LUISS

Department of Management

Course of **International Operations and Supply Chain**

Operational risk management in an e-Commerce platform: A Case Study.

Prof. Maleki Vishkaei Behzad
SUPERVISOR

Prof. De Giovanni Pietro
CO-SUPERVISOR

Natalia Tabares Urrea ID 741341
CANDIDATE

Academic Year **2021/2022**

Table of Contents

Table of elements (Tables)

Table of figures

Operational risk management in an e-Commerce platform: A Case Study

Abstract

E-commerce refers to the execution of commercial transactions via the internet and has become an integral aspect of the global retail landscape in recent years. To maximize market opportunities, businesses across a range of industries have switched to e-commerce. However, the growth of e-commerce is accompanied by an increase in risk exposure, meaning that risk management is necessary and needs to be part of the e-commerce culture. Many of the firms who have chosen a digital store, have done it through the use of electronic platforms since they offer features that enable merchants to construct a branded online storefront to sell their products and services (Nguyen, 2022). However, there is not much research related to the risk management for e-commerce platforms, the literature addresses risk from the point of view of the buyers and sellers but not about the internal operations, furthermore considering more than 2.5 million users according to Fundera (2021) and Galov (2022), it is relevant to address them. In this work, a risk management proposal is presented for a recognized electronic commerce platform. The proposal includes the identification, prioritization through the application of FQFD, and lastly, a definition of action plans to mitigate or reduce the main identified risks.

Keywords: *e-commerce, risk management, e-commerce platform, risk identification, risk prioritization, risk management and monitoring*

1. Introduction

The emergence of the internet and its rapid development of computing services in the 1990s transformed how companies did business. One clear example of this is the emergence of electronic commerce (e-commerce). According to Quyet & Cuong, (2017) e-commerce is defined as the purchase and sale of goods, services, and exchange of information based on communications networks and the Internet.

E-commerce is expanding rapidly worldwide and has been recognized as a major engine that drives the evolution of logistics (S. X. Xu & Huang, 2016). However, it is not only logistics, but this phenomenon also has a big impact on the management of the supply chain of any organization and it is relevant to analyze its trends and behaviors to provide continuous improvement. E-commerce has become an integral aspect of the global retail landscape in recent years. The retail sector, like many other businesses, has changed dramatically since the introduction of the internet. Given the ongoing digitalization of modern life, consumers from practically every country now benefit from the convenience of online purchases.

According to the portal Statista (2021), in 2020, over two billion people purchased goods or services online, and during the same year, e-retail sales surpassed 4.2 trillion U.S. dollars worldwide. In the year of the pandemic, global retail e-commerce sales grew more than 25%. It is clear then that, organizations can no longer ignore the importance of digital transformation since this is one of the most effective enablers for creating a different and unique competitive advantage.

Different companies, from the smallest to the largest ones, have already implemented a digital store that uses e-commerce platform providers to execute their digital sales strategy creating a Business to Business (B2B) relationship. An e-commerce platform is a software that allows businesses to create, host, and manage online stores. The platform offers features that enable merchants to construct a branded online storefront to sell their products and services (Nguyen, 2022). This means that an e-commerce platform provider integrates the multiple flows of the supply chain of a business, the execution of order involves the product, the trading, the payment, and the logistics (Kayikci, 2018). Therefore, the operation process of e-commerce sales is composed of many steps that are led by different stakeholders, these are clustered in different phases but are still interconnected at the same time, in that order of ideas, it is highly relevant to guarantee the functioning of the platform, so the purchase process runs smoothly.

However, the electronic commerce environment is daily exposed to a high number of threats and risks. Understanding the nature of the exposure and finding effective treatment techniques are currently major challenges to managers in the company (McNichol et al., 2001).

Multiple articles reviewed study electronic commerce risk, probably the most popular is cyberattacking. Although information security is one of the most obvious and relevant aspects of electronic commerce, it is not the only one. For instance, inside an electronic commerce platform, there is an existing process to complete one purchase order that highly depends on technology, humans, partners, infrastructure, etc. and it needs to be taken into consideration. Therefore, a review of the operational risk needs to be carried out inside a platform. Operational risks which are associated with failures linked to people, internal processes, technology, or the effects of external processes (Tang, 2006) needs to be carried out inside a platform.

According to Fundera (2021) and Galov (2022), Shopify and Magento are some of the biggest e-commerce platforms in the world with 2.5 million merchants combined on their platforms. For instance, if any of their internal processes fail or are exposed then several consequences could occur for the merchants, the final customers, and the platform.

The above points led us to conclude that there is a need to identify appropriate strategies for operational risks in e-commerce platforms, to understand the causes of risks, and to be able to anticipate and try to solve them. Risk management must be part of the organizational culture and operational processes, regardless of the type of company that is being discussed.

1.1 Research questions

The literature generally mentions the different aspects of risk in electronic commerce, but most of them are from the lenses of the customer or the owners of the stores, (Vijayaraghavan, 2003), (Pappas, 2016), (Viehland, 2001), (Nyshadham & Ugbaja 2006). Moreover, some articles talk about the importance of risk management in electronic commerce, but the landscape of electronic commerce platform providers is barely mentioned (Liu et al., 2020), (Shurrab, 2014), (Soleimani, 2021), (Kumar & Jose, 2017).

Few studies have been done on electronic commerce platforms. The innovation of this study lies in the idea of studying internally and operationally the risk from the service hub´s point of view, in this case, the electronic commerce platforms that currently have more than 2.5 million users, and millions of end customers with transactions. Therefore, it is considered pertinent to further study the risks associated with the operation of this business model.

In addition to this, this project applies the FQFD proposed by Osorio (2011). A tool that considers the customer's desires and evaluates them against the strategic objectives of the business. In other words, the components that were studied independently can now be studied under the same scheme with this proposal. Also, by using a fuzzy component, the ambiguity of linguistic judgments can be resolved, and reference values can be established to prioritize risks within a specific case study, taking into account the opinions of experts.

Therefore, this research project addresses a case study of a well-known e-commerce platform, in which it will seek to propose a solution to the following research questions:

- RQ1: How can the operational risks of an e-commerce platform be prioritized?
- RQ2: What strategies should be used to minimize or mitigate the impact of the operational risks?

To do so, three main stages are taken into consideration: risk identification, risk prioritization, and risk management and monitoring. To start with the identification of a literature review of supply chain risk management (SCRM) and e-commerce platforms is conducted. In this way, the basis for the research and development process of the project is generated, where sought evidence for possible events or occurrences that imply an impact on the operations of the organization.

The prioritization is done using the Fuzzy Quality Function Deployment (FQFD) methodology that will allow having the risks that have the greatest impact on the strategic objectives of the organization. Once the risks are prioritized it is important then to define an action plan to mitigate or avoid the occurrence of the risk to guarantee a seamless operation in the electronic commerce platform.

1.2. Case study

The company for this business case was created in 2010 in Portugal, it is a SaaS e-commerce solution, which allows small and medium-sized businesses to easily create their online stores and run their e-commerce businesses without technical knowledge. Currently, the company has stores created around the world and has reached a volume of 25M euros/month in transactions.

Inside the platform, there are different teams divided into the following groups: the store, checkout, marketing, apps, support, business development, design, and development.

Although the company counts on reliable infrastructure and guarantees 99.9% of uptime to the merchants, the company needs to improve internally the procedures to follow given the presence of operational risk.

Moreover, the company has improvement objectives, which they have often left aside due to the focus on daily operations and the maintenance of processes directly related to development and servers. Therefore, an intervention is necessary to identify operational risks to correct or mitigate them.

The purpose of this intervention is to identify the current risks and then prioritize the order of intervention according to the impact and probability of occurrence of each of these identified risks. The management gave their approval for the implementation of this methodology and expects that it can be associated with the parameters or improvement processes already defined in the organization. This study is developed to fulfill the defined objectives, identifying, and prioritizing through the fuzzy QFD methodology and finally applying actions that mitigate the associated risks.

The growth of e-commerce is accompanied by an increase in risk exposure, meaning that risk management in online transactions is one of the most important factors in promoting the survival of business organizations in the long-term (Toleuuly et al., 2020). It is valid to mention first, that the operation process of e-commerce sales is composed of many steps that are led by different stakeholders. These are clustered in different phases but are still interconnected at the same time, each of these could face diverse risks (G. Xu et al., 2019).

2. Literature Review

Under the pressure of global competition, shifting market trends and customer preferences, and economic and financial crises, many businesses and organizations are losing the option to not integrate e-commerce into their operations. The Organization for Economic Cooperation and Development (OECD) defines electronic commerce as the electronic exchange of information that supports and governs commercial activities, including organizational management, commercial management, commercial negotiations and contracts, legal and regulatory frameworks, financial settlement arrangements, and taxation (Wyckoff et al., 1999). Shurrab (2014) argues that e-commerce enables its adopters to effectively respond to survive and prosper. Commerce is a trading act in which two parties negotiate the exchange of that act under a set of mutually acceptable conditions, so that both parties are pleased with the outcome. Similarly, e-commerce has the same concept as a traditional business, but it is conducted over a network of computers that can be connected through the internet globally. Hence, it can be said that e-commerce is the process of buying and selling goods or services on the Internet. It encompasses a wide variety of data, systems, and tools for online buyers and sellers, including mobile shopping and online payment encryption (Bigcommerce, 2022).

2.1. The e-commerce trajectory

Electronic commerce has existed in various forms, it started with the appearance of Electronic Data Interchange (EDI) in the late sixties and then evolved with the introduction of the World Wide Web (WWW) and Internet browsers in early 1990 (Anumba & Ruikar, 2002). The first generation of e-commerce was characterized by the development of electronic data interchange (EDI), the exchange of business documents from one computer to another in a standard format. EDI originated in the mid-1960s, when companies in transportation and some retail industries were attempting to create "paperless" offices. Compuserve, which originated in 1969, was the first e-commerce company (Tian 2007). After that, Michael Aldrich, a British engineer, connected a modified television to a computer in 1979. Aldrich then connected a television to a transaction processing computer via a telephone line, thereby creating teleshopping, also known as shopping at a distance. One of the biggest, even in the development of e-commerce (Guevarra, 2018).

In 1982, France introduced Minitel, an online service accessible via telephone lines and a Videotex terminal machine. The Minitel connected millions of users to a computing network at no cost to telephone subscribers.

Over 7 million households had Minitel terminals by 1997. The Minitel system was popular until the success of the internet three years later which caused it to lose favor (Miva, 2020).

The second generation of e-commerce is characterized by the transaction of goods and services through the Internet, which started as a research tool, but has generally evolved into a commercial tool. (Tian 2007). The WorldWideWeb hypertext project was finally created by Tim Berners Lee and Robert Cailliau in the year 1990. Both the first web server and web browser were written by Lee using a NeXT computer. Lee also created the first web browser. The World Wide Web became accessible to the public for the first time on the Internet in 1990 (Guevarra, 2018). This was succeeded by Netscape Navigator in 1994, (where the first retail transaction occurred) and Microsoft Internet Explorer in 1995. Navigator and Explorer became the leading search engines rapidly. The creation of the browser was indeed an inflection point in the history of e-commerce since now the use of internet was easily accessible to a broader audience. The second half of the 1990s witnessed the rise of the internet. In 1995, Amazon and eBay (originally known as AuctionWeb) went live. In the same year, DoubleClick introduced the first online advertisements (Rheude, 2021).

As an acquired bank that handles payment processing for online retailers, auction sites, and business users, PayPal enabled worldwide e-commerce in 1998. Customers are able to transmit, receive, and retain 24 distinct currencies (Guevarra, 2018) . In the same years, Alibaba, the biggest e-commerce website in China, was founded in 1999. This was a period of exponential expansion for e-commerce. Investors were awestruck by the potential of e-commerce. In the late 1990s, they invested heavily in online businesses. By 2000, the bubble had popped. Following the dot-com boom was the dot-com bust (Rheude, 2021).

Paradoxically, despite the failure of numerous Internet businesses, e-commerce sales increased in 2000 and 2001. As Tian (2007) cited, according to the Department of Commerce (2001), retail e-commerce sales were estimated at $5.27 billion in the fourth quarter of 1999, $8.88 billion in the fourth quarter of 2000, and $10.04 billion in the fourth quarter of 2001. Although e-commerce and Internet companies may have been overvalued in the 1990s, the increase in e-commerce sales during the dot-com crash suggests that e-commerce itself was still viable and growing. (Tian 2007). With the revival of e-commerce, regulation merits special consideration. Consumer protection, user agreements, contracts, and privacy in e-commerce raise new concerns for the regulation of commercial activities especially as e-commerce contributes to the globalization of economic activity (Füstös & López, 2004).

Along with the increase in usage of online shopping came the evolution of the online payment security. The Payment Card Industry Security Standards Council was established in 2004 to ensure that businesses adhere to security standards. This organization creates and executes security guidelines for the protection of account information. In 2005, Amazon introduced Amazon Prime, a membership offering free two-day shipping on all eligible purchases within the contiguous United States for a flat annual fee. The membership quickly gained popularity, putting pressure on other retailers to provide quick and affordable shipping alternatives (Guevarra, 2018) Also, in the same year, Etsy was introduced as a global marketplace where individuals could open shops to sell their distinctive, typically handcrafted things (McFerrin, 2020).

Another milestone in the history of e-commerce is the introduction of e-commerce platforms in 2006 with the origin of Shopify. An e-commerce platform is a software that allows businesses to create, host, and manage online stores. The platform offers features that enable merchants to construct a branded online storefront to sell their products and services (Nguyen, 2022). With the arrival of several technologies such as smartphones social media, Google ads even the different appearance of e-payment methods, it is clear that e-commerce is progressing at a rapid rate. As technology evolves, both e-commerce and consumer trends will continue to develop. It is difficult to make e-commerce forecasts. The history of e-commerce demonstrates that the sector is highly dynamic. A clear example of it, is the COVID-19 pandemic in 2020. This epidemic itself influenced customer behavior. During the COVID-19 crisis, a greater proportion of consumers from each generational cohort reported making digital purchases of goods and services (Jílková & Králová, 2021)

According to Brewster (2022), e-commerce sales rose by $244.2 billion, or 43 percent, in 2020, the first year of the pandemic, growing from $571.2 billion in 2019 to $815.4 billion in 2020.

As per the future of e-commerce it is to conclude that this phenomenon is present is a highly dynamic environment, however, its usage and adoption will continue to grow. According to (Statista, 2022) e-commerce revenue is estimated to expand at a 14.56 percent annual pace, culminating in a market volume of $1,365.00 billion by 2025. With the rise of omnichannel shopping experiences, digital buyers should expect to be able to research, explore, shop, and purchase across several devices and commerce platforms.

2.2. Risk Management

Risk is defined as a result of uncertainty about objectives (ISO 31000:2018). Moreover, according to the Society for Risk Analysis (SRA 2021) glossary, risk is the potential for realization of unwanted, negative consequences of an event. A risk factor is considered as the uncertainty and unexpectedness associated with the occurrence of any event (Gurnani et al., 2011).

According to Ngai and Wat (2005) there is no official definition of risk in e-commerce. However, Viehland (2001, p.983) proposed that “electronic commerce risk is the likelihood that a negative outcome will occur in the course of developing and operating an electronic commerce strategy”.

"Risk management refers to strategies, methods, and supporting tools to identify and control risk to an acceptable level" (Alhawari et al., 2012; Gurtu & Johny, 2021) In addition, risk management may also be defined as a coordinated collection of actions and strategies that drive an organization to minimize the risk associated with attaining its objectives. Risk management enables decision-makers to comprehend and evaluate the impact of risk in a supply chain network (Gurtu & Johny, 2021).

The capacity to manage risk enables companies to make more confident business decisions in the future. Their understanding of the risks they face provides them with several options for dealing with a potential crisis. Although companies work every day to mitigate risks, events such as the 2008 financial crisis (Mitra et al., 2015) or the COVID-19 pandemic show that risk management still has a long way to go.

Modern supply chains are complicated networks that stretch over different geographical locations, which makes them vulnerable to a variety of risks (Vilko & Hallikas, 2012). Risk management has become essential to minimize corporate losses. Risk events are defined in the context of Supply Chain Risk Management (SCRM) by their probability of occurring and their repercussions within the chain (Heckmann et al., 2015)

According to Heckmann et al. (2015), supply chain risk is the potential loss of a supply chain in terms of its target values of efficiency and effectiveness due to the uncertain evolution of chain characteristics when triggering events occur. Wu et al. (2006) state that there are various ways to categorize the different types of risks, but the most important in terms of supply chain management are Internal risks and external risks. Internal risks arise from the interaction between companies throughout the supply chain and are called operational risks, such as those associated with supply, demand, and trade in credit. External risks are also called disruptive risks and are due to the interaction between the supply chain and the environment, such as natural disasters.

An organized approach to risk management might result in a competitive strategy. For this reason, companies and researchers have now immersed themselves in a closer study of the risk management process and, along with it, different stages have been defined for the execution of the process. To ensure a continuous and error-free flow across supply chains, the ISO 31000:2018 standard has been created, with the goal of establishing a risk management standard, composed of risk identification, risk analysis, and risk evaluation and treatment.

Risks exist in numerous types. Firstly, they may be operational and have minor implications, yet they occur frequently. They may have produced supply chain disruptions that are not viewed as major, but if they occur simultaneously or create a snowball effect, they can have severe implications (Vilko and Hallikas, 2012). This study is focused on operational risk.

There are a few different ways to explain operational risk, which mostly differ in how specific and narrow they are. Although there has been significant debate, it is generally agreed that interruptions or failures linked to people, internal processes, technology, or the effects of external processes are at the very least included (Tang, 2006).

Operational risk is defined by Hahn and Kuhn (2012) cited in (Mitra, S et al 2015) as the result of the uncertainty of future occurrences in the usual course of business. I.T. failures (physical or software), damage to physical assets (e.g., due to natural catastrophes), administrative errors (e.g., improper data input), fraud, and other operational activities are examples of operational risk. Moreover, (Bolance et al., 2012) also define operational risk as unexpected events that arise because of changes in a normal operation. Operational risk includes all things that can happen in day-to-day activity (Bolancé et al., 2012). According to the Basel Committee (2001), operational risk is the risk of loss owing to inadequate or failing internal processes, staff, and systems, or due to external occurrences. Based on the previous, in addition to the definitions, managers should keep in mind that activities, functions, and procedures all have an influence on the performance of the organization and its sub-areas. As a result, risks might arise that may have an influence on the company's strategic objectives.

There is a link between rate of return and operational risk management (Borghesi & Gaudenzi, 2012); therefore, when businesses operate under a stable environment and the risks that may show up during the daily activities are under control, their operations are more efficient and there is a tendency to maintain control of the volatility of their profits, bringing great benefits in the short and long term.

On the other hand, Manotas-Duque et al. (2016) show that a risk management system should consist of at least four phases: identification, prioritization, monitoring, and maintenance. This work is mostly about the three first phases mentioned above by Manotas, Osorio, and Rivera, and their development will be shown throughout. The first two steps are critical for risk management and have a direct impact on the measures to be taken to minimize or remove the risk.

2.2.1. Risk Identification:

Companies should methodically collect any potential interruptions or threats; this allows them to have the correct knowledge at the right time to comprehend the challenges that may arise in a process. The first step in risk management is to identify the sources or actors of risk (Wee et al., 2012). Risk identification is the process of discovering, defining, documenting, and communicating risks that may occur and affect the performance of the supply chain, positively or negatively (Aqlan & Lam, 2015).

Management needs a clear understanding of its environment and the dangers it faces successfully manage and control hazards. Without this knowledge, Poor decision-making happens which could lead to future problems. To have a better understanding of the existing risks, start by listing the failures that can result in negative outcomes, and then define the sources that can affect or influence each failure from within the organization (Tummala & Schoenherr, 2011).

Different strategies for risk identification might be employed, according to the techniques described in the literature. All of them, however, have one thing in common: the involvement of people with the knowledge and experience to identify them, and who, in this case, managerial activities and are involved in the company's operations. managerial activities and are involved in the company's operations.

According to Tummala & Schoenherr (2011), some of the tools to identify risk are supply chain mapping, checklists, fault tree analysis, failure mode and effects analysis (FMEA), and Ishikawa cause and effect analysis. Additionally, Manotas-Duque et al. (2016) summarize the most common tools shown in Table (1).

Table 1. Techniques used to identify risks (adapted from Manotas-Duque et al., (2016))

Techniques	Authors
Semi-structured Interviews	(Vilko & Hallikas, 2012), (Schmitt & Singh, 2012),(Sofyalıoğlu & Kartal, 2012), (Berenji, Anantharaman, & Karegar, 2011), (Elmsalmi & Hachicha, 2013) (Berenji & Anantharaman, 2011), (Liu, Peideliugmailcom, & Wang, 2008), (Gaudenzi & Borghesi, 2006), (Ritchie & Brindley, 2007)(Wen & Xi, 2007), (Kull &Talluri, 2008) (Guan, Dong, & Li, 2011) (Aggarwarl & Sharma, 2013) (Wu et al., 2006), (Tuncel&Alpan, 2010), (Manuj&Mentzer, 2008) (Oke & Gopalakrishnan, 2009)
Surveys	(Cheng, Yip, & Yeung, 2012), (Trkman & McCormack, 2009),(Wagner & Bode, 2006) (Jeng, 2004) (Luan, Xie, Duan, Wang, & Xiong, 2009)(Avelar-Sosa, García-Alcaraz, & Castrellón-Torres, 2014) (Zandhessami & Savoji, 2011) (Ouabouch & Amri, 2013)(Bavarsad et al., 2014)(Squire & Chu, 2012)(Hillman & Keltz, 2007)
Panel of experts, Delphi Method	(Tse & Tan, 2012), (Hanning, et al, 2007) (Squire & Chu, 2012) (Badenhorst-weiss et al., 2014)
Checklist	(Hallikas et al., 2004), (Borghesi & Gaudenzi, 2013)

2.2.2. Risk prioritization and evaluation

Prioritization of risks should be based on the company's strategic objectives, so that they are the first to be addressed and negative repercussions on the company's core may be minimized. Risk assessment and prioritizing are carried out to determine which measures should be taken to eliminate, mitigate, or ignore each of the previously identified risks.

According to Borghezi & Gaudenzi (2012), risk assessment aids in understanding the negative effects of unfavorable events and the possibility of negative repercussions, which is why two essential criteria are mentioned when discussing risks:

- The severity of anticipated negative outcomes.
- The probability of each of the consequences occurring.

This step of risk management tries to evaluate the impact of each risk by assessing the effects through procedures that involve the probability of the risks becoming a reality, and the possible breadth of the damage (Lavastre et al., 2012).

Any approach to risk management, must have a larger scope than that of a single company and give insights into how the essential processes should work across organizations. As a result, while examining supply-chain vulnerabilities, businesses must identify risks not just to their own operations but also to all other entities, as well as those induced by inter-organizational links (Jüttner, 2005).

According to the literature reviews, there is a significant participation of multi-criteria and fuzzy logic methods to carry out risk prioritization tasks, such as the ANP and AHP methods, due to their ability to use both qualitative and quantitative data. These solutions address an issue for many businesses, which is exacerbated in supply chains due to the variety of actors, such is the lack of data to carry out the risk management process.

As shown in Table (2), the literature review conducted shows that there is a tendency toward using multi-criteria or fuzzy logic tools for prioritizing, notably in AHP, and risk assessment matrixes are specifically utilized for risk problems. In this situation, new approaches or the integration of current ones might be examined enhance the process and ensure better organizational decisions (Manotas Duque et al., 2016). These solutions address a problem that is quite frequent for many businesses and is much more prevalent in supply chains due to the variety of the actors: a lack of data to carry out the risk management process.

Table 2. Prioritization techniques according to the literature. (Author)

Techniques	**Authors**
Multicriteria techniques (AHP-ANP-Topsis-FAHP-FANP-DEMATEL)	(Guan et al., 2011), (Aqlan & Lam, 2015), (Wu et al., 2006), (Borghesi & Gaudenzi, 2012) (Lavastre et al.,2012), (de Oliveira et al., 2017)
QFD and FQFD	Costantino et al. (2012), Bevilacqua et al. (2006), (Bottani & Rizzi, 2006), (Sohn & Choi, 2001), (Zarei et al., 2011), (Osorio Gomez et al 2018), (Pastrana-Jaramillo & Osorio-Gómez, 2019) (Agudelo-Ibarguen et al 2021), (Gento et al., 2001).
Delphi method - Risk Assessment Matrix	(Markmann et al., 2013), (Mulyati & Geldermann, 2016), (Yang & Haugen, 2016)

As stated by author's Nan et al. (2009), this categorization criterion might have quantitative or qualitative elements. They indicate that risk quantification can be separated into two categories: one based on probability and statistics, and the other, based on expert knowledge and experience.

