logistics

MDPI

Article

Global Supply Chains Made Visible through Logistics Security Management

Pablo Emilio Mora Lozano [1,2] and Jairo R. Montoya-Torres [2,*]

[1] Faculty of Economics, Administratives and Accounting Sciences, Institución Universitaria Americana, Barranquilla 080002, Colombia; pmora@coruniamericana.edu.co
[2] School of Engineering, Universidad de La Sabana, Chía 250001, Colombia
* Correspondence: jairo.montoya@unisabana.edu.co

Abstract: *Background:* For several years, two of the major concerns of logistics managers are (i) the visibility of global supply chains and (ii) the uncertainty in deciding which existing logistics security program is the most appropriate according to the security levels for their organization. This last decision is needed to ensure traceability and visibility of the supply chain. The purpose of this paper is to present an analysis of the main public and private supply chain security management programs in Latin America and the Caribbean. *Methods:* A qualitative and quantitative research methodology based on thematic content analysis is followed. The four main existing security programs in Latin America and the Caribbean are systematically compared and a common general framework is developed. *Results:* The analysis shows a high degree of similarity between the levels of security contained in the selected programs. *Conclusions:* We found that there is little guidance available for companies interested in managing security risks in their supply chains through these logistics' security programs. This article contributes to the literature on logistics security programs that is currently gaining momentum in managing security risks in global supply chains and provides academic insights into the choice and/or complementarity of one or more logistics security programs.

Keywords: supply chain security; logistics security; visibility; security levels

Citation: Mora Lozano, P.E.; Montoya-Torres, J.R. Global Supply Chains Made Visible through Logistics Security Management. *Logistics* **2024**, *8*, 6. https://doi.org/10.3390/logistics8010006

Academic Editor: Robert Handfield

Received: 8 September 2023
Revised: 18 November 2023
Accepted: 27 November 2023
Published: 4 January 2024

1. Introduction

In the current economic and international context, global supply chain visibility has been a major concern for logistics and supply chain (SC) managers to keep their supply chains running smoothly and has been a global challenge for managers. Supply chain visibility is a concept that is receiving increasing attention from researchers. Increasing visibility levels in the supply chain is considered beneficial at the upstream level for suppliers and downstream level for customers [1]. Together with information sharing, they have become indispensable requirements to achieve efficient and effective supply chain management, facilitate decision making, and improve cooperation between supply chain partners [2–4]. Therefore, visibility is an outcome of external integration, which requires a dual approach that aligns increased visibility with extensive information processing capabilities of internal integration, as a complementary capability to visibility [5].

On the other hand, there are supply chain security management systems or logistics security programs based on security risk management (SCR), which allow the identification and assessment of risks to address security uncertainty affecting the smooth operation of the SC. There is a significant relationship between supply chain visibility (SCV) and supply chain risk management. Indeed, by having a clear visibility of the activities and processes throughout the supply chain with each of the actors, it allows the identification, analysis, and assessment of the risks associated with security, and allows the necessary preventive or corrective measures to be taken to mitigate potential risks that disrupt the SC. Therefore, SCV and SCR complement each other and are fundamental to achieving a resilient and secure supply chain.

While it is recognized that there is are wide range of risks that affect supply chains, we limit our scope to supply chain security risks, given the recent development of logistics security programs that are contributing to the implementation of visibility in supply chains. Thus, there is a need for supply chain managers to better understand the joint issues of risk and visibility [6], which provides risk management capabilities and, in turn, a broader view of their supply chains.

This is where the uncertainty associated with choosing which existing logistics security program is the most appropriate in terms of security criteria, costs, and benefits for the organization. In addition, this selected security program must ensure real-time visibility of the supply chain and provide faster and more effective responses to risk events.

Since 2001, a series of logistics security programs have been proliferating worldwide in both the public and private sectors. Their aim is to ensure supply chain security through the adoption and implementation of security standards in their processes. These are also called initiatives or programs for security management in the supply chain. Indeed, supply chain security (SCS) has been a key part of integrated supply chain risk management since the terrorist attacks of 11 September 2001 (commonly known as 9/11), and is a crucial factor for both companies and government authorities [7]. Clearly, it has become an important concern for both the public and private sectors [8].

Globalization has contributed to make supply chains more extensive, complex, and less visible, due to the multitude of actors involved in foreign trade processes. This makes supply chains more vulnerable to disruptions because of existing and changing threats [9]. Therefore, organizations should not only focus on optimizing logistics times and costs but also on strengthening their processes to face security risks, which lead to interruptions and affect the continuity of their business. According to Manuj and Mentzer [10], global supply chains are riskier than national supply chains due to the numerous links that interconnect a large network of companies. These links are prone to disruptions, bankruptcies, breakdowns, macroeconomic and political changes, and disasters that generate greater risks and make risk management more difficult [11].

To mitigate these risks, companies opt to implement a supply chain security management system or a logistics security program to prevent the different illicit activities to which they are exposed, and that can interrupt operations with negative results that impact their finances, their reputation, and possibly have legal effects. Several logistics security programs have been designed, but the question to be answered by both logistics and supply chain management academicians and practitioners is this: Which of the logistics security programs or initiatives should be adopted at a given organization to mitigate the risks associated with security in the supply chain? This question can be addressed by identifying the main characteristics, the benefits, and the costs of implementation of the different available logistics security programs. To understand the context of existing logistics security programs, a brief review of their origin and conceptual evolution on security in the supply chain, logistics security, and risk management in the supply chain is described next.

Currently, for Latin American and Caribbean countries, there are four main logistics security programs available, which can be adopted and implemented. While there are studies in the literature covering the topic and presenting a list of existing initiatives or programs by governmental organizations to provide responses and actions in supply chain security with their different origin agencies and specific objectives [12], there is little guidance available to companies on the best option for minimizing supply chain risks [13] through the implementation of such different logistics security programs, based on the costs of access and benefits they offer in their implementation.

This paper allows, in the first instance, to fill this gap in the existing literature, through the dissemination and clarity of good security practices offered by the different security programs (C-TPAT, AEO, BASC, and ISO 28000) against common threats in the region. This paper systematically analyzes such existing logistics security programs for Latin America and the Caribbean. This intends to become a guide for companies in order to have a

clearer view when selecting one or more logistics security programs, with the final aim of strengthening the visibility processes of their global supply chains.

In terms of scientific knowledge, this paper proposes a novel analysis, which has been non-existent to date in the literature, about the relationship between the four security programs (C-TPAT, AEO, BASC, and ISO 28000). Indeed, this paper also relates the main criminal trends that put the security of supply chains in the Latin America and the Caribbean region at risk. Subsequently, inspired by a content analysis methodology, the paper presents a review of the four main security programs, through the design of a common general framework for comparing their content in their normative structure. The research considers the relationship and analysis of the benefits offered by each program, as well as their average costs to access their respective programs.

To achieve the above-mentioned objectives, this paper is organized as follows. Section 2 overviews the literature related to the topic under study. Section 3 describes the research focus and methodology, while Section 4 focuses on the description of the selected logistics security programs. Section 5 is devoted to analyzing the main risks in global supply chain management. The findings of the study are presented in Section 6, regarding (i) the content analysis of the four selected security programs, (ii) the benefits of their implementation, and (iii) the related costs. Section 7 presents open research problems. This paper concludes in Section 8 by presenting the conclusions and discussions of the work, as well as recommendations for companies that have more than one logistics security program in their supply chain management processes.

2. Related Literature

Supply chain security management (SCSM) or logistics security has its genesis at the beginning of the 21st century, prompted by the fateful events of 11 September 2001, in the United States (i.e., airplane crashes into the Twin Towers, the Pentagon, etc.). Since then, governments and international organizations have been developing a series of programs related to supply chain security. At the same time, supply management researchers and professionals have organized and published a series of articles, books, and journals, mainly in the United States, followed by Europe, Asia, and Latin America, that contribute today to the study and knowledge of this new discipline of logistics security [12].

The World Bank, in its Supply Chain Security Guide [14], conceptualizes supply chain security (SCS) as programs, systems, procedures, technologies, and solutions applied to address threats to the supply chain and the resulting threats to the economic, social, and physical well-being of citizens and organized society. The program in this guide is understood as complex and composed of interrelated or interwoven parts, methods, procedures, systems, standards, and regulations applied to the segments or components of the supply chain to improve its security. Programs, also defined as "initiatives", can be worldwide, regional, national, governmental, sectoral, multilateral, bilateral, mandatory, or voluntary.

Pérez [15] defines supply chain security as the set of actions carried out to ensure the correct and timely functioning of supply chains, since they integrate flows of goods, information, and financial resources between different actors (producers, clients, logistics operators), very often among different and distant countries. Hintsa et al. [12] specify that a company's logistics function must integrate this new dimension of security management into its strategy and organization, reaching throughout the entire supply chain. Logistics practitioners must help the executive management team realize the importance of considering SCSM measures from product sourcing and development to final customer distribution, in order to prevent, detect, or recover from criminal acts as quickly as possible, to ensure the continuity and profitability of the company.

Therefore, Pérez [15] argues that logistics security is a topic of growing regional importance and crucial for the development of Latin America and the Caribbean due to its harmful economic and social effects. It is essential to coordinate the different public and private initiatives nationally and regionally in this matter. The disruption of a supply chain,

whether due to administrative failure, criminal, or terrorist acts, has enormous repercussions on the competitiveness of the national economy, where the direct losses produced by the event must be added to its propagation effects in the rest of the supply chain (e.g., delays and non-compliance with customers, contract losses, increase in inventory levels). Ultimately, all of these are necessary to deal with the greater variability in delivery times, among other factors, that ultimately end up aggravating national logistics costs.

Activities within the supply chain are inherently exposed to a series of risks. The ISO 31000 standard, published by the International Standard Organization (ISO), defines risk as "the effect of uncertainty on objectives" [16]. Under this definition, an effect is an impact or consequence of what is expected, whether positive, negative, or both; uncertainty is the state, even partial, of deficiency of information related to the understanding or knowledge of an event, its consequence, or its probability of occurrence; and objectives represent the different levels of the organization, products, and processes.

The Supply Chain Risk Leadership Council [17] exposes the "supply chain risk" as the probability and consequence of events at any point in the end-to-end supply chain, from sources of raw materials to end-use by customers, and "supply chain risk management (SCRM)" as the coordination of activities to direct and control the end-to-end supply chain of a company regarding supply chain risks. Supply chain risk management integrates several previous or ongoing initiatives, including those related to business continuity and supply chain security.

The U.S. National Security [18], in its declassified document Intelligence Community Standard 731-01, Supply Chain Criticality Assessments, defines supply chain risk management (SCRM) as a systematic process for managing the risk to the integrity, reliability, and authenticity of products and services within the supply chain. It addresses the activities of foreign intelligence entities and any adversary attempts aimed at compromising the supply chain. It is carried out through the identification of threats, vulnerabilities, and consequences throughout the supply chain and the development of mitigation strategies to address the respective threats.

It is important to highlight that the concepts of supply chain disruption management, supply chain vulnerability, and supply chain resilience are all also related to security in supply chains [19–30]. However, as pointed out by Williams et al. [31], the study of security issues in the supply chain is relatively new, and much of the attention to supply chain security (SCS) comes from the growing complexity and globalization of supply chains. These realities have increased the number of companies and people involved in bringing goods and services to the market.

It is clear that studies on supply chain security issues are relatively new. It was not until two decades ago that the different logistics security programs were initiated by international organizations to address these supply chain security problems, and with them a number of publications have been developed that contribute to the study and knowledge of each program.

However, there is no updated analysis in the literature on the logistics security programs under study (C-TPAT, AEO, BASC, and ISO 28000) and their relationship with each other. Between 2001 (start date of the first security program) and 2011, there is only one study conducted in 2009 by Gutierrez and Hintsa of the Cross-border Research Association (CBRA) in Lausanne, Switzerland (see [32]), where they conducted a comparative analysis of nine worldwide security initiatives, including the C-TPAT, AEO, BASC, and ISO 28000 programs, to establish their compatibility and identify the security measures that may become mandatory in the near future. Over the last decade (2012–2022), several research studies have been developed. So, an analysis of the published literature is proposed following a systematic review methodology as proposed by Tranfield et al. [33]. The steps of the review protocol are shown in Figure 1.

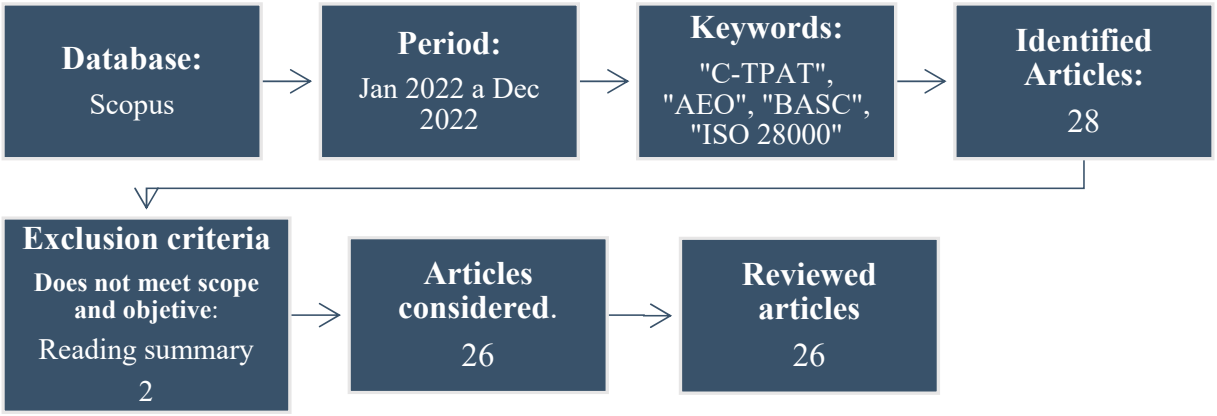

Figure 1. Literature review process (adapted from [33]).

