital

Vodafone. (n.d.). *Vodafone Secure Net*. Vodafone Portugal. Retrieved February 12, 2023, from https://www.vodafone.pt/telemoveis/apps-servicos/secure-net.html

Vodafone UK. (2022). *Vodafone Secure Net*. Vodafone.co.uk. https://securenet.vodafone.co.uk/Landing

Vonage. (n.d.). *A History of Telecommunications: How Telecoms Became Just Another Interface*. Www.vonage.com. Retrieved February 12, 2023, from https://www.vonage.com/resources/articles/a-history-of-telecommunications-how-telecoms-became-just-another-interface/

Wagner, E. (2019, March 8). *Price or Value: Which One Will Compel Customers to Buy from You?* Www.i7marketing.com. https://www.i7marketing.com/blog/small-business/price-value-one-will-compel-customers-buy

Wooden, A. (2022, August 2). *Remote working shift sees "major rise in cybercrime."* Telecoms.com. https://telecoms.com/516837/remote-working-shift-sees-major-rise-in-cybercrime/

Worten. (n.d.). *Worten Online | Soluções Antivirus*. Worten.pt. Retrieved April 12, 2023, from https://www.worten.pt/search?query=antivirus

Y!mobile. (n.d.). *Security Pack Plus*. Y!Mobile. Retrieved February 8, 2023, from https://www.ymobile.jp/service/security_pack/

Yosifovich, D., Moshe, D., Newman, A., Dudu, Y., Wolkstein, E., & Djanogly, A. (2023, January). *Consumer Cybersecurity Market Trends Report 2023 | ReasonLabs*. Reasonlabs.com. https://reasonlabs.com/research/consumer-cybersecurity-trends-report-2023

12 Annexes

12.1 Glossary

DNS Protection stands for "Domain Name System," which offers a first level of defense against cybercrime through Fixed & Mobile Telecommunications Networks, preventing and blocking access to specific domain names or IP addresses.

End-Point Protection consists of providing safety against online threats at the device level. It can offer a wide range of defense features through a software application that shields any compatible device, such as smartphones, tablets, and computers.

Real-Time Protection regards the inspection of online traffic to filter out malicious or unwanted content. It prevents and blocks access to specific domain names or IP addresses associated with adult content, fraudulent websites, entailing viruses, phishing, and other online threats.

Antivirus software protects computer systems and end-points from malware spread. It prevents data breaches, illegal access, system damage, and other undesirable effects of cyberattacks such as trojans, worms, spyware, and ransomware.

Parental Controls allow guardians to follow and manage minors' online activities while ensuring their online safety using the internet and technologies. It offers filters and settings to shield kids from harmful content, internet dangers, and potentially dangerous online interactions. It also provides time restrictions and activity reporting functions.

Password Manager securely stores numerous passwords, and synchronizing them across various devices enables logging in with just one click. Also, it supports the creation of secure passwords for multiple accounts, ensuring maximum protection.

VPN safeguards online privacy by encrypting browsing activity, masking IP addresses, and preventing websites and advertisers from tracking online actions. Also, it protects security and privacy when utilizing less secure public Wi-Fi networks and enables access to geographically restricted content.

Identity Protection continuously scans the internet for users' personal information, searching for data breaches so that they get a thorough activity history and are instantly alerted to any efforts at illegal usage of their private information. Further, users are supported to recover and protect their identity.

Cloud enables users to store and remotely access their data and files over the internet, which can be accessed and maintained from any internet-connected device. Data encryption and user authentication guarantee privacy and enable users to sync files across devices, access older versions, and share files or folders with others.

Cyber Insurance safeguards people from risks associated with the internet and offers financial assistance in the event of an online incident. It can cover costs related to identity theft, including attorney fees, credit monitoring services, and help with identity restoration. Also, it can support financial loss or extortion, and data breaches, among others.

The Churn rate represents the number of customers that canceled or unsubscribed a service within a given period and is divided by the total number of customers at the start of that period plus the new subscribers. The outcome displays the percentage of clients lost during that time.