In this respect, risk assessment can be done using quantitative or qualitative methods; however, the latter is preferred when information is exchanged among numerous people from various functions and risk perception is varied. In the literature and in practice there are several methods that combine both. The use of Fuzzy Set Theory (FST) in combination with Quality Function Deployment (QFD) is the basis for a strategic tool that seeks to respond to customer needs and translates them into engineering characteristics (Osorio-Gómez et al., 2018).

QFD was originally thought to be a tool for product design and development, but it has now evolved to be utilized as a multi-criteria decision-making tool. Fuzzy logic contains the uncertainty inherent in the reality of expert language judgments; it is a technique that makes it possible to mathematically articulate the intermediate values found in real-world circumstances. Fuzzy logic is significant because of the approach it takes between models and organizational reality. By combining QFD with fuzzy logic, it may include the ambiguity found in the subjective assessments and evaluations of individuals participating in the process, improving the application's outcomes.

FQFD is a multi-criteria tool utilized for risk management in several articles (Osorio et al, 2017; Costantino et al., 2012; Gento et al., 2001). To better understand this tool, it is important to describe its components. As was stated before, among the multiple available tools for risk prioritization, experts are tending to combine them to close the gap that could exist given the problems that managers could face now of gathering data. On one hand, the tool is based on fuzzy logic, which allows and offers mathematical options to model the preferences defined by the experts of a characteristic process (Wang et al., 2012). On the other hand, there is the use of the QFD (Quality Function Deployment tool), a strategic technique for developing and improving goods and services based on consumer needs. This methodical procedure turns what the client requires into engineering features of the product or service, assuring a degree of quality that fulfills the customer's expectations (Sener & Ozturk, 2015)

FQFD (Fuzzy Quality Function Deployment) is obtained by combining QFD and fuzzy logic, which allows us to involve the ambiguity present in the subjective judgments and evaluations of those involved in the process, and this is to improve the results of the application. This has become a widely used and developed quality tool to meet customer requirements on a given product. FQFD is a mechanism for converting client requirements into technical product features that fulfill their criteria. However, in recent years, the emphasis has shifted to multi-criteria decision-making techniques (Osorio, 2011).

Considering this case study, as already mentioned, there are few studies done to prioritize risks within the business model of e-commerce platforms. Now, in the same way this business model has the necessary elements to apply this tool because it must consider the desires or needs of customers but also has strategic objectives, then, it is possible to prioritize risks focused on the objectives of the processes, which implicitly include the needs of the users. Additionally, the ambiguity of language judgments can be reduced by adding a fuzzy component, and reference values can be generated to rank risk within a certain case study while considering the views of experts, having this in considerations the proposal made by Osorio (2011) is used for this project.

2.2.3. Risk monitoring and management.

Risk monitoring is activated in action plans, which comprise responsible parties, dates, budgets, and activities to control the success of taken actions and contribute to the company's improvement process (Osorio et al., 2018).

The goal of risk monitoring is to provide a regular check on risk-mitigation techniques. The control is carried out by following up on the objectives defined within the accepted strategies to detect any variation in the expected outcomes, which, if present, necessitates the formulation of corrective actions (Burchett & Tummala, 1999).

Monitoring risks identifies potential increases in the probability of occurrence and impact of hazards, as well as an effective strategy for mitigating them (Delfiner & Pailhé, 2009). Because businesses' surroundings are not stochastic, the status of risks fluctuates, necessitating monitoring. Such monitoring involves following changes in the supply chain, customer requirements, and technology, allowing the associated risk assessment to be updated (Hallikas et al., 2004).

Strategies and action plans for risk management and monitoring could vary depending on the type of industry. According to Quyet and Cuong (2017) in e-commerce firms, risk management is the process of establishing goals and targets for protection, analyzing risks or security attacks, and exploiting vulnerabilities, measuring and ranking risk levels, and choosing countermeasures. They also stated four main strategies for risk management:

- Transfer of risk is a measure of risk control used in risk management to describe the shift of the risk burden to another party
- Risk acceptance is adopted as a response to risk when the cost of avoiding the risk is much higher than the cost of accepting it.
- Risk reduction refers to the use of appropriate techniques to reduce the likelihood of an incident, loss, or both.
- Risk avoidance is using a different route in which this alternative route may have no risk, lower risk, or lower risk-taking costs.

Moreover, ISO 31000: 2018 states that options for risk management are not always complementary or applicable in all situations. They also mention some strategies to treat risks, for example, removing the risk source, changing the likelihood, or sharing the risk, and avoiding the risk.

On the other hand, Manuj and Mentzer (2008) developed a model of global supply chain risk management strategies, where six strategies were found to risk management: Postponement, Speculation, Hedging, Control/share/transfer, Security, Avoidance.

2.3. E-commerce platforms operation process

As it was mentioned previously, one important event in the evolution of e-commerce is the introduction of the e-commerce platforms, this event allowed many merchants to start their journey into the e-commerce sector. According to Anumba (2002); Sharma et al. (2016) and Adamovich (2021), electronic commerce can be generally categorized into five categories.

- **Business-to-Business (B2B**): Business-to-Business, or B2B as it is generally known, is a method of conducting business transactions electronically between two or more businesses. B2B encompasses manufacturers and service providers alike. A company that uses the Internet to place orders with suppliers or retailers, receive electronic invoices, and make electronic payments would be an example of a company that employs this technique of conducting business.
- **Business-to-Consumer (B2C):** Business-to-Consumer is conceptually comparable to traditional commerce, with the Internet serving as the primary difference between the two. This way of doing business transactions presumes that the consumer has Internet connectivity. By selling directly to clients or minimizing the number of intermediaries, businesses can increase profits while lowering prices. This elimination of intermediary businesses or business process layers is known as disintermediation.
- **Business-to-Administration (B2A):** This category encompasses all transactions between businesses and government organizations. This category is now in its infancy, but it has the potential to expand as a result of government initiatives.
- **Consumer-to-consumer (C2C):** Consumer-to-consumer e-commerce, one of the earliest forms of e-commerce, involves the sale of items or services between consumers. This includes consumer-to-consumer (C2C) relationships, such as those seen on eBay and Amazon (Bigcommerce)
- **Consumer-to-business (C2B):** It inverts the conventional retail such that individual customers offer their products and services to business purchasers.

Based on the definition of Shopify one the pioneers in this business model an e-commerce platform is the software a business employs to handle all their B2B and B2C e-commerce needs Sheehan (2022). These needs include product pages, reviews, transactions, order fulfillment, customer support and returns. On the other hand, Bigcommerce, 2022 defines it as a software application that allows online businesses to manage their website, marketing, sales, and operations, they can be Open-source or Software as a service (SaaS) platform.

The benefits of using e-commerce platforms are that they establish value networks by connecting multiple participants and provide a robust mechanism and environment for the exchange of information, transactions, and secure payments. E-Commerce platforms provide the space and conditions for other stakeholders to co-create value and encourage participants to engage in more interactive behaviors. Strong e-commerce platforms entice an increasing number of participants to join, thereby, enhancing the network effect. (Zhang, 2022)._

Figure (1) proposed by G. Xu et al., (2019) presents in a clear way the general operation process of e-commerce logistics.

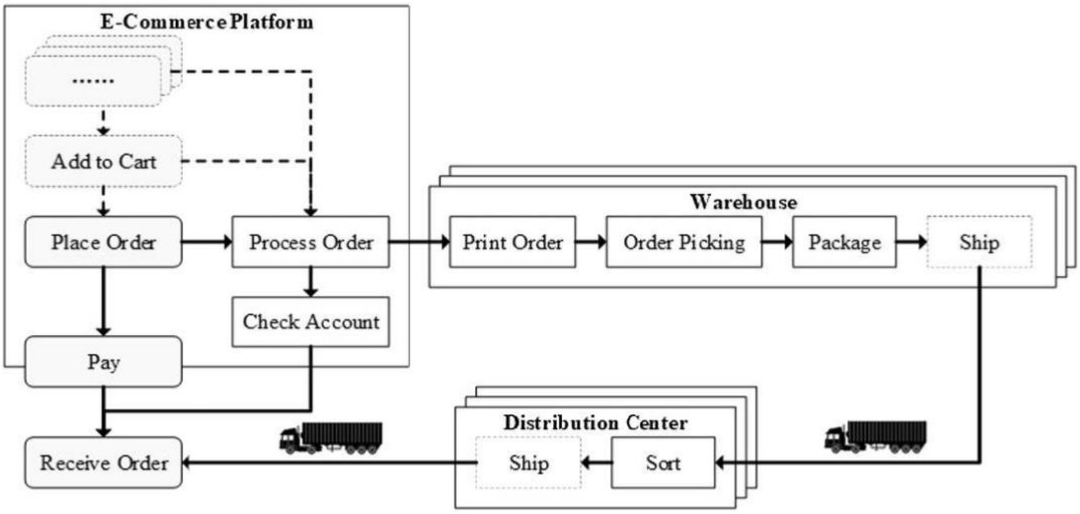


Figure 1. Figure 1. Operation process of e-commerce logistics. (G. Xu et al., 2019)

2.4. Operational risk in e-Commerce platforms

An e-commerce system incorporates several procedures at various levels. Tens of thousands of orders are processed, and numerous automated processes are used. These automated backend processes, which also include order tracking, inventory control, and shipping systems, are susceptible to failure. The failures might be due to their own internal software/hardware failures, engineers, upgrades, etc.; if they occurred this can have a significant impact on the business, causing major problems for the company, its reputation, and its ultimate customers (Toleuuly et al., 2020).

During the order process, a huge amount of information is processed, and if this is not well handled this could leave adverse effects associated with online business. Clearly, information assets are susceptible to several types of threats, which can have direct and indirect effects on an organization's operations. As e-commerce business investments develop, there is a rising need to implement effective risk management approaches to secure the know-how, financial information, and trade secrets, among other parts of a company's information resources, which face significant threats (Toleuuly et al., 2020).

According to Watson, Worm, Palmatier, & Ganesan, (2015) B2B e-commerce platforms have become an important marketing channel that effectively facilitates trade between selling and buying; therefore, their contribution to the economy is high. For this, and for the amount of information exchanged, users, and money that is involved, it is pertinent to identify, prioritize, and manage the risks that are involved in the electronic commerce platform.

From the literature, it has been possible to identify multiple articles related to the general risk of electronic commerce from the perspective of the businesses that own a digital store and the clients of these companies, but very few related to the e-commerce platforms and the importance of the prioritization of the risks. Mostly, these platforms work as an intermediary firm that facilitates multiple sellers to connect and present their products to prospective buyers. Table (3) presents the articles found in the literature that are related to risk from the perspective of sellers and buyers, electronic commerce, and electronic commerce risk management from a technical and traditional point of view:

Table 3. Literature review electronic commerce risk and platforms (Author)

Category	Article	Risk Identification	Prioritizing Risks	Risk monitoring and mitigation	Seller	Buyers	Platform
Electronic commerce risk	(Kim et al., 2008)	x				x	
	(Westland, 2002)			x	x	x	
	(Visa Asia-Pacific, 2000),	x			x		
	(Vijayaraghavan, 2003)	x	x		x		
	(Pappas, 2016)	x				x	
	(Viehland, 2001)	x	x	x	x		
	(Nyshadham & Ugbaja 2006)					x	
	(Javaria et al., 2020)	x				x	
	(Sutton et al., 2008)	x			x	x	
	(Lagkas, 2007)	x	x	x	x	x	
	Xu et al., 2019)	x		x	x		
	(Wu, 2014)	x		x	x		
	(Zirakja, 2011)	x	x	x	x		
	(Toleuuly et al., 2020)	x		x	x		
	(Quyet & Cuong, 2017),	x	x	x	x		
	(Sharma et al., 2016).	x	x	x	x	x	
	(Jin, 2011)	x	x	x	x		
Electronic commerce platforms	(Liu et al., 2020),						x
	Shurrab, 2014),						x
	(Soleimani, 2021				x	x	x
	(Kumar & Jose, 2017)						x
This study		x	x	x	x	x	x

The work of Lagkas (2007) focuses on Risk Assessment and Risk Management, using Brainstorming and Documented Knowledge as identification techniques. The study is applied for a B2C and determines that 50% of the critical risks identified come from technical issues. Moreover, The findings also highlighted the value of customers' trust in EC and the B2C relationship in general. 20% more of the significant risks had to do with the organization's strategy. More specifically, risks associated with staff quality are seen as critical to the operation of online enterprises. Although it is a very detailed study, it does not mention the component of platforms or the third party where the store is hosted.

Furthermore, the work of Vijayaraghavan, (2003), proposes a taxonomy of e-commerce risk and failures, his work follows a deep literature review and brainstorming for the risk identification and then proposes to follow a framework of Failure Mode and Effect Analysis (FMEA) to provide a list of potential failure modes in an e-commerce site and a taxonomy of failures to hold the failure modes. As well as Lagkas's (2007) work, although both types of research are well defined the component of platforms is left aside.

On the other hand, the articles of Liu et al., (2020), Shurrab, (2014), Soleimani, (2021), and Kumar & Jose, (2017) mentioned the innovation presented in the electronic commerce platforms, and how they transformed the traditional modes of transaction, the impact of the open-source platforms, how to increase trust on the user’s side and how to improve its usability. However, based on the literature review performed it was notable the lack of research on this business model, moreover, neither of the articles reviewed mentioned the risk management component. Therefore, this work will contribute to the research of risk management in this modern business model.

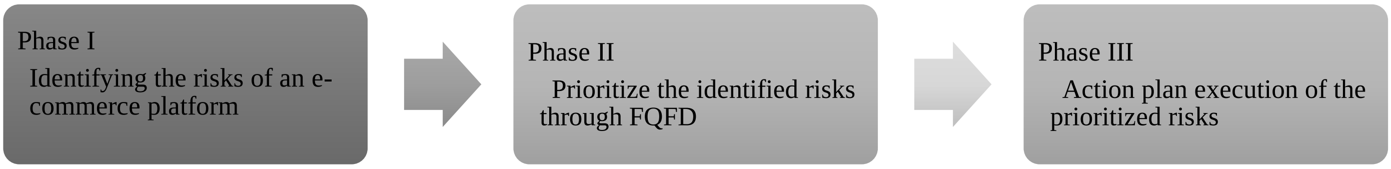
Also, in the literature, it is notable that some companies that are in the field of electronic commerce have considered a risk management process, but the methods used do not yet include a perspective that involves the desires of the users, in this case, the merchants who own a digital business and the objectives of the platform organization. In Javaria et al., (2020), the study's objectives are to identify the various theories and dimensions of risks faced by consumers when making purchases through e-commerce, analyze the steps taken by the consumer to reduce risk during the purchase process using various strategies, and gauge how satisfied the consumer is with the shopping experience. On the other hand, Wu, (2014) proposed a risk management framework for enterprises to handle security issues from a technical point of view. Lastly, Quyet & Cuong (2014) analyzes the Vietnam Airlines e-commerce risk management case using the DREAD model to demonstrate the theory of e-commerce risk management. The paper offers talks and concise recommendations for other businesses in today's e-commerce risk management.

As it was stated previously, electronic commerce is a global phenomenon. It has become a popular form of business for both small and large companies. But one of the problems with this phenomenon is that it is not immune to operational risk. This project will discuss the challenges that e-commerce platforms face in terms of operational risk and how companies in the industry are willing to identify and mitigate those risks. To reach this aim, first, we identify the operational risks associated with each stage of the distribution process. Then, we prioritize the operational risks of the distribution process, to classify those that cause and generate a greater impact on the platform's strategic objectives. Finally, we propose mitigation strategies to minimize the impacts associated with the analyzed operational risks.

3. Methodology

The following methodology is presented with the overall goal of identifying operational risks and then prioritizing them to determine the most significant ones; and based on them, the firm may generate action plans to reduce or eliminate the negative repercussions for the organization.

For the execution of this methodology, the article by Osorio Gómez, (2011) is taken as a reference, as well as the specific methodological proposal for prioritization described in (Osorio-Gomez et al., 2018), which determines the following phases:


Phase I
Identifying the risks of an e-commerce platform
Phase II
Prioritize the identified risks through FQFD
Phase III
Action plan execution of the prioritized risks

3.1. Phase I: Risk identification

To identify the risk, a literature review about electronic commerce risks and a validation of them in the electronic platform was performed. These are the inputs of the survey that was built and applied to the selected group of experts, to consolidate information about the probability and the magnitude of the risk and obtain the impact-probability matrix to identify the risks to prioritize. These experts were selected considering their level of experience and their role within the company.

The structure of the survey is presented in Table (5) and is built using a linguistic scale presented in Table (4), these respondents are asked to make the relevant qualifications to consolidate the answers and determine the viability of the previously selected risks, according to the observation of the process, and then obtain the weighted probability and magnitude of the risk.

Table 4. Linguistic scale (Pastrana-Jaramillo & Osorio-Gómez, 2019).

Linguistic scale		**Numerical rating**
VL	Very low	1
L	low	2
wy	Medium	3
H	High	4
VH	Very High	5

Table 5. Survey heading((Pastrana-Jaramillo & Osorio-Gómez, (2019)).

Risk identified	Apply as operational risk?	
	Yes	No

Select the magnitude if it occurs					***Select the probability of the Risk***				
VL	*L*	*M*	*H*	*VH*	*VL*	*L*	*M*	*H*	*VH*

These will allow the construction of the probability and impact matrix of the preliminary risks as shown in figure 2 based on Equation (1) and Equation (2). These two equations calculate weighted average of the magnitude of risk and weighted average of the probability of risks respectively. Note that, n shows the number of experts, $\overline{X}_i$ is the weighted average of the magnitude of risk i, $\overline{Y}_i$ is the Weighted average of the probability of risk I, $B_{i,j}$ is a binary variable which defines expert *j*'s criterion of whether *i* applies as a risk (1,0), $M_{i,j}$ shows expert *j*'s rating of the impact of risk i, and $P_{i,j}$ indicates Expert *j*'s rating of the probability of risk *i*.

Equation 1 Weighted average of the magnitude of risk i

$$(1)\ \overline{X}_i = \frac{\sum_{j=1}^{n} B_{i,j} M_{i,j}}{n}$$

Equation 2 weighted average of the probability of risk i

$$(2)\, \overline{Y}_i = \frac{\sum_{j=1}^{n} B_{i,j} P_{i,j}}{n} \quad ; \quad \forall\, i$$

Figure (2) shows the impact-probability matrix is created. Using the matrix, one may graphically group risks according to their amount of impact. The hazards listed in the green area are minor, those in the yellow section have a considerable chance of happening, and the risks listed in the orange and red sections are high or critical and need to be addressed (Osorio-Gomez et al., 2018)

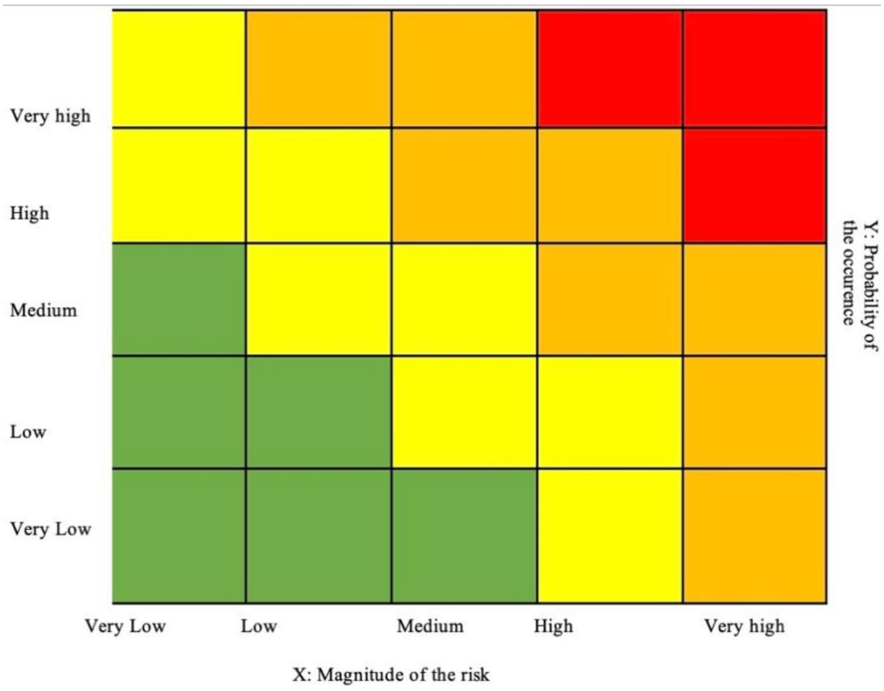


Figure 2.Matrix impact–probability (adapted from Osorio-Gomez et al., 2018).

3.2.Phase II: Risk prioritization using FQFD

Fuzzy Quality Function Deployment (FQFD) approach (Osorio Gómez, 2022; Osorio-Gomez et al., 2018) is considered to prioritize the identified risks. The following phases are used for the execution of this methodology.

3.2.1. Stage 1: Identify the What's

Taking into consideration the customer's feedback and the Net Promoter Score (NPS) surveys a set of expected attributes to have on the business are defined and selected. These aspects are known in the tools as "the what´s"

3.2.2. Stage 2: Determine the relative importance of the "What's".

The survey is built and sent to a sample of users of the company. The sample is composed by active users of the platform. These users determine the importance of the What's, evaluating each attribute with a linguistic qualification according to Table (6) based on Bevilacqua et al (2006).

Table 6. Fuzzy rating scale adapted from Bevilacqua, (2006).

Linguistic scale		**Triangular fuzzy rating (a, b, c)**
VL	Very low	(0,1,2)
L	low	(2,3,4)
M	Medium	(4,5,6)
H	High	(6,7,8)
VH	Very High	(8,9,10)

Once the ratings are determined, they need to be processed by adding the boxes corresponding to each of the triangular numbers acquired and ultimately dividing each of the values by the number of respondents, as shown in Equation (3).

Equation 3 Calculation of the relative weight of what´'s

$$Weight\ of\ What\acute{}s = \{w_i, where\ i = 1, \dots, q\}, \qquad w_i = \frac{1}{n_1} \otimes \left(w_{i1} \oplus w_{i2} \oplus \dots \oplus w_{in_1}\right) \quad (3)$$

Where q is the number of whats's and n_1 the number of respondents (users of the platform). Each element of the vector Weight of What's is a triangular fuzzy number defined by the set $w_i = (w_{ia}, w_{ib}, w_{ic})$.

3.2.3. Stage 3: Identify Strategic Objectives or “How’s”

These are defined by the team of experts and are considered the strategic objectives of the electronic platform related to the company and to the operational process. These can be strategic objectives or management indicators; the prioritization will be based on the impact that the risks have on the organization's strategy.

3.2.4. Stage 4: Determine the “What”- “How” correlation

The same linguistic scale from Table (6) is used to measure the relationship that exists between the What's and the How’s. This establishes the level at which the What's are tied to the organization's strategic objectives (Osorio, (2011)). It is determined as follows:

Equation 4 Correlation between What's and How's

$$Correlation = \left(r_{ij}, where\ i = (1, \dots, q)\ \ and\ j = (1, \dots, c)\ \right)$$

$$r_{ij} = \frac{1}{n} \otimes (r_{ij1} \oplus\ r_{ij2} \oplus\ \dots \oplus\ r_{ijn})\ (4)$$

Where ***c*** is the number of "How's", ***q*** the number of "What's" and ***n*** the number of experts. Each ***rij*** represents the correlation between the i-th ***“What”*** and the j-th ***“How”.*** And is represented by a fuzzy triangular number $r_{ij} = \left(r_{ija}\ , r_{ijb}\ , r_{ijc}\right)$.