As indicated in [33], the search process began with the selection of articles published between January 2012 and December 2022. The Scopus database was used, due to its ability to access a larger number of international open access articles. The review was performed using the keywords "C-TPAT", "AEO", "BASC", and "ISO 28000". Twenty-eight articles were obtained during the study period. After considering the exclusion criteria (only articles within the objective and scope of the research), two articles were eliminated.

To characterize the data, Table 1 was prepared with short-listed contributions over the period 2012 to 2022. The table allows us to visualize the research on these programs and define the novelty of this study.

Table 1. Papers between 2012 and 2022 studying C-TPAT, AEO, BASC, and ISO 28000 programs (source: own elaboration).

Reference	Security Initiatives				Focus
	C-TPAT	AEO	BASC	ISO 28000	
Ritchie and Melnyk (2012) [34]	X				Analysis of performance vs. level of investment in C-TPAT.
Melnyk et al. (2013) [35]	X				Decision factors for C-TPAT adoption.
Voss and Williams (2013) [36]	X				Relational security of public–private partnership (PPP) of C-TPAT. Focus is also given because C-TPAT encourages firms to voluntarily improve their security competence and that of their supply chain partners.
Herrera (2014) [37]			X		Evaluation of productivity in companies of the city of Cartagena certified in BASC, through productivity indicators.
Schramm (2015) [38]		X			Beneficiaries of the AEO program.
Blos et al. (2016) [39]				X	ISO 31000 as a complement to ISO 28000.
Ni et al. (2016) [40]	X				Motivations for the adoption of the C-TPAT program.
Chang-Bong et al. (2016) [41]		X			Factors to be taken into account when using an AEO program.

Table 1. *Cont.*

Reference	Security Initiatives				Focus
	C-TPAT	AEO	BASC	ISO 28000	
Herrera (2016) [42]			X		Evaluation of financial efficiency in BASC-certified companies in Cali, through a non-parametric approach and data envelopment analysis (DEA), specifically the CCR-O model, focused on results.
Souza et al. (2017) [43]	X				Impacts on international logistics for supply chain agents to ensure the AEO program—case of port terminals in Brazil.
Karlson (2017) [44]		X			The area of compliance management and identifies how the Authorized Economic Operator (AEO) instrument is about to transform into more mature and developed models.
Bagchi and PaulJomon (2017) [45]	X				Conducting a game between the government, an importer, and a terrorist group to measure the impact of the CTPAT program and its role in conjunction with other government policies such as espionage.
Houe and Murphy (2018) [46]		X			How an Authorized Economic Operator (AEO) certificate can affect the creation of a competitive advantage for a logistics service provider (freight forwarder) and its practical implications.
Burns (2018) [47]	X				Development of a "Participatory Operational Assessment" tool between the U.S. Department of Homeland Security and stakeholders to address operational and security challenges on both sides of the border and facilitate trade and resilience.
Chin and Sorooshian (2019) [48]				X	Identification and explanation of 16 barriers to ISO 28000 implementation.
Chin and Sorooshian (2019) [48]				X	Presents a list of pushes and pulls for the implementation of ISO 28000, considering that still many organizations in the Pahangque mining industry have not yet applied for this standard.
Dos Santos Marqués et al. (2019) [49]		X			Analysis of performance indicators related to international trade and cross-border operations from the Authorized Economic Operator (AEO) perspective.
Gupta et al. (2019) [50]	X				Empirical examination of the certification benefits associated with C-TPAT, the connection between the size of a company. The development of a framework based on drivers and barriers for companies to participate in the C-TPAT program rather than the commonly used cost–benefit analysis framework.

Table 1. *Cont.*

Reference	Security Initiatives				Focus
	C-TPAT	AEO	BASC	ISO 28000	
Erfan (2019) [51]		X			AEO programs should provide standard levels of measurable benefits that should be extended to include exemptions for certification of origin and proof of origin procedures that would provide certified companies with a competitive advantage.
Ing et al. (2019) [52]				X	Benefits to basic supply chain security that attracts industry to implement ISO 28000.
Kim et al. (2019) [53]		X			Analysis of the effect of the Authorized Economic Operator Mutual Recognition Agreement (AEO-MRA) on the performance of Korean exporters and importers.
Jażdżewska-Gutta et al. (2020) [54]		X			Motives and benefits of Authorized Economic Operator (AEO) certification in the supply chain. And significant differences in the perception of AEO status as a necessity or a privilege between cargo owners and service providers.
Zimon and Madzik (2020) [55]				X	The impact of standardized management systems (ISO 9001, ISO 14001, ISO 22000, and ISO 28000) in minimizing selected aspects of risk in the supply chain, regardless of the organization's role in the supply chain.
Kusrini et al. (2021) [56]				X	Analysis of compliance and supply chain security risks and proposed mitigation based on ISO 28001 in a logistics service provider in Indonesia.
Kusrini and Hanim (2021) [57]				X	Analysis of compliance and supply chain security risks and proposed mitigation based on ISO 28001 in a logistics service provider in Indonesia.
Tong et al. (2022) [58]	X				Empirical study focusing on if and how the adoption of C-TPAT certification could improve the operational performance of adopting companies.
This paper	X	X	X	X	To identify the main characteristics, the benefits and the costs of implementation of the different available logistics security programs

The analysis of the table leads to the hypothesis that previous work in the published academic literature over the last 10 years has not addressed the four security programs together, nor has the relationship between them been studied. The current paper hence presents a novelty that contributes to the existing body of literature on issues related to logistics security programs, which are every day gaining strength in organizations as part of global supply chains.

3. Research Focus and Methodology

Considering the aim of the present study and the research question, it was determined to develop an exploratory study on the main logistics security programs issued by different

international organizations for supply chain security management. In order to focus the research, the scope is set to be the security programs available in Latin America and the Caribbean, taking into account that Latin American companies have been experiencing a growth in their participation in international trade, due to the multiple trade agreements they have signed with countries in the region and with developed economies such as the United States and the European Union, through unilateral and discretionary tariff preferences [59].

However, this dynamic has led companies to form agile, flexible, secure, and resilient global supply chains, requiring the integration of logistics service providers and the participation of public control agencies for the development of their operations. This dynamic offers opportunities and challenges for supply chain management. One of the major challenges is to secure the supply chains against common threats in the region, through the implementation of logistics security programs available, which contribute to the visibility and management of security risks in the region's supply chains.

Taking these elements into account, the application of this study is geographically limited to this region in order to provide greater clarity and dissemination of these security programs to logistics managers when selecting the appropriate programs for the development and implementation of good security practices.

Based on this study focus, a brief description of the beginnings and evolution of each logistics security program (C-TPAT, BASC, AEO, and ISO) over the last two decades is first described, using publicly available sources of information from international organizations. It then presents the main security risks that threaten global supply chains in the Latin American and Caribbean region and their materialization in criminal actions that affect the security and continuity of operations of the companies that are part of the supply chains.

To carry out a comparison and content analysis of the selected security programs, the thematic content analysis methodology is defined with a qualitative and quantitative approach, through a general process based on six phases as proposed in [60]. These steps are: (1) data collection and preparation, (2) familiarization, (3) generating codes, (4) constructing themes or categories, (5) revising and defining the themes, and (6) producing the report. The four logistics security programs are studied, and a standard framework of security levels is developed for qualitative analysis, defining the security objectives that these programs mainly promote, represented in eight chapters and five main security requirements for each chapter, with their respective coding. Then, the General Logistics Security Management Framework is prepared with an evaluation for quantitative analysis of the four programs, using a 0/1 evaluation scale (1 if the program complies, 0 otherwise). Finally, the results of the thematic content analysis are given, represented in degrees of similarity of the four logistics security programs. This paper presents those results for the first time.

Likewise, the benefits offered by each program, as well as their average costs to access these initiatives from the public and private sectors, are described. Finally, conclusions and discussions are presented that offer greater clarity to supply chain and logistics academicians and practitioners when deciding to adopt one or more security initiatives in their organizational processes.

4. Description of the Analyzed Logistics Security Programs

Shortly after the terrorist attacks of 11 September 2001, several organizations and countries launched a series of security initiatives and regulations to improve the security of international trade [60], which have been of great interest to companies, especially in Latin America and the Caribbean (the focal region of this study), committed to safe and reliable trade. These initiatives, both voluntary and mandatory, have become an integral part of the risk management of their supply chains. Table 2 presents a comprehensive list of existing initiatives by government organizations to provide responses and actions regarding supply chain security with their respective agencies and actors. The content of the table is adapted from [12]. In addition to list the programs or initiatives, the table also presents the originating actors (public or private), the scope of supply chain actors to

be considered when implementing the program or initiative, the enforceability as being voluntary or mandatory, and an overview of actions or responses to security issues of the supply chain.

Table 2. Classification of security initiatives (source: adapted from [12]).

Initiatives/Programs	Originating Actors	Actors in the International Supply Chain	Enforceability	Action/Response
PIP (Canada) StairSec (Sweden) ACP & Frontline (Australia) AEO (European Union)	Governmental agencies	All	Voluntary	Adding a security layer to existing Customs Compliance programs
C-TPAT (USA) Secured Export Partnership (New Zealand)	Governmental agencies	All	Voluntary	Designing and implementing supply chain security programs
CSI Container Security Initiative. US customs officers control cargo in foreign ports before they arrive at US borders.	US government	Ports Terminal	Voluntary	Preventing threats at the source and using advance information
24 h rule advance manifest rule and 96 h notification of arrival vessel.		Maritime Transportation	Mandatory	
BASC (Latin America), Business Alliance for Secure Commerce. TAPA (Transported Asset Protection Association) against cargo theft.	Private sector	All	Voluntary	Companies with high-risk products or operating in risky regions designing security programs
ISPS (International Ship and Port Facility Security Code) by IMO.	International Organizations	Maritime Transportation	Mandatory	Establishing specific regulations for risky transport modes
Aviation security plan of action by ICAO.		Air Transportation	Mandatory	
AEO—Authorized Economic Operator (WCO Framework of Standards to Secure and Facilitate Global Trade).	International Organizations	All	Voluntary	Establish security standards that can be generalized for the entire customs and trading community
ISO 28000–ISO 28001 (International organization for standardization)	International Organizations	All	Voluntary	Become the leading supply chain security management standard

For the purposes of this research, four security programs have been selected, because they represent standard security criteria for risk management and prevention of illicit activities such as theft, smuggling, money laundering, terrorist financing, terrorism, drug trafficking, cargo damage, and loss, among others:

(1) Customs Trade Partnership Against Terrorism (C-TPAT) program of the U.S. Customs and Border Protection (CBP);

(2) Business Alliance for Secure Commerce (BASC) program of the BASC World Organization (WBO);
(3) Authorized Economic Operator (AEO) program of the World Customs Organization (WCO);
(4) International Standards for Supply Chain Security Management ISO 28000 and ISO 28001 of the International Organization for Standardization (ISO).

The reader must note that the security criteria of C-TPAT (Customs Trade Partnership Against Terrorism) have been an inspiration for the implementation and adoption of other supply chain security programs by the private and public sectors, as summarized in their evolutionary process in Figure 2. Indeed, the figure chronologically presents the release and updating of security programs by organizations in the last two decades, with C-TPAT being the first logistics security program issued by the U.S. Customs and Border Protection (CBP) in 2001, in response to the events of 9/11. The aim was to strengthen international supply chains and improve the country's border security. A brief overview of each of these four programs is given next.

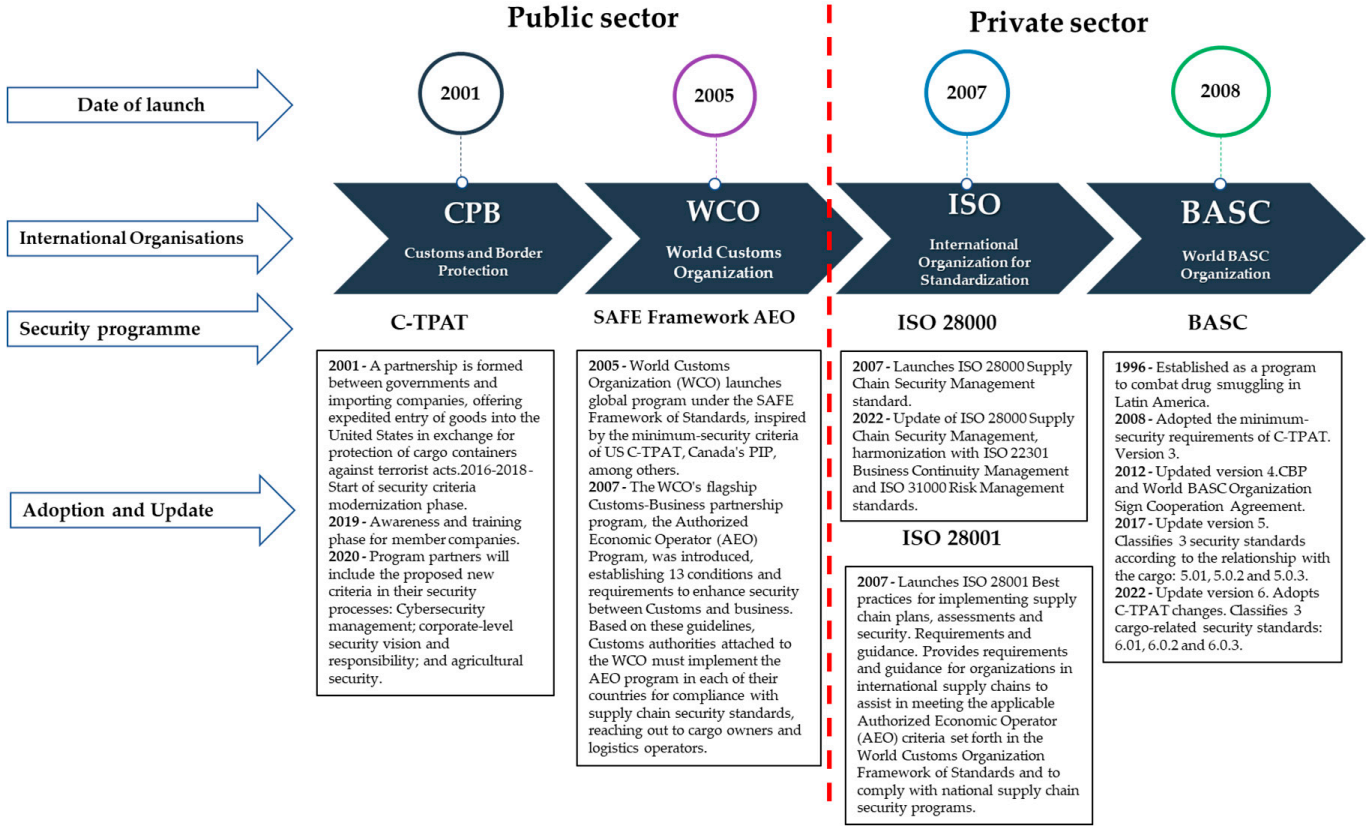

Figure 2. Evolution of the main public and private sector security programs (source: own elaboration after the works of [61–67]).