12.2 International Players' Cybersecurity Offers

Figure 12-1: International Players' Cybersecurity Offers

Source: Author's elaboration based on O2 (n.d.), Bispo (2023), VIVO (n.d.), Movistar (n.d.-a), Movistar (n.d.-b), Virgin Media (n.d.), Vodafone UK (2022), Proximus (n.d.-a), Proximus (n.d.-b), Sunrise (n.d.-a), Sunrise (n.d.-b), Sunrise (n.d.-c), TELUS (n.d.), Y!mobile (n.d.); TIM (2023a), TIM (2023b), TIM (n.d.-a), TIM (n.d.-b), TIM (n.d.-c), Orange (n.d.); DNA (2023), Telenor (n.d.-a), Telenor (n.d.-b), and SKY (n.d.)

Operator	Services	End-Point	Price p/Month	Nº Licenses	Nº Features	Price p/License	Price p/Feature	Partner
O2 (UK)								
Vivo (Brazil)	HERO Protect	■	€ 2,2	3	7	€0,7	€0,3	Hero
	HERO Protect	■	€ 2,9	5	7	€0,6	€0,4	Hero
	HERO Family	■	€ 5,4	10	7	€0,5	€0,8	Hero
	McAfee Digital Safety	■	€ 1,0	1	9	€1,0	€0,1	McAfee
	McAfee Digital Safety Parental Control	■	€ 3,6	5	10	€0,7	€0,4	McAfee
	McAfee Safe Connect	■	€ 1,6	1	7	€1,6	€0,2	McAfee
	McAfee Safe Connect	■	€ 2,7	5	7	€0,5	€0,4	McAfee
Movistar (Spain)	Secure Connection		€ -	n	6	€-	€-	McAfee
Virgin Media (UK)	Web Safe		€ -	n	5	€-	€-	n.a.
	VM Internet Security	■	€ 3,4	n	8	€-	€0,4	F-Secure
VDF (UK)	Secure Net		€ 1,2	1	8	€1,2	€0,1	Allot
Proximus (Belgium)	Safety First - Norton Security	■	€ 2,0	1	8	€2,0	€0,3	Norton
	Safety First - Norton Security	■	€ 5,0	5	8	€1,0	€0,6	Norton
Sunrise (Switzerland)	Surf Protect		€ 2,9	1	5	€2,9	€0,6	Aryaka
	Surf Protect Home		€ 5,0	n	5	€-	€1,0	Aryaka
TELUS (Canada)	Online Security Standard	■	€10,0	3	10	€3,3	€1,0	Norton
	Online Security Complete	■	€15,0	10	10	€1,5	€1,5	Norton
	Online Security Ultimate	■	€20,0	20	10	€1,0	€2,0	Norton
Y!mobile (Japan)	Security Pack Plus	■	€ 4,5	1	7	€4,5	€0,6	McAfee
TIM (Brazil)	Protect Essential	■	€ 1,0	3	5	€0,3	€0,2	FS Security
	Protect Family	■	€ 1,8	5	6	€0,4	€0,3	FS Security
TIM (Italy)	TIM Safe Navigation		€ 2,0	1	6	€2,0	€0,3	Cisco
	TIM Basic Safe Navigation (Family)		€ 1,9	n	5	€-	€0,4	Cisco
	TIM Safe Navigation (Family)		€ 5,0	n	6	€-	€0,8	Cisco
	TIM Safe Navigation APP	■	€ 1,0	1	8	€1,0	€0,1	F-Secure
	TIM Safe Navigation 360	■	€ 4,0	5	10	€0,8	€0,4	F-Secure
ORANGE (France)	Security Suite	■	€ 5,0	5	9	€1,0	€0,6	Kaspersky
DNA (Finland)	DNA Digital Security	■	€ 6,9	2	11	€3,5	€0,6	F-Secure
	DNA Digital Security	■	€10,0	10	11	€1,0	€0,9	F-Secure
	DNA Digital Security	■	€15,0	25	11	€0,6	€1,4	F-Secure
Telenor (Norway)	SAFE	■	€12,0	5	11	€2,4	€1,1	EyeOnID
	Network Security		€ -	n	5	€-	€-	EyeOnID
SKY (UK)	SKY Broadband Shield		€ -	n	5	€-	€-	McAfee
	SKY Mobile		€ -	n	6	€-	€-	McAfee

Note: "n" stands for unlimited devices, associated with Fixed DNS solutions; "n.a." stands for non-available;