3.2.5. Stage 5. Determine the weight of the "How's".

From the application of fuzzy mathematics and based on the previous correlation, the weights of the ***How's*** can be determined. The result is obtained by multiplying the ratings of each expert regarding the **“What”-“How”** by the weight of the ***What's*** obtained in stage two. The result will be a triangular fuzzy number $W_j = (W_{ja}\ , W_{jb}, W_{jc})$ expressed in Equation 5.

$$Weight\ how\acute{} s = \left\{W_j, where\ j = 1, \dots, c\right\},$$

Equation 5. Calculation of the weight of the How's

$$W_j = \frac{1}{q} \otimes \left[\left(r_{j1} \otimes w_1\right) \oplus\ \dots \oplus \left(r_{jq} \otimes\ w_q\right)\right]\quad (5)$$

3.2.6. Stage 6. Determine the impact of the risk on the strategic objectives ("How´s")

In this phase, the relationship between each of the risks that have been identified in terms of the How's must be established; this relationship will be defined by the experience of the decision-making group and configured based on Equation 6. Where p is the number of alternatives.

$$RI = \left(RI_{hj}, where\ h = (1, \dots, p)\ \ y\ j = (1, \dots, c)\ \right),$$

Equation 6 Calculation of risk impact

$$RI_{hj} = \frac{1}{n} \otimes (ri_{hj1} \oplus ri_{hj2} \oplus \dots \oplus ri_{hjn}) \ (6)$$

3.2.7. Stage 7. Prioritizing risks.

To obtain the ranking of the risks, multiply the values obtained from the relationship between the risks and their impact on the strategic objectives, obtained in the previous phase; by the relative importance of the ***How's*** found in stage 5. What is obtained is a risk prioritization index, a fuzzy RPI $(RPI_{ha}, RPI_{hb}, RPI_{hc})$:

$$RPI = \{RPI_h, where\ h = 1, \dots, p\},$$

Equation 7 Calculation of the Risk Prioritization Index

$$RPI_h = \frac{1}{c} \otimes [(RI_{h1} \otimes\ W_1) \oplus \dots \oplus (RI_{hc} \otimes\ W_c)] \ (7)$$

Finally, to obtain a consolidated (non-fuzzy) rating, the triangular fuzzy number defuzzification approach defined by Facchinetti is used as shown in equation 8:

Equation 8. Defuzzification of triangular fuzzy numbers defined by Facchinetti

$$RPIF = \frac{RPI_{ha} + (2 * RPI_{hb}) + RPI_{hc}}{4} \ (8)$$

3.3. Phase III. Risk management and mitigation

Based on past assessments, measures must be devised to minimize or remove process risks and thereby enhance the process (Osorio-Gomez et al. 2018).

Finally, it is critical to stress the adoption of activities targeted at transferring, eliminating, and/or decreasing process risks, as well as employing tactics centered on the individual or related machinery (Lavastre et al. 2012).

Once the risks are prioritized, meetings are held to the people in charge of the process to present the results, validate the prioritization and review the current activities. After this, an improvement plan is held in case of need.

4. Results

Following the methodology previously defined, three phases are applied. For risk identification, a literature review is performed. Once the list is created, the risks are evaluated in terms of probability and magnitude by experts of the company. The following phase is the application of the FQFD tool which is composed of 7 stages. To begin with, a survey was applied to the users and two more surveys were applied to the experts, this will allow the risks to be prioritized, and finally, after obtaining the results, the highest ranked risk are reviewed and discusses with the electronic commerce platform and action plans are proposed.

4.1. Phase I. Risk identification

Risk identification is a process that reveals and determines the possible organizational risks as well as conditions, arising risks. By risk identification the organization is able to study activities and places where its resources are exposed to risks (Williams et al., 1998. as cited in Lagkas, 2007). Several articles were reviewed from multiple sources, an exhaustive search of operational risk in electronic commerce was performed. The preliminary risks in the electronic commerce platform are obtained from the literature review.

Table 7. List of risks identified from the literature (Author)

List of risks in e-commerce present in e-commerce platforms			
ID	Name	Description	Literature review
R1	Loss of customers' private data	Businesses that use EC should consider the possibility of clients losing the private information they communicate online when making a purchase. This information is typically "lost" because hackers are attempting to steal and abuse it for personal gain without the customer's consent.	(Deloitte, 2018), (Bader, 2022) (Lagkas, 2007), (Edwards, 2020)
R2	Customer´s monetary loss	Customers who shop online may incur monetary losses for a variety of reasons (i.e., identity theft, transfer of money to fake EC businesses, etc.). Customers must interact not with a salesperson but with impersonal software that contains a lot of exploitable weaknesses.	(Vijayaraghavan, 2003), (Lagkas, 2007)
R3	Navigation failure: Lack of understanding of web-page design principles (Poor usability design)	The website of EC companies is the initial point of client contact with the company. If it lacks fundamental design principles, it can produce a negative first impression and fail to attract clients.	(Edwards,2020),(Vijayaraghavan, 2003), (Lagkas, 2007)
R4	Failure to gain and sustain brand loyalty	In the rapidly changing environment of EC, client interactions become increasingly transient. Failure to acquire and maintain long-term brand loyalty threatens the success of the business.	(Vijayaraghavan, 2003), (Lagkas, 2007)
R5	Lack of customers´s trust in internet technology	If E-businesses do not invest in promoting the use of the internet as a purchase method, consumers' trust in internet technology will be poor, which will have a negative impact on their popularity and revenue.	(Vijayaraghavan, 2003), (Lagkas, 2007), (Viehland, 2001)
R6	Low quality of services	In any platform, service quality is a crucial aspect in achieving success. Especially in an EC context where B2C ties are transient and impersonal, service quality plays a crucial role in establishing and maintaining these partnerships.	(Vijayaraghavan, 2003), (Lagkas, 2007), Chopra and Sodhi (2004),
R7	Misunderstanding of the user requirements	In a constant evolution business, understanding and correctly implementing customer needs is key for the success of any EC platform.	(Vijayaraghavan, 2003), (Lagkas, 2007)
R8	Failure to manage end-user expectations	This new channel of transactions (EC) requires additional consideration because the customer has multiple options. This risk mostly represents the company's inability to deliver the advertised or expected service.	(Vijayaraghavan, 2003), (Lagkas, 2007)
R9	Copyright and/or trademark violation	An e-commerce platform host thousands of stores, it is very common that some of them could be illegally using trademarks or copyrighted material in them. It could be by ignorance but there is high exposure.	(Vijayaraghavan, 2003), (Lagkas, 2007), (Deloitte, 2018)
R10	Prohibition in some countries	The use of some payment gateways, apps, or products might be banned by some countries.	(Vijayaraghavan, 2003), (Deloitte, 2018)

List of risks in e-commerce present in e-commerce platforms			
R11	Incompletion of contract terms	The risk of incompletion of contract terms refers to any inconsistencies related to customers, vendors, and employees, on behalf of the e-business. Risk managers should focus on this risk because it could damage the company's image rendering the company as not trustworthy.	(Vijayaraghavan, 2003), Chopra and Sodhi (2004), (Lagkas, 2007)
R12	Intellectual property risk	Risks associated with the unauthorized use or promotion of music, images, product, systems, software, etc. Also related to the exposure of unauthorized use of the know-how of the platform to the externals.	Chopra and Sodhi (2004), (Vijayaraghavan, 2003), (Lagkas, 2007), (Deloitte, 2018)
R13	Non-Compliance	Certain standards governing the privacy and security of customer data must be followed by e-commerce platforms. If a business owner disregards the appropriate rules, he or she runs the danger of incurring substantial fines, serving time in prison or having their firm shut down.	(Bader, 2022)
R14	Hacker attacks	Hackers present a threat to e-businesses because they typically exploit software weaknesses to steal, destroy, or corrupt sensitive data.	(Vijayaraghavan, 2003), (Lagkas, 2007)
R15	Unauthorized Access	Unauthorized access is responsible for a substantial amount of data loss.	(Bader, 2022)
R16	Disruption of system's functionality due to industrial espionage	Competition is not always legitimate; industrial espionage is a risk that always existed, and businesses should protect themselves from it.	(Vijayaraghavan, 2003), (Lagkas, 2007)
R17	Use of outdated or inappropriate software and hardware	The risk of employing obsolete or incorrect software depends on how reliable and knowledgeable the experts are about current software releases. 'Applying incorrect technology', combining the risk of using both incorrect software and hardware, which is also a crucial risk for e-businesses.	(Vijayaraghavan, 2003), (Lagkas, 2007), (Bader, 2022)
R18	Inadequate backup systems	As EC systems' failures result in major losses in terms of money, inadequate backup systems expose the assets of the companies.	(Vijayaraghavan, 2003), (Lagkas, 2007)
R19	Inadequate testing procedures	Lack of planning and knowledge on testing new technologies that are about to be released	(Vijayaraghavan, 2003), (Lagkas, 2007), (Bader, 2022)
R20	Risks Due to Software Upgrade Errors	Due to the nature of their dynamic content, online stores and, shopping carts undergo frequent updates, upgrades, and modifications. However, these frequent changes tend to break things and cause chaos when the site reopens for business following an upgrade.	(Vijayaraghavan, 2003), (Lagkas, 2007), (Bader, 2022)
R21	Process Failures	An e-commerce system incorporates numerous processes at various stages. These include processes that handle order taking, payment processing, and order fulfillment; if they fail, they can impact an e-commerce site's ability to fulfill transactions on time and in full.	(Yuan & Peng, 2007)
R22	Lack of system security	Related to Password disclosure vulnerabilities, viruses, and worms, Errors: Input Validation, Access Control, Buffer Overflow, Authentication, and Configuration, among others.	(Yuan & Peng, 2007), (Deloitte, 2018)
R23	Nontrustworthy employees responsible for sensitive information	The risk of having nontrustworthy employees handling sensitive customer or organization data can influence other aspects of the business, such as reputation and security.	(Vijayaraghavan, 2003), (Lagkas, 2007)

List of risks in e-commerce present in e-commerce platforms			
R24	Untrained and unexperienceded staff	Inadequate recruiting procedures increase the likelihood of employing untrained or inexperienced staff. Numerous positions within the EC platforms require a high level of technical expertise so that potentially dangerous situations for the system can be dealt with appropriately.	(Yuan & Peng, 2007), (Bader, 2022),(Deloitte, 2018)
R25	Lack of pricing strategy	Ecommerce platforms are present around the world, market volatility, inflation in some countries, and poor analysis of the market/pricing could affect the business model and therefore reduce the market participants in some countries.	(Deloitte, 2018)
R26	Denial of service attacks	Malicious code attacks as a cause of system crashes. the situation of systems failing due to 'site or network overload and disruption'.	(Yuan & Peng, 2007), (Vijayaraghavan, 2003), (Lagkas, 2007)
R27	Poor customer service	Poor combination of strategies, people, and technology used to provide customers with online stores. High time to response, inaccurate responses, high time to resolve, low courtesy of the agent	(e-commerce Customer Service Guide, 2017) ,(Yuan & Peng, 2007)
R28	Insufficient Capacity Planning	This involves: -Risks Based on the Number of Users and Usage for example, the risk that thread the shopping cart performance, overconsumption of the resource. -Risks Based on Computing Infrastructure -Risks Based on Site Content Complexity	(Deloitte, 2018), (Vijayaraghavan, 2003)
R29	High dependence on Third-party Software	E-commerce platforms work with many parties from billing, payment gateway, fulfillment, design, and marketing apps among others. The loss of one or more specialized website functions could be an indication of third-party failures.	(Deloitte, 2018)
R30	Physical attacks	Risks associated with natural disasters, sabotage of physical assets, robbery, etc.	(Bader, 2022),(Vijayaraghavan, 2003), (Lagkas, 2007)
R31	Miscommunication among teams	All the processes of the e-commerce platform are interconnected, and poor communication among the team could lead to failures in the operations and the communication with the external client.	(Bader, 2022)

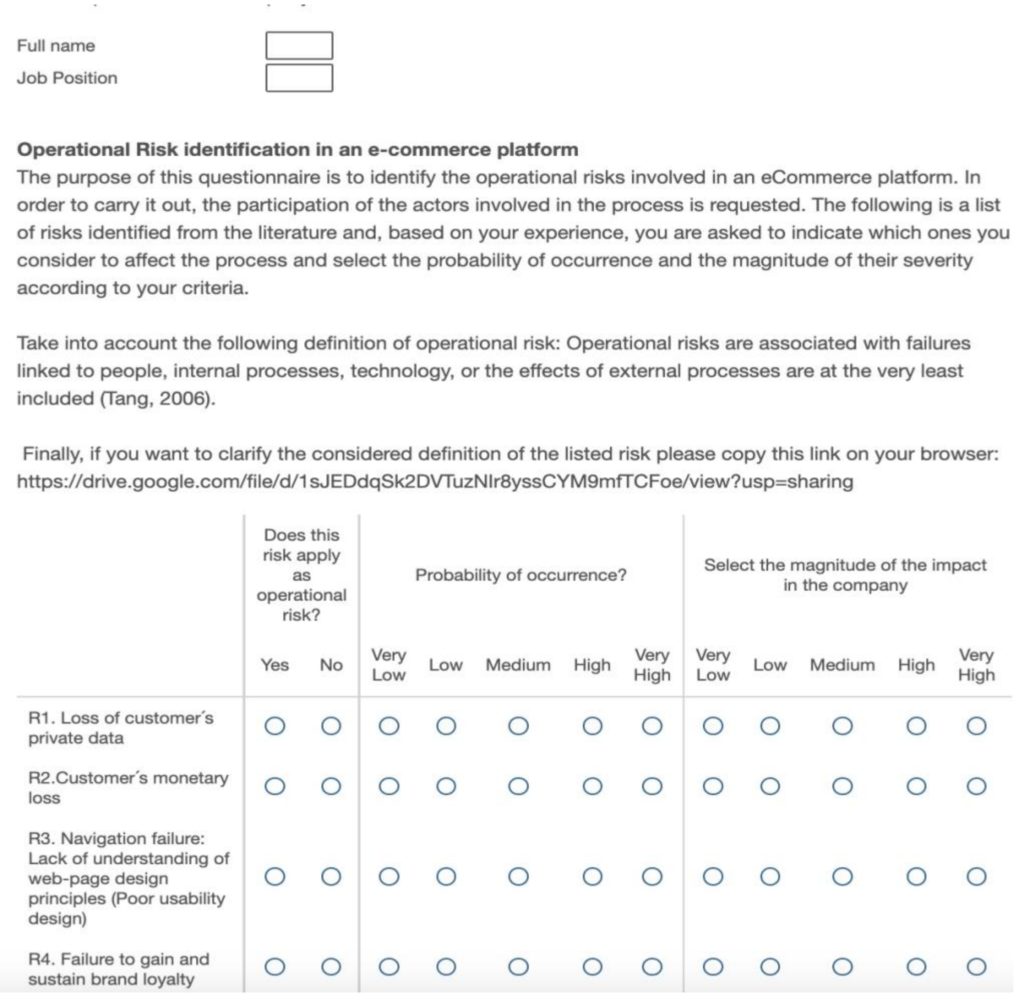
Considering the experience and position in the platform and given the relationship between the risks presented on the table above and the role inside the company, the group of experts is selected and is presented in table (8).

Table 8. Group of experts from the company (Author)

ID	Job position
E1	Software Engineer/checkout team leader
E2	Business developer head
E3	Marketing head
E4	Co-founder 1
E5	Co-founder 2
E6	Agile coach
E7	Software Engineer/apps team leader

The definition of the questionnaire begins with the preliminary risks in the electronic commerce platform presented in table (7). The survey is constructed, considering the probability of occurrence and impact (see figure (3)). Based on the questionnaire, these experts are asked to make the pertinent qualifications to consolidate the answers and determine the viability of the previously selected risks, according to the observation of the process, and then obtain the weighted probability and impact of the risk. These will allow the construction of the probability and impact matrix of the preliminary risks as shown in figure 4 based on Equation (1) and Equation (2).

According to Figure (4) the risks found in the critical zones marked in red and orange, presented in Table (9), are considered for the analysis based on the FQFD methodology. And it is from these risks that the decision-making group, formed by the people listed in Table (8), are asked to qualify the risks based on fuzzy logic. Survey I and its results are presented in Figure (3) and Table (10).



Full name □
Job Position □

Operational Risk identification in an e-commerce platform
The purpose of this questionnaire is to identify the operational risks involved in an eCommerce platform. In order to carry it out, the participation of the actors involved in the process is requested. The following is a list of risks identified from the literature and, based on your experience, you are asked to indicate which ones you consider to affect the process and select the probability of occurrence and the magnitude of their severity according to your criteria.

Take into account the following definition of operational risk: Operational risks are associated with failures linked to people, internal processes, technology, or the effects of external processes are at the very least included (Tang, 2006).

Finally, if you want to clarify the considered definition of the listed risk please copy this link on your browser: https://drive.google.com/file/d/1sJEDdqSk2DVTuzNIr8yssCYM9mfTCFoe/view?usp=sharing

	Does this risk apply as operational risk?		Probability of occurrence?					Select the magnitude of the impact in the company				
	Yes	No	Very Low	Low	Medium	High	Very High	Very Low	Low	Medium	High	Very High
R1. Loss of customer´s private data	○	○	○	○	○	○	○	○	○	○	○	○
R2.Customer´s monetary loss	○	○	○	○	○	○	○	○	○	○	○	○
R3. Navigation failure: Lack of understanding of web-page design principles (Poor usability design)	○	○	○	○	○	○	○	○	○	○	○	○
R4. Failure to gain and sustain brand loyalty	○	○	○	○	○	○	○	○	○	○	○	○

Figure 3. Survey I structure (Risk identification). (Author)

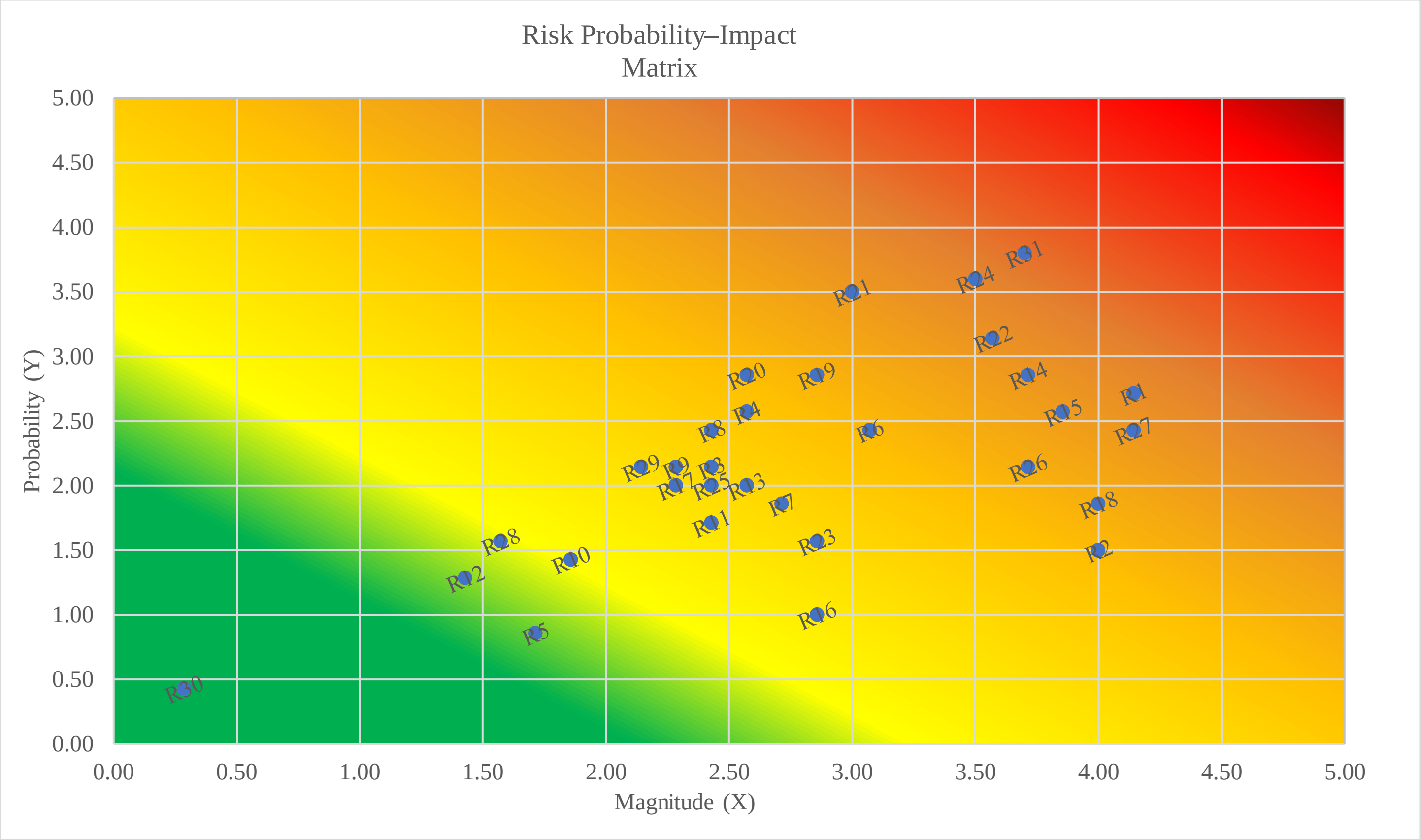


Figure 4. Risk probability-impact matrix. (Author)

Table 9. List of risks to prioritize based on probability-impact matrix. (Author)

List of risks to prioritize based on probability-impact matrix			
ID	**Name**	**Description**	**Literature review**
R1	Loss of customer´s private data	Businesses that use EC should give considerable consideration to the possibility of clients losing the private information they communicate online when making a purchase. This information is typically "lost" because hackers are attempting to steal and abuse it for personal gain without the customer's consent.	(Deloitte, 2018), (Bader, 2022) (Lagkas, 2007), (Edwards, 2020)
R14	Hacker attacks	Hackers present a threat to e-businesses because they typically exploit software weaknesses to steal, destroy, or corrupt sensitive data.	(Vijayaraghavan, 2003), (Lagkas, 2007)
R15	Unauthorized Access	Unauthorized access is responsible for a substantial amount of data loss.	(Bader, 2022)
R21	Process Failures	An e-commerce system incorporates numerous processes at various stages. These include processes that handle order taking, payment processing, and order fulfillment; if they fail, they can impact an e-commerce site's ability to fulfill transactions on time and in full.	(Yuan & Peng, 2007)
R22	Lack of system security	Related to Password disclosure vulnerabilities,vurus and worms, Errors: Input Validation, Access Control, Buffer Overflow, Authentication, Configuration	(Yuan & Peng, 2007), (Deloitte, 2018)
R24	Untrained-unexperienced staff	Inadequate recruiting procedures increase the likelihood of employing untrained or inexperienced staff. Numerous positions within the EC platforms requires a high level of technical expertise so that potentially dangerous situations for the system can be dealt with appropriately.	(Yuan & Peng, 2007), (Bader, 2022),(Deloitte, 2018)
R26	Denial of service attacks	Malicious code attacks' as a cause of system's crashes. the situation of systems failing due to 'site or network overload and disruption'.	(Yuan & Peng, 2007), (Vijayaraghavan, 2003), (Lagkas, 2007)
R27	Poor customer service	Poor combination of strategies, people, and technology used to provide customers of online stores. High time to response, unaccurate responses, high time to resolve, low courtesy of the agent	(eCommerce Customer Service Guide, 2017) ,(Yuan & Peng, 2007)
R31	Miscommunication among teams	All the proccesses of the ecommerce platform are interconnected, poor communication among the team could lead to failures in the operations and the communication to the external client	(Bader, 2022)

Table 10. Survey I results. (Author)

Risk	**Risk id**	**Magnitude (X)**	**Probability (Y)**
- R1. Loss of Customers' private data	R1	4,14	2,71
- R2. Customers' monetary loss	R2	4,00	1,50
- R3. Navigation failure: Lack of understanding of web-page design principles (Poor usability design)	R3	2,43	2,14
- R4. Failure to gain and sustain brand loyalty	R4	2,57	2,57
- R5. Lack of customers´ trust in internet technology	R5	1,71	0,86
- R6. Low quality of services	R6	3,07	2,43
- R7. Misunderstanding of the user requirements	R7	2,71	1,86
- R8. Failure to manage end-user expectations	R8	2,43	2,43
- R9. Copyright and/or trademark violation	R9	2,29	2,14
- R10. Prohibition in some countries	R10	1,86	1,43
- R11. Incompletion of contract terms	R11	2,43	1,71
- R12. Intellectual property risk	R12	1,43	1,29
- R13. 0n-Compliance	R13	2,57	2,00
- R14. Hacker attacks	R14	3,71	2,86
- R15. Unauthorized Access	R15	3,86	2,57
- R16. Disruption of system’s functionality due to industrial espionage	R16	2,86	1,00
- R17. Use of outdated or inappropriate software and hardware	R17	2,29	2,00
- R18. Inadequate backup systems	R18	4,00	1,86
- R19. Inadequate testing procedures	R19	2,86	2,86
- R20. Risks Due to Software Upgrade Errors	R20	2,57	2,86
- R21. Process Failures	R21	3,00	3,50
- R22. Lack of system security	R22	3,57	3,14
- R23. 0ntrustworthy employees responsible for sensitive information	R23	2,86	1,57
- R24. Untrained and unexperienced staff	R24	3,50	3,60
- R25. Lack of pricing strategy (price volatility)	R25	2,43	2,00
- R26. Denial of service attacks	R26	3,71	2,14
- R27. Poor customer service	R27	4,14	2,43
- R28. Insufficient Capacity Planning	R28	1,57	1,57
- R29. High dependence on Third-party Software	R29	2,14	2,14
- R30. Physical attacks	R30	0,29	0,43
- R31. Miscommunication among teams	R31	3,70	3,80

4.2.Phase II: Risk prioritization

4.2.1. Stage 1: Identify the What’s

The What´s are determined by the desires of the customers or merchants when having or choosing an electronic commerce platform. These “what´s” were defined using the customer support feedback, the passed reviews from different users, and NPS results which are mentioned Table (11).