C-TPAT (Customs Trade Partnership Against Terrorism) is a voluntary program of partnership between the public and private sectors that recognizes that CBP (U.S. Customs and Border Protection) can provide the highest level of cargo security only through close cooperation with key stakeholders in the international supply chain. The C-TPAT program comprises two different program divisions: C-TPAT Security and C-TPAT Trade Compliance. The C-TPAT Security program is designed to protect the global commercial industry from terrorists and smugglers by pre-screening its participants. It applies to U.S. and non-Canadian importers, U.S. exporters, customs brokers, consolidators, port and terminal operators, air, sea, and land cargo carriers, third-party logistics providers (3PLs), Mexican long-haul truck carriers, and Canadian and Mexican manufacturers. The

C-TPAT Trade Compliance program is an optional component of the CTPAT program and adds commercial compliance aspects to the security aspects of the C-TPAT Security program [61]. The certification process begins with the interested company submitting its application to participate in the AEO Program to CBP through the C-TPAT Portal. Participants complete the security profile corresponding to the type of company and then must conduct a comprehensive self-assessment of their supply chain security procedures, using C-TPAT's minimum security criteria according to their category. Once the application and self-assessment are completed, it ends with a validation visit by a Supply Chain Security Specialist (SCSS) designated by CBP and begins to receive the benefits of the C-TPAT program. Certification is carried out annually by the CBP customs authority.

BASC (Business Alliance for Secure Commerce) is a voluntary program led by the World BASC Organization (WBO), based on an international business alliance that promotes secure trade in cooperation with governments and international organizations. Its mission is to generate a culture of security throughout the supply chain, through the implementation of management systems and instruments applicable to international trade and sectors related to the logistics chain: importers, exporters, shipping lines, container yards, logistics operators, maritime/port terminals, free zones, security and surveillance companies, customs agents, airports/airlines, and hotels. Currently, BASC has a presence through its BASC Chapters in the following countries in the Americas and the Caribbean: Colombia, Costa Rica, Ecuador, El Salvador, the United States of America, Guatemala, Mexico, Panama, Peru, the Dominican Republic, and Venezuela [62]. The certification process is carried out by each BASC Chapter in the countries where it is present and certifies those companies where there is no Chapter presence, such as Argentina, Honduras, Paraguay, and Uruguay. It begins with the request from the interested company, receiving indications of the process through the BASC Chapter where it is located, and then the company has implemented the BASC program within its processes. A security specialist designated by the corresponding Chapter validates the member company's facilities for compliance with BASC security standards and regulations for certification, with a validity of one year.

Authorized Economic Operator (AEO) is also a voluntary program driven globally by the World Customs Organization (WCO), adopted under the SAFE Framework of Standards in 2005. It consists of a series of guidelines that must be applied by customs and demanded from operators, aimed at improving security in the supply chain, reducing both the risks of intentional manipulation and accidents that could jeopardize shipments, whatever their contents may be. Then, through mutual recognition of National Authorized Economic Operator (AEO) Programs, it seeks to facilitate secure trade [63]. The SAFE Framework establishes that implementing this instrument (AEO) will not only require capacity building, but also an understanding that a gradual approach will be needed. It is not reasonable to expect every customs administration to implement the SAFE Framework immediately. While the SAFE Framework is considered a minimum set of standards, it will be implemented in several stages according to the capacity of each administration and the necessary legislative power. In this sense, the AEO program has been progressively adopted and implemented by customs authorities in countries affiliated with the WCO, under the standards issued by the SAFE Framework and according to the 2020 edition of the Compendium of Authorized Economic Operator Programs [64], developed by the WCO. There are currently 97 operational AEO programs and 20 programs under development, 33 operational Customs Compliance programs, and 4 Customs Compliance programs in the launch phase.

In Latin America and the Caribbean, there are currently around 18 countries that already have operational AEO programs (Argentina, Bolivia, Brazil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Jamaica, Honduras, Mexico, Panama, Paraguay, Peru, the Dominican Republic, and Uruguay). In the case of Venezuela, its AEO Program is still under development. The certification process is carried out after verifying that the applicant company complies with the requirements demanded by the relevant AEO program in the country. The Customs Authority grants the AEO accreditation as a

guarantee of its reliability to carry out operations with the Customs Authority. The main requirements are a satisfactory history of compliance with customs and tax requirements, accredited financial solvency, and adequate levels of security [65].

ISO 28000 is a voluntary standard for Supply Chain Security Management. It is an international standard that specifies the requirements for a security management system, including aspects relevant to the supply chain. This standard is applicable to all types and sizes of organizations (e.g., commercial businesses, government agencies, or other public agencies, and non-profit organizations) that intend to establish, implement, maintain, and improve a security management system. It provides a holistic and common approach and is not specific to an industry or sector [66]. ISO 28001 is a voluntary standard for Security Management Systems for the Supply Chain, providing best practices for implementing plans, assessments, and supply chain security. It provides requirements and guidance for organizations in international supply chains to develop and implement supply chain security processes; establish and document a minimum level of security within the supply chain or segment of a supply chain; assist in compliance with applicable Authorized Economic Operator (AEO) criteria established in the World Customs Organization Framework of Standards; and comply with national supply chain security programs. Users of ISO 28001 can define the part of an international supply chain within which they have established security; conduct security assessments in that part of the supply chain and develop appropriate countermeasures; develop and implement a supply chain security plan; and train security personnel in their security-related functions [67]. The ISO 28000 and 28001 standards are issued by the International Organization for Standardization (ISO), an independent non-governmental international organization with a membership of 167 national standardization bodies. Through its members, it brings together experts to share knowledge and develop voluntary International Standards, based on consensus and relevant to the market, supporting innovation and providing solutions to global challenges.

Currently, there are a significant number of cargo owners (importers and exporters) and logistics service providers that are part of global supply chains, which have progressively adopted the programs within their corporate processes since the official launch of security standards by international organizations. According to the following international organizations on their portals and reports for the year 2020, they record several companies in the Americas and the Caribbean with certifications of logistic security programs, including C-TPAT, BASC, AEO, and ISO 28000, as shown in Table 3.

Table 3. Certified companies in 2020 in the Americas and the Caribbean in logistics security programs C-TPAT, BASC, AEO, and ISO.

Originating Actors	Program and Date of Launch	Number of Certified Companies in 2020 in the Americas and the Caribbean	Countries of Certified Companies	Scope
U.S. CBP	C-TPAT 2001	11.400	United States Mexico Canada	U.S. importers/exporters; U.S./Canadian trucking carriers; U.S./Mexican trucking carriers; rail and ocean carriers; licensed U.S. customs brokers; U.S. marine terminal operators/port authorities; U.S. freight consolidators; ocean freight brokers; and non-operating common carriers; Mexican and Canadian manufacturers; and Mexican long-haul carriers.

Table 3. *Cont.*

Originating Actors	Program and Date of Launch	Number of Certified Companies in 2020 in the Americas and the Caribbean	Countries of Certified Companies	Scope
WBO	BASC 2008	3.800	Colombia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, Mexico, Panama, Peru, United States, Venezuela, and Guatemala.	Importers, exporters, shipping lines, container yards, logistics operators, marine/port terminals, free trade zones, security and surveillance companies, customs brokers, airports/airlines, and hotels.
WCO	AEO 2007	2.606	Argentina, Bolivia, Brazil, Chile, Colombia, Costa Rica, Cuba, Dominican Republic, Ecuador, El Salvador, Guatemala, Jamaica, Honduras, Mexico, Panama, Paraguay, Peru, and Uruguay.	Importers, exporters, freight forwarders, customs agencies, logistic operators and other stakeholders.
ISO	ISO 28000 ISO 28001 2007	162	Argentina, Bolivia Brazil, Colombia Costa Rica, Dominican Republic, Ecuador, Guatemala Mexico, Peru, and Uruguay	Importers, exporters, maritime terminals, freight forwarders, carriers, logistics operators, border crossings.

Data contained in Compendium of Authorized Economic Operator Programs, WCO 2020 edition, Survey of Authorized Economic Operator Programs in ALADI member countries with special emphasis on the requirements to obtain 2020 certification, The ISO Survey of Management System Standard Certifications 2020, and official pages of C-TPAT, BASC, and ISO.

Table 3 reflects that the ISO 28000 program has few certified companies in the region (162 companies) and 358 companies in the rest of the world, for a total of 520 companies worldwide, according to the ISO Survey of Management System Standard Certifications 2020 [68]. Despite being a standard published in 2007, there are still many companies in the world that do not apply it, due to barriers related to its implementation [48]. However, ISO launched the new version of ISO 28000 in 2021 with adjustments to its High-Level Structure (HLS) and harmonization with the ISO 22301 Business Continuity Management [69] and ISO 31000 Risk Management standards [16]. It is expected that with this new update, companies will be motivated to apply this standard and integrate it into their organizational processes.

It should be noted that the implementation of AEO programs has been progressive worldwide and especially in Latin America and the Caribbean by the customs authorities of each country since its official launch in 2007. Most of these programs date back to the last eight years on average. Table 4 presents the status of operational and developing programs, their name, launch dates, eligible actors, number of AEO certificates per country, and national authorities involved in certification.

According to the table, in the Americas and the Caribbean region, there are currently around eighteen countries that already have operational AEO Programs (Argentina, Bolivia, Brazil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Jamaica, Honduras, Mexico, Panama, Paraguay, Peru, Dominican Republic, and Uruguay). In the case of Venezuela, its AEO program is pending regulation. The implementation of these programs in the region has been gradual, as each country, through its customs authorities, issues the AEO Program in accordance with its administrative capacity and legislative powers.

Table 4. Status of operational and developing programs in Latin America and the Caribbean.

Country	Program Title	Date of Launch	Type of Operator	Number of Operators	Authorities Involved in Certification	Status
Argentina	AEO	2017	Exporters, importers, customs brokers, customs freight forwarders, and inland freight forwarders related to foreign trade.	49	AFIP–DGA	Operative
Bolivia	AEO	2015	Exporters, importers, customs brokers, freight forwarders, freight consolidators and deconsolidators, bonded warehouse concessionaire.	43	National Customs	Operative
Brasil	AEO	2014	Importer, exporter, freight forwarders, customs bonded warehouses, port and airport operators, transporters, Special Precinct for Customs Export Clearance (REDEX).	490	Receita Federal, ANVISA, VIGIAGRO, Army, ANAC, INMETRO (the last 3 under development)	Operative
Chile	AEO	2017	Exporters, importers, customs brokers, and postal service providers PSP/couriers.	19	National Customs Service.	Operative
Colombia	AEO	2011	Exporters, importers, customs agents, and ports Gradually incorporating other operators.	201	DIAN, ICA, INVIMA, National Police, Ministry of Transportation, and DIMAR	Operative
Costa Rica	Customs Facilitation for Reliable Trade Program (PROFAC)	2011	Exporters, importers, port operators, and export cargo terminals.	30	Ministry of Finance, Agriculture and Health (under negotiation)	Operative
Cuba	AEO	2016	Exporters and importers.	4	General Customs of the Republic	Operative
Ecuador	AEO	2015	Exporters and importers.	6	SENAE	Operative

Table 4. *Cont.*

Country	Program Title	Date of Launch	Type of Operator	Number of Operators	Authorities Involved in Certification	Status
El Salvador	El Salvador Authorized Economic Operator—AEO-SV	2015	Exporters, importers, customs brokers, bonded warehouse operators, postal service providers PSP/couriers, and gradually incorporating other operators.	2	Ministry of Finance	Operative
Guatemala	Guatemala Authorized Economic Operator AEO-GT	2011	All actors along the supply chain.	50	SAT	Operative
Jamaica	AEO	2014	Importers.	136	Customs, Health and Agriculture Agency	Operative
Honduras	AEO	2020	Exporters/importers. Gradually incorporating other operators.	0	Honduras Customs Administration	Operative
Mexico	AEO	2012	Exporters/importers, customs brokers, inland trucking, bonded warehouses, strategic bonded warehouses, couriers and parcels, industrial parks and logistics outsourcing.	1.073	General Administration of Foreign Trade Auditing of the SAT	Operative
Panama	AEO	2013	Importers, customs brokers, freight forwarders, warehouses and bonded warehouses, postal service providers PSP/couriers and logistics service providers.	27	Customs and all border agencies are considered support and control entities	Operative
Paraguay	AEO	2018	Exporters, importers, customs agents. Gradually incorporating other operators.	1	National Customs Office	Operative
Perú	AEO	2012	Exporters, importers, customs brokers, bonded warehouses, express delivery service companies.	164	SUNAT	Operative

Table 4. *Cont.*

Country	Program Title	Date of Launch	Type of Operator	Number of Operators	Authorities Involved in Certification	Status
Dominican Republic	AEO	2012	Exporters, importers, freight consolidators, customs brokers, warehouse operators, Free Trade Zones, manufacturers, seaports, airports and maritime transportation.	246	DGARD, Health, Agriculture, Environment, Drugs, CESPA, and the CNZFE	Operative
Uruguay	OEC Qualified Economic Operator (QEO)	2014	All actors in the supply chain.	65	National Customs Office	Operative
Venezuela	AEO	2014	Producers, manufacturers, importers, exporters, customs brokers, warehouses and bonded warehouses, postal service providers PSP/couriers, shipping agents, and port operators.	--	SENIAT	Under development

Data contained in OMA—Compendium of Authorized Economic Operator Programs, 2020 edition, and Study on Authorized Economic Operator Programs in ALADI member countries with special emphasis on the requirements to obtain 2020 certification.