Figure 12-2: International Players' Cybersecurity Offers - Subscription Plans

Source: Author's elaboration based on O2 (n.d.), Bispo (2023), VIVO (n.d.), Movistar (n.d.-a), Movistar (n.d.-b), Virgin Media (n.d.), Vodafone UK (2022), Proximus (n.d.-a), Proximus (n.d.-b), Sunrise (n.d.-a), Sunrise (n.d.-b), Sunrise (n.d.-c), TELUS (n.d.), Y!mobile (n.d.); TIM (2023a), TIM (2023b), TIM (n.d.-a), TIM (n.d.-b), TIM (n.d.-c), Orange (n.d.); DNA (2023), Telenor (n.d.-a), Telenor (n.d.-b), and SKY (n.d.)

12.3 National Players' Cybersecurity Offers

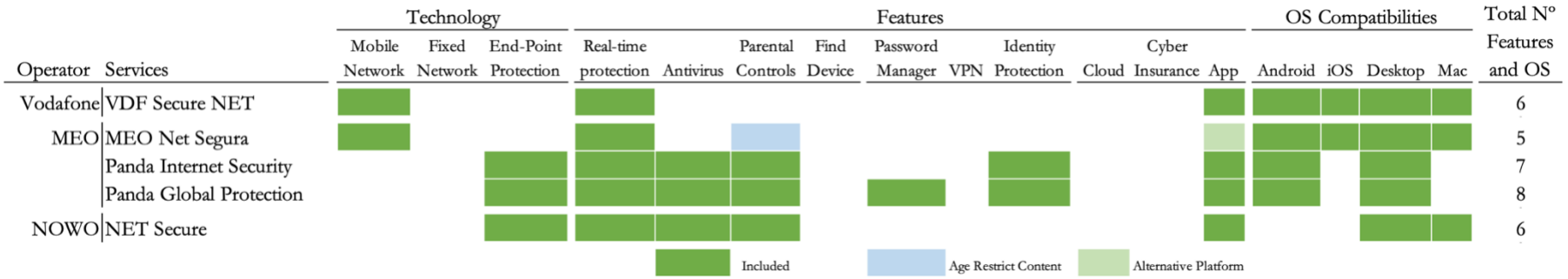


Figure 12-3: National Players' Cybersecurity Offers

Source: Author's elaboration based on Vodafone (n.d.), MEO (n.d.-a), MEO (n.d.-b), and NOWO (n.d.)

Operator	Services	End-Point	Price p/Month	Nº Licenses	Nº Features	Price p/License	Price p/Feature	Partner
Vodafone	VDF Secure NET		€ 1,1	1	6	€ 1,1	€ 0,2	Allot
MEO	MEO Net Segura		€ 1,0	1	5	€ 1,0	€ 0,2	Allot
	Panda Internet Security *	■	€ 2,3	2	7	€ 1,1	€ 0,3	Panda
	Panda Global Protection *	■	€ 3,3	2	8	€ 1,6	€ 0,4	Panda
NOWO	NET Secure	■	€ 2,0	3	6	€ 0,7	€ 0,3	F-Secure

* Additional Licenses +€0,79/month

Figure 12-4: National Players' Cybersecurity Offers - Subscription Plans

Source: Author's elaboration based on Vodafone (n.d.), MEO (n.d.-a), MEO (n.d.-b), and NOWO (n.d.)