Table 11. List of "what´s". (Author)

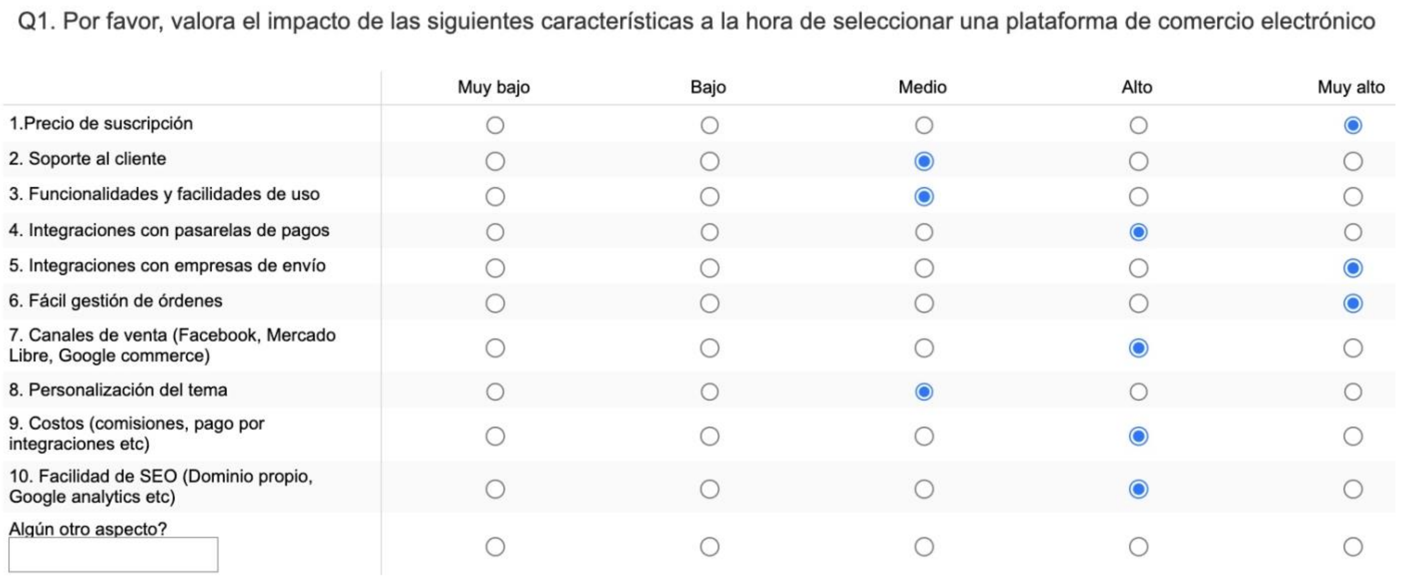
Id	What´s	Description
1	Subscription Price	Monthly fee paid by the merchant for the service of store hosting and operations
2	Customer support	Quality and time of response given doubts or failures in the platform
3	Store Functionality & Ease of Use	How responsive and intuitive the platform is, to be able to create and design a user experience and to manage the store (orders, payments, inventory, shipping)
4	Payment Gateways integration	Availability of multiple payment gateways
5	Shipping partners integrations	Connected third parties to perform the delivery logistics
6	Orders management	Orders status, Inventory management, product management
7	Sales Channels	External integrations with partners to increase sales (Facebook commerce, Google commerce, Alibaba)
8	Theme Customization	Options for store front design
9	Hidden cost (Commissions, locked features, etc)	Cost of operations of the store
10	SEO friendliness (Own domain, Google Analytics, etc)	specific elements and characteristics that assist with search engines understand the purpose of the website

4.2.2. Stage 2: Determine the relative importance of the "What's".

The relative importance or weight should be assigned to each of these What's according to the consideration made by the respondents.

As stipulated by the company for the development of this project, the questionnaire was sent as a "newsletter" to certain users of the platform located in Colombia, 150 surveys were sent, and 55 responses were processed.

They answered the survey I shown below in figure (5) using the linguistic scale described in the methodology, they were asked the following question “Please rate the impact of the following features when selecting an e-commerce platform”



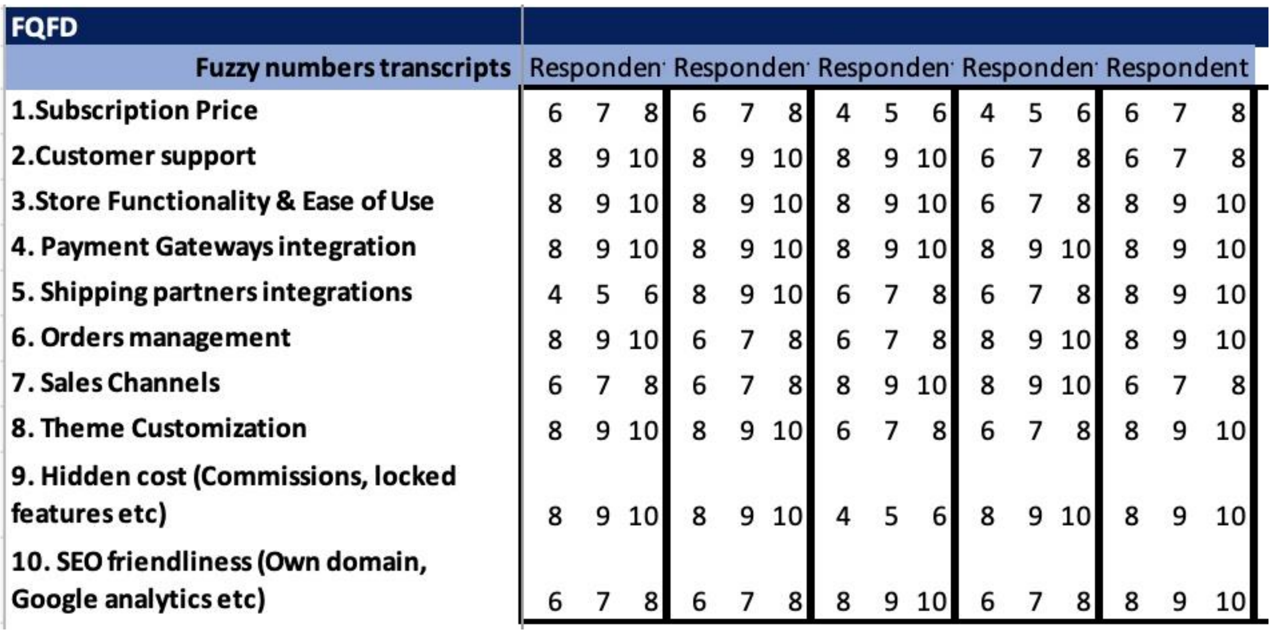
Q1. Por favor, valora el impacto de las siguientes características a la hora de seleccionar una plataforma de comercio electrónico

	Muy bajo	Bajo	Medio	Alto	Muy alto
1.Precio de suscripción	○	○	○	○	●
2. Soporte al cliente	○	○	●	○	○
3. Funcionalidades y facilidades de uso	○	○	●	○	○
4. Integraciones con pasarelas de pagos	○	○	○	●	○
5. Integraciones con empresas de envío	○	○	○	○	●
6. Fácil gestión de órdenes	○	○	○	○	●
7. Canales de venta (Facebook, Mercado Libre, Google commerce)	○	○	○	●	○
8. Personalización del tema	○	○	●	○	○
9. Costos (comisiones, pago por integraciones etc)	○	○	○	●	○
10. Facilidad de SEO (Dominio propio, Google analytics etc)	○	○	○	●	○
Algún otro aspecto?	○	○	○	○	○

Figure 5.Survey II, the relative importance of what´s. (Author)

Once the answers were received, they were processed using fuzzy numbers and Excel as Table (12) is showing and then after processing all the responses, equation (3) was applied to obtain the weights of the What's, as shown in Table (13).

Table 12. Transcripts of responses survey II into fuzzy numbers. (Author)



FQFD															
Fuzzy numbers transcripts	Responden			Responden			Responden			Responden			Respondent		
1.Subscription Price	6	7	8	6	7	8	4	5	6	4	5	6	6	7	8
2.Customer support	8	9	10	8	9	10	8	9	10	6	7	8	6	7	8
3.Store Functionality & Ease of Use	8	9	10	8	9	10	8	9	10	6	7	8	8	9	10
4. Payment Gateways integration	8	9	10	8	9	10	8	9	10	8	9	10	8	9	10
5. Shipping partners integrations	4	5	6	8	9	10	6	7	8	6	7	8	8	9	10
6. Orders management	8	9	10	6	7	8	6	7	8	8	9	10	8	9	10
7. Sales Channels	6	7	8	6	7	8	8	9	10	8	9	10	6	7	8
8. Theme Customization	8	9	10	8	9	10	6	7	8	6	7	8	8	9	10
9. Hidden cost (Commissions, locked features etc)	8	9	10	8	9	10	4	5	6	8	9	10	8	9	10
10. SEO friendliness (Own domain, Google analytics etc)	6	7	8	6	7	8	8	9	10	6	7	8	8	9	10

Table 13. Weights of the what´s (triangular-fuzzy numbers). (Author)

What´s	Weight of what´s		
	Triangular fuzzy number		
	a	**b**	**c**
Subscription Price	6,09	7,09	8,09
Customer support	5,45	6,45	7,45
Store Functionality & Ease of Use	6,36	7,36	8,36
Payment Gateways integration	6,00	7,00	8,00
Shipping partners integrations	5,55	6,55	7,55
Orders management	6,36	7,36	8,36
Sales Channels	4,64	5,64	6,64
Theme Customization	5,64	6,64	7,64
Hidden cost (Commissions, locked features etc)	6,40	7,40	8,40
SEO friendliness (Own domain, Google analytics etc)	5,11	6,11	7,11

4.2.3. Stage 3: Identify strategic objectives or “How’s”

According to Alogan & Yet[idot]ş, (2006), Strategic objectives are the necessary tools of operationalizing the desired movements of an organization. They are essential for coordinating strategy with process effectiveness.

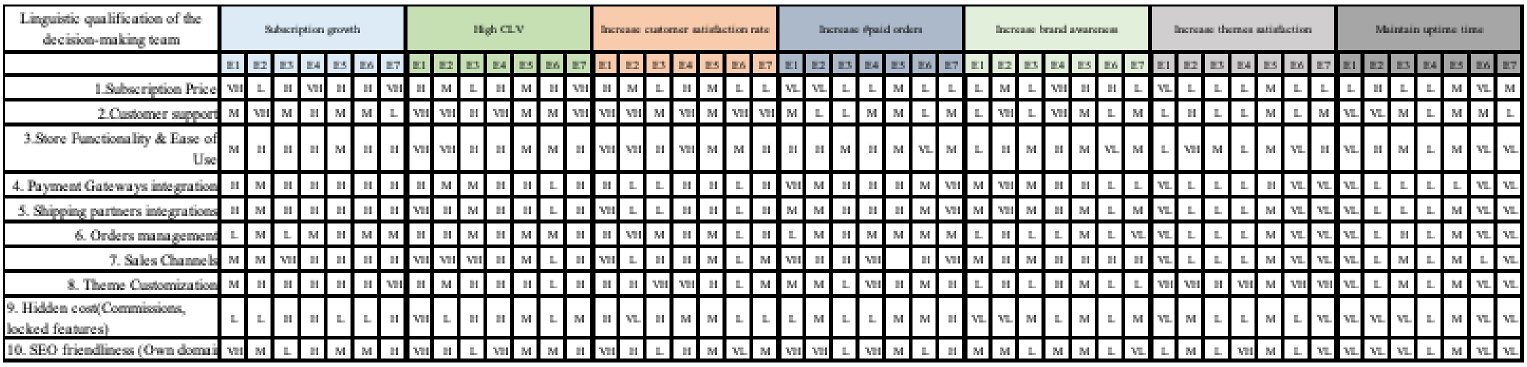
To determine the strategic objective or How's in this work, the OKRs (Objectives and Key Results) of each team of the platform's areas were reviewed and some of the metrics that lead to achieving the company's strategic goals were used in the same way. The "how's" can be found in Table (14).

Table 14. Strategic objectives or “How’s” (Author)

Strategic objectives (How´s)	**Description**
1. Subscription growth	Increase number of paying and active stores of the platform
2. High CLV	Measure of the total revenue a company can anticipate from a typical customer for the duration that person or account continues to be a client (Caldwell, 2022)
3. Increase customer satisfaction rate	Increase rate: Total positive ratings/Total ratings * 100
4. Increase #paid orders	Increase number of place orders made by the clients of the stores
5. Increase brand awareness	Increase the probability that consumers are familiar about the life and availability of the brand (Juneja, n.d.)
6. Increase themes satisfaction	Satisfaction related to the store UI and themes
7. Maintain uptime	Percentage of time that the hosting service is active and operational.

4.2.4. Stage 4: Determine the “What”- “How” correlation

In the next step, the decision-making team defined in Table (8) qualifies the relationship between each of the what´s with respect to the how´s, for example for member E1 the relationship between subscription price and subscription growth has a Very high relationship (VH), while for the same expert the relationship between customer support and subscription growth is Medium (M). This sequence is followed by the rest of the experts and correlation is presented in figure (6) According to equation (4), an average is made from the fuzzy numbers that represent the rating of each of the experts, i.e. each of the fuzzy components is selected, as shown in figure (7).



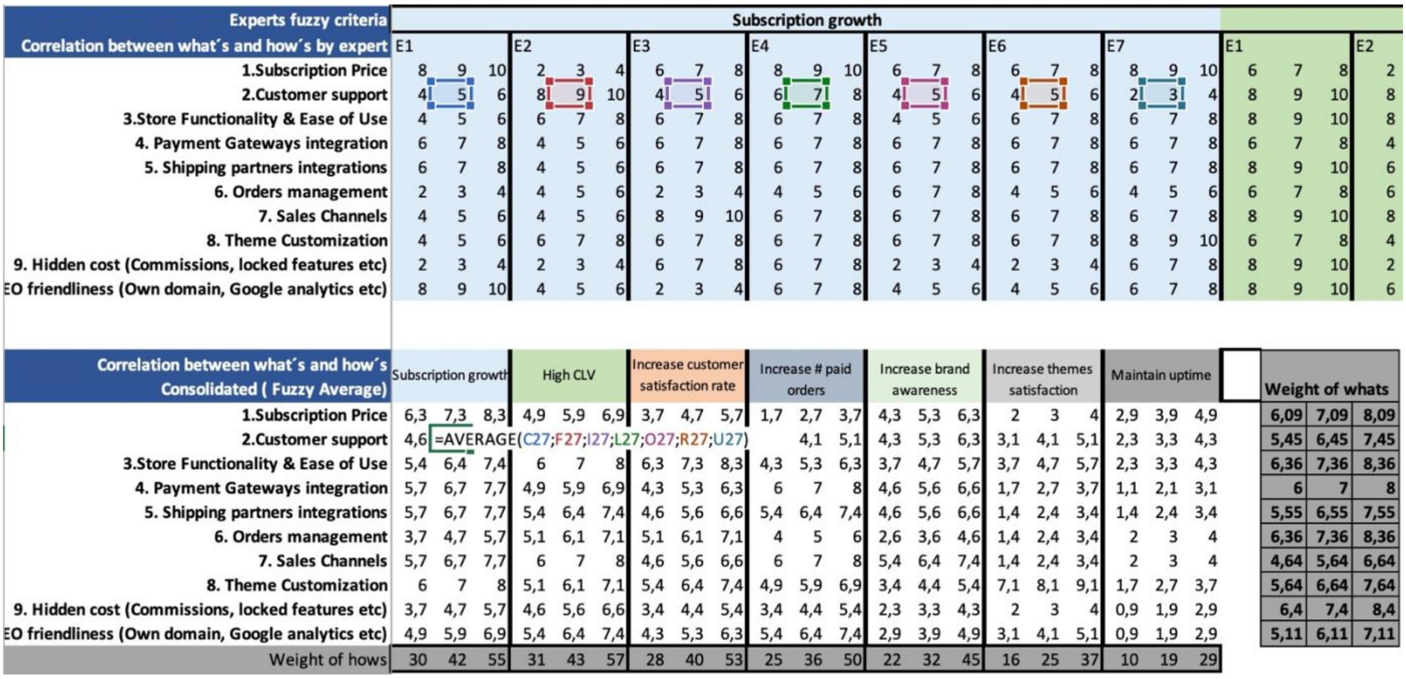
Linguistic qualification of the decision-making team	Subscription growth							High CLV							Increase customer satisfaction rate							Increase #paid orders							Increase brand awareness							Increase themes satisfaction							Maintain uptime time						
	E1	E2	E3	E4	E5	E6	E7	E1	E2	E3	E4	E5	E6	E7	E1	E2	E3	E4	E5	E6	E7	E1	E2	E3	E4	E5	E6	E7	E1	E2	E3	E4	E5	E6	E7	E1	E2	E3	E4	E5	E6	E7	E1	E2	E3	E4	E5	E6	E7
1.Subscription Price	VH	L	H	VH	H	H	VH	H	M	L	H	M	H	VH	H	M	L	H	M	L	L	VL	VL	L	L	M	L	L	L	M	L	VH	H	H	L	VL	L	L	L	M	L	L	L	H	L	L	M	VL	M
2.Customer support	M	VH	M	H	M	M	L	VH	VH	H	VH	M	M	VH	VH	VH	M	VH	M	VH	VH	M	L	L	M	M	L	M	L	VH	L	VH	M	L	M	L	H	L	L	M	L	M	VL	VL	M	L	M	M	L
3.Store Functionality & Ease of Use	M	H	H	H	M	H	H	VH	VH	H	H	M	M	H	VH	VH	H	VH	M	M	H	H	H	M	H	M	VL	M	L	H	M	H	M	VL	M	L	VH	M	L	M	VL	H	VL	H	M	L	M	VL	VL
4. Payment Gateways integration	H	M	H	H	H	H	H	H	M	M	H	H	L	H	H	L	L	H	H	L	H	VH	M	H	H	H	M	VH	M	VH	M	H	H	L	L	VL	L	L	L	H	VL	VL	VL	L	L	L	L	VL	VL
5. Shipping partners integrations	H	M	H	H	H	H	H	VH	H	M	H	H	L	H	VH	L	L	H	H	L	H	M	M	H	H	H	M	VH	M	VH	M	H	M	L	M	VL	L	L	L	M	VL	VL	VL	L	L	L	M	VL	VL
6. Orders management	L	M	L	M	H	M	M	H	H	M	H	M	M	H	H	VH	M	H	M	L	H	L	M	H	M	M	M	M	L	H	L	L	M	L	VL	VL	L	L	L	M	VL	VL	VL	L	H	L	M	VL	VL
7. Sales Channels	M	M	VH	H	H	H	H	VH	VH	VH	H	M	L	H	VH	L	H	H	M	L	M	VH	H	H	VH		H	VH	M	H	M	H	H	H	H	VL	L	L	L	M	VL	VL	VL	L	M	L	M	L	VL
8. Theme Customization	M	H	H	H	H	H	VH	H	M	H	H	H	L	H	H	H	VH	VH	H	L	M	M	M	L	VH	H	M	H	L	H	L	H	M	L	L	VH	VH	H	VH	M	VH	VH	VL	L	M	L	M	VL	VL
9. Hidden cost(Commissions, locked features)	L	L	H	H	L	L	H	VH	L	H	H	M	L	M	H	VL	H	M	M	L	L	L	M	L	L	M	M	H	VL	VL	M	L	M	L	M	VL	M	L	L	M	L	VL	VL	VL	VL	L	M	VL	VL
10. SEO friendliness (Own domai	VH	M	L	H	M	M	H	VH	H	L	VH	M	M	H	VH	H	L	H	M	VL	M	VH	VH	L	VH	M	L	H	M	M	L	M	M	L	VL	L	M	L	VH	M	L	VL	VL	VL	VL	L	M	VL	VL

Figure 6. Linguistic qualification of the experts about the what´s and how´s. (Author)

4.2.5. Stage 5. Determine the weight of the "How's".

According to the evaluation of Figure (7) and making use of fuzzy mathematics, the weights of the how´s are calculated using equation (5) and are presented in Table (15). The calculation is as follows, the weighted average between the weight of the what's and the overall rating of the correlation divided by the number of what's as observed in figure (8).

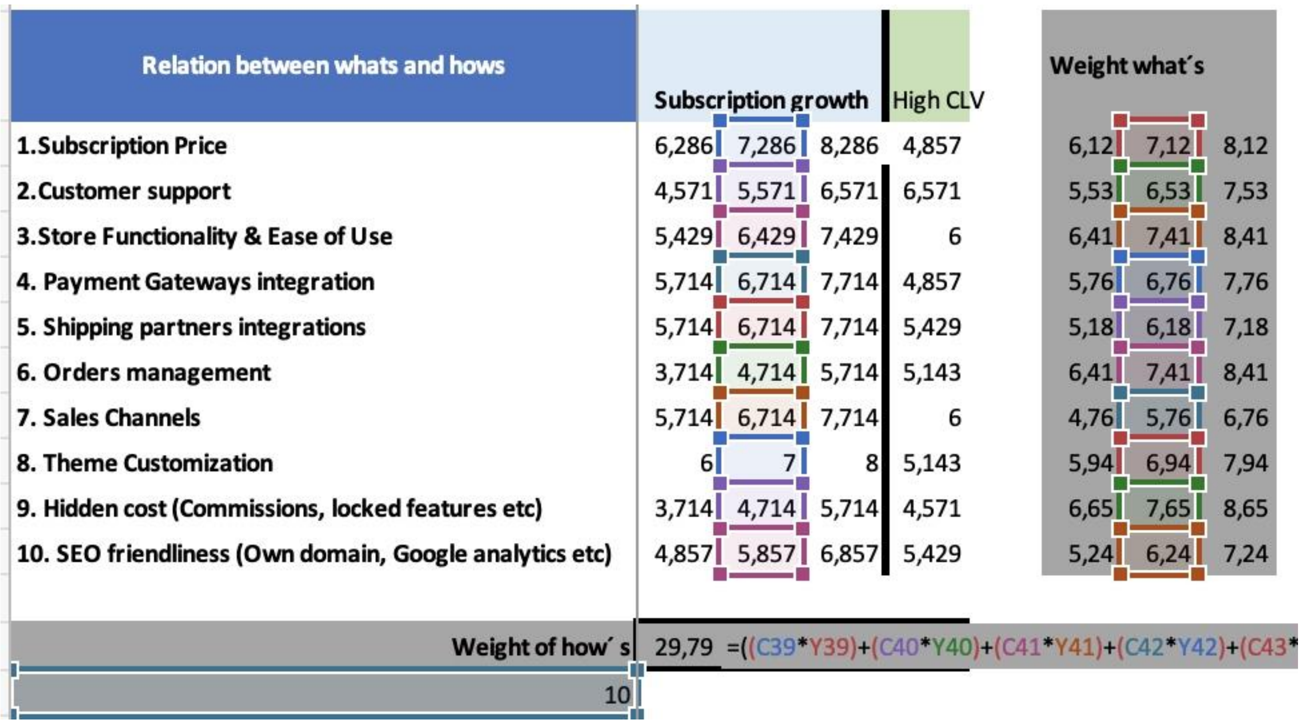
Figure 7. Calculation of correlation between what´s and how´s (Excel). (Author)



Experts fuzzy criteria	Subscription growth																								
Correlation between what´s and how´s by expert	E1			E2			E3			E4			E5			E6			E7			E1			E2
1.Subscription Price	8	9	10	2	3	4	6	7	8	8	9	10	6	7	8	6	7	8	8	9	10	6	7	8	2
2.Customer support	4	5	6	8	9	10	4	5	6	6	7	8	4	5	6	4	5	6	2	3	4	8	9	10	8
3.Store Functionality & Ease of Use	4	5	6	6	7	8	6	7	8	6	7	8	4	5	6	6	7	8	6	7	8	8	9	10	8
4. Payment Gateways integration	6	7	8	4	5	6	6	7	8	6	7	8	6	7	8	6	7	8	6	7	8	6	7	8	4
5. Shipping partners integrations	6	7	8	4	5	6	6	7	8	6	7	8	6	7	8	6	7	8	6	7	8	8	9	10	6
6. Orders management	2	3	4	4	5	6	2	3	4	4	5	6	6	7	8	4	5	6	4	5	6	6	7	8	6
7. Sales Channels	4	5	6	4	5	6	8	9	10	6	7	8	6	7	8	6	7	8	6	7	8	8	9	10	8
8. Theme Customization	4	5	6	6	7	8	6	7	8	6	7	8	6	7	8	6	7	8	8	9	10	6	7	8	4
9. Hidden cost (Commissions, locked features etc)	2	3	4	2	3	4	6	7	8	6	7	8	2	3	4	2	3	4	6	7	8	8	9	10	2
EO friendliness (Own domain, Google analytics etc)	8	9	10	4	5	6	2	3	4	6	7	8	4	5	6	4	5	6	6	7	8	8	9	10	6