5. Main Security Risks in Global Supply Chains

As pointed out before, supply chains have experienced significant growth due to a radical shift in manufacturing and marketing strategy from the past, which was dominated by "local for local". Nowadays, thanks to outsourcing procurement, manufacturing, and assembly, supply chains extend from one end of the planet to the other. This increases their complexity, to the point of preventing those who need to know what is happening from having clear visibility, leading to higher levels of risk and therefore vulnerability [16]. Supply chain security has become a major concern for supply chain professionals, and especially for global supply chains where security-related risk is a particular concern [70].

On the other hand, authors such as Young and Esqueda [71] suggest that companies have multiple forms of supply chains and the fact that global chains are inherently complex by nature, they are often inflexible and inherently vulnerable to interruptions and disturbances. Therefore, many modern supply chains around the world have been characterized by high levels of complexity and uncertainty that often expose them to supply chain disruptions [72]. These disruptions represent a risk in global supply chains. Peck and Christopher [21] suggests four categories of risks that global chains face: supply risks, demand risks, operational risks, and security risks. The latter is represented in the distribution of results related to adverse events that threaten human resources, the integrity of operations, and information systems. It can lead to outcomes such as transportation breaches, stolen data or knowledge, vandalism, crime, and sabotage [73]. Theft, smuggling, violations of intellectual property, and terrorism are just some examples of the pending threats to supply chains.

In general terms, the Supply Chain Risk Leadership Council [17] presents "supply chain risk" as the probability and consequence of events at any point in the end-to-end supply chain, from raw material sources to end use by customers. For some authors (see [73]), security risks arise in supply chains at three main moments, as shown in Table 5.

Table 5. Security risks in the major moments in the supply chain (source: [73]).

Major Moments in Supply Chains	Security Risks
Loading of trucks or other transportation means	During loading of containers onto transportation means, effective measures must ensure that neither weapons, nor explosives, nor other prohibited materials are introduced into containers.
Transportation, transshipment, and warehousing.	During transportation, the major concern is for the cargo not to be tampered with and so, the declared goods remain those, and only those, carried in the shipment.
Unloading/receiving of shipments and containers	Upon unloading/receiving of a shipment, security measures ensure that no undeclared items are added to a shipment, and also that declared items are not subtracted from the cargo. Security measures must ensure that only authorized personnel perform the intended operations, which guarantee that the declared goods are indeed those carried in a shipment.

The vulnerability of the supply chain is transmitted to the transportation network. This depends on the simple fact that transportation and freight activities physically link the facilities of a supply chain. Therefore, risks, uncertainties, and vulnerabilities in the supply chain and the transportation network affect, contribute to, and neutralize each other. Supply chain security is intended to safeguard the supply chain (in this sense, transportation and cargo activities) from different antagonistic threats and thus reduce the vulnerability of modern global trade [74].

However, there are a number of supply chain security risks that disrupt global supply chains, generated in large part by criminal activity. According to the International Criminal Police Organization (INTERPOL) 2022 Summary Report on Global Crime Trends [75], threat generators, both individually and collectively, have demonstrated their agility in overcoming obstacles and seeking opportunities to carry out illicit activities. In this context, law enforcement must be able to quickly detect and decipher the complex dynamics of ever-changing criminal markets and networks, to design and implement strategies of the utmost effectiveness aimed at preventing and combating crime. This report highlights current or emerging trends in crime and terrorism, which, due to their scope, volume, frequency, or harmful impact, pose a significant threat to transnational security. The resulting analysis points to five broad areas of crime that dominate the landscape of global crime threats and, therefore, take advantage of global supply chains to carry out some of their criminal activities. These criminal trends include organized crime, illicit trafficking (notably drug trafficking, human trafficking, and migrant smuggling), financial crimes (particularly money laundering, financial scams, and corruption, as a crucial facilitator of crimes), cybercrime (especially ransomware, phishing, and internet fraud), and terrorism. The report's findings underline that each of these five types of crimes has either remained steady or increased, particularly during the global pandemic, and continues to pose a serious threat to the security and well-being of both public and private entities and agents, from government and business organizations to individual citizens.

The main conclusions about the specific motivations and manifestations of these crime trends for the Americas and the Caribbean region are summarized in Table 6. Furthermore, the security risks that these criminal trends pose to global supply chains in Latin America

and the Caribbean are defined. It also defines the actions proposed by logistics security programs to address these crime trends.

Table 6. Crime trends in the Americas and the Caribbean Region (source: own elaboration based on data from INTERPOL Report 2022 [75]).

Trends	Americas and the Caribbean Crime Trends	Security Risks for Global Supply Chains	Actions Proposed by Logistics Security Programs
Organized Crime	• Organized crime ranked fifth among the crime trends most frequently perceived to represent a 'high' or 'very high' threat to member countries from the region. • Criminal networks and mafia-style criminal groups are present and represent an important driving force of organized crime in the region, with state actors and corruption likely playing a fundamental role in facilitating organized crime.	This threat from organized crime can be represented in different types of risks for supply chains, such as extortion, bribery, corruption, sabotage, information theft, cargo theft, and smuggling, among others.	Establish a risk management system focused on the international supply chain that anticipates illicit activities generated by organized crime, including money laundering, drug trafficking and terrorist financing, extortion, bribery, corruption, sabotage, information theft, cargo theft, smuggling, drug trafficking, cargo contamination, arms trafficking, human trafficking, and terrorism, among others. To have a demanding selection and continuous monitoring of business partners (suppliers and customers), to protect themselves from illegal activities or being involved in incidents of contamination of their supply chains. Implement oriented measures to maintain the integrity of the container and other cargo units, as well as the means of transport, in order to prevent the occurrence of security incidents. Have access control to the company's facilities, which includes control measures to prevent unauthorized access to the facilities, maintain control of employees and visitors, and protect the company's assets. As well as measures to ensure the security of all its facilities (surveillance and control of the exterior and interior perimeters). Have a personnel selection process to guarantee the knowledge of its employees. Have procedures in place to ensure the integrity and security of the processes related to the handling, storage, and transportation of cargo in the supply chain.
Illicit Trafficking	• Member countries in the region most frequently indicated illicit firearms trafficking as the crime trend perceived to pose a 'high' or 'very high' threat. • The illicit production and distribution of cocaine was the drug-related trend most frequently perceived to pose a 'high' or 'very high' threat by member countries from the region. • Human trafficking and migrant smuggling also represent pervasive criminal markets throughout the entire region.	This threat from illicit trafficking can be represented in different types of risks to supply chains, such as drug trafficking, cargo contamination, arms trafficking, and human trafficking.	
Financial Crime and Corruption	• Member countries from the region most frequently indicated money laundering as the financial crime trend perceived to represent a 'high' or 'very high' threat. • Money laundering, although a crime unto itself, is a critical crime-enabler, and financial institutions in the region have likely played a central role in laundering illicit proceeds which sustain and empower organized crime.	This threat of financial crime and corruption can be represented in different types of risks for supply chains, such as money laundering and financing of terrorism through business relationships with suppliers and customers.	

Table 6. *Cont.*

Trends	Americas and the Caribbean Crime Trends	Security Risks for Global Supply Chains	Actions Proposed by Logistics Security Programs
Cybercrime	• Ransomware was the cybercrime trend most commonly perceived by member countries to represent a 'high' or 'very high' cybercrime threat. Member countries also indicated high expectations for most cybercrime trends to escalate in the next three to five years. • OCSEA ranked third among the top ten crime trends which member countries from the region perceived as posing a 'high' or 'very high' threat.	This Cybercrime threat can be represented in different types of risks to supply chains, such as these: Cybercrime includes individual actors or groups attacking systems for financial gain or illicitly causing disruption. Cyber-attacks often involve information gathering for political, economic and/or reputational purposes. Cyberterrorism aims to weaken electronic systems to cause panic or fear.	It must have tools to ensure the traceability of the cargo from the filling point abroad to the importer's headquarters or from the warehouse to the buyer's headquarters, through satellite seals, GPS, RFID for the security of products and information within a global supply chain. Having tools to report to the competent authority in cases where irregularities or illegal or suspicious activities are detected in their international supply chains. Have measures in place to protect unauthorized access to information, documentation, and their IT systems, to maintain the confidentiality, integrity, and availability of information on their operations. Implement training programs for employees at all levels to develop the ability to maintain supply chain security by recognizing internal and external threats at every point in the chain.
Terrorism	• Politically motived terrorism, in particular, extreme far-right terrorism, has increased substantially in Western countries, and most notably in North America. While only one far-right terrorist attack was recorded in 2010, the number of such attacks peaked at 49 in 2019. Of the total deaths resulting from terrorism in North America in 2019, 87 per cent can be attributed to extreme far-right terrorism.	This threat of terrorism can be represented in different types of risks for supply chains, such as terrorist actions that consider the use of means of transportation (including the container) and facilities as a weapon or containment device for explosive, radioactive, or contaminating elements.	

However, there are other risks that translate into security risks in the international supply chain, such as the risks of natural disasters, biological disasters, inflation, and forced labor, as shown in Table 7.

Table 7. Risks that affect that translate into security risks for global supply chains. Own elaboration.

Type of Risk	Risk Description	Security Risks for Global Supply Chains	Actions Proposed by Logistics Security Programs
Natural disasters (Moody's Analytics Insights, 2022) [76]	• These are disasters caused by natural phenomena, the aggressor agent being water, wind or fire, such as earthquakes, hurricanes, fires, floods, and tsunamis, among others.	Supply chains are vulnerable to property damage and business disruption due to natural disasters. Companies need to quantify the financial and operational impact in real time and assess site-specific risks. These events lend themselves to criminal activity, such as looting, theft, and robbery of goods on the premises and/or in transport.	To have a plan that guarantees the continuity of its operations in the event of natural disasters, fires, power outages, communication and transportation failures, viruses, and inflation.

Table 7. *Cont.*

Type of Risk	Risk Description	Security Risks for Global Supply Chains	Actions Proposed by Logistics Security Programs
Biological	• Hazards related to microorganisms, viruses, bacteria, fungi, and other biological agents that can cause disease.	The biosecurity measures established by supply chain actors can have an indirect impact on the physical security of their facilities, since access controls are reduced through the use of identification cards or biometric readers that allow the registration of personnel entry and exit. Likewise, facial registration is reduced by the mandatory use of face masks through monitoring and surveillance systems.	Establish emergency and recovery plans for natural disasters. Protocols for unexpected events in land cargo transportation including unexpected stops, theft or looting of the vehicle, route deviation, road blockage, traffic accident, mechanical failure, and violation of security seals. Biosecurity protocols for the prevention and propagation of biological risks.
Inflation (Zurich Insurance Group Ltd., 2022) [77]	• Inflation measures the rate of price increases in the economy. Inflation in the supply chain can cause a ripple effect on prices, which causes supply chain costs to rise, leading to more inflation and higher prices. • Current inflationary pressure is caused by increases in production costs, such as wages, raw materials, energy, and transportation. • If the increased costs must be passed on to the buyer, then demand generally falls, so producers may require fewer goods or services.	If left unchecked, inflation can result in a severe loss of consumer or organizational purchasing power. This generates a social impact in developed and emerging countries. For the former, inflation could manifest itself, for example, in the form of higher prices for appliances, recreation, meat, travel, or motor vehicles. For the other, it could be that the prices that are rising the most are those of fuels, basic foodstuffs, and electric power [78,79], and this could somehow lead to a social standoff, where looting, theft from shops, and robbery in the transportation network could occur.	
Forced Labor (Global Slavery Index—GSI, 2023) [79]	• Modern slavery is an umbrella term that encompasses several types of exploitation, including forced labor, human trafficking, and forced marriage.	Vulnerability to modern slavery in the Americas region is largely due to inequality, political instability and discrimination against migrants and minority groups. This risk can be represented by a supplier or subcontractor in the supply chain being linked to forced labor.	Conduct a review of the hiring processes of personnel linked to their suppliers and/or subcontractors. If there is any link to forced labor activity, companies should terminate contracts and relationships with these suppliers and report them to the competent authorities as part of their social responsibility policy.

The risks referenced in the table translate into threats to global supply chains, disrupting the achievement of efficient and effective supply chain management, which must be contemplated in risk management by logistics managers in their organizations.