12.4 Competitor Telcos' Positioning

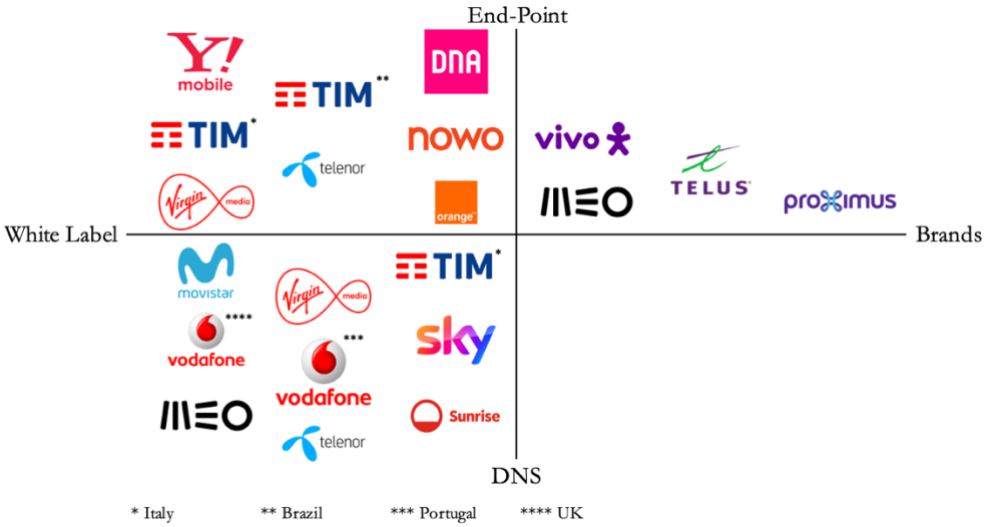


Figure 12-5: Service Branding Strategic Groups Map *Source: Author's Elaboration*

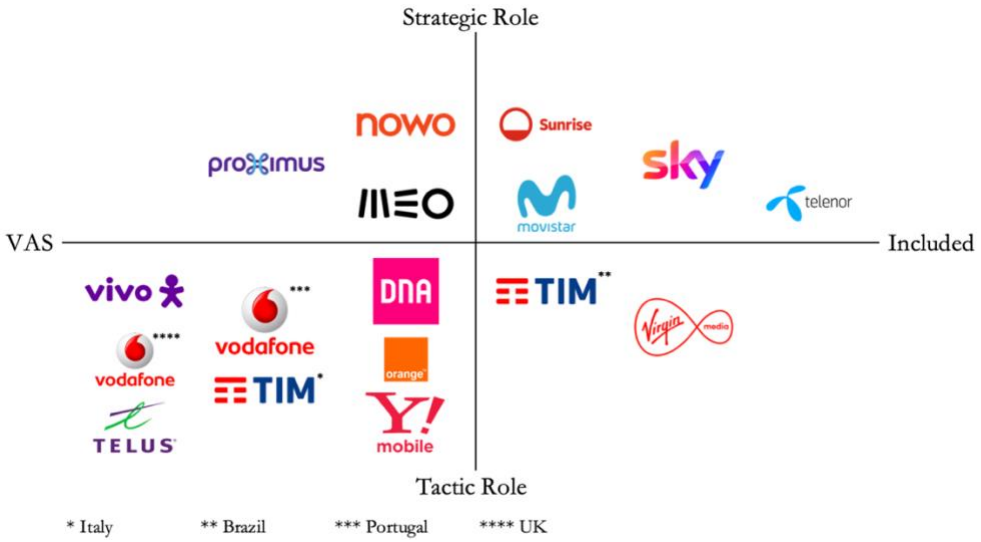
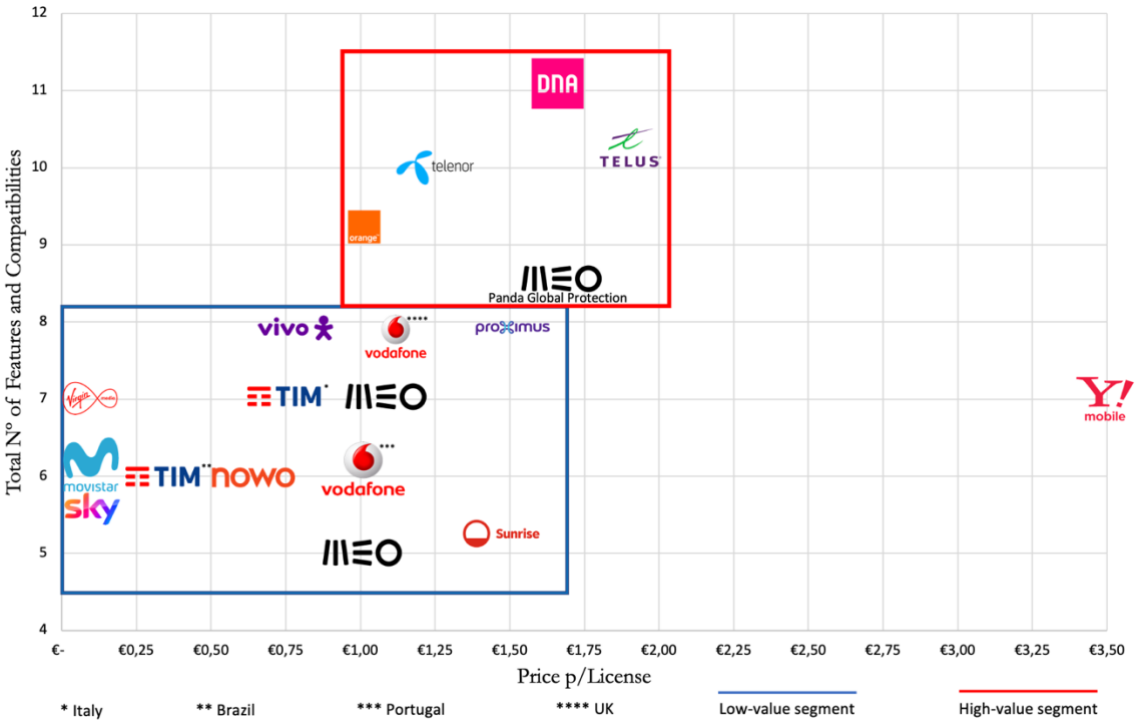