Correlation between what´s and how´s Consolidated (Fuzzy Average)	Subscription growth			High CLV			Increase customer satisfaction rate			Increase # paid orders			Increase brand awareness			Increase themes satisfaction			Maintain uptime				Weight of whats		
1.Subscription Price	6,3	7,3	8,3	4,9	5,9	6,9	3,7	4,7	5,7	1,7	2,7	3,7	4,3	5,3	6,3	2	3	4	2,9	3,9	4,9		6,09	7,09	8,09
2.Customer support	4,6	=AVERAGE(C27;F27;I27;L27;O27;R27;U27)									4,1	5,1	4,3	5,3	6,3	3,1	4,1	5,1	2,3	3,3	4,3		5,45	6,45	7,45
3.Store Functionality & Ease of Use	5,4	6,4	7,4	6	7	8	6,3	7,3	8,3	4,3	5,3	6,3	3,7	4,7	5,7	3,7	4,7	5,7	2,3	3,3	4,3		6,36	7,36	8,36
4. Payment Gateways integration	5,7	6,7	7,7	4,9	5,9	6,9	4,3	5,3	6,3	6	7	8	4,6	5,6	6,6	1,7	2,7	3,7	1,1	2,1	3,1		6	7	8
5. Shipping partners integrations	5,7	6,7	7,7	5,4	6,4	7,4	4,6	5,6	6,6	5,4	6,4	7,4	4,6	5,6	6,6	1,4	2,4	3,4	1,4	2,4	3,4		5,55	6,55	7,55
6. Orders management	3,7	4,7	5,7	5,1	6,1	7,1	5,1	6,1	7,1	4	5	6	2,6	3,6	4,6	1,4	2,4	3,4	2	3	4		6,36	7,36	8,36
7. Sales Channels	5,7	6,7	7,7	6	7	8	4,6	5,6	6,6	6	7	8	5,4	6,4	7,4	1,4	2,4	3,4	2	3	4		4,64	5,64	6,64
8. Theme Customization	6	7	8	5,1	6,1	7,1	5,4	6,4	7,4	4,9	5,9	6,9	3,4	4,4	5,4	7,1	8,1	9,1	1,7	2,7	3,7		5,64	6,64	7,64
9. Hidden cost (Commissions, locked features etc)	3,7	4,7	5,7	4,6	5,6	6,6	3,4	4,4	5,4	3,4	4,4	5,4	2,3	3,3	4,3	2	3	4	0,9	1,9	2,9		6,4	7,4	8,4
EO friendliness (Own domain, Google analytics etc)	4,9	5,9	6,9	5,4	6,4	7,4	4,3	5,3	6,3	5,4	6,4	7,4	2,9	3,9	4,9	3,1	4,1	5,1	0,9	1,9	2,9		5,11	6,11	7,11
Weight of hows	30	42	55	31	43	57	28	40	53	25	36	50	22	32	45	16	25	37	10	19	29				

Figure 8. Calculation of the weight of the how´s. (Author)



Relation between whats and hows	Subscription growth			High CLV		Weight what´s		
1.Subscription Price	6,286	7,286	8,286	4,857		6,12	7,12	8,12
2.Customer support	4,571	5,571	6,571	6,571		5,53	6,53	7,53
3.Store Functionality & Ease of Use	5,429	6,429	7,429	6		6,41	7,41	8,41
4. Payment Gateways integration	5,714	6,714	7,714	4,857		5,76	6,76	7,76
5. Shipping partners integrations	5,714	6,714	7,714	5,429		5,18	6,18	7,18
6. Orders management	3,714	4,714	5,714	5,143		6,41	7,41	8,41
7. Sales Channels	5,714	6,714	7,714	6		4,76	5,76	6,76
8. Theme Customization	6	7	8	5,143		5,94	6,94	7,94
9. Hidden cost (Commissions, locked features etc)	3,714	4,714	5,714	4,571		6,65	7,65	8,65
10. SEO friendliness (Own domain, Google analytics etc)	4,857	5,857	6,857	5,429		5,24	6,24	7,24
Weight of how´ s	29,79	=((C39*Y39)+(C40*Y40)+(C41*Y41)+(C42*Y42)+(C43*						
10								

36

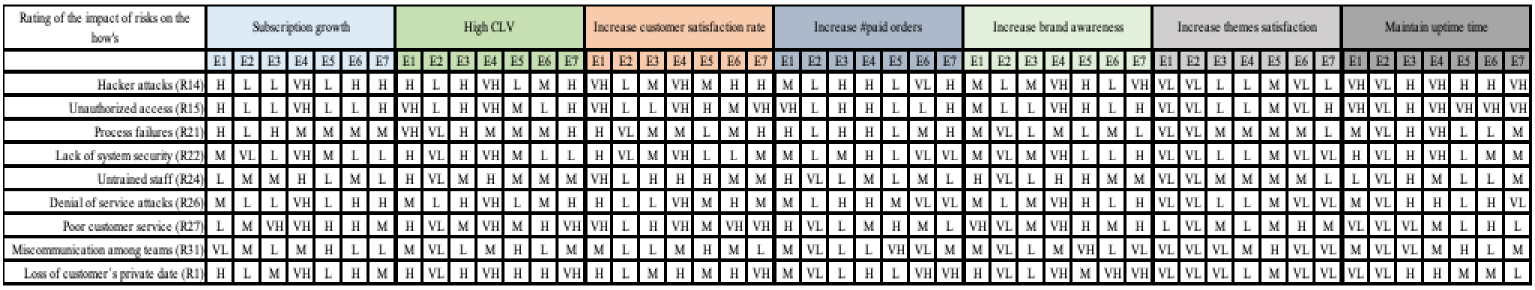
Table 15. Weight of the how´s (triangular fuzzy number), (Author.)

How´s	Weight of how´s		
	Triangular fuzzy number		
	a	**b**	**c**
Subscription growth	29,63	41,57	55,50
High CLV	30,94	43,10	57,27
Increase customer satisfaction rate	27,95	39,57	53,19
Increase #paid orders	25,13	36,32	49,51
Increase brand awareness	21,60	32,16	44,72
Increase themes satisfaction	15,61	25,08	36,56
Maintain uptime time	10,07	18,58	29,08

4.2.6. Stage 6. Determine the impact of the risk on the strategic objectives ("How´s")

As stated previously, the risks that were on the red and orange quadrant of the matrix presented in Figure 4, were the input to build the survey where the experts now need to determine the relation and impact between the risks and the how´s (strategic objectives). The linguistic responses to the relationship between the risks and the "how's" are presented in Figure 9.

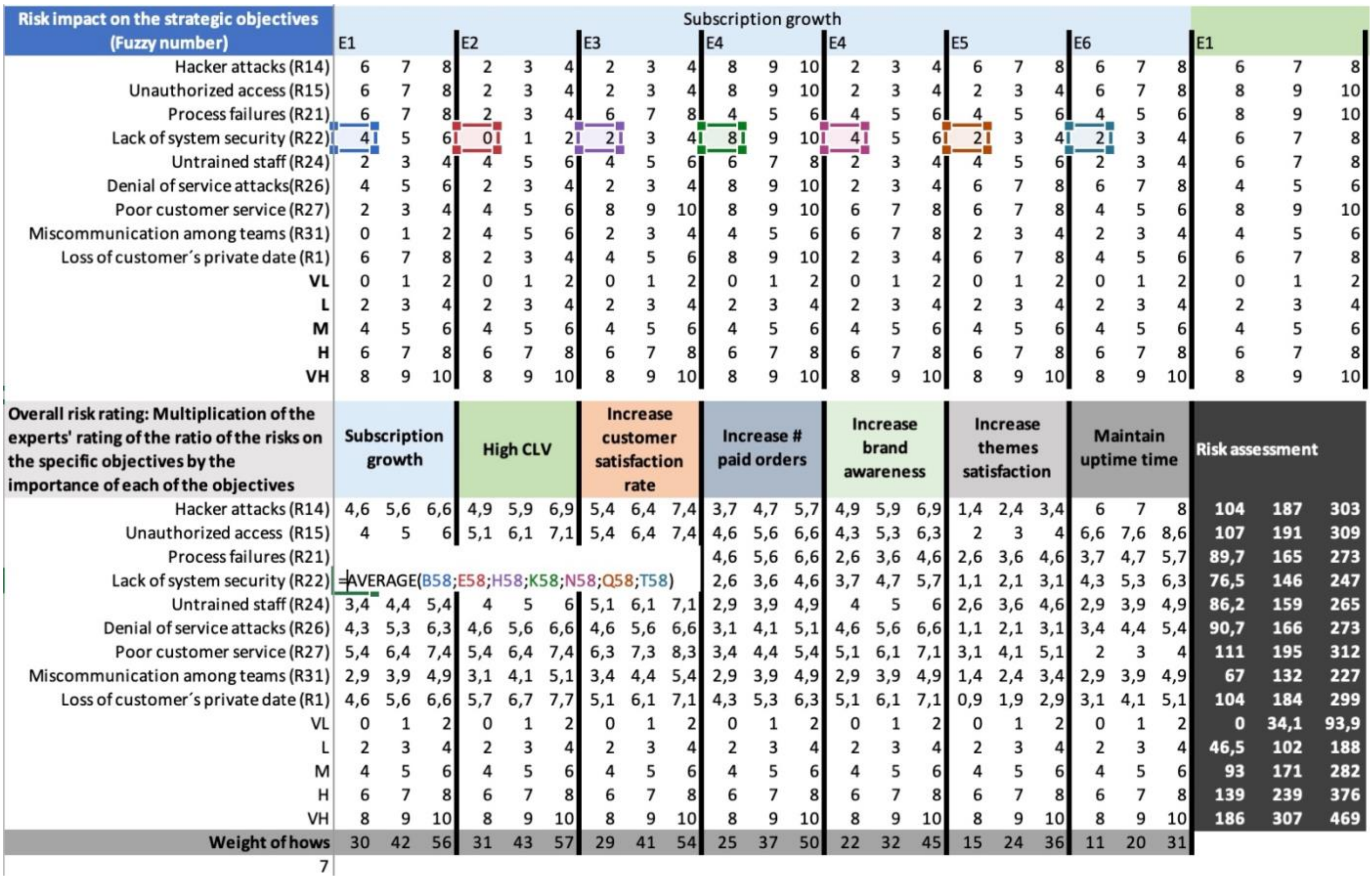
These responses were then translated into fuzzy numbers, and equation (6) was applied. The equation (6) corresponds to the impact of the risk which is the average of the responses of the experts when evaluating the impact of the risks on the how's. The procedure is shown on Figure (10).



Rating of the impact of risks on the how's	Subscription growth							High CLV							Increase customer satisfaction rate							Increase #paid orders						
	E1	E2	E3	E4	E5	E6	E7	E1	E2	E3	E4	E5	E6	E7	E1	E2	E3	E4	E5	E6	E7	E1	E2	E3	E4	E5	E6	E7
Hacker attacks (R14)	H	L	L	VH	L	H	H	H	L	H	VH	L	M	H	VH	L	M	VH	M	H	H	M	L	H	H	L	VL	H
Unauthorized access (R15)	H	L	L	VH	L	L	H	VH	L	H	VH	M	L	H	VH	L	L	VH	H	M	VH	VH	L	H	H	L	L	H
Process failures (R21)	H	L	H	M	M	M	M	VH	VL	H	M	M	M	H	H	VL	M	M	L	M	H	H	L	H	H	L	M	H
Lack of system security (R22)	M	VL	L	VH	M	L	L	H	VL	H	VH	M	L	L	H	VL	M	VH	L	L	M	M	L	M	H	L	VL	VL
Untrained staff (R24)	L	M	M	H	L	M	L	H	VL	M	H	M	M	M	VH	L	H	H	H	M	M	H	VL	L	M	L	M	L
Denial of service attacks (R26)	M	L	L	VH	L	H	H	M	L	H	VH	L	M	H	H	L	L	VH	M	H	M	M	L	H	H	M	VL	VL
Poor customer service (R27)	L	M	VH	VH	H	H	M	H	VL	M	VH	M	H	VH	VH	L	H	VH	M	VH	VH	H	VL	L	M	H	M	L
Miscommunication among teams (R31)	VL	M	L	M	H	L	L	M	VL	L	M	H	L	M	M	L	L	M	H	M	L	M	VL	L	L	VH	VL	M
Loss of customer´s private date (R1)	H	L	M	VH	L	H	M	H	VL	H	VH	H	H	VH	H	L	M	H	M	H	VH	M	VL	L	H	L	VH	VH

Rating of the impact of risks on the how's	Increase brand awareness							Increase themes satisfaction							Maintain uptime time						
	E1	E2	E3	E4	E5	E6	E7	E1	E2	E3	E4	E5	E6	E7	E1	E2	E3	E4	E5	E6	E7
Hacker attacks (R14)	M	L	M	VH	H	L	VH	VL	VL	L	L	M	VL	L	VH	VL	H	VH	H	H	VH
Unauthorized access (R15)	M	L	L	VH	H	L	H	VL	VL	L	L	M	VL	H	VH	VL	H	VH	VH	VH	VH
Process failures (R21)	M	VL	L	M	L	M	L	VL	VL	M	M	M	M	L	M	VL	H	VH	L	L	M
Lack of system security (R22)	M	VL	M	VH	L	L	H	VL	VL	L	L	M	VL	VL	H	VL	H	VH	L	M	M
Untrained staff (R24)	H	VL	L	H	H	M	M	VL	VL	M	M	M	M	L	L	VL	H	M	L	L	M
Denial of service attacks (R26)	M	L	M	VH	H	L	H	VL	VL	L	L	M	VL	VL	M	VL	H	H	L	H	VL
Poor customer service (R27)	VH	VL	M	VH	H	M	H	L	VL	M	L	M	H	M	VL	VL	VL	M	L	H	L
Miscommunication among teams (R31)	M	VL	L	M	VH	L	VL	VL	VL	VL	M	H	VL	VL	M	VL	VL	M	H	L	M
Loss of customer´s private date (R1)	H	VL	L	VH	M	VH	VH	VL	VL	VL	L	M	VL	VL	VL	VL	H	H	M	M	L

Figure 9.Linguistic qualification of the experts about the risks and the how´s. (Author)



Risk impact on the strategic objectives (Fuzzy number)	Subscription growth																							
	E1			E2			E3			E4			E4			E5			E6			E1		
Hacker attacks (R14)	6	7	8	2	3	4	2	3	4	8	9	10	2	3	4	6	7	8	6	7	8	6	7	8
Unauthorized access (R15)	6	7	8	2	3	4	2	3	4	8	9	10	2	3	4	2	3	4	6	7	8	8	9	10
Process failures (R21)	6	7	8	2	3	4	6	7	8	4	5	6	4	5	6	4	5	6	4	5	6	8	9	10
Lack of system security (R22)	4	5	6	0	1	2	2	3	4	8	9	10	4	5	6	2	3	4	2	3	4	6	7	8
Untrained staff (R24)	2	3	4	4	5	6	4	5	6	6	7	8	2	3	4	4	5	6	2	3	4	6	7	8
Denial of service attacks(R26)	4	5	6	2	3	4	2	3	4	8	9	10	2	3	4	6	7	8	6	7	8	4	5	6
Poor customer service (R27)	2	3	4	4	5	6	8	9	10	8	9	10	6	7	8	6	7	8	4	5	6	8	9	10
Miscommunication among teams (R31)	0	1	2	4	5	6	2	3	4	4	5	6	6	7	8	2	3	4	2	3	4	4	5	6
Loss of customer´s private date (R1)	6	7	8	2	3	4	4	5	6	8	9	10	2	3	4	6	7	8	4	5	6	6	7	8
VL	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2
L	2	3	4	2	3	4	2	3	4	2	3	4	2	3	4	2	3	4	2	3	4	2	3	4
M	4	5	6	4	5	6	4	5	6	4	5	6	4	5	6	4	5	6	4	5	6	4	5	6
H	6	7	8	6	7	8	6	7	8	6	7	8	6	7	8	6	7	8	6	7	8	6	7	8
VH	8	9	10	8	9	10	8	9	10	8	9	10	8	9	10	8	9	10	8	9	10	8	9	10

Overall risk rating: Multiplication of the experts' rating of the ratio of the risks on the specific objectives by the importance of each of the objectives	**Subscription growth**			**High CLV**			**Increase customer satisfaction rate**			**Increase # paid orders**			**Increase brand awareness**			**Increase themes satisfaction**			**Maintain uptime time**			**Risk assessment**		
Hacker attacks (R14)	4,6	5,6	6,6	4,9	5,9	6,9	5,4	6,4	7,4	3,7	4,7	5,7	4,9	5,9	6,9	1,4	2,4	3,4	6	7	8	**104**	**187**	**303**
Unauthorized access (R15)	4	5	6	5,1	6,1	7,1	5,4	6,4	7,4	4,6	5,6	6,6	4,3	5,3	6,3	2	3	4	6,6	7,6	8,6	**107**	**191**	**309**
Process failures (R21)										4,6	5,6	6,6	2,6	3,6	4,6	2,6	3,6	4,6	3,7	4,7	5,7	**89,7**	**165**	**273**
Lack of system security (R22)	=AVERAGE(B58;E58;H58;K58;N58;Q58;T58)									2,6	3,6	4,6	3,7	4,7	5,7	1,1	2,1	3,1	4,3	5,3	6,3	**76,5**	**146**	**247**
Untrained staff (R24)	3,4	4,4	5,4	4	5	6	5,1	6,1	7,1	2,9	3,9	4,9	4	5	6	2,6	3,6	4,6	2,9	3,9	4,9	**86,2**	**159**	**265**
Denial of service attacks (R26)	4,3	5,3	6,3	4,6	5,6	6,6	4,6	5,6	6,6	3,1	4,1	5,1	4,6	5,6	6,6	1,1	2,1	3,1	3,4	4,4	5,4	**90,7**	**166**	**273**
Poor customer service (R27)	5,4	6,4	7,4	5,4	6,4	7,4	6,3	7,3	8,3	3,4	4,4	5,4	5,1	6,1	7,1	3,1	4,1	5,1	2	3	4	**111**	**195**	**312**
Miscommunication among teams (R31)	2,9	3,9	4,9	3,1	4,1	5,1	3,4	4,4	5,4	2,9	3,9	4,9	2,9	3,9	4,9	1,4	2,4	3,4	2,9	3,9	4,9	**67**	**132**	**227**
Loss of customer´s private date (R1)	4,6	5,6	6,6	5,7	6,7	7,7	5,1	6,1	7,1	4,3	5,3	6,3	5,1	6,1	7,1	0,9	1,9	2,9	3,1	4,1	5,1	**104**	**184**	**299**
VL	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	**0**	**34,1**	**93,9**
L	2	3	4	2	3	4	2	3	4	2	3	4	2	3	4	2	3	4	2	3	4	**46,5**	**102**	**188**
M	4	5	6	4	5	6	4	5	6	4	5	6	4	5	6	4	5	6	4	5	6	**93**	**171**	**282**
H	6	7	8	6	7	8	6	7	8	6	7	8	6	7	8	6	7	8	6	7	8	**139**	**239**	**376**
VH	8	9	10	8	9	10	8	9	10	8	9	10	8	9	10	8	9	10	8	9	10	**186**	**307**	**469**
Weight of hows	30	42	56	31	43	57	29	41	54	25	37	50	22	32	45	15	24	36	11	20	31			
7																								

Figure 10. Fuzzy qualification of the risk impact on the strategic objectives "how´s". (Author)

4.2.7. Stage 7. Prioritizing risks.

Once the results were obtained, equation (7) was applied to get the risk prioritization index or global valuation of the risk, the results are presented in the following table (Table 16) but are not yet prioritized. Moreover, the results were given in fuzzy numbers so equation (8) was applied to obtain a non-fuzzy number and allowed the prioritization.

As Table (16) is showing, top values were established where all the risks were given an equal rating concerning the linguistic scale, i.e., one risk against each "How" took only values of VH, H, M, L, and VL. This is to define rating intervals to know limits and impacts in a better way.

One of the advantages of the FQFD is that it allows establishing reference values so that, based on the data, managers can focus their decisions on the risks with the greatest impact or, failing that, on those that they consider could be grouped.

Table 16. Risk prioritization Index. (Author)

Risk	Triangular fuzzy number RPI			RPIF
	a	b	c	
Hacker attacks (R14)	104,48	186,74	303,45	195,35
Unauthorized access (R15)	106,81	190,60	309,15	199,29
Process failures (R21)	89,72	164,73	272,77	172,99
Lack of system security (R22)	76,49	145,83	247,27	153,86
Untrained staff (R24)	86,20	159,48	265,47	167,66
Denial of service attacks (R26)	90,71	165,58	273,44	173,83
Poor customer service (R27)	111,12	194,56	312,43	203,17
Miscommunication among teams (R31)	66,99	131,64	227,48	139,44
Loss of customer´s private date (R1)	104,15	184,40	298,55	192,87
VL	0,00	34,11	93,89	40,52
L	46,49	102,32	187,77	109,73
M	92,98	170,53	281,66	178,93
H	139,47	238,75	375,55	248,13
VH	185,96	306,96	469,43	317,33

The following table (Table 17) presents the results of the prioritization of the risks according to the FQFD and the expert's responses.

Table 17. Risk prioritization with limits (Author)

Risk	RPIF
VH	317,33
H	248,13
Poor customer service (R27)	203,17
Unauthorized access (R15)	199,29
Hacker attacks (R14)	195,35
Loss of customer´s private date (R1)	192,87
M	178,93
Denial of service attacks (R26)	173,83
Process failures (R21)	172,99
Untrained staff (R24)	167,66
Lack of system security (R22)	153,86
Miscommunication among teams (R31)	139,44
L	109,73
VL	40,52

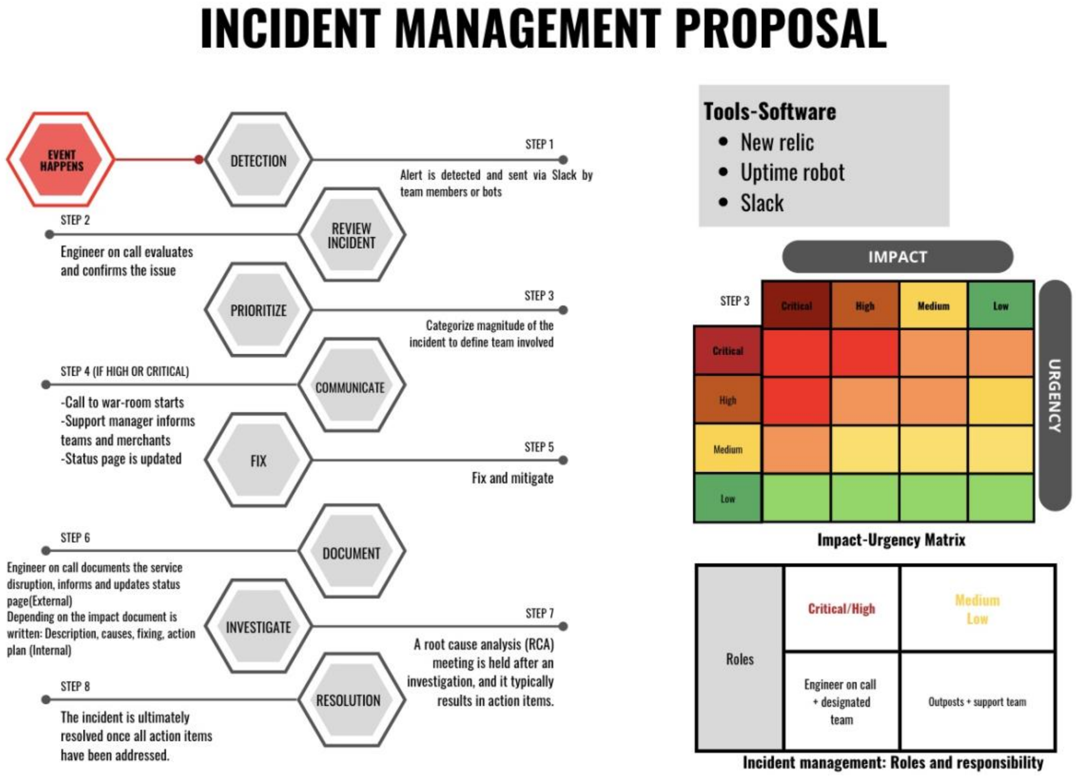
4.3.Phase III. Risk management and mitigation

As shown in Table (17), each of the 9 risks that entered the prioritization process using the FQFD methodology is between the low and high range. According to this prioritization and the method proposed, the case study company should focus its efforts on establishing mechanisms initially for the monitoring or mitigation of the first four risks because were the one who scored highest. Poor customer service (R27), Unauthorized access (R15), Hacker attacks (R14), Loss of customer's private data (R1) which are the highest rated, and then review on the remaining ones, to optimize its platform and further increase security.