6. Findings

6.1. Comparison and Analysis of the Content of Logistics Security Programs

As mentioned earlier in this paper, the review of the regulatory framework focuses on the four main security programs issued by different international organizations for supply chain security management. The scope is limited to Latin America and the Caribbean. The selected programs are C-TPAT, BASC, SAFE Framework (AEO), and ISO 28000.

In order to carry out the comparison and content analysis of the selected security programs, the following general thematic content analysis process was defined using a qualitative and quantitative approach, based on six phases proposed in [60] (see Figure 3).

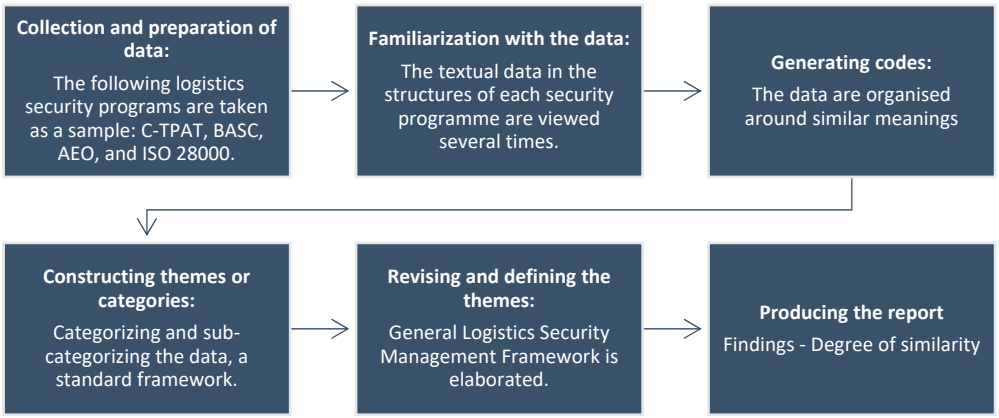

Figure 3. General process diagram of a thematic content analysis. Adapted from [60].

This diagram shows the general process of a thematic content analysis, where each of the phases is described:

Phase 1: Collection and preparation of data: In this phase, data from the four security programs C-TPAT, BASC, AEO, and ISO 28000 are collected and prepared, using publicly available sources of information from international bodies, and a description of their regulatory structure is provided in chapters representing the security levels of each program.
Phase 2: Familiarization with the data: The textual data in the structures of each security program is viewed several times. This allows you to become familiar with the information, recognize variations, and understand the context.
Phase 3: Generating codes: At this stage, the data are organized around similar meanings, coded under a deductive orientation, assigning labels called chapters and security requirements. Not all security program requirements are included in their entirety as they are irrelevant to the analysis.
Phase 4: Constructing themes or categories: Categories are created using the axial coding process. By categorizing and sub-categorizing the data, a standard framework of security levels is constructed for qualitative analysis.
Phase 5: Revising and defining the themes: Based on the standard framework of security levels, the General Logistics Security Management Framework is elaborated with an assessment for quantitative analysis of the eight chapters and 40 security requirements in the four programs. Defining an evaluation scale, if it complies it is 1, and if it does not comply, it is 0.
Phase 6: Producing the report: This final phase presents the results of the thematic content analysis, represented in degrees of similarity of the four logistics security programs.

It takes the four security programs under study, using public information sources. These programs are based on a chapter or number structure for logistics security. Table 8 presents a comparison of the contents defined by each initiative. According to the chapter or numeral structure related to the table, these programs aim at the same security and resilience objectives, with a similar structure to achieve them.

Table 8. Structure of security criteria in C-TPAT, BASC, SAFE Framework (AEO), and ISO 28000 (source: own elaboration).

C-TPAT	BASC	SAFE Framework—AEO	ISO 28000	ISO 28001
1. Security Vision and Responsibility. 2. Risk Assessment. 3. Business Partners. 4. Cybersecurity. 5. Conveyance and Instruments of International Traffic Security. 6. Seal Security. 7. Procedural Security. 8. Agricultural safety. 9. Physical security. 10. Physical access controls.	BASC norm: 1. Company context. 2. Leadership. 3. Planning. 4. Support. 5. Performance evaluation. 6. Improvement. BASC Standards 1. Associated business requirements. 2. Safety of the loading units and transport unit. 3. Safety in the cargo handling processes and other processes defined in the scope of the Control and Security Management System (CSMS).	1. Demonstrated Compliance with Customs Requirements. 2. Satisfactory System for Management of Commercial Records. 3. Financial Viability. 4. Consultation, Co-operation and Communication. 5. Measurement, Analyses and Improvement. 6. Trading Partner Security. 7. Cargo Security. 8. Premises Security. 9. Personnel Security. 10. Conveyance Security. 11. Crisis Management and Incident Recovery. 12. Information Exchange, Access and Confidentiality. 13. Education, Training and Awareness.	1. Scope. 2. Normative references. 3. Terms and definitions. 4. Context of the organization. 4.1 Understanding the organization and its context. 4.2 Understanding the needs and expectations of interested parties. 4.3 Determining the scope of the security management system. 4.4 Security management system. 5. Leadership 5.1 Leadership and commitment. 5.2 Security policy. 5.3 Roles, responsibilities, and authorities. 6. Planning. 6.1 Actions to address risks and opportunities. 6.2 Security objectives and planning to achieve them. 6.3 Planning of changes.	1. Scope. 2. Normative references. 3. Terms and definitions. 4. Field of application. 4.1 Statement of application. 4.2 Business partners. 4.3 Internationally accepted certificates or approvals. 4.4 Business partners exempt from security declaration requirement. 4.5 Security reviews of business partners. 5. Supply chain security process. 5.1 General. 5.2 Identification of the scope of security assessment. 5.3 Conduction of the security assessment. 5.4 Development of the supply chain security plan. 5.5 Execution of the supply chain security plan. 5.6 Documentation and monitoring of the supply chain security process.

Table 8. *Cont.*

C-TPAT	BASC	SAFE Framework—AEO	ISO 28000	ISO 28001
11. Personnel security. 12. Education, Training and Awareness. CTPAT Foreign MSC-Minimum Security Criteria CBP (version 2020).	4. Safety in the processes related to the Personnel. 5. Access Control and Physical Security. 6. Information Security. Implementation Guide for BASC International Standards and Norms Version 6—World BASC Organization (2022 version).	Based on this standard, the customs authorities attached to the WCO adopt and implement the Authorized Economic Operator program in their countries. SAFE Framework of Standards World Customs Organization—WCO. ANNEX V: Resolution of the Customs Cooperation Council on the SAFE Framework of Standards to Secure and Facilitate World Trade (version 2021).	7. Support 7.1 Resources. 7.2 Competence. 7.3 Awareness. 7.4 Communication. 7.5 Documented information. 8. Operation 8.1 Operational planning and control. 8.2 Dentification of processes and activities. 8.3 Risk assessment and treatment. 8.4 Controls. 8.5 Security strategies, procedures, processes, and treatments. 8.6 Security plans. 9. Performance evaluation 9.1 Monitoring, measurement, analysis, and evaluation. 9.2 Internal audit. 9.3 Management review. 10. Improvement. 10.1 Continual improvement. 10.2 Nonconformity and corrective action. ISO 28000:2022—Security and resilience—Security management systems—Requirements	5.7 Actions required after a security incident. 5.8 Protection of the security information. ISO 28001:2007 Security management systems for the supply chain; Best practices for implementing supply chain security, assessments, and plans; Requirements and guidance.

According to the structures of the security programs outlined above, there is a great similarity in terms of the level of security measures and controls to be implemented. However, the ISO 28000 program provides a structure that translates into procedures, activities, controls, tools, and technologies, leaving it up to each company to adopt within the processes the security measures it considers necessary to guarantee the security of the supply chain. Despite these differences, it is observed that the programs promote the following security objectives or chapters: risk management, physical security, access control, personnel security, education and training, procedural security, document handling security, trading partner security, transport security, crisis management, and disaster recovery [7]. Each chapter or number in these programs has a set of minimum requirements or security measures represented in procedures, activities, controls, tools, and technologies that "must" or "should" be implemented within the organization's processes. According to ISO, the word "must" implies a mandatory requirement, while the word "should" suggests an action.

Based on the above, the following Security Level Standard Framework is elaborated for qualitative analysis, which includes the codification of the common chapters or numbers and the main minimum security requirements (not all security program requirements are included in their entirety as they are irrelevant for the analysis). Eight chapters and five main security requirements are defined for each chapter, with their respective codification. This is shown in Table 9.

Table 9. Standard Security Level Framework (source: own elaboration).

Chapter/Item	Security Objectives	ID/Principal Minimum Security Criteria
1. Risk management.	Manage risks through context analysis, risk assessment, risk treatment, monitoring, and review to mitigate the likelihood and impact of security risks to which global supply chains are exposed and be consistent with security policies.	1.1 Must have a security management policy focused on risk assessment to ensure supply chain security. 1.2 The policy should have security management objectives, goals, and programs. 1.3 It should have a risk management system focused on the supply chain. 1.4 It should disseminate the security policy to stakeholders through the company's website, be posted within the company (bulletin board, email, etc.) in key locations. 1.5 Should have documented procedures for crisis management, business continuity and recovery plans.
2. Knowledge of business partners/business associates.	Ensure a reliable selection and evaluation of business partners (customers and suppliers) to protect against activities related to money laundering and terrorist financing, as well as those actions that may affect the security and integrity of the goods carried out by logistics operators.	2.1 Must have documented procedures for purchasing, selection, and contracting of suppliers that guarantee their reliability. 2.2 Must have documented procedures for customer selection and contracting that guarantee their reliability. 2.3 It must carry out security visits to the facilities where its business partners carry out their operations, to verify that they have implemented security measures in the international supply chain. 2.4 It must issue security agreements for those trading partners that do not have security program certificates from other international public or private organizations. 2.5 The company and its members (managers) should have their background checked against national and international lists for the prevention of crimes related to money laundering and terrorism.

Table 9. *Cont.*

Chapter/Item	Security Objectives	ID/Principal Minimum Security Criteria
3. Conveyance and transportation unit security.	Maintain the integrity of containers and other cargo units, as well as means of transport, to protect them against the occurrence of security incidents.	3.1 Must have documented procedures and controls to ensure the integrity of containers and other cargo units at the point of filling to protect them against the introduction of unauthorized persons or materials. 3.2 Shall use security seals under the standards contained in the current ISO 17712 standard on containers and other sealable cargo units. 3.3 Inspect the physical integrity of the container structure (internal and external) and other cargo units, as well as the means of transport. A documentary record of the inspection shall be kept by the person responsible for the activity. 3.4 Ensure that the areas where containers and other cargo units (full or empty) are stored are secure and prevent unauthorized access and/or manipulation. 3.5 Have procedures in place to detect and report unauthorized entry to containers and other cargo units, as well as when security seals have been breached.
4. Physical access controls and physical security.	Prevent unauthorized access to the facilities and ensure the security of the facilities through surveillance and perimeter control, especially in critical areas of the company.	4.1 Have documented procedures and measures to identify and control access of people and vehicles to the facilities. 4.2 Provide all related personnel with an identification or access device for entry to the facilities. 4.3 Require visitors to identify themselves for entry to the facilities and provide them with an identification or temporary access device. 4.4 Check persons, vehicles, packages, bags, and other objects upon entering and leaving the facilities. 4.5 Must use alarm systems and/or video surveillance cameras to monitor, alert, record, and supervise the facilities and prevent unauthorized access to critical areas and cargo handling, inspection or storage areas.
5. Safety in the processes related to handling, storage, and conveyance.	Ensure the integrity, safety and traceability of the processes related to the handling, storage and transportation of cargo in the supply chain.	5.1 Must have documented procedures for handling, storage and transportation of cargo. 5.2 Must have tools to ensure traceability of the cargo and the vehicle transporting it from the point of filling to the port of shipment to the outside (downstream). 5.3 Must have tools to ensure traceability of the cargo from the point of filling abroad to the importer's headquarters or distribution point (upstream). 5.4 Must have a protocol to act and report suspicious activities or security incidents that affect the security of the supply chain to the competent authority. 5.5 You must protect the physical and electronic documentation of your international supply chain operations.

Table 9. *Cont.*

Chapter/Item	Security Objectives	ID/Principal Minimum Security Criteria
6. Personnel security.	Ensure the reliability of its employees through procedures that allow you to know the personnel linked and the definition of critical positions within the company.	6.1 It shall have documented procedures for the selection and dismissal of personnel. 6.2 It shall evaluate the background of employees in national and international lists to ensure their reliability. 6.3 Maintain updated employee work history, including personal and family data, photographic records, and background checks, among others. 6.4 Must carry out home visits and socioeconomic studies of its employees to detect unjustified changes in their assets. 6.5 Must have security provisions for the supply and handling of the supplies given to its employees.
7. Information technology security.	Establish IT security measures to protect the company's information, data, networks and programs against cybercrime, cyberattacks and cyberterrorism.	7.1 Have documented and sensitized IT security policies within the company to protect information technology (IT) systems. 7.2 It must contemplate software programs and equipment to protect against common external cybersecurity threats (viruses, worms, spyware, Trojans, and hackers, among others) and against internal threats of theft or leakage of information through the use of USB or storage devices, emails, and unintentional human error. 7.3 It must assign individual access accounts to the technological platform, with periodic changes of passwords with n characteristics that increase security levels. 7.4 It must have an IT contingency plan that guarantees the integrity, confidentiality, and availability of the company's information. 7.5 It must have a defined area (computer center) with appropriate security measures that guarantee access only to authorized personnel.
8. Education, training, and awareness.	Strengthen the security culture through periodic training and education programs on security, threats and risks.	8.1 A periodic induction and re-induction program should be in place for all employees on the company's security measures. 8.2 It shall have specialized training programs on security, threats, and risks to prevent and act against any criminal activity that affects the continuity of its supply chain operations. 8.3 Must have an alcohol and drug use prevention program in place. 8.4 It shall have a program of drills for crisis management, business continuity, and emergency plans. 8.5 An induction program shall be in place for visitors and contractors, where applicable, to ensure that they are aware of the company's security measures and possible threats and risks.