Figure 12-6: Safety Positioning Strategic Groups Map *Source: Author's Elaboration*



Note: Y!mobile Price per License is €4,5;

Figure 12-7: Competitors' Positioning towards Customers *Source: Author's Elaboration*

12.5 NOS Group

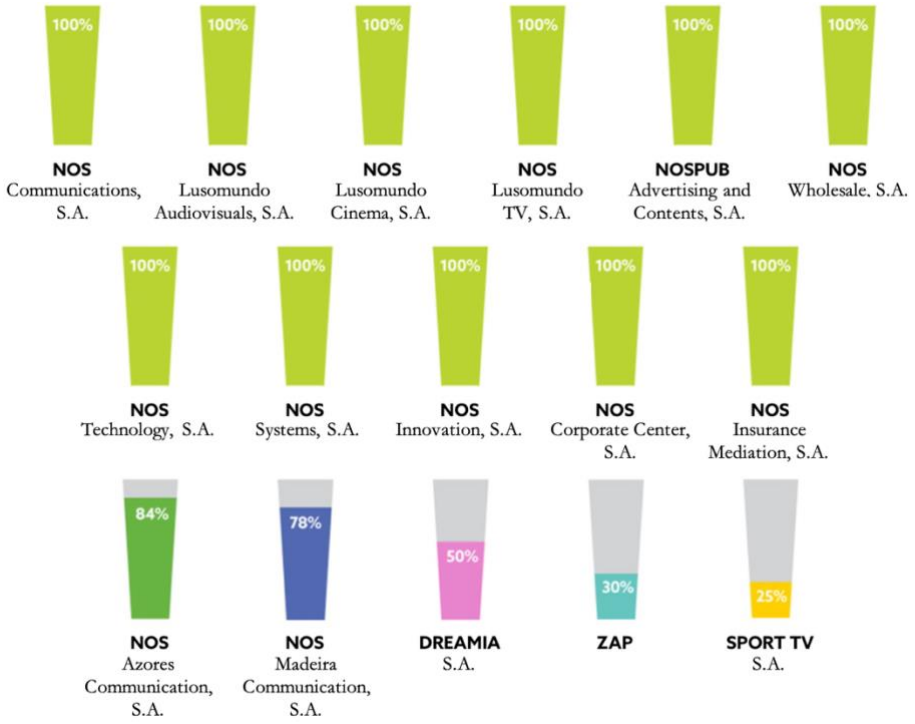


Figure 12-8: NOS Group Companies *Source: NOS (2023a)*

12.6 NOS' Cybersecurity Offers

		Technology			Features								OS Compatibilities				Total N° Features and OS
Operator	Services	Mobile Network	Fixed Network	End-point Protection	Real-time protection	Antivirus	Parental Controls	Find Device	Password Manager	VPN	Identity Protection	Cyber Cloud	Insurance	App	Android	iOS	Desktop	Mac	
NOS	Safe Browsing Mobile	■			■										■	■	■	■	5
	Safe Browsing Fixed		■		■										■	■	■	■	5
	NOS SAFE NET			■	■	■	■							■	■	■	■	■	8
	NOS Antivirus Total			■	■	■	■		■	■	■			■	■	■	■	■	11
						■	Included												