An interview was conducted with the members of the infrastructure and security team of the platform to understand the current process they follow. Given the nature of the business, threads are always present on the internet therefore, they adopt risk avoidance and risk reduction as a strategy to respond to the threads. Tools of monitoring and response to attacks are currently adopted by the company. However, after interviewing the heads of each team, they manifested that although a procedure is followed, there was lack of normalization of it, therefore, an incident management process was proposed and validated by the security team for this project and is presented in Figure (11).

Lastly, although the company intents to follow the framework of ISO/IEC 27001: Information security management, they manifest that a short-term goal is to initiate the certification process.

Figure 11. Incident management process proposed. (Author)



STEP 1
Alert is detected and sent via Slack by team members or bots

STEP 2
Engineer on call evaluates and confirms the issue

STEP 3
Categorize magnitude of the incident to define team involved

STEP 4 (IF HIGH OR CRITICAL)
-Call to war-room starts
-Support manager informs teams and merchants
-Status page is updated

STEP 5
Fix and mitigate

STEP 6
Engineer on call documents the service disruption, informs and updates status page(External)
Depending on the impact document is written: Description, causes, fixing, action plan (Internal)

STEP 7
A root cause analysis (RCA) meeting is held after an investigation, and it typically results in action items.

STEP 8
The incident is ultimately resolved once all action items have been addressed.

Tools-Software
- New relic
- Uptime robot
- Slack

IMPACT / URGENCY

STEP 3	Critical	High	Medium	Low
Critical	🟥	🟥	🟧	🟧
High	🟥	🟧	🟧	🟨
Medium	🟧	🟨	🟨	🟨
Low	🟩	🟩	🟩	🟩

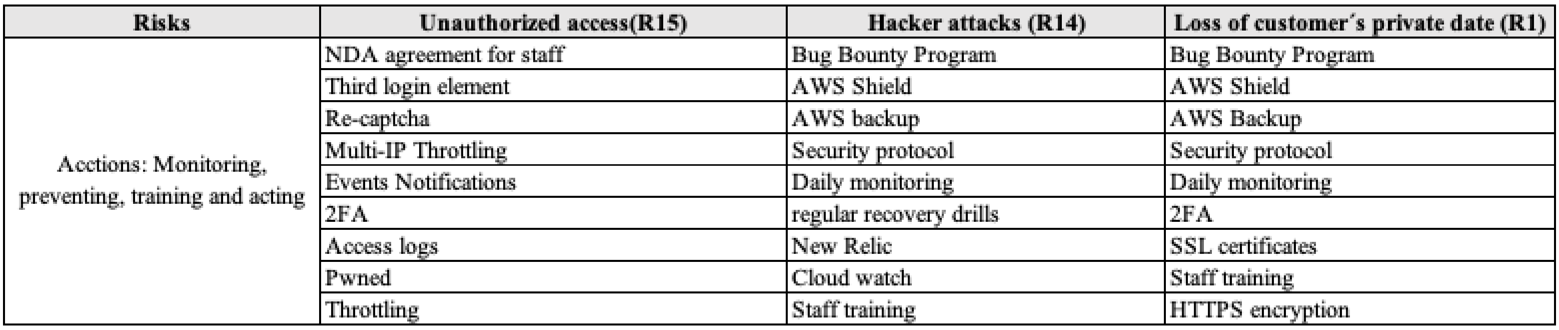
Impact-Urgency Matrix

Roles	Critical/High	Medium Low
	Engineer on call + designated team	Outposts + support team

Incident management: Roles and responsibility

As per the actions to avoid and mitigate technical risks like 14,15, and 1, the platform already has multiple software against these threats that were prioritized previously, its method and strategies are mostly for monitoring, measuring, diagnostic and acting and are shown in the following table (Table 18).

Table 18. Software and tools used by the platform to guarantee cybersecurity. (Author)

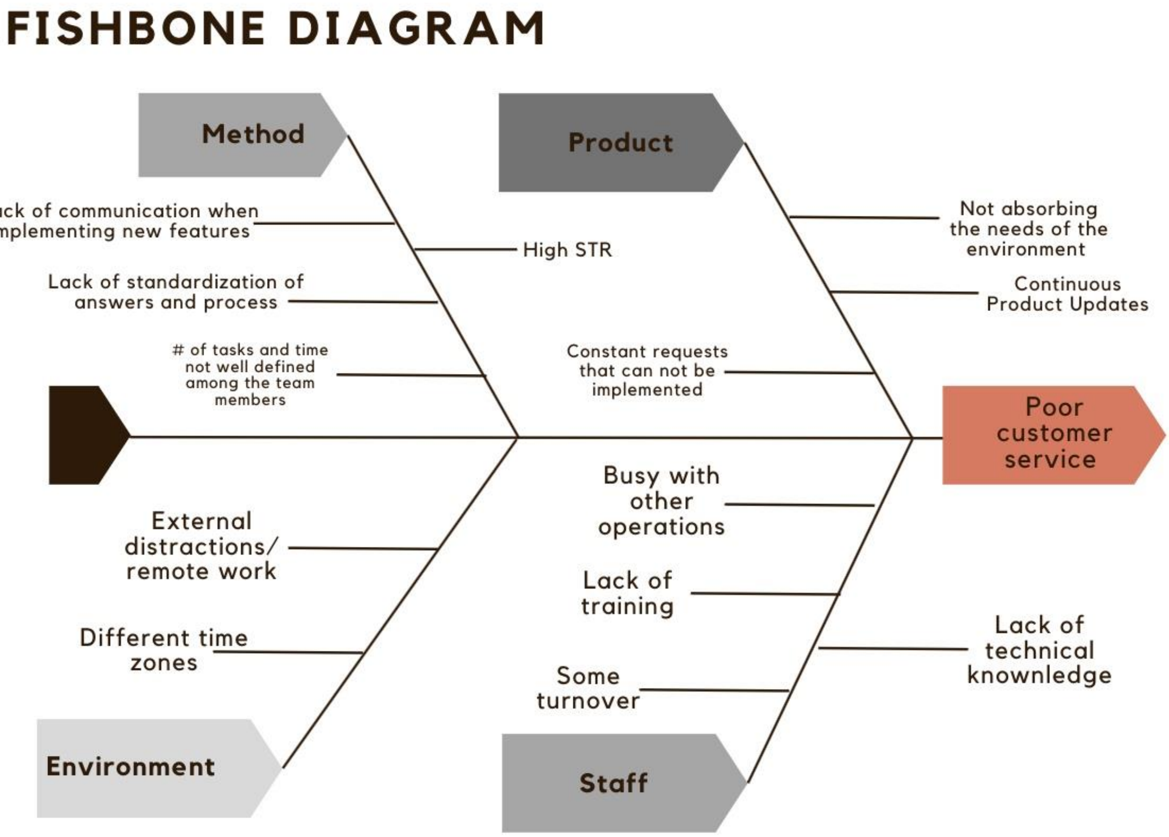


Risks	Unauthorized access(R15)	Hacker attacks (R14)	Loss of customer´s private date (R1)
Acctions: Monitoring, preventing, training and acting	NDA agreement for staff	Bug Bounty Program	Bug Bounty Program
	Third login element	AWS Shield	AWS Shield
	Re-captcha	AWS backup	AWS Backup
	Multi-IP Throttling	Security protocol	Security protocol
	Events Notifications	Daily monitoring	Daily monitoring
	2FA	regular recovery drills	2FA
	Access logs	New Relic	SSL certificates
	Pwned	Cloud watch	Staff training
	Throttling	Staff training	HTTPS encryption

On the other hand, the risk 27 "poor customer service" was the highest ranked and the one that caught the attention of the management team, since the tool was applied to the seven most experienced members of the company, the management team claimed it was interesting that the expert's results conveyed to prioritize this one as the most relevant, therefore they acknowledged the applicability of the tool since it took in consideration aspects like the actions of the human resource and the impact it had to the corporate objectives. A mitigation plan for risk 27 is proposed for this project.

- Apply a fishbone diagram from 4 axes: Method, product, environment, and staff to identify causes of risk: A meeting was held with the support team of the company and the Agile coach, four main causes were identified and analyzed, and from them, sub causes were discussed, to understand the roots of the risk and how the team could be mitigated.

Figure 12. Fisbone diagram "Poor customer service" (Author)


FISHBONE DIAGRAM
Method
Product
Lack of communication when implementing new features
High STR
Not absorbing the needs of the environment
Lack of standardization of answers and process
Continuous Product Updates
# of tasks and time not well defined among the team members
Constant requests that can not be implemented
Poor customer service
Busy with other operations
External distractions/ remote work
Lack of training
Lack of technical knowledge
Different time zones
Some turnover
Environment
Staff

Elaborate an action plan with the area and create, improve, and monitor some metrics. (See Table 19).

Table 20. Action plan Risk 27 "Poor customer service".(Author)

Cause	Actions	Responsible	Measures
Method			
Lack of communication when implementing new features	1. Promote the use of "announcements" channels 2. Each member will participate in the planning of the other teams	All team leaders and support team	Satisfaction rate % FTR average STR average Total time of resolution
Lack of standardization of answers	1. Build a common question pool and define the scope of the answer 2. Training on new features or implementations 3. Review feedback, define and improve the answer	Support team leader	
# of tasks and time not well defined among the team members	1. Track tasks defined, and tasks completed 2. Implementation of board timetable and schedule 3. More control of the timetable 4. Team lead should balance workloads	Support team leader	
High STR (second-time response)	1. Track FTR, STR, and metrics 2. Build and share the report 3. Track trends and implement improvements	Support team leader	
Product			
Continuous Product Updates	1. Communicate and build documentation on the new feature	Product Manager Business development manager	Number of business cases created Performance review of agents
Constant requests that cannot be implemented	1. Define the scope of the platform features. 2. Reply to the customers with convincing answers about why is not possible.	Support team	
Not absorbing the needs of the environment	1. Create proposals to the product team. 2. Benchmarking of platforms and creating business cases	Support team	
Staff			
Busy with other operations	1.Create a board of operations 2. Balance tasks among teams 3. Track metrics and performance	Support team leader	1. FTR average 2. Satisfaction rate 3. Completion rate
Lack of training	1. Set a goal of training per month 2. Provide training to the support team	All teams' leaders and support team leader	1. Number of trainings performed 2. Satisfaction rate
Some turnovers	1. Improve retention conditions 2. Touch base periodically	Human resources	Turnover rate
Lack of technical knowledge	1. Participate in planning and meetings of other teams 2. create programs to promote external courses	Human resources/ support team leader	Performance review of agent
Environment			
External distractions/remote work	1. Track tickets response 2. Review slack time 3. Follow up with employee	Support team leader	% Slack time Number of tickets replied/month
Different time zones	1. Coordinate timetable	General management/support team leader	

5. Discussion

E-commerce refers to the execution of commercial transactions via the internet, and it is a significant development in the modern world. To benefit from the global market, firms have increasingly moved their transactions to online platforms (Toleuuly et al. (2020). As stated before, According to the portal Statista (2021), in 2020, over two billion people purchased goods or services online, and during the same year, e-retail sales surpassed 4.2 trillion U.S. dollars worldwide. In the year of the pandemic, global retail e-commerce sales grew more than 25%. However, as e-commerce expands, risk exposure rises as well, requiring risk management. Which is a fundamental point to be addressed in this work.

This research previously talked about the trajectory of e-commerce, speaking from the revolution that made the internet what it is today, it is important to emphasize that an important point was the creation of electronic commerce platforms, which allowed multiple businesses to make these transactions to the digital world. Currently, the largest platforms have around 2.5 million merchants, but according to the literature review made, in the academy, there is still not much talk about the operational processes of the same, nor is there talk of internal risks that could lead to fatal consequences.

The literature found talks about e-commerce risk from the perspective of end customers and business owners, but few talk about platforms and their business models. That is why this paper is a case study on a prestigious platform on which the following research questions were posed:

- RQ1: How can the operational risks of an e-commerce platform be prioritized?
- RQ2: What strategies should be used to minimize or mitigate the impact of the operational risks?

To carry it out, three phases were proposed for the case study, risk identification, risk prioritization, and risk management and monitoring.

To begin with, risk identification was done through a literature review where possible risks were found in the platform where a probability-impact matrix was proposed that categorized the most serious risks and nine were those that were entered for the prioritization process. Although most of the risks were technical and cybersecurity, the experts also found events, such as communication, type of training, customer service, and attacks on physical property, as relevant risks that can affect daily operations.

The prioritization process was done through the Fuzzy QFD tool proposed by Osorio, (2011) which has 7 phases. This tool was chosen because it is flexible, uses fuzzy logic and takes into account customer requirements, and evaluates them with the company's objectives, ensuring a level of quality to meet customer expectations. To carry it out, a questionnaire was applied to users of the platform, then a list of platform experts was selected, and they were the ones who evaluated the risks based on the desires of customers and the strategic objectives of the platform, of the nine risks, identified, four obtained the highest rating and were within the medium and high range of the proposed scale: Poor customer service (R27), Unauthorized access (R15), Hacker attacks (R14), Loss of customer's private data (R1).

After applying the tool, the results of the prioritization were presented to the team leaders of the platform operations and the management team as well, to start the mitigation and management of the risk. They acknowledged and validated the application of the tool and highlighted the importance of monitoring operational risk. In this business model, the prevalence of IT is notorious but as table 13 presented us, the higher risk after prioritization for this case study is “Poor customer service” which is an important aspect and competitive advantage of this electronic commerce platform, therefore, needs to be monitored and improved.

A plan was proposed, starting with a discussion with the support team and the agile coach, a fishbone diagram was built to identify the main causes of the risk to be able to create and propose an action plan that allows the creation of some metrics to mitigate the risk.

As per the other three risks, a normalization of the incident management procedure was built and validated by the security team of the platform. They added this procedure to the policy and security page, and it was shared with the members of the company.

According to the results and the discussion held, the proposed methodology answered the research questions, moreover, it contributed to the research of electronic commerce platforms, and it also validated that regardless of the company's industry, it is vitally important to maintain a check and balance between people, technology, and internal operational processes.

6. Conclusion

Although identifying risks is a crucial and significant step, it could lose relevance without the participation of company experts who can confirm that these risks have a real impact on the performance of the organization. Given the nature of the business, it is obvious that the associated risks in the company under study are focused on cybersecurity, but an extremely crucial factor to consider is the type of employees, their access, and internal procedures which, if not monitored or defined, can generate operational risks.

Prioritization is among the most essential stages because it is the important part at which actions are directed or more focused strategies can be developed; on those risks that generate the greatest impact and have a probability of affecting the strategic objectives outlined by the company and finally being able to control, eliminate, or mitigate them.

Through the implementation of the methodology of deployment of the fuzzy quality function or FQFD, it was possible to establish the priority of the risks in terms of their impact on the strategic objectives of the company, this methodological scheme can be applied throughout any business process; in this way, the organization manages to have a clear picture of what are the critical risks associated with its processes and how to generate actions that lead to their mitigation.

Although there aren't many documents or articles in the literature review that use FQFD, it is notable it has been used to assess a process's risks and link the expertise of the personnel in charge of those risks to the strategic goals of the organization. Therefore, it is evident that the decision-making team's alignment is crucial and a key factor in determining the qualifications and ranking of the risks to be assessed.

The methodology utilized considers the knowledge and experience of the staff, in addition, fuzzy logic was applied, which enables the incorporation of the subjective components discovered in the management team ratings. It was feasible to acquire findings using these two components that take into account all the specifics of the participants' judgments, making the results more precise and enabling a tighter correlation between the models and reality.

On the other hand, it can be said that risks in e-commerce are imminent, but in the literature review, there is little research on them and their impact on platform business models.

E-commerce platforms have about 3 million merchants, there is a need to increase academic research on the operation and compliance processes of these business models. This type of platform has complex models not only at a technical and technological level but also at a logistic, regulatory, operations, and marketing level so it is a very interesting topic to study further.

Currently, the study organization, in the e-commerce sector, has good technology and good staff to deploy a process to protect against a cyber-attack, but the results of the FQFD methodology gave the company a start to better document and stabilize these processes to mitigate risk, even the recognition of the tool used to prioritize the risks gave the company an idea of the importance of generating processes with staff to train them on these aspects of security.

The company has found this work to be interesting as a result of its relevance to all of the company's processes and its potential for helping decision-makers focus their efforts.

For future work, continuing research into risk management in the electronic commerce and the electronic commerce platforms in general.

Finally, the quantification of the impact of each risk on the financial structure of the organization remains an opportunity for study, i.e. to translate the occurrence of each risk and its impact into economic or financial terms.

7. References

30 Shopify Statistics for 2021. (2021, August 20). Fundera. https://www.fundera.com/resources/shopify-statistics#

Adamovich, K. (2021, June 10). B2B, B2C, C2C, C2B and other types of business. PaySpace Magazine. https://payspacemagazine.com/tech/b2b-b2c-c2c-c2b-etc/

Aldin, N., & Stahre, F. (2003). Electronic commerce, marketing channels and logistics platforms—a wholesaler perspective. European Journal of Operational Research, 144(2), 270–279. https://doi.org/10.1016/s0377-2217(02)00393-4

Alhawari, S., Karadsheh, L., Nehari Talet, A., & Mansour, E. (2012). Knowledge-Based Risk Management framework for Information Technology project. International Journal of Information Management, 32(1), 50–65. https://doi.org/10.1016/j.ijinfomgt.2011.07.002

Alogan, G. B., & Yet[idot]ş, N. (2006, July). Defining strategic objectives: A methodology suited for public organizations. Total Quality Management &Amp; Business Excellence, 17(6), 669–684. https://doi.org/10.1080/14783360600594172

Anumba, C., & Ruikar, K. (2002). Electronic commerce in construction—trends and prospects. Automation in Construction, 11(3), 265–275. https://doi.org/10.1016/s0926-5805(01)00087-5

Aqlan, F., & Lam, S. S. (2015). A fuzzy-based integrated framework for supply chain risk assessment. International Journal of Production Economics, 161, 54–63. https://doi.org/10.1016/j.ijpe.2014.11.013

Bader, S. (2022, June 16). Common Risks with Ecommerce (and How to Avoid Them). Rewind. https://rewind.com/blog/ecommerce-risks-how-to-avoid/#:%7E:text=These%20risks%20include%20the%20unlawful,regulations%2C%20and%20customer%20service%20issues.

Bevilacqua, M., Ciarapica, F., & Giacchetta, G. (2006). A fuzzy-QFD approach to supplier selection. Journal of Purchasing and Supply Management, 12(1), 14–27. https://doi.org/10.1016/j.pursup.2006.02.001

Bigcommerce. (2022, July 21). Ecommerce 101: The History and Future of Online Shopping. BigCommerce. https://www.bigcommerce.com/articles/ecommerce/#the-future-of-ecommerce

Bolance, C., Guillén, M., Gustafsson, J., & Nielsen, J. P. (2012). Quantitative Operational Risk Models. Chapman and Hall/CRC. https://doi.org/10.1201/b11602

Borghesi, A., & Gaudenzi, B. (2012). Risk Management: How to Assess, Transfer and Communicate Critical Risks (Perspectives in Business Culture). In No Title (2013th ed.). Springer.

Bottani, E., & Rizzi, A. (2006). Strategic management of logistics service: A fuzzy QFD approach. International Journal of Production Economics, 103(2), 585–599. https://doi.org/10.1016/j.ijpe.2005.11.006

Brewster, M. (2022). Annual Retail Trade Survey Shows Impact of Online Shopping on Retail Sales During COVID-19 Pandemic. https://www.census.gov/. https://www.census.gov/library/stories/2022/04/ecommerce-sales-surged-during-pandemic.html

Caldwell, A. (2022, July 21). What Customer Lifetime Value (CLV) Is & How to Calculate It. Oracle NetSuite. Retrieved September 8, 2022, from https://www.netsuite.com/portal/resource/articles/ecommerce/customer-lifetime-value-clv.shtml

CareersinAudit.com. (2013, August 15). The Importance of Risk Management In An Organisation. https://www.careersinaudit.com/article/the-importance-of-risk-management-in-an-organisation/

de Oliveira, U. R., Marins, F. A. S., Rocha, H. M., & Salomon, V. A. P. (2017). The ISO 31000 standard in supply chain risk management. Journal of Cleaner Production, 151, 616–633. https://doi.org/10.1016/j.jclepro.2017.03.054

Deloitte. (2018). Managing Risk in Digital Transformation. https://www2.deloitte.com/it/it.html. Retrieved July 23, 2022, from https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-managing-risk-digital-transformation-1-noexp.pdf

Edwards, H. (2020, August 11). Three Key Risks To E-Commerce Businesses (And What You Can Do About Them). Forbes. https://www.forbes.com/sites/forbesbusinesscouncil/2020/08/12/three-key-risks-to-e-commerce-businesses-and-what-you-can-do-about-them/?sh=5e0876612e17

Füstös, J. T., & López, L. M. (2004). LEGAL ASPECTS OF E-COMMERCE PRACTICES IN THE UNITED STATES AND THE EUROPEAN UNION. Competitiveness Review: An International Business Journal, 14(1/2), 96–101. https://doi.org/10.1108/eb046472

Galov, N. (2022, April 29). 25 Magento Statistics You Need in 2022 to Boost Your Online Business. WebTribunal. https://webtribunal.net/blog/magento-statistics/#gref

Gento, A. M., Minambres, M. D., Redondo, A., & Perez, M. E. (2001). QFD application in a service environment: A new approach in risk management in an university. Operational Research, 1(2), 115–132. https://doi.org/10.1007/bf02936289

Guan, G. F., Dong, Q. L., & Li, C. H. (2011). Risk identification and evaluation research on F-AHP evaluation based supply chain. 2011 IEEE 18th International Conference on Industrial Engineering and Engineering Management. https://doi.org/10.1109/icieem.2011.6035447

Guevarra, L. M. (2018, July 18). E-commerce: The Past, Present, and Future. Spiralytics. https://www.spiralytics.com/blog/past-present-future-ecommerce/

Gurnani, H., Mehrotra, A., & Ray, S. (2011). Supply Chain Disruptions: Theory and Practice of Managing Risk. In No Title (2012th ed.). Springer.

Gurtu, A., & Johny, J. (2021). Supply Chain Risk Management: Literature Review. Risks, 9(1), 16. https://doi.org/10.3390/risks9010016

Hahn, G., & Kuhn, H. (2012). Designing decision support systems for value-based management: A survey and an architecture. Decision Support Systems, 53(3), 591–598. https://doi.org/10.1016/j.dss.2012.02.016

Heckmann, I., Comes, T., & Nickel, S. (2015). A critical review on supply chain risk – Definition, measure and modeling. Omega, 52, 119–132. https://doi.org/10.1016/j.omega.2014.10.004

Javaria, K., Masood, O., & Garcia, F. (2020, December 30). Strategies to manage the risks faced by consumers in developing e-commerce. Insights Into Regional Development, 2(4), 774–783. https://doi.org/10.9770/ird.2020.2.4(4)

Jílková, P., & Králová, P. (2021). Digital Consumer Behaviour and eCommerce Trends during the COVID-19 Crisis. International Advances in Economic Research, 27(1), 83–85. https://doi.org/10.1007/s11294-021-09817-4

Jin, H. (2011, August). Risk Management and Audit for E-Commerce. 2011 International Conference on Future Computer Science and Education. https://doi.org/10.1109/icfcse.2011.150

Juneja, P. (n.d.). What is Brand Awareness ? Retrieved September 8, 2022, from https://www.managementstudyguide.com/brand-awareness.htm

Jüttner, U. (2005). Supply chain risk management. The International Journal of Logistics Management, 16(1), 120–141. https://doi.org/10.1108/09574090510617385

Kayikci, Y. (2018). E-Commerce in Logistics and Supply Chain Management. Encyclopedia of Information Science and Technology, Fourth Edition, 5367–5377. https://doi.org/10.4018/978-1-5225-2255-3.ch466

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. Decision Support Systems, 44(2), 544–564. https://doi.org/10.1016/j.dss.2007.07.001

Kumar, G. S., & Jose, J. T. (2017). Developing an electronic commerce platform. 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI). https://doi.org/10.1109/icpcsi.2017.8391922

Lagkas, T. (2007). Risk Assessment and Risk Management in E-Commerce Environment. Cass Business School City of London.