Standard Security Level Framework, which includes the common chapters or items and the main minimum-security requirements (not all security measures are included). Own elaboration.

Based on the above standard framework of security levels, the General Logistics Security Management Framework is elaborated with an evaluation of its quantitative analysis of the eight chapters and 40 security requirements in the four programs, defining an evaluation scale of 1 (if it complies) or 0 (otherwise), as shown in Table 10.

Table 10. General Logistics Security Management Framework (source: own elaboration adapted from [32]).

Chapter—Minimum Security Criteria/Security Program	C-TPAT	BASC	SAFE Framework AEO	ISO
1. Risk management.				
1.1 Must have a security management policy focused on risk assessment to ensure supply chain security.	1	1	1	1
1.2 The policy should have security management objectives, goals and programs.	1	1	1	1
1.3 It should have a risk management system focused on the supply chain.	1	1	1	1
1.4 It should disseminate the security policy to stakeholders through the company's website, and be posted within the company (bulletin board, email, etc.) in key locations.	1	1	1	1
1.5. Should have documented procedures for crisis management, business continuity, and recovery plans.	1	1	1	1
2. Knowledge of business partners/business associates.				
2.1 Must have documented procedures for purchasing, selection, and contracting of suppliers that guarantee their reliability.	1	1	1	1
2.2 Must have documented procedures for customer selection and contracting that guarantee their reliability.	1	1	1	1
2.3 It must carry out security visits to the facilities where its business partners carry out their operations, to verify that they have implemented security measures in the international supply chain.	1	1	1	1
2.4 It must issue security agreements for those trading partners that do not have security program certificates from other international public or private organizations.	1	1	1	1
2.5 The company and its members (managers) should have their background checked against national and international lists for the prevention of crimes related to money laundering and terrorism.	1	1	1	1
3. Conveyance and transportation unit security.				
3.1 Must have documented procedures and controls to ensure the integrity of containers and other cargo units at the point of filling to protect them against the introduction of unauthorized persons or materials.	1	1	1	1
3.2 Shall use security seals under the standards contained in the current ISO 17712 standard on containers and other sealable cargo units.	1	1	1	1
3.3 Inspect the physical integrity of the container structure (internal and external) and other cargo units, as well as the means of transport. A documentary record of the inspection shall be kept by the person responsible for the activity.	1	1	1	1
3.4 Ensure that the areas where containers and other cargo units (full or empty) are stored are secure and prevent unauthorized access and/or manipulation.	1	1	1	1
3.5 Have procedures in place to detect and report unauthorized entry to containers and other cargo units, as well as when security seals have been breached.	1	1	1	1

Table 10. *Cont.*

Chapter—Minimum Security Criteria/Security Program	C-TPAT	BASC	SAFE Framework AEO	ISO
4. Physical access controls and physical security.				
4.1 Have documented procedures and measures to identify and control access of people and vehicles to the facilities.	1	1	1	1
4.2 Provide all related personnel with an identification or access device for entry to the facilities.	1	1	1	1
4.3 Require visitors to identify themselves for entry to the facilities and provide them with an identification or temporary access device.	1	1	1	1
4.4 Check persons, vehicles, packages, bags, and other objects upon entering and leaving the facilities.	1	1	1	1
4.5 Must use alarm systems and/or video surveillance cameras to monitor, alert, record, and supervise the facilities and prevent unauthorized access to critical areas and cargo handling, inspection, or storage areas.	1	1	1	1
5. Safety in the processes related to handling, storage, and conveyance.				
5.1 Must have documented procedures for handling, storage, and transportation of cargo.	1	1	1	1
5.2 Must have tools to ensure traceability of the cargo and the vehicle transporting it from the point of filling to the port of shipment to the outside (downstream).	1	1	1	1
5.3 Must have tools to ensure traceability of the cargo from the point of filling abroad to the importer's headquarters or distribution point (upstream).	1	1	1	1
5.4 Must have a protocol to act and report suspicious activities or security incidents that affect the security of the supply chain to the competent authority.	1	1	1	1
5.5 You must protect the physical and electronic documentation of your international supply chain operations.	1	1	1	1
6. Personnel security.				
6.1 It shall have documented procedures for the selection and dismissal of personnel.	1	1	1	1
6.2 It shall evaluate the background of employees in national and international lists to ensure their reliability.	1	1	1	1
6.3 Maintain updated employee work history, including personal and family data, photographic records, and background checks, among others.	1	1	1	1
6.4 Must carry out home visits and socioeconomic studies of its employees to detect unjustified changes in their assets.	1	1	1	1
6.5 Must have security provisions for the supply and handling of the supplies given to its employees.	1	1	1	1
7. Information technology security.				
7.1 Have documented and sensitized IT security policies within the company to protect information technology (IT) systems.	1	1	1	1
7.2 It must contemplate software programs and equipment to protect against common external cybersecurity threats (viruses, worms, spyware, Trojans, hackers, among others). And internal threats of theft or leakage of information through the use of USB or storage devices, emails, and unintentional human error.	1	1	1	1

Table 10. *Cont.*

Chapter—Minimum Security Criteria/Security Program	C-TPAT	BASC	SAFE Framework AEO	ISO
7.3 It must assign individual access accounts to the technological platform, with periodic changes of passwords with n characteristics that increase security levels.	1	1	1	1
7.4 It must have an IT contingency plan that guarantees the integrity, confidentiality, and availability of the company's information.	1	1	1	1
7.5 It must have a defined area (computer center) with appropriate security measures that guarantee access only to authorized personnel.	1	1	1	1
8. Education, training, and awareness.				
8.1 A periodic induction and re-induction program should be in place for all employees on the company's security measures.	1	1	1	1
8.2 It shall have specialized training programs on security, threats, and risks to prevent and act against any criminal activity that affects the continuity of its supply chain operations.	1	1	1	1
8.3 Must have an alcohol and drug use prevention program in place.	0	1	1	1
8.4 It shall have a program of drills for crisis management, business continuity, and emergency plans.	1	1	1	1
8.5 An induction program shall be in place for visitors and contractors, where applicable, to ensure that they are aware of the company's security measures and possible threats and risks.	1	1	1	1
Degree of similarity with the General Logistics Security Management Framework	98%	100%	100%	100%

According to the developed General Logistics Security Management Framework, it is observed that current programs contain a 99% similarity degree in their chapters and largely aim at the same minimum-security requirements. Previous works in the literature published (see [32]) analyzed a total of nine programs by comparing their contents with the General Framework for Supply Chain Security. In contrast to the results of the current papers, those previous works showed an overall average similarity degree of 62% for the set of four programs analyzed here. The high degree of similarity in our results is due to the fact that, in the last two decades, logistics security programs have been updated through mutual cooperation between international organizations, governments, and control authorities for the exchange of experience and information to develop new security measures against new global threats, with the main objective of facilitating reliable and secure international trade.

It should be noted that ISO standards, despite not having a certain similarity in the chapter designations, are translated into procedures, activities, controls, tools, and technologies that the organization must adopt within the processes to ensure supply chain security. On the other hand, it is important to note that the structure of BASC and ISO 28000/28001 programs is focused on a management system. The ISO standard defines the management system as a "set of interrelated or interacting elements and activities of an organization that establish policies, objectives, and processes to achieve goals" [67,68]. Management systems have a managerial or strategic initiative within organizations because they generate added value in their mission and vision regarding stakeholders.

However, the C-TPAT and AEO programs can be considered as a management system because they contain base elements such as policies, objectives, and processes, and because they aim at a managerial initiative to generate value in their strategic, mission, and support

processes in supply chain security management issues. In addition, they can be integrated with other management systems or programs that the company may have. And for those companies that do not have a management system, these programs facilitate its adoption for the implementation of a management system.

Finally, management systems are subject to periodic assessment or audits that ensure continuous improvement for certification and compliance with requirements for system conformity by the public or private sector certifying agency, as reflected in Table 11.

Table 11. Periodic assessment of C-TPAT, BASC, AEO, and ISO 28000 programs (source: own elaboration).

Initiatives	Periodic Assessment	Certifying Agency	
		Public Sector	Private Sector
C-TPAT	1 year	X	
BASC V6	1 year		X
AEO	2–3 years	X	
ISO 28000–ISO 28001	1 year		X

The table reflects the period of external assessment or external audits for each program. However, once a company is certified for any program, it must conduct and document annual internal audits to verify compliance with and maintenance of the minimum requirements of the relevant security program.

6.2. Benefits of Implementing a Logistics Security Program

Each logistics security program offers a series of common benefits to member companies, such as international recognition as a secure and committed company with safety in its logistics processes, trust from stakeholders, participation in training activities, strengthening of resilience capacity, and continuity of operations in the face of unexpected events, as described in Table 12.

It is evident from the table that the public sector logistics security programs, in addition to the benefits described above, have additional benefits on the part of the customs authority, such as the assignment of an official specialized in logistics security, facilities in simplified customs procedures and submissions of brief declarations of entry and exit of goods, and a reduction in physical and documentary controls, among others.

6.3. Monetary Costs for the Implementation of a Logistics Security Program

The implementation of a security program in the supply chain involves the adoption of measures, controls, tools, and resources aimed at preventing, detecting, and mitigating security risks to which they are exposed, and helping the supply chain recover from disruptions caused by criminal trends. Therefore, cargo owners and logistics service providers require the necessary resources to meet the minimum-security requirements for any logistics security program they wish to adopt, mainly in terms of monetary investments and time.

In general, monetary, and time costs are divided into two categories: (a) implementation costs to receive certification, and (b) costs to maintain certification [52]. The implementation and maintenance costs depend on the socio-economic situation of the country and the economic sector to which the company belongs [50]. Similarly, these security programs are designed for the participation of small, medium, and large companies that are part of the supply chains.

Table 12. C-TPAT, BASC, and WCO official web pages/ISO 28000 (source: own elaboration from information in [80]).

C-TPAT	BASC	AEO	ISO 28000–28001
The program includes the following benefits for supply chain actors: • Reduction in the number of CBP exams. • Frontline inspections. • Possible exemption from stratified exams. • Shorter waiting times at the border. • Assignment of a supply chain security specialist to the company. • Access to Free and Secure Trade (FAST) lanes at land borders. • Access to the CTPAT web portal system and a library of training materials. • Potential for additional benefits by being recognized as a Trusted Business Partner by foreign customs administrations that have signed Mutual Recognition with the United States. • Opportunity to participate in other U.S. government pilot programs, such as the Food and Drug Administration's Secure Supply Chain Program. • Priority in resuming business operations after a natural disaster or terrorist attack. • Importer eligibility to participate in the Importer Self-Assessment (ISA) Program. • Priority consideration at CBP Centers of Excellence and Expertise focused on the industry.	The program defines the following benefits for companies participating in the international supply chain: • International recognition by belonging to the World BASC Organization (WBO) and its associated chapters. • Differentiation by implementing the BASC Control and Security Management System (SGCS). • Inclusion in WBO's database of certified companies. • Availability of competent international auditors for the implementation and review of the BASC SGCS. • Beneficiary of Memoranda of Understanding signed by WBO with customs, control entities, and international organizations. • Representation and facilitation of contacts with authorities involved in foreign trade. • Increased trust from authorities. • Decreased costs and risks associated with process control. • Knowledge and experience transfer in Supply Chain Security. • Facilitation of contacts in different countries through BASC chapters. • Specialized training courses on topics related to international trade security. • Preferential rates for participation in WBO events. • Information and updates on topics related to international trade activities.	At the international level, most programs offer the following benefits: • Recognition as a secure and reliable operator in the supply chain. • Assignment of an operations officer by each control authority to provide support in operations. • Reduction in the number of inspections, physical and documentary, by the respective authorities. • Prioritization in foreign trade operations processed by control authorities. • Participation in training activities organized by the program-involved authorities. • Ease of adopting simplified customs procedures and submitting brief declarations for entry and exit of goods. • Reduction in physical and documentary controls. • Facility to carry out relevant controls at the operator's premises. • Priority in clearance and access to fast lanes. • Financial advantages when paying duties and tariffs. • Reduction in time and costs, and increased competitiveness in international markets. • Obtaining a seal of guarantee that certifies operators as reliable and secure. WCO member countries define the benefits for each actor in the supply chain in their respective AEO programs implemented by customs authorities.	Benefits that attract companies in the implementation of ISO 28000 to secure the supply chain: • Organizations that have the ability to secure their entire supply chain. • Improvement in processes while increasing work efficiency. • Allows management of other variables such as quality, occupational safety, and customer satisfaction. • Provides significant benefits of economic efficiency to the company. • Maintains the durability of the company and increases employee performance. • Leads to maximizing the utilization of resources. • Internal and external security in the supply chain can increase company productivity. • Helps reduce workplace accidents and prevent occupational diseases. • Recognition from customers. • Reinforces the trust of stakeholders. • Drives business cooperation throughout the supply chain. • Provides systematic tracking for customers to trace their product or material, allowing easy access to information. • All supply chain processes will be more visible. • Integrates with other standards. • Facilitates implementation in AEO programs.