Figure 12-9: NOS' Cybersecurity Offers

Source: Author's Elaboration based on NOS (n.d.-b) and NOS' internal data

Operator	Services	End-Point	Price p/Month	N° Licenses	N° Features	Price p/License	Price p/Feature	Partner
NOS	Safe Browsing Mobile		€ 1,5	1	5	€ 1,5	€ 0,3	Cisco
	Safe Browsing Fixed		€ 3,0	n	5	€ -	€ 0,6	Cisco
	NOS Safe Net	■	€ 1,5	2	8	€ 0,8	€ 0,2	F-Secure
	NOS Safe Net	■	€ 2,5	5	8	€ 0,5	€ 0,3	F-Secure
	NOS Safe Net	■	€ 4,0	10	8	€ 0,4	€ 0,5	F-Secure
	NOS Antivirus Total	■	€ 6,0	5	11	€ 1,2	€ 0,5	F-Secure

Note: "n" stands for unlimited devices, associated with Fixed DNS solutions;

Figure 12-10: NOS' Cybersecurity Offers - Subscription Plans

Source: Author's Elaboration based on NOS (n.d.-b) and NOS' internal data

12.7 NOS' Cybersecurity Portfolio Customer Base

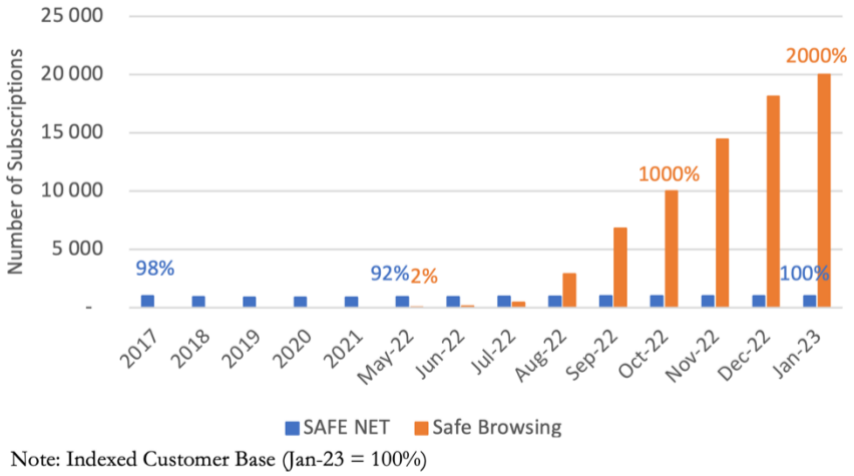


Figure 12-11: NOS' Cybersecurity Portfolio Indexed Customer Base
Source: Author's Elaboration based on NOS' internal data

12.8 NOS' Cybersecurity Market Study

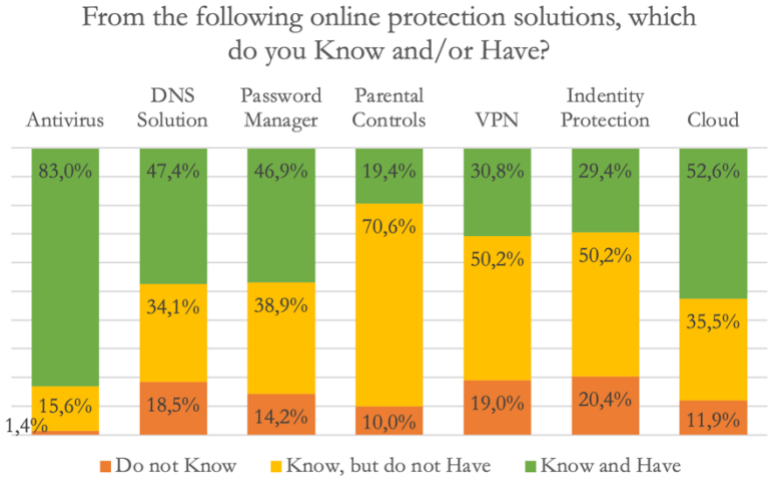


Figure 12-12: NOS' Cybersecurity Market Study - Online Protection Solutions
Source: Author's elaboration based on NOS (2021)