Lavastre, O., Gunasekaran, A., & Spalanzani, A. (2012). Supply chain risk management in French companies. Decision Support Systems, 52(4), 828–838. https://doi.org/10.1016/j.dss.2011.11.017

Liu, Y., Chen, D. Q., & Gao, W. (2020). How does customer orientation (in)congruence affect B2B electronic commerce platform firms' performance? Industrial Marketing Management, 87, 18–30. https://doi.org/10.1016/j.indmarman.2020.02.027

Mageplaza. (2022, July 1). 10 Best eCommerce Platforms. https://www.mageplaza.com/blog/ecommerce-platform.html

Manotas-Duque, D. F., Osorio-Gómez, J. C., & Rivera, L. (2016). Operational Risk Management in Third Party Logistics (3PL). Handbook of Research on Managerial Strategies for Achieving Optimal Performance in Industrial Processes, 218–239. https://doi.org/10.4018/978-1-5225-0130-5.ch011

Manuj, I., & Mentzer, J. T. (2008). Global supply chain risk management strategies. International Journal of Physical Distribution &Amp; Logistics Management, 38(3), 192–223. https://doi.org/10.1108/09600030810866986

Markmann, C., Darkow, I. L., & von der Gracht, H. (2013). A Delphi-based risk analysis — Identifying and assessing future challenges for supply chain security in a multi-stakeholder environment. Technological Forecasting and Social Change, 80(9), 1815–1833. https://doi.org/10.1016/j.techfore.2012.10.019

McFerrin, J. (2020, April 24). The History of eCommerce: How Did it All Begin? IWD Agency. https://www.iwdagency.com/blogs/news/the-history-of-ecommerce-how-did-it-all-begin

McNichol, K. S., Greenstein, M., & Feinman, T. M. (2001). Electronic Commerce: Security, Risk Management and Control. The Journal of Risk and Insurance, 68(2), 371. https://doi.org/10.2307/2678109

Mitra, S., Karathanasopoulos, A., Sermpinis, G., Dunis, C., & Hood, J. (2015). Operational risk: Emerging markets, sectors and measurement. European Journal of Operational Research, 241(1), 122–132. https://doi.org/10.1016/j.ejor.2014.08.021

Miva. (2020, November). The History Of Ecommerce: How Did It All Begin? https://blog.miva.com/the-history-of-ecommerce-how-did-it-all-begin

Mulyati, H., & Geldermann, J. (2016). Managing risks in the Indonesian seaweed supply chain. Clean Technologies and Environmental Policy, 19(1), 175–189. https://doi.org/10.1007/s10098-016-1219-7

Nagurney, A., Cruz, J., Dong, J., & Zhang, D. (2005). Supply chain networks, electronic commerce, and supply side and demand side risk. European Journal of Operational Research, 164(1), 120–142. https://doi.org/10.1016/j.ejor.2003.11.007

Nan, J., Huo, J. Z., & Liu, H. H. (2009). Supply chain purchasing risk evaluation of manufacturing enterprise based on Fuzzy-AHP method. In 3(70772077) (pp. 1001–1005). ICICTA.

Ngai, E., & Wat, F. (2005). Fuzzy decision support system for risk analysis in e-commerce development. Decision Support Systems, 40(2), 235–255. https://doi.org/10.1016/j.dss.2003.12.002

Nguyen, J. (2022, July 1). 10 Best eCommerce Platforms. Mageplaza. https://www.mageplaza.com/blog/ecommerce-platform.html#conclusion

Nyshadham, Easwar A. and Ugbaja, Monica, "A Study of Ecommerce Risk Perceptions among B2C Consumers: A Two Country Study" (2006). BLED 2006 Proceedings. 17. https://aisel.aisnet.org/bled2006/17

Osorio-Gómez, J. C., Manotas-Duque, D. F., Rivera-Cadavid, L., & Canales-Valdiviezo, I. (2018). Operational Risk Prioritization in Supply Chain with 3PL Using Fuzzy-QFD. Management and Industrial Engineering, 91–109. https://doi.org/10.1007/978-3-319-56871-3_5

Pappas, Nikolaos. (2016). Marketing Strategies, Perceived Risks, and Consumer Trust in Online Buying Behaviour. Journal of Retailing and Consumer Services. 29. 92-103. 10.1016/j.jretconser.2015.11.007.

Pastrana-Jaramillo, C. A., & Osorio-Gómez, J. C. (2019). Operational Risk Management in a Retail Company. Intelligent Systems Reference Library, 91–107. https://doi.org/10.1007/978-3-030-26488-8_5

Quyet, C. B., & Cuong, H. C. (2017). Ecommerce risk management: analysing the case Vietnam Airlines incident. Open Science Journal, 2(4). https://doi.org/10.23954/osj.v2i4.1166

Rheude, J. (2021, January 13). The History of ECommerce. Red Stag Fulfillment. https://redstagfulfillment.com/history-of-ecommerce/

Sener, Z., & Ozturk, E. (2015). A QFD-Based Decision Model for Ship Selection in Maritime Transportation. International Journal of Innovation, Management and Technology, 6(3), 202–205. https://doi.org/10.7763/ijimt.2015.v6.602

Sharma, S., Cheng-Yuan, K., & Chuang, Y. (2016). AN APPROACH TO RISK MANAGEMENT FOR E-COMMERCE. In PACIS (Ed.), Pacific Asia Conference on Information Systems (p. 34).

Sheehan, A. (2022, March 23). The 12 Best Ecommerce Platforms for 2022. Shopify. https://www.shopify.com/blog/best-ecommerce-platforms

Shurrab, H. (2014, April). Open source E-commerce platforms . https://doi.org/10.13140/2.1.2926.2088

Sohn, S. Y., & Choi, I. S. (2001). Fuzzy QFD for supply chain management with reliability consideration. Reliability Engineering &Amp; System Safety, 72(3), 327–334. https://doi.org/10.1016/s0951-8320(01)00022-9

Soleimani, M. (2021). Buyers' trust and mistrust in e-commerce platforms: a synthesizing literature review. Information Systems and E-Business Management, 20(1), 57–78. https://doi.org/10.1007/s10257-021-00545-0

SRA. (2021, May 6). Risk Analysis Fundamental Principles from the. Society for Risk Analysis. https://www.sra.org/risk-analysis-introduction/risk-analysis-fundamental-principles/

Statista. (2022). eCommerce - United States. https://www.statista.com/outlook/dmo/ecommerce/united-states

Sutton, S., Hampton, C., Khazanchi, D., & Arnold, V. (2008). Risk Analysis in Extended Enterprise Environments: Identification of Critical Risk Factors in B2B E-Commerce Relationships. Journal of the Association for Information Systems, 9(4), 151–174. https://doi.org/10.17705/1jais.00155

Tang, C. S. (2006). Perspectives in supply chain risk management. International Journal of Production Economics, 103(2), 451–488. https://doi.org/10.1016/j.ijpe.2005.12.006

Tian, Y. (2007). History of E-Commerce. Encyclopedia of E-Commerce, E-Government, and Mobile Commerce, 559–564. https://doi.org/10.4018/9781599049434.ch001

Toleuuly, A., Yessengeldin, B., Khussainova, Z., Yessengeldina, A., Zhanseitov, A., & Jumabaeva, S. (2020). Features of E-Commerce Risk Management in Modern Conditions. Academy of Strategic Management Journal , 19(1). https://www.abacademies.org/articles/features-of-ecommerce-risk-management-in-modern-conditions-8998.html

Tummala, R., & Schoenherr, T. (2011). Assessing and managing risks using the Supply Chain Risk Management Process (SCRMP). Supply Chain Management: An International Journal, 16(6), 474–483. https://doi.org/10.1108/13598541111171165

Viehland, D. (2001). Managing Business Risk in Electronic Commerce. In AMCIS 2001 Proceedings (pp. 191–191).

Vijayaraghavan, G. (2003, May). A taxonomy of the e-commerce risks and failures. Florida Institute of Technology.

Vilko, J. P., & Hallikas, J. M. (2012). Risk assessment in multimodal supply chains. International Journal of Production Economics, 140(2), 586–595. https://doi.org/10.1016/j.ijpe.2011.09.010

Visa Asia-Pacific. (2000, April). Electronic commerce risk management merchant best practices. https://www.banksa.com.au/content/dam/bsa/downloads/Merchant_%20ecommerce_merchant.pdf

Wang, L., Juan, Y. K., Wang, J., Li, K. M., & Ong, C. (2012). Fuzzy-QFD approach based decision support model for licensor selection. Expert Systems With Applications, 39(1), 1484–1491. https://doi.org/10.1016/j.eswa.2011.08.037

Warren, M., & Hutchinson, W. (2003). A security risk management approach for e-commerce. Information Management &Amp; Computer Security, 11(5), 238–242. https://doi.org/10.1108/09685220310509028

Wee, H. M., Blos, M. F., & Yang, W. H. (2012). Risk Management in Logistics. Handbook on Decision Making, 285–305. https://doi.org/10.1007/978-3-642-25755-1_15

Westland, J. (2002). Transaction risk in electronic commerce. Decision Support Systems, 33(1), 87–103. https://doi.org/10.1016/s0167-9236(02)00010-6

Wu, T., Blackhurst, J., & Chidambaram, V. (2006). A model for inbound supply risk analysis. Computers in Industry, 57(4), 350–365. https://doi.org/10.1016/j.compind.2005.11.001

Wu, Y. (2014, May 31). Research on e-commerce security based on risk management perspective. International Journal of Security and Its Applications, 8(3), 153–162. https://doi.org/10.14257/ijsia.2014.8.3.17

Wyckoff, A., Colecchia, A., & OECD (Organisation for Economic Co-operation and Development). (1999). The Economic and Social Impact of Electronic Commerce: Preliminary Findings and Research Agenda. In No Title (Underlined, Notations). Organization for Economic Cooperation and Development.

Xu, G., Qiu, X., Fang, M., Kou, X., & Yu, Y. (2019). Data-driven operational risk analysis in E-Commerce Logistics. Advanced Engineering Informatics, 40, 29–35. https://doi.org/10.1016/j.aei.2019.03.001

Xu, S. X., & Huang, G. Q. (2016). Efficient Multi-Attribute Multi-Unit Auctions for B2B E-Commerce Logistics. Production and Operations Management, 26(2), 292–304. https://doi.org/10.1111/poms.12638

Zarei, M., Fakhrzad, M., & Jamali Paghaleh, M. (2011). Food supply chain leanness using a developed QFD model. Journal of Food Engineering, 102(1), 25–33. https://doi.org/10.1016/j.jfoodeng.2010.07.026

Zirakja, M.H., & Samizadeh, R. (2011). Risk Analysis in E-commerce via Fuzzy Logic. International Journal of Management and Business Research, 1, *99-112.*

8. Summary

Abstract

E-commerce refers to the execution of commercial transactions via the internet and has become an integral aspect of the global retail landscape in recent years. To maximize market opportunities, businesses across a range of industries have switched to e-commerce. However, the growth of e-commerce is accompanied by an increase in risk exposure, meaning that risk management is necessary and needs to be part of the e-commerce culture. Many of the firms who have chosen a digital store, have done it through the use of electronic platforms since they offer features that enable merchants to construct a branded online storefront to sell their products and services (Nguyen, 2022). However, there is not much research related to the risk management for e-commerce platforms, the literature addresses risk from the point of view of the buyers and sellers but not about the internal operations, furthermore considering more than 2.5 million users according to Fundera (2021) and Galov (2022), it is relevant to address them. In this work, a risk management proposal is presented for a recognized electronic commerce platform. The proposal includes the identification, prioritization through the application of FQFD, and lastly, a definition of action plans to mitigate or reduce the main identified risks.

Keywords: *e-commerce, risk management, e-commerce platform, risk identification, risk prioritization, risk management and monitoring*

1. Introduction: According to Quyet & Cuong, (2017) e-commerce is defined as the purchase and sale of goods, services, and exchange of information based on communications networks and the Internet.

According to the portal Statista (2021), in 2020, over two billion people purchased goods or services online, and during the same year, e-retail sales surpassed 4.2 trillion U.S. dollars worldwide. In the year of the pandemic, global retail e-commerce sales grew more than 25%.

Different companies, from the smallest to the largest ones, have already implemented a digital store that uses e-commerce platform providers to execute their digital sales strategy creating a Business to Business (B2B) relationship. An e-commerce platform is a software that allows businesses to create, host, and manage online stores. The platform offers features that enable merchants to construct a branded online storefront to sell their products and services (Nguyen, 2022). The operation process of e-commerce sales is composed of many steps that are led by different stakeholders, these are clustered in different phases but are still interconnected at the same time, in that order of ideas, it is highly relevant to guarantee the functioning of the platform, so the purchase process runs smoothly.

However, the electronic commerce environment is daily exposed to a high number of threats and risks. Understanding the nature of the exposure and finding effective treatment techniques are currently major challenges to managers in the company (McNichol et al., 2001).

Multiple articles reviewed study electronic commerce risk, probably the most popular is cyberattacking. Although information security is one of the most obvious and relevant aspects of electronic commerce, it is not the only one. For instance, inside an electronic commerce platform, there is an existing process to complete one purchase order that highly depends on technology, humans, partners, infrastructure, etc. and it needs to be taken into consideration. Therefore, a review of the operational risk needs to be carried out inside a platform. Operational risks which are associated with failures linked to people, internal processes, technology, or the effects of external processes (Tang, 2006) needs to be carried out inside a platform.

According to Fundera (2021) and Galov (2022), Shopify and Magento are some of the biggest e-commerce platforms in the world with 2.5 million merchants combined on their platforms. For instance, if any of their internal processes fail or are exposed then several consequences could occur for the merchants, the final customers, and the platform.

1.1 Research questions: The literature generally mentions the different aspects of risk in electronic commerce, but most of them are from the lenses of the customer or the owners of the stores, (Vijayaraghavan, 2003), (Pappas, 2016), (Viehland, 2001), (Nyshadham & Ugbaja 2006).

Few studies have been done on electronic commerce platforms. The innovation of this study lies in the idea of studying internally and operationally the risk from the service hub´s point of view, in this case, the electronic commerce platforms who currently have more 2.5 million users, and millions of end customers with transactions. Therefore, it is considered pertinent to further study the risks associated with the operation of this business model.

In addition to this, this project applies the FQFD proposed by Osorio (2011). A tool that considers the customer's desires and evaluates them against the strategic objectives of the business. By using a fuzzy component, the ambiguity of linguistic judgments can be resolved, and reference values can be established to prioritize risks within a specific case study, taking into account the opinions of experts.

Therefore, this research project addresses a case study of a well-known e-commerce platform, in which it will seek to propose a solution to the following research questions:

- RQ1: How can the operational risks of an e-commerce platform be prioritized?
- RQ2: What strategies should be used to minimize or mitigate the impact of the operational risks?

To do so, three main stages are taken into consideration: risk identification, risk prioritization, and risk management and monitoring. To start with the identification of a literature review of supply chain risk management (SCRM) and e-commerce platforms is conducted. The prioritization is done using the Fuzzy Quality Function Deployment (FQFD) methodology that will allow having the risks that have the greatest impact on the strategic objectives of the organization. Once the risks are prioritized it is important then to define an action plan to mitigate or avoid the occurrence of the risk to guarantee a seamless operation in the electronic commerce platform.

1.2. Case study: The company for this business case was created in 2010 in Portugal, it is a SaaS e-commerce solution, which allows small and medium-sized businesses to easily create their online stores and run their e-commerce businesses without technical knowledge.

Inside the platform, there are different teams divided into the following groups: the store, checkout, marketing, apps, support, business development, design, and development.

Although the company counts on reliable infrastructure and guarantees 99.9% of uptime to the merchants, the company needs to improve internally the procedures to follow given the presence of operational risk.

Moreover, the company has improvement objectives, which they have often left aside due to the focus on daily operations and the maintenance of processes directly related to development and servers. Therefore, an intervention is necessary to identify operational risks to correct or mitigate them.

This study is developed to fulfill the defined objectives, identifying, and prioritizing through the fuzzy QFD methodology and finally applying actions that mitigate the associated risks. The management gave their approval for the implementation of this methodology and expects that it can be associated with the parameters or improvement processes already defined in the organization.

2. Literature Review

Many businesses and organizations are losing the option to not integrate e-commerce into their operations. The Organization for Economic Cooperation and Development (OECD) defines electronic commerce as the electronic exchange of information that supports and governs commercial activities, including organizational management, commercial management, commercial negotiations and contracts, legal and regulatory frameworks, financial settlement arrangements, and taxation (Wyckoff et al., 1999). Similarly, e-commerce has the same concept as a traditional business, but it is conducted over a network of computers that can be connected through the internet globally. Hence, it can be said that e-commerce is the process of buying and selling goods or services on the Internet. It encompasses a wide variety of data, systems, and tools for online buyers and sellers, including mobile shopping and online payment encryption (Bigcommerce, 2022).

2.1. The e-commerce trajectory

The first generation of e-commerce was characterized by the development of electronic data interchange (EDI), the exchange of business documents from one computer to another in a standard format. After that, Michael Aldrich, a British engineer, connected a modified television to a computer in 1979. Aldrich then connected television to a transaction processing computer via a telephone line, thereby creating teleshopping, also known as shopping at a distance. One of the biggest, even in the development of e-commerce (Guevarra, 2018).

The second generation of e-commerce is characterized by the transaction of goods and services through the Internet, which started as a research tool, but has generally evolved into a commercial tool. (Tian 2007). The World Wide Web became accessible to the public for the first time on the Internet in 1990 (Guevarra, 2018). This was succeeded by Netscape Navigator in 1994, (where the first retail transaction occurred) and Microsoft Internet Explorer in 1995. Navigator and Explorer became the leading search engines rapidly. The creation of the browser was indeed an inflection point in the history of e-commerce since now the use of the internet was easily accessible to a broader audience. The second half of the 1990s witnessed the rise of the internet. In 1995, Amazon and eBay (originally known as AuctionWeb) went live.

As an acquired bank that handles payment processing for online retailers, auction sites, and business users, PayPal enabled worldwide e-commerce in 1998. In the same year, Alibaba, the biggest e-commerce website in China, was founded in 1999. This was a period of exponential expansion for e-commerce. Investors were awestruck by the potential of e-commerce. In the late 1990s, they invested heavily in online businesses. By 2000, the bubble had popped. Following the dot-com boom was the dot-com bust (Rheude, 2021).

Paradoxically, despite the failure of numerous Internet businesses, e-commerce sales increased in 2000 and 2001. With the revival of e-commerce, regulation merits special consideration. Consumer protection, user agreements, contracts, and privacy in e-commerce raise new concerns for the regulation of commercial activities especially as e-commerce contributes to the globalization of economic activity (Füstös & López, 2004).

Along with the increase in usage of online shopping came the evolution of online payment security. The Payment Card Industry Security Standards Council was established in 2004 to ensure that businesses adhere to security standards. In 2005, Amazon introduced Amazon Prime, a membership offering free two-day shipping on all eligible purchases within the contiguous United States for a flat annual fee. Another milestone in the history of e-commerce is the introduction of e-commerce platforms in 2006 with the origin of Shopify. An e-commerce platform is a software that allows businesses to create, host, and manage online stores. The platform offers features that enable merchants to construct a branded online storefront to sell their products and services (Nguyen, 2022). With the arrival of several technologies such as smartphones social media, Google ads even the different appearance of e-payment methods, it is clear that e-commerce is progressing at a rapid rate. The history of e-commerce demonstrates that the sector is highly dynamic. A clear example of it, is the COVID-19 pandemic in 2020. This epidemic itself influenced customer behavior. During the COVID-19 crisis, a greater proportion of consumers from each generational cohort reported making digital purchases of goods and services (Jílková & Králová, 2021)

According to Brewster (2022), e-commerce sales rose by $244.2 billion, or 43 percent, in 2020, the first year of the pandemic, growing from $571.2 billion in 2019 to $815.4 billion in 2020.

As per the future of e-commerce it is to conclude that this phenomenon is present is a highly dynamic environment, however, its usage and adoption will continue to grow. According to (Statista, 2022) e-commerce revenue is estimated to expand at a 14.56 percent annual pace, culminating in a market volume of $1,365.00 billion by 2025.

2.2. Risk Management

According to the Society for Risk Analysis (SRA 2021) glossary, risk is the potential for realization of unwanted, negative consequences of an event. A risk factor is considered as the uncertainty and unexpectedness associated with the occurrence of any event (Gurnani et al., 2011).

According to Ngai and Wat (2005) there is no official definition of risk in e-commerce. However, Viehland (2001, p.983) proposed that “electronic commerce risk is the likelihood that a negative outcome will occur in the course of developing and operating an electronic commerce strategy”.

“Risk management refers to strategies, methods, and supporting tools to identify and control risk to an acceptable level” (Alhawari et al., 2012; Gurtu & Johny, 2021) In addition, risk management may also be defined as a coordinated collection of actions and strategies that drive an organization to minimize the risk associated with attaining its objectives. Risk management has become essential to minimize corporate losses. Risk events are defined in the context of Supply Chain Risk Management (SCRM) by their probability of occurring and their repercussions within the chain (Heckmann et al., 2015)

According to Heckmann et al. (2015), supply chain risk is the potential loss of a supply chain in terms of its target values of efficiency and effectiveness due to the uncertain evolution of chain characteristics when triggering events occur. Wu et al. (2006) state that there are various ways to categorize the different types of risks, but the most important in terms of supply chain management are Internal risks and external risks. Internal risks arise from the interaction between companies throughout the supply chain and are called operational risks, such as those associated with supply, demand, and trade in credit. External risks are also called disruptive risks and are due to the interaction between the supply chain and the environment, such as natural disasters.

Risks exist in numerous types. Firstly, they may be operational and have minor implications, yet they occur frequently. They may have produced supply chain disruptions that are not viewed as major, but if they occur simultaneously or create a snowball effect, they can have severe implications (Vilko and Hallikas, 2012). This study is focused on operational risk.

Although there has been significant debate, it is generally agreed that interruptions or failures linked to people, internal processes, technology, or the effects of external processes are at the very least included (Tang, 2006).

Operational risk includes all things that can happen in day-to-day activity (Bolancé et al., 2012). As a result, risks might arise that may have an influence on the company's strategic objectives.

Manotas-Duque et al. (2016) show that a risk management system should consist of at least four phases: identification, prioritization, monitoring, and maintenance. This work is mostly about the three first phases mentioned above by Manotas, Osorio, and Rivera, and their development will be shown throughout. The first two steps are critical for risk management and have a direct impact on the measures to be taken to minimize or remove the risk.

2.2.1. Risk identification:

Risk identification is the process of discovering, defining, documenting, and communicating risks that may occur and affect the performance of the supply chain, positively or negatively (Aqlan & Lam, 2015).

Different strategies for risk identification might be employed, according to the techniques described in the literature. All of them, however, have one thing in common: the involvement of people with the knowledge and experience to identify them, and who, in this case, managerial activities and are involved in the company's operations. managerial activities and are involved in the company's operations.

2.2.2. Risk prioritization and evaluation

Prioritization of risks should be based on the company's strategic objectives, so that they are the first to be addressed and negative repercussions on the company's core may be minimized. Risk assessment and prioritizing are carried out to determine which measures should be taken to eliminate, mitigate, or ignore each of the previously identified risks.

Risk assessment can be done using quantitative or qualitative methods; however, the latter is preferred when information is exchanged among numerous people from various functions and risk perception is varied. In the literature and in practice there are several methods that combine both. The use of Fuzzy Set Theory (FST) in combination with Quality Function Deployment (QFD) is the basis for a strategic tool that seeks to respond to customer needs and translates them into engineering characteristics (Osorio-Gómez et al., 2018).

FQFD is a multi-criteria tool utilized for risk management in several articles (Osorio et al, 2017; Costantino et al., 2012; Gento et al., 2001). To better understand this tool, it is important to describe its components. As was stated before, among the multiple available tools for risk prioritization, experts are tending to combine them to close the gap that could exist given the problems that managers could face now of gathering data. On one hand, the tool is based on fuzzy logic, which allows and offers mathematical options to model the preferences defined by the experts of a characteristic process (Wang et al., 2012). On the other hand, there is the use of the QFD (Quality Function Deployment tool), a strategic technique for developing and improving goods and services based on consumer needs. This methodical procedure turns what the client requires into engineering features of the product or service, assuring a degree of quality that fulfills the customer's expectations (Sener & Ozturk, 2015)

2.2.3. Risk monitoring and management.

Risk monitoring is activated in action plans, which comprise responsible parties, dates, budgets, and activities to control the success of taken actions and contribute to the company's improvement process (Osorio et al., 2018).

According to Quyet and Cuong (2017) in e-commerce firms, risk management is the process of establishing goals and targets for protection, analyzing risks or security attacks, and exploiting vulnerabilities, measuring and ranking risk levels, and choosing countermeasures. They also stated four main strategies for risk management: Transfer of risk, Risk acceptance, Risk reduction, Risk avoidance.