There are very few research studies estimating the implementation costs of the security measures required by security programs for certification and their subsequent annual maintenance costs. The first research conducted was a study on the BASC program in Latin America (2005–2007) by researchers from the Cross-border Research Association (CBRA) through a survey targeted at 800 contacted BASC member companies, with 102 surveys receiving complete responses (response rate of 13% and a sampling error of 10%) [81]. The survey covered 78% of member countries and represented companies engaged in various operations related to international trade (manufacturers, traders, port operators, logistics service providers, and others providing support services such as security surveillance and vehicle rentals). It included companies of different sizes and annual business volumes. The study concluded regarding BASC implementation costs that certification costs appear to be more expensive for companies with a small annual business volume (less than USD 50,000), while maintenance costs are proportionally more expensive for companies with higher business volumes, as shown in Table 13. In the same study [81], it establishes the measures of time and resources needed to implement the BASC program, as illustrated in Table 14.

Table 13. Average certification and maintenance costs for different types of companies according to their annual turnover (sample size: 90) (source: [81]).

Annual Turnover USD	Number of Companies	Average Value in USD			
		Implementation Cost USD	Annual Maintenance USD	Maintenance/ Certification Cost	Certification Cost/Turnover
<50,000	4	28.625	2.888	10%	≥57%
50,000–500,000	13	17.176	8.539	50%	3–34%
500,000–1 million	13	13.585	6.698	49%	1–3%
1–5 million	25	61.820	15.826	26%	1–6%
>5 million	35	52.742	28.448	54%	≤1%
Total	90	34.790	12.487	38%	

Table 14. Measures of time and resources required to implement BASC (sample size: 90 complete responses) (source: [82]).

Time	Average Values
Months necessary for certification process	8
Total hours of work for certification	2.337
Resources	
Number of employees involved in certification process	48
Number of employees involved/Total employees	23%
Time per resource	
Hours per person	49 (~6 working days)

On the other hand, being a private organization, it has administrative fees that the World BASC Organization (WBO) charges to its members to cover the organization's operating costs. These administrative fees can vary from USD 800 to USD 2500 for certification, and from USD 800 to USD 2000 for annual maintenance [50].

Other authors, such as Varun et al. [82] conducted a case study of motivations, obstacles and company size associated with the C-TPAT program, where they compile a series of studies by different authors and the CBP body since 2006. The results reflected the monetary costs to receive certification and their average maintenance cost and time commitment for C-TPAT, as described in Table 15.

Table 15. Monetary costs and time commitment for C-TPAT (source: own elaboration based on data provided in [52]).

Research	Monetary Cost
Bichou [83]	At the beginning of the program in 2004, the average implementation cost was estimated at USD 200,000, and the average maintenance cost was USD 113,000. However, over time, the implementation and maintenance costs have reduced.
CBP [84]	Average implementation cost USD 38,471 and average maintenance cost USD 69,000.
CBP:2011 [84]	A subsequent study conducted by CBP in 2010 further reports that the implementation of physical security is the most significant factor in estimating certification costs, while the maintenance of physical security/cargo is the most important factor in calculating maintenance costs. The average implementation cost reported is USD 137,899 (with a median of USD 17,370), and the average maintenance cost is USD 47,749 (with a median of USD 9000).
Sheu et al. [85]	Another study examined the initial monetary costs and time commitments by interviewing four C-TPAT certified companies, including a broker, an import service provider, a carrier/transporter, and an importer. Their study reports that the initial certification cost ranges from USD 3500 to USD 18,000, with a time commitment varying between 160 and 210 days.
Thibault et al. [86]	They also found that smaller companies may have lower compliance costs. Furthermore, they discovered that smaller ocean carriers had lower implementation costs but incurred higher maintenance costs compared to larger ocean carriers.
Gettinger [87]	For importers, on average, there are three implementation costs they incur, with an average implementation cost of USD 39,500 represented by the following components: Physical security: USD 15,000. IT systems: USD 12,500. Additional salaries: USD 12,000.
Ni et al. [40]	The initial implementation and maintenance costs for early adopters were substantial due to the lack of best practices.

The C-TPAT program is voluntary and free of charge, companies must invest in relevant infrastructure and security upgrades to meet program requirements and security standards according to industry (foreign manufacturers and 3PL logistics service providers) [73].

7. Open Research Problems

Considering the present study allows the definition of open research problems for future promising research, which can be addressed from academia and complement the existing supply chain security literature, providing a dissemination and clarity of good security practices offered by the different security programs against common threats in the region and contributes to the visibility of CV) supply chains (Sa through security risk management (SCRS).

Listed below are the main open research issues for readers and researchers:

- This study can be used to establish compatible security programs or develop global security standards, such as the proposal for a standardized regional AEO program for Latin America and the Caribbean, like the C-TPAT and BASC programs, with a single structure that organizes the chapters and minimum-security requirements in a standardized manner for implementation by any WCO member in the region, could be considered for future discussion and research. This would facilitate a clear language

to manage homogeneous threats at the regional level and the operations of certified companies and intra-regional trade, as well as the promotion of Mutual Recognition Agreements (MRAs) for greater benefits.
- The private sector benefits from the BASC and ISO programs can be considered for future research studies as a source of customer-facing competitive advantages to secure and optimize global operations.
- There is scope for a case study reviewing the benefits of the AEO program proposed by a country's customs authority versus the perception of benefits received by cargo-owning companies and logistics service operators that adhere to this initiative.
- The adoption of a maturity model to assess logistics security systems in global supply chains in Latin America and the Caribbean could derive opportunities to improve security and resilience to future disruptions in the context of supply chain security risk management.
- Another opportunity is the application of logical and systematic methods for supply chain security risk assessment.

8. Managerial Implications, Discussion, and Conclusions

The objective of this paper was to present a description and analysis of the four main supply chain security programs available for Latin America and the Caribbean (C-TPAT, BASC, AEO, and ISO 28000), led by international organizations from the public and private sectors. The analysis was conducted based on a thematic content analysis methodology with a qualitative and quantitative approach, under a common framework to compare the four programs. It showed a high degree of similarity in the chapters and security objectives, with a similar structure to achieve them. These objectives were primarily represented in risk management, knowledge of business partners or associates, cargo and transportation unit security, physical security and access controls, handling, storage, and transportation processes, reliability of human resources, security training and threat awareness, and information technology security.

This work allows us, in the first instance, to fill this gap in the existing literature, through the dissemination and clarification of the good security practices offered by the different security programs (C-TPAT, AEO, BASC, and ISO 28000) in the face of common threats in the region. This document systematically analyses these existing logistics security programs for Latin America and the Caribbean. It can become a guide for companies to have a clearer vision when selecting one or more logistics security programs, with the ultimate goal of strengthening the visibility processes of their global supply chains. It is novel, as there is no up-to-date analysis of the relationship between security programs (C-TPAT, AEO, BASC, and ISO 28000) in the literature. To this end, a contribution table developed by the authors in the related literature is provided, listing the existing studies published over the last decade. Between 2001 (when the first security program was launched) and 2011, there was only one study conducted in 2009, by researchers Gutiérrez and Hintsa, from the Cross-border Research Association (CBRA) in Lausanne (Switzerland), in which they carried out a comparative analysis of nine global security initiatives, including the C-TPAT, AEO, BASC, and ISO 28000 programs, to establish their compatibility and identify the security measures that could be mandatory in the near future.

The SAFE Framework defines the guidelines for implementing the AEO program, which must be applied by the customs authorities of WCO member countries and required of companies that wish to voluntarily join the program. This initiative led each country's customs authorities in Latin America and the Caribbean to issue their own AEO program, resulting in a high degree of similarity among the programs, despite the SAFE Framework setting a standard for implementation.

Regarding the benefits obtained by companies through the adoption of a logistics security program, first and foremost, international recognition is achieved in the form of a company committing to supply chain security. Other benefits include facilitating foreign trade operations, gaining greater trust from authorities and stakeholders, participating

in training activities, strengthening resilience and continuity of operations in the face of security incidents or unexpected events.

From the analysis of this work, it was shown that publicly led programs associated with customs authorities offer special benefits in customs procedures, including simplified procedures, reduced physical and documentary controls, and prioritized clearance and fast lanes. In terms of taxation and tariffs, these programs led by customs authorities represent financial advantages when paying taxes and tariffs for certified companies.

These security programs are designed for the participation of small, medium, and large companies that are part of the supply chains. The costs and implementation timelines vary according to the company's structure, infrastructure, and industry sector. Costs are associated with implementing tools, equipment, systems, controls, and security measures within their organizational processes and procedures. However, the costs encompass the certification process and the annual maintenance costs to maintain the recognition. The costs are also associated with the types of threats. The higher the risk of threats, the greater the need for implementing controls and security measures. For Latin America and the Caribbean, according to the analysis of the INTERPOL's 2022 summary report, the criminal trends in this region include organized crime, illicit trafficking, financial crimes, cybercrimes, and terrorism. These criminal activities dominate the global threat landscape and exploit global supply chains to carry out their illicit activities.

Based on this study, it is concluded that the implementation of these programs allows organizations to have broader visibility in global supply chains, which are increasingly fragile and complex due to security risks they are susceptible to. Similarly, technology plays a vital role in improving supply chain visibility and security [2]. The exchange of information through the use of global positioning systems (GPS) in land freight vehicles, electronic security devices for containers, blockchain, the Internet of Things (IoT), the development of cargo tracking platforms and transportation means, among others, have become prerequisites for traceability and tracking of goods, providing a clear view of the logistics activities throughout the supply chain.

This study provided supply chain and logistics managers and researchers, as well as decision makers in cargo-owning companies and logistics service providers with firsthand knowledge for choosing and/or complementing one or more logistics security management systems in their organizational processes to strengthen security and resilience in their operations within the global supply chain.

To sum up, it is important to recommend to practitioners that have multiple implemented logistics security programs not to eliminate any of them due to cost issues. While it is true that the analyzed programs maintain great similarity in their contents, the continuity of one program would enable the maintenance of the other program and vice versa. It also strengthens controls and best practices transferred between programs by private and public organizations, which ultimately translates into greater resilience and security for mitigating security risks associated with the supply chain. Failing to do so would result in higher risk costs compared to the investment and maintenance costs of the adopted programs.

Author Contributions: Conceptualization, P.E.M.L. and J.R.M.-T.; methodology, P.E.M.L. and J.R.M.-T.; validation, P.E.M.L. and J.R.M.-T.; formal analysis, P.E.M.L. and J.R.M.-T.; investigation, P.E.M.L.; writing—original draft preparation, P.E.M.L.; writing—review and editing, J.R.M.-T.; visualization, P.E.M.L. and J.R.M.-T.; supervision, J.R.M.-T.; project administration, J.R.M.-T.; funding acquisition, J.R.M.-T. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Universidad de La Sabana, Colombia, grant number INGPhD-57-2023, and by the Colombian Ministry of Science, Technology and Innovation (Minciencias), under a doctoral grant (SGR-22 grant 00TC-3902-1000-2022-00010-0075).

Data Availability Statement: No new data were created in this study. Data are contained within the article and publicly accessible through the cited references.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. Kalaiarasan, R.; Olhager, J.; Agrawal, T.K.; Wiktorsson, M. The ABCDE of supply chain visibility: A systematic literature review and framework. *Int. J. Prod. Econ.* **2022**, *248*, 108464. [CrossRef]
2. Boile, M.; Sdoukopoulos, L. Supply chain visibility and security—The SMART-CM project solution. *Int. J. Shipp. Transp. Logist.* **2014**, *6*, 280–292. [CrossRef]
3. Barratt, M.; Barratt, R. Exploring internal and external supply chain linkages: Evidence from the field. *J. Oper. Manag.* **2011**, *29*, 514–528. [CrossRef]
4. Goh, M.; De Souza, R.; Zhang, A.N.; He, W.; Tan, P.S. Supply chain visibility: A decision making perspective. In Proceedings of the 4th IEEE Conference on Industrial Electronics and Applications, ICIEA, Xi'an, China, 25–27 May 2009; pp. 2546–2551.
5. Williams, B.D.; Roh, J.; Tokar, T.; Swink, M. Leveraging supply chain visibility for responsiveness: The moderating role of internal integration. *J. Oper. Manag.* **2013**, *31*, 543–554. [CrossRef]
6. Yu, M.-C.; Goh, M. A multi-objective approach to supply chain visibility and risk. *Eur. J. Oper. Res.* **2014**, *233*, 125–130. [CrossRef]
7. Yang, Y.-C. Risk management of Taiwan's maritime supply chain security. *Saf. Sci.* **2011**, *49*, 382–393. [CrossRef]
8. Nikoofal, M.E.; Pourakbar, M.; Gumuz, M. Securing containerized supply chain through public and private partnership. *Prod. Oper. Manag.* **2023**. *early view*. [CrossRef]
9. Montoya-Torres, J.R.; Muñuz-Villamizar, A.F.; Mejía-Argueta, C. Mapping research in logistics and supply chain management during COVID-19 pandemic. *Int. J. Logist. Res. Appl.* **2023**, *26*, 421–441. [CrossRef]
10. Manuj, I.; Mentzer, J. Global supply chain risk management strategies. *Int. J. Phys. Distrib. Logist. Manag.* **2008**, *38*, 192–223. [CrossRef]
11. Montoya-Torres, J.R. Managing Disruptions in Supply Chains. In *Service Oriented, Holonic and Multi-Agent Manufacturing Systems for Industry of the Future. SOHOMA 2021. Studies in Computational Intelligence*; Trentesaux, D., Borangiu, T., Leitão, P., Jimenez, J.F., Montoya-Torres, J.R., Eds.; Springer: Berlin/Heidelberg, Germany, 2022; Volume 987, pp. 272–284.
12. Hintsa, J.; Gutiérrez, X.; Weiser, P.; Hameri, A.-P. Supply Chain Security Management: An overview. *Int. J. Logist. Syst. Manag.* **2009**, *5*, 344–355. [CrossRef]
13. Asamoah, D.; Nuertey, D.; Agyei-Owusu, B.; Acquah, I. Antecedents and outcomes of supply chain security practices: The role of organizational security culture and supply chain disruption occurrence. *Int. J. Qual. Reliab. Manag.* **2022**, *39*, 1059–1082. [CrossRef]
14. Donner, M.; Kruk, C. *Supply Chain Security Guide*; World Bank: Washington, DC, USA, 2009; Available online: http://hdl.handle.net/10986/28128 (accessed on 28 May 2023).
15. Pérez, G. *Seguridad de la Cadena Logística Terrestre en América Latina*; Comisión Económica para América Latina y el Caribe (Cepal): Santiago, Chile, 2013; p. 9.
16. *ISO 31000:2018*; Risk Management Guidelines. International Standard Organization: Geneva, Switzerland, 2018. Available online: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en (accessed on 28 May 2023).
17. Supply Chain Risk Leadership Council (SCRLC). Available online: http://www.scrlc.com/articles/Supply_Chain_Risk_Management_A_Compilation_of_Best_Practices_final[1].pdf (accessed on 28 May 2023).
18. ICS 731-01. Intelligence Community Standard. Available online: https://www.dni.gov/files/NCSC/documents/supplychain/ICS%20731-01%20Supply%20Chain%20Criticality%20Assessments.pdf (accessed on 29 May 2023).
19. Svensson, G. A conceptual framework for the analysis of vulnerability in supply chains. *Int. J. Phys. Distrib. Logist. Manag.* **2000**, *30*, 731–749. [CrossRef]
20. Jüttner, U.; Peck, H.; Christopher, M. Supply chain risk management: Outlining an agenda for future research. *Int. J. Logist. Res. Appl.* **2003**, *6*, 197–210. [CrossRef]
21. Peck, H.; Christopher, M. Building the resilient Supply Chain. *Int. J. Logist. Manag.* **2004**, *15*, 1–14.
22. Tang, C. Perspectives in supply chain risk management. *Int. J. Prod. Econ.* **2006**, *103*, 451–488. [CrossRef]
23. Williams, Z.; Lueg, J.E.; LeMay, S.A. Supply chain security: An overview and research agenda. *Int. J. Logist. Manag.* **2008**, *19*, 254–281. [CrossRef]
24. Rao, S.; Goldsby, T.J. Supply chain risk: A review and typology. *Int. J. Logist. Manag.* **2009**, *20*, 97–123. [CrossRef]
25. Melnyk, S.A.; Rodrigues, A.; Ragatz, G.L. Using simulation to investigate supply chain disruptions. In *Supply Chain Risk—A Handbook of Assessment, Management, and Performance*; Zsidisin, G.A., Ritchie, B., Eds.; International Series of Operations Research & Management Sciences; Springer: Berlin/Heidelberg, Germany, 2009; Volume 124, pp. 103–122.
26. Ponomarov, S.Y.; Holcomb, M.C. Understanding the concept of supply chain resilience. *Int. J. Logist. Manag.* **2009**, *20*, 124–143. [CrossRef]
27. Pfohl, H.-C.; Köhler, H.; Thomas, D. State of the art in supply chain risk management research: Empirical and conceptual findings and a roadmap for the implementation in practice. *Logist. Res.* **2010**, *2*, 33–44. [CrossRef]
28. Wieland, A. Selecting the right supply chain based on risks. *J. Manuf. Technol. Manag.* **2013**, *24*, 652–668. [CrossRef]

29. Munoz, A.; Dunbar, M. On the quantification of operational supply chain resilience. *Int. J. Prod. Res.* **2015**, *53*, 6736–6751. [CrossRef]
30. Tordecilla, R.D.; Juan, A.A.; Montoya-Torres, J.R.; Quintero-Araujo, C.L.; Panadero, J. Simulation-Optimization Methods for Designing and Assessing Resilient Supply Chain Networks under Uncertainty Scenarios: A Review. *Simul. Model. Pract. Theory* **2021**, *106*, 102166. [CrossRef] [PubMed]
31. Williams, Z.; Garver, M.S.; Richey, R.G., Jr. Security capability and logistics service provider selection: An adaptive choice study. *Int. J. Phys. Distrib. Logist. Manag.* **2019**, *49*, 330–355. [CrossRef]
32. Gutierrez, X.; Hintsa, J. Voluntary supply chain security programs: A systematic comparison. In Proceedings of the International Conference on Information Systems, Logistics and Supply Chain (ILS2006), Lyon, France, 15–17 May 2006.
33. Tranfield, D.; Denyer, D.Y.; Smart, P. Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *Br. J. Manag.* **2003**, *14*, 207–222. [CrossRef]
34. Ritchie, W.J.; Melnyk, S.A. The impact of emerging institutional norms on adoption timing decisions: Evidence from C-TPAT-A government antiterrorism initiative. *Strateg. Manag. J.* **2012**, *33*, 860–868. [CrossRef]
35. Melnyk, S.A.; Ritchie, W.J.; Calantone, R.J. The case of the C-TPAT border security initiative: Assessing the adoption/persistence decisions when dealing with a novel, institutionally driven administrative innovation. *J. Bus. Logist.* **2013**, *34*, 289–300. [CrossRef]
36. Voss, M.D.; Williams, Z. Public-private partnerships and supply chain security: C-TPAT as an indicator of relational security. *J. Bus. Logist.* **2013**, *34*, 320–334. [CrossRef]
37. Herrera, T.J.F. Application of discriminant analysis to assess productivity as a result from the BASC certification in Cartagena companies. *Account. Adm.* **2014**, *59*, 43–62.
38. Schramm, H.-J. Who benefits most from AEO certification? An Austrian perspective. *World Cust. J.* **2015**, *9*, 59–67.
39. Blos, M.F.; Hoeflich, S.L.; Dias, E.M.; Wee, H.-M. A note on supply chain risk classification: Discussion and proposal. *Int. J. Prod. Res.* **2016**, *53*, 1568–1569. [CrossRef]
40. Ni, J.Z.; Melnyk, S.A.; Ritchie, W.J.; Flynn, B.F. Why be first if it doesn't pay? The case of early adopters of C-TPAT supply chain security certification. *Int. J. Oper. Prod. Manag.* **2016**, *36*, 1161–1181. [CrossRef]
41. Chang-Bong, K.; Chun, H.-U.; Kwon, S.-H. Impact of application factors of the AEO program on its performance. *J. Korea Trade* **2016**, *20*, 332–348. [CrossRef]
42. Herrera, T.J.F. Analysis of the financial efficiency in BASC certified companies through data envelopment analysis: Evidence from Cali—Colombia. In Proceedings of the 27th International Business Information Management Association Conference—Innovation Management and Education Excellence Vision 2020: From Regional Development Sustainability to Global Economic Growth, IBIMA, Milan, Italy, 4–5 May 2016.
43. The Program Authorized Economic Operator (Brazilian OEA) and the Port Operations: An Exploratory Study with Port Terminals. Available online: http://www.ifac.portafolio.revistaespacios.com/a17v38n21/a17v38n21p17.pdf (accessed on 28 May 2023).
44. Karlsson, L. Back to the future of Customs: A new AEO paradigm will transform the global supply chain for the better. *World Cust. J.* **2017**, *11*, 23–34.
45. Bagchi, A.; Paul, J.A. Espionage and the optimal standard of the Customs-Trade Partnership against Terrorism (C-TPAT) program in maritime security. *Eur. J. Oper. Res.* **2017**, *262*, 89–107. [CrossRef]
46. Houe, T.; Murphy, E. The AEO status as a source of competitive advantage. *Eur. Bus. Rev.* **2018**, *30*, 591–606. [CrossRef]
47. Burns, M.G. Participatory Operational & Security Assessment on homeland security risks: An empirical research method for improving security beyond the borders through public/private partnerships. *J. Transp. Secur.* **2018**, *11*, 85–100.
48. Chin, C.Y.; Sorooshian, S. Possible barriers affecting implementation of ISO28000 for the supply chain. *Int. J. Supply Chain. Manag.* **2019**, *8*, 90–97.
49. Dos Santos Marques, L.G.; Kondrashova, A.; Morini, C. Diving deeper in performance indicators: What do we know about the AEO in Brazil? *World Cust. J.* **2019**, *13*, 81–100.
50. Gupta, V.; Ding, X.; Testa, T.M. A case study of drivers, barriers, and company size associated with C-TPAT program. *Supply Chain Forum* **2019**, *20*, 332–347. [CrossRef]
51. Erfan, S. The practical implications of AEO on preferential origin certification. *Glob. Trade Cust. J.* **2019**, *14*, 479–481. [CrossRef]
52. Ing, W.H.; Sorooshian, S.; Hasan, M. Benefits that attract industry to implement ISO 28000 to secure supply chain. *TEM J.* **2019**, *8*, 119–124.
53. Kim, C.-B.; Chung, I.-S.; Joo, H.-Y. Effects of AEO-MRA on the performance of exporters and importers in Korea. *J. Korea Trade* **2019**, *23*, 52–67. [CrossRef]
54. Jażdżewska-Gutta, M.; Grottel, M.; Wach, D. AEO certification—Necessity or privilege for supply chain participants. *Supply Chain Manag.* **2020**, *25*, 679–691. [CrossRef]
55. Zimon, D.; Madzík, P. Standardized management systems and risk management in the supply chain. *Int. J. Qual. Reliab. Manag.* **2020**, *37*, 305–327. [CrossRef]
56. Kusrini, E.; Hanim, K. Analysis of compliance and supply chain security risks based on ISO 28001 in a logistic service provider in Indonesia. *Int. J. Saf. Secur. Eng.* **2021**, *11*, 135–142. [CrossRef]
57. Kusrini, E.; Anggarani, I.; Praditya, T.A. Analysis of Supply Chain Security Management Systems Based on ISO 28001: 2007: Case Study Leather Factory in Indonesia. In Proceedings of the 2021 IEEE 8th International Conference on Industrial Engineering and Applications, ICIEA 2021, Virtual, 23–26 April 2021.

58. Tong, X.; Lai, K.-H.; Lo, C.K.Y.; Cheng, T.C.E. Supply chain security certification and operational performance: The role of upstream complexity. *Int. J. Prod. Econ.* **2022**, *247*, 108433. [CrossRef]
59. El Ministerio de Comercio, Industria y Turismo. Informe sobre los acuerdos comerciales vigentes de Colombia. En cumplimiento de la Ley 1868 de 2017, por medio de la cual se establece la entrega del Informe anual sobre el desarrollo, avance y consolidación de los acuerdos comerciales ratificados. MINCIT; 2021; pp. 6–7. Available online: https://www.tlc.gov.co/temas-de-interes/informe-sobre-el-desarrollo-avance-y-consolidacion/documentos/informe-tlc-2023.aspx (accessed on 3 November 2022).
60. Chapter Thematic Analysis. Available online: https://sk.sagepub.com/reference/the-sage-handbook-of-qualitative-research-in-psychology/i425.xml (accessed on 3 November 2022).
61. Li, T.S. Establishing an integrated framework for security capability development in a supply chain. *Int. J. Logist. Res. Appl.* **2014**, *17*, 283–303. [CrossRef]
62. CBP Enforcement Statistics. U.S. Customs and Border Protection (CPB). 2022. Available online: https://www.cbp.gov/ (accessed on 30 January 2023).
63. Business Alliance for Secure Commerce (BASC). 2022. Available online: https://wbasco.org/es (accessed on 2 November 2022).
64. Boletín FAL C-TPAT y AEO: Las nuevas vías del Comercio Internacional. Available online: https://repositorio.cepal.org/items/f27ff02b-e14d-4aa7-b6d5-5eb5741c1602 (accessed on 30 January 2023).
65. Compendium of Authorized Economic Operator Programmes—Ed. 2020. Available online: http://www.wcoomd.org/en/media/newsroom/2020/december/now-available-aeo-compendium-2020-edition.aspx (accessed on 15 May 2023).
66. *FAC 2022-2*; SAFE Framework of Standards. World Customs Organization (WCO): Brussels, Belgium, 2021.
67. *ISO 28000:2022*; Security and Resilience—Security Management Systems—Requirements. International Standard Organization (ISO): Geneve, Switzerland, 2022.
68. *ISO 28001:2007*; Security Management Systems for the Supply Chain—Best Practices for Implementing Supply Chain Security, Assessments and Plans—Requirements and Guidance. International Standard Organization (ISO): Geneve, Switzerland, 2007.
69. *The ISO Survey of Management System Standard Certifications 2020*; International Standard Organization (ISO): Geneve, Switzerland; Available online: https://www.iso.org/the-iso-survey.html. (accessed on 29 May 2023).
70. Cranfield School of Management. *Supply Chain Vulnerability*; Department for Transport, Local Government and the Regions—Department of Trade and Industry: Cranfield, UK, 2002.
71. Meixell, M.J.; Norbis, M. Integrating carrier selection with supplier selection decisions to improve supply chain security. *Int. Trans. Oper. Res.* **2012**, *19*, 711v732. [CrossRef]
72. Young, R.R.; Esqueda, P. Vulnerabilidades de la cadena de suministros: Consideraciones para el caso de América Latina. *Acad. Rev. Latinoam. De Adm.* **2005**, *34*, 63–78.
73. Park, K.; Min, H.; Min, S. Inter-relationship among risk taking propensity, supply chain security practices, and supply chain disruption occurrence. *J. Purch. Supply Manag.* **2016**, *22*, 120–130. [CrossRef]
74. Hintsa, J.; Uronen, K. *Common Assessment and Analysis of Risk in Global Supply Chains