12.9 NOS Antivirus Total – Customer Experience

Awareness	Information	Subscription	Usage	Payment	Cancelation
Clients identify the need to protect themselves from online dangers and find that NOS offers a Cybersecurity service in partnership with F-Secure;	Clients get informed on the product characteristics and commercial conditions on NOS' website;	Clients decide to subscribe to the monthly or annual plan and select their preferred payment method on the service landing page through Centili's platform;	Clients are provided with the licenses and can install the service on their devices; Once the service is installed, clients can start to benefit from the functionalities;	After the trial period, the client starts to pay the subscribed plan thought the selected payment method;	Clients can cancel their subscription plan through the service's App or the online portal;

Figure 12-13: NOS Antivirus Total – Customer Experience *Source: Author's Elaboration*

12.10 STP – Targeting

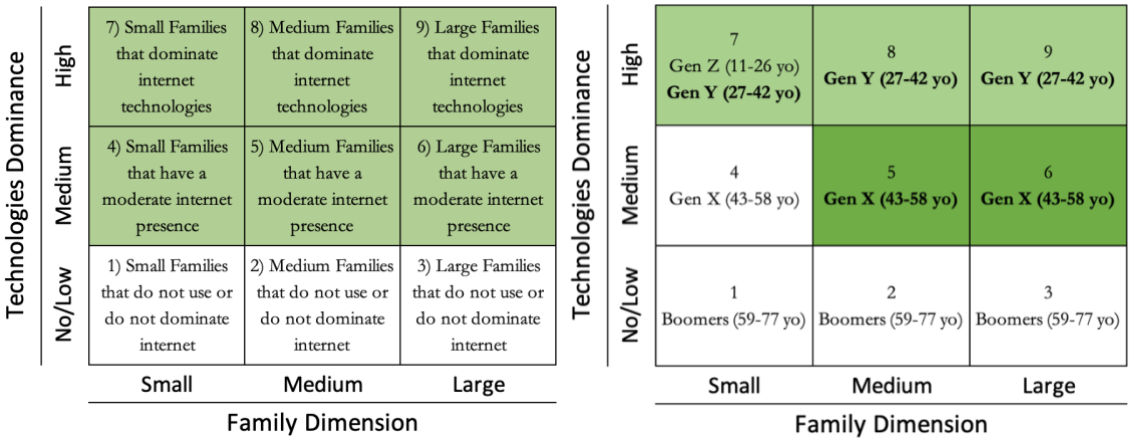


Figure 12-14: STP Analysis, Target Selection *Source: Author's Elaboration*

12.11 NOS Cybersecurity Portfolio Image

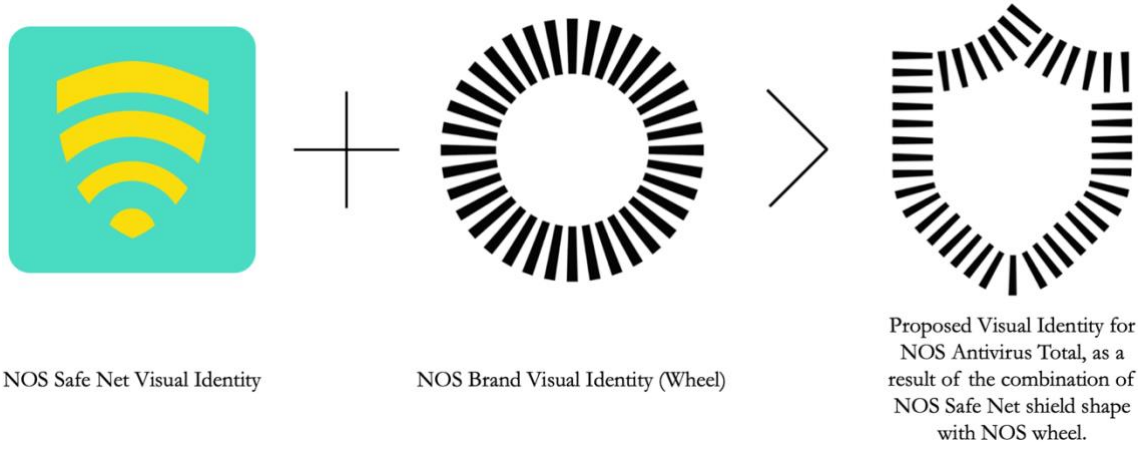


Figure 12-15: NOS Cybersecurity Portfolio Visual Identity Shift
Source: Author's Elaboration based on NOS' internal data