2.3. E-commerce platforms operation process

As it was mentioned previously, one important event in the evolution of e-commerce is the introduction of the e-commerce platforms, this event allowed many merchants to start their journey into the e-commerce sector. According to Anumba (2002); Sharma et al. (2016) and Adamovich (2021), electronic commerce can be generally categorized into five categories: Business-to-Business (B2B), Business-to-Consumer (B2C), Business-to-Administration (B2A), Consumer-to-consumer (C2C), Consumer-to-business (C2B)

Based on the definition of Shopify, an e-commerce platform is software a business employs to handle all their B2B and B2C e-commerce needs Sheehan (2022). These needs include product pages, reviews, transactions, order fulfillment, customer support, and returns.

E-Commerce platforms provide the space and conditions for other stakeholders to co-create value and encourage participants to engage in more interactive behaviors. Strong e-commerce platforms entice an increasing number of participants to join, thereby, enhancing the network effect. (Zhang, 2022).

2.4. Operational risk in e-Commerce platforms

An e-commerce system incorporates several procedures at various levels. Tens of thousands of orders are processed, and numerous automated processes are used. These automated backend processes, which also include order tracking, inventory control, and shipping systems, are susceptible to failure. The failures might be due to their own internal software/hardware failures, engineers, upgrades, etc.; if they occurred this can have a significant impact on the business, causing major problems for the company, its reputation, and its ultimate customers (Toleuuly et al., 2020).

According to Watson, Worm, Palmatier, & Ganesan, (2015) B2B e-commerce platforms have become an important marketing channel that effectively facilitates trade between selling and buying; therefore, their contribution to the economy is high. For this, and for the amount of information exchanged, users, and money that is involved, it is pertinent to identify, prioritize, and manage the risks that are involved in the electronic commerce platform.

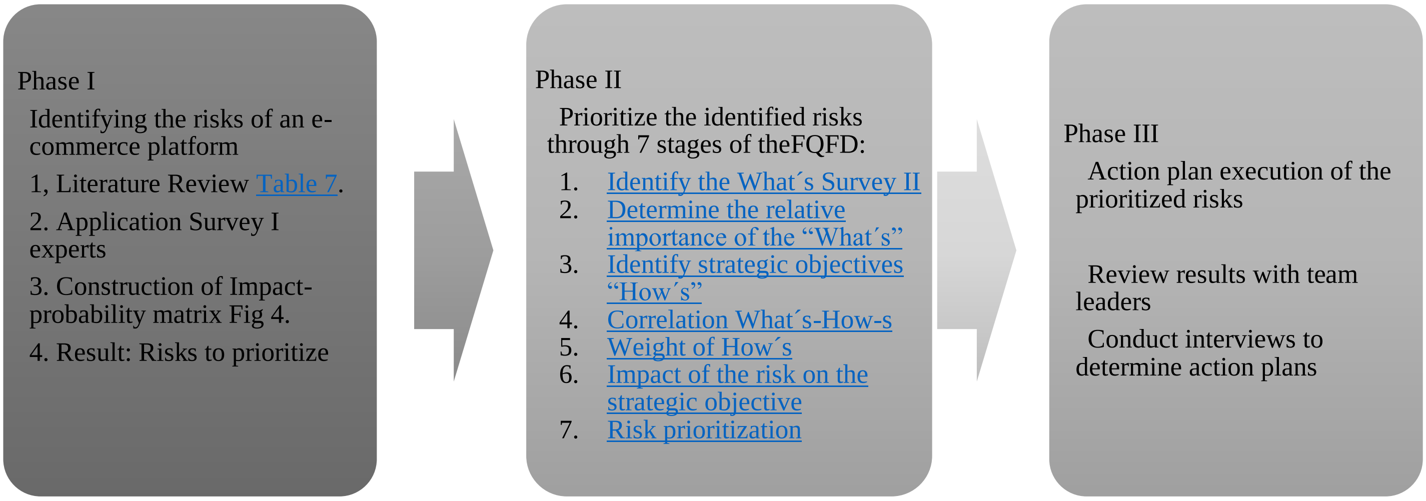
From the literature, it has been possible to identify multiple articles related to the general risk of electronic commerce from the perspective of the businesses that own a digital store and the clients of these companies, but very few related to the e-commerce platforms and the importance of the prioritization of the risks. Mostly, these platforms work as intermediary firm that facilitates multiple sellers to connect and present their products to prospective buyers. Table (3) presents the articles found in the literature that are related to risk from the perspective of sellers and buyers, electronic commerce, and electronic commerce risk management from a technical and traditional point of view:

Table 3. Literature review electronic commerce risk and platforms (Author)

Category	Article	Risk Identification	Prioritizing Risks	Risk monitoring and mitigation	Seller	Buyers	Platform
Electronic commerce risk	(Kim et al., 2008)	x				x	
	(Westland, 2002)			x	x	x	
	(Visa Asia-Pacific, 2000),	x			x		
	(Vijayaraghavan, 2003)	x	x		x		
	(Pappas, 2016)	x				x	
	(Viehland, 2001)	x	x	x	x		
	(Nyshadham & Ugbaja 2006)					x	
	(Javaria et al., 2020)	x				x	
	(Sutton et al., 2008)	x			x	x	
	(Lagkas, 2007)	x	x	x	x	x	
	Xu et al., 2019)	x		x	x		
	(Wu, 2014)	x		x	x		
	(Zirakja, 2011)	x	x	x	x		
	(Toleuuly et al., 2020)	x		x	x		
	(Quyet & Cuong, 2017),	x	x	x	x		
	(Sharma et al., 2016).	x	x	x	x	x	
	(Jin, 2011)	x	x	x	x		
Electronic commerce platforms	(Liu et al., 2020),						x
	Shurrab, 2014),						x
	(Soleimani, 2021				x	x	x
	(Kumar & Jose, 2017)						x
This study		x	x	x	x	x	x

4. Methodology

For the execution of this methodology, the article by Osorio Gómez, (2011) is taken as a reference, as well as the specific methodological proposal for prioritization described in (Osorio-Gomez et al., 2018), which determines the following phases, see structure in the following image:



Phase I

Identifying the risks of an e-commerce platform

1, Literature Review Table 7.

2. Application Survey I experts

3. Construction of Impact-probability matrix Fig 4.

4. Result: Risks to prioritize

Phase II

Prioritize the identified risks through 7 stages of theFQFD:

1. Identify the What´s Survey II
2. Determine the relative importance of the “What´s”
3. Identify strategic objectives “How´s”
4. Correlation What´s-How-s
5. Weight of How´s
6. Impact of the risk on the strategic objective
7. Risk prioritization

Phase III

Action plan execution of the prioritized risks

Review results with team leaders

Conduct interviews to determine action plans

4. Results:

Phase I: Risk identification

Literature review was applied, and the following table present the list of risks to prioritize after the survey I was applied:

Table 9. List of risks to prioritize based on probability-impact matrix

List of risks to prioritize based on probability-impact matrix			
ID	**Name**	**Description**	**Literature review**
R1	Loss of customer´s private data	Businesses that use EC should give considerable consideration to the possibility of clients losing the private information they communicate online when making a purchase. This information is typically "lost" because hackers are attempting to steal and abuse it for personal gain without the customer's consent.	(Deloitte, 2018), (Bader, 2022) (Lagkas, 2007), (Edwards, 2020)
R14	Hacker attacks	Hackers present a threat to e-businesses because they typically exploit software weaknesses to steal, destroy, or corrupt sensitive data.	(Vijayaraghavan, 2003), (Lagkas, 2007)
R15	Unauthorized Access	Unauthorized access is responsible for a substantial amount of data loss.	(Bader, 2022)
R21	Process Failures	An e-commerce system incorporates numerous processes at various stages. These include processes that handle order taking, payment processing, and order fulfillment; if they fail, they can impact an e-commerce site's ability to fulfill transactions on time and in full.	(Yuan & Peng, 2007)
R22	Lack of system security	Related to Password disclosure vulnerabilities,vurus and worms, Errors: Input Validation, Access Control, Buffer Overflow, Authentication, Configuration	(Yuan & Peng, 2007), (Deloitte, 2018)
R24	Untrained-unexperienced staff	Inadequate recruiting procedures increase the likelihood of employing untrained or inexperienced staff. Numerous positions within the EC platforms requires a high level of technical expertise so that potentially dangerous situations for the system can be dealt with appropriately.	(Yuan & Peng, 2007), (Bader, 2022),(Deloitte, 2018)
R26	Denial of service attacks	Malicious code attacks’ as a cause of system’s crashes. the situation of systems failing due to ‘site or network overload and disruption’.	(Yuan & Peng, 2007), (Vijayaraghavan, 2003), (Lagkas, 2007)
R27	Poor customer service	Poor combination of strategies, people, and technology used to provide customers of online stores. High time to response, unaccurate responses, high time to resolve, low courtesy of the agent	(eCommerce Customer Service Guide, 2017) ,(Yuan & Peng, 2007)
R31	Miscommunication among teams	All the proccesses of the ecommerce platform are interconnected, poor communication among the team could lead to failures in the operations and the communication to the external client	(Bader, 2022)

Phase II: Application of FQFD in seven stages

Stage I and II Identification of what´s and relative importance: The What´s are determined by the desires of the customers or merchants when having or choosing an electronic commerce platform. As stipulated by the company, a second survey was sent as a "newsletter" to certain users of the platform located in Colombia, 150 surveys were sent, and 55 responses were processed. The numbers were processed using fuzzy mathematics

Table 13. Weights of the what´s (triangular-fuzzy numbers)

What´s	Weight of what´s		
	Triangular fuzzy number		
	a	**b**	**c**
Subscription Price	6,09	7,09	8,09
Customer support	5,45	6,45	7,45
Store Functionality & Ease of Use	6,36	7,36	8,36
Payment Gateways integration	6,00	7,00	8,00
Shipping partners integrations	5,55	6,55	7,55
Orders management	6,36	7,36	8,36
Sales Channels	4,64	5,64	6,64
Theme Customization	5,64	6,64	7,64
Hidden cost (Commissions, locked features etc)	6,40	7,40	8,40
SEO friendliness (Own domain, Google analytics etc)	5,11	6,11	7,11

Stage III - V **Strategic objectives “How´s” and its weights.**

To determine the strategic objective or How's in this work, the OKRs (Objectives and Key Results) of each team of the platform's areas were reviewed and some of the metrics that lead to achieving the company's strategic goals were used in the same way, then a third survey was applied to identified the correlation between the what´s and how´s, the numbers were processed using fuzzy mathematics and then the calculation of the weight of the “How´s” was performed as follows the weighted average between the weight of the what's and the overall rating of the correlation divided by the number of what's (See table 15)

Table 15. Weight of the how´s (triangular fuzzy number)

How´s	Weight of how´s		
	Triangular fuzzy number		
	a	b	c
Subscription growth	29,63	41,57	55,50
High CLV	30,94	43,10	57,27
Increase customer satisfaction rate	27,95	39,57	53,19
Increase #paid orders	25,13	36,32	49,51
Increase brand awareness	21,60	32,16	44,72
Increase themes satisfaction	15,61	25,08	36,56
Maintain uptime time	10,07	18,58	29,08

Stage V- VII **Impact of the risk on the strategic objective**

The experts now need to determine the relation and impact between the risks and the how´s (strategic objectives). These responses were then translated into fuzzy numbers and processed using Fuzzy mathematics, once the results are obtained the risks are prioritized.

Table 16. Risk prioritization Index

Risk	Triangular fuzzy number RPI			RPIF
	a	b	c	
Hacker attacks (R14)	104,48	186,74	303,45	195,35
Unauthorized access (R15)	106,81	190,60	309,15	199,29
Process failures (R21)	89,72	164,73	272,77	172,99
Lack of system security (R22)	76,49	145,83	247,27	153,86
Untrained staff (R24)	86,20	159,48	265,47	167,66
Denial of service attacks (R26)	90,71	165,58	273,44	173,83
Poor customer service (R27)	111,12	194,56	312,43	203,17
Miscommunication among teams (R31)	66,99	131,64	227,48	139,44
Loss of customer´s private date (R1)	104,15	184,40	298,55	192,87
VL	0,00	34,11	93,89	40,52
L	46,49	102,32	187,77	109,73
M	92,98	170,53	281,66	178,93
H	139,47	238,75	375,55	248,13
VH	185,96	306,96	469,43	317,33

Phase III. Risk management and mitigation

Action plans and discussion were held for the four first risks that were the ones who obtained the higher values.

A plan was proposed, starting with a discussion with the support team and the agile coach, a fishbone diagram was built to identify the main causes of the risk to be able to create and propose an action plan that allows the creation of some metrics to mitigate the risk.

As per the other three risks, a normalization of the incident management procedure was built and validated by the security team of the platform. They added this procedure to the policy and security page, and it was shared with the members of the company.

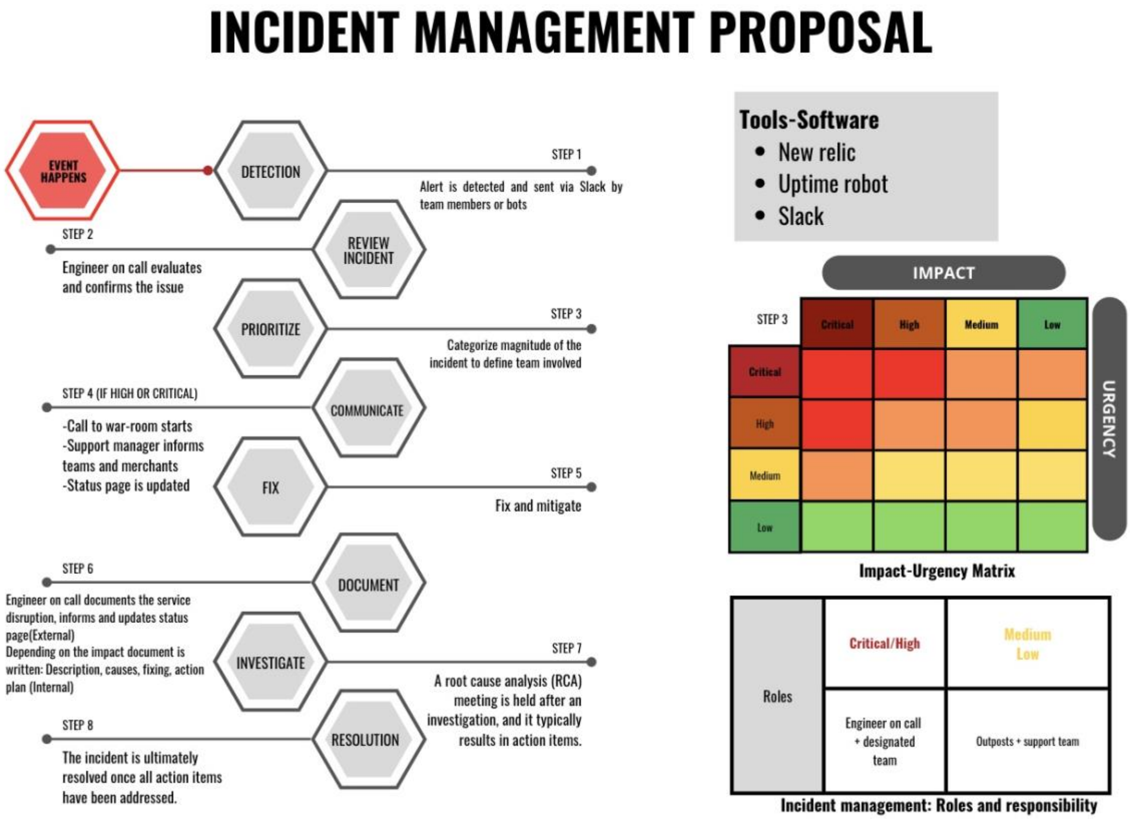
According to the results and the discussion held, the proposed methodology answered the research questions, moreover, it contributed to the research of electronic commerce platforms, and it also validated that regardless of the company's industry, it is vitally important to maintain a check and balance between people, technology, and internal operational processes. See Table (18), Table (19) and figura (12)

Table 17. Risk prioritization with limits (Author)

Risk	**RPIF**
VH	317,33
H	248,13
Poor customer service (R27)	203,17
Unauthorized access (R15)	199,29
Hacker attacks (R14)	195,35
Loss of customer´s private date (R1)	192,87
M	178,93
Denial of service attacks (R26)	173,83
Process failures (R21)	172,99
Untrained staff (R24)	167,66
Lack of system security (R22)	153,86
Miscommunication among teams (R31)	139,44
L	109,73
VL	40,52

Proposal of Incident management

Figure 11. Incident management process proposed



INCIDENT MANAGEMENT PROPOSAL

EVENT HAPPENS

DETECTION — STEP 1: Alert is detected and sent via Slack by team members or bots

REVIEW INCIDENT — STEP 2: Engineer on call evaluates and confirms the issue

PRIORITIZE — STEP 3: Categorize magnitude of the incident to define team involved

COMMUNICATE — STEP 4 (IF HIGH OR CRITICAL)
-Call to war-room starts
-Support manager informs teams and merchants
-Status page is updated

FIX — STEP 5: Fix and mitigate

DOCUMENT — STEP 6: Engineer on call documents the service disruption, informs and updates status page(External)
Depending on the impact document is written: Description, causes, fixing, action plan (Internal)

INVESTIGATE — STEP 7: A root cause analysis (RCA) meeting is held after an investigation, and it typically results in action items.

RESOLUTION — STEP 8: The incident is ultimately resolved once all action items have been addressed.

Tools-Software
- New relic
- Uptime robot
- Slack

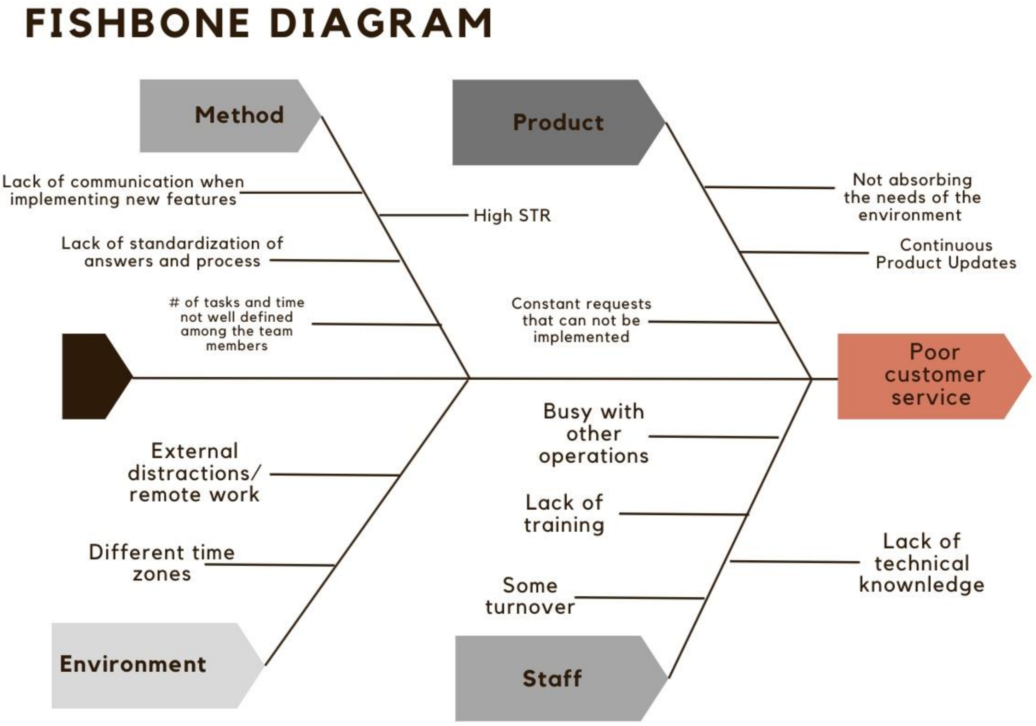
STEP 3	IMPACT: Critical	High	Medium	Low
URGENCY: Critical	🟥	🟥	🟧	🟧
High	🟥	🟧	🟧	🟨
Medium	🟧	🟨	🟨	🟨
Low	🟩	🟩	🟩	🟩

Impact-Urgency Matrix

Roles	Critical/High	Medium Low
	Engineer on call + designated team	Outposts + support team

Incident management: Roles and responsibility

Figure 12. Fishbone diagram “Poor customer service”



FISHBONE DIAGRAM

Method
- Lack of communication when implementing new features
- Lack of standardization of answers and process
- # of tasks and time not well defined among the team members

Product
- High STR
- Not absorbing the needs of the environment
- Continuous Product Updates
- Constant requests that can not be implemented

Environment
- External distractions/ remote work
- Different time zones

Staff
- Busy with other operations
- Lack of training
- Some turnover
- Lack of technical knowledge

Poor customer service

Table 19. Action plan Risk 27 "Poor customer service"

Cause	Actions	Responsible	Measures
Method			
Lack of communication when implementing new features	1. Promote the use of "announcements" channels 2. Each member will participate in the planning of the other teams	All team leaders and support team	Satisfaction rate % FTR average STR average Total time of resolution
Lack of standardization of answers	1. Build a common question pool and define the scope of the answer 2. Training on new features or implementations 3. Review feedback, define and improve the answer	Support team leader	
# of tasks and time not well defined among the team members	1. Track tasks defined, and tasks completed 2. Implementation of board timetable and schedule 3. More control of the timetable 4. Team lead should balance workloads	Support team leader	
High STR (second-time response)	1. Track FTR, STR, and metrics 2. Build and share the report 3. Track trends and implement improvements	Support team leader	
Product			
Continuous Product Updates	1. Communicate and build documentation on the new feature	Product Manager Business development manager	Number of business cases created Performance review of agents
Constant requests that cannot be implemented	1. Define the scope of the platform features. 2. Reply to the customers with convincing answers about why is not possible.	Support team	
Not absorbing the needs of the environment	1. Create proposals to the product team. 2. Benchmarking of platforms and creating business cases	Support team	
Staff			
Busy with other operations	1.Create a board of operations 2. Balance tasks among teams 3. Track metrics and performance	Support team leader	1. FTR average 2. Satisfaction rate 3. Completion rate
Lack of training	1. Set a goal of training per month 2. Provide training to the support team	All teams' leaders and support team leader	1. Number of trainings performed 2. Satisfaction rate
Some turnovers	1. Improve retention conditions 2. Touch base periodically	Human resources	Turnover rate
Lack of technical knowledge	1. Participate in planning and meetings of other teams 2. create programs to promote external courses	Human resources/ support team leader	Performance review of agent
Environment			
External distractions/remote work	1. Track tickets response 2. Review slack time 3. Follow up with employee	Support team leader	% Slack time Number of tickets replied/month
Different time zones	1. Coordinate timetable	General management/support team leader	

5. Discusion

The literature found talks about e-commerce risk from the perspective of end customers and business owners, but few talk about platforms and their business models.

To respond the two proposed research questions the following process was follow: To begin with, risk identification was done through a literature review where possible risks were found in the platform where a probability-impact matrix was proposed that categorized the most serious risks and nine were those that were entered for the prioritization process.

Although most of the risks were technical and cybersecurity, the experts also found events, such as communication, type of training, customer service, and attacks on the physical property, as relevant risks that can affect daily operations.

They acknowledged and validated the application of the tool and highlighted the importance of monitoring operational risk. In this business model, the prevalence of IT is notorious but as table 13 presented us, the higher risk after prioritization for this case study is "Poor customer service" which is an important aspect and competitive advantage of this electronic commerce platform, therefore, needs to be monitored and improved.

According to the results and the discussion held, the proposed methodology answered the research questions, moreover, it contributed to the research of electronic commerce platforms, and it also validated that regardless of the company's industry, it is vitally important to maintain a check and balance between people, technology, and internal operational processes.

6. Conclusions

Given the nature of the business, it is obvious that the associated risks in the company under study are focused on cybersecurity, but an extremely crucial factor to consider is the type of employees, their access, and internal procedures which, if not monitored or defined, can generate operational risks.

Through the implementation of the methodology of deployment of the fuzzy quality function or FQFD, it was possible to establish the priority of the risks in terms of their impact on the strategic objectives of the company, this methodological scheme can be applied throughout any business process; in this way, the organization manages to have a clear picture of what are the critical risks associated with its processes and how to generate actions that lead to their mitigation.

Currently, the study organization, in the e-commerce sector, has good technology and good staff to deploy a process to protect against a cyber-attack, but the results of the FQFD methodology gave the company a start to better document and stabilize these processes to mitigate risk, even the recognition of the tool used to prioritize the risks gave the company an idea of the importance of generating processes with staff to train them on these aspects of security.