12.12 End-Point Services Price Benchmark

Operator	Services	Price p/month	Nº Licenses	Nº Features	Price p/License	Price p/Feature
National						
MEO	Panda Internet Security *	€2,29	2	7	€1,1	€0,3
	Panda Global Protection *	€3,29	2	8	€1,6	€0,4
NOWO	NET Secure	€1,99	3	6	€0,7	€0,3
NOS	NOS Antivirus Total	€5,99	5	11	€1,2	€0,5
International						
	End-Point (Average)	€5,91	5	9	€1,2	€0,7

* Additional Licenses +€0,79/month

Figure 12-16: End-Point Services Price Benchmark *Source: Author's Elaboration*

12.13 NOS Antivirus Total – Target Market Dimension

Market Dimension	Market Segments				
	Independents	Classical Parents	Technological Parents	Other Segments	Total
Number of Households	300 000	460 000	810 000	2 530 000	4 100 000
Market Segment weight on Total	7%	11%	20%	62%	100%
Target Market	300 000	460 000	810 000		**1 570 000**
Market Segment weight on Total	7%	11%	20%		**38%**

Figure 12-17: NOS Antivirus Total – Market Dimension
Source: Author's Elaboration based on NOS (2017)

12.14 NOS Antivirus Total – Main Target Market Dimension

NOS Clients		Market Segments			
		Independents	Classical Parents	Technological Parents	Total
Target Market		300 000	460 000	810 000	**4 100 000**
NOS Market Share		33%	30%	29%	
		100 000	140 000	230 000	**470 000**
Cyberthreat Awareness					
Highly Worried	13%	12 800	17 900	29 400	**60 100**
Already has an Antivirus					
	83%	10 600	14 800	24 400	**49 800**
Willness to Pay		13%	25%	33%	
		1 400	3 700	7 900	**13 000**

Figure 12-18: NOS Antivirus Total – Main Target Market Dimension
Source: Author's Elaboration based on NOS (2017) and NOS (2021)

12.15 NOS Antivirus Total – Non-Clients Target Market Dimension

Non-Clients		Market Segments			
		Independents	Classical Parents	Technological Parents	Total
Target Market		300 000	460 000	810 000	**4 100 000**
Remaining Market Share		67%	70%	71%	
		200 000	320 000	580 000	**1 100 000**
Cyberthreat Awareness					
Highly Worried	13%	25 600	41 000	74 200	**140 800**
Already has an Antivirus					
	83%	21 200	34 000	61 500	**116 700**
Willness to Pay		13%	25%	33%	
		2 800	8 400	20 000	**31 200**
Willness to Subscribe					
	40%	1 100	3 400	8 000	**12 500**

Figure 12-19: NOS Antivirus Total – Non-Clients Target Market Dimension
Source: Author's Elaboration based on NOS (2017) and NOS (2021)

12.16 NOS Antivirus Total – NOS Convergent Clients Market Dimension

Convergent Clients	
N° Familes	4 100 000
NOS Market Share	30%
Convergent Plans	80%
NOS Convergent Customer Base	**980 000**
Conversion Rate	1%
Expected Convergent Base	**9 800**

Figure 12-20: NOS Antivirus Total – Convergent Customer Market Dimension

Source: Author's Elaboration based on NOS Communicações (2017)

12.17 NOS Antivirus Total – Customer Base and Revenue Projection

	Year 0	Year 1	Year 2	Year 3
NOS Safe Net Clients	1 000			
New Customers		6 500	6 500	
Convergent Clients		4 900	4 900	
Non-Clients		6 250	6 250	
Churn		- 1 040	- 2 940	
Market Growth Rate				7%
Total Customer Base	**1 000**	**17 610**	**32 320**	**34 600**
Subscriptions	**€ 36 000**	**€ 565 000**	**€ 1 429 000**	**€ 1 922 000**
NOS Safe Net Clients Discount		-€ 30 000		
Free Trials		-€ 172 000	-€ 180 000	
Revenue	**€ 36 000**	**€ 363 000**	**€ 1 249 000**	**€ 1 922 000**

Figure 12-21: NOS Antivirus Total – Customer Base and Revenue Projection

Source: Author's Elaboration based on NOS (2017) and NOS (2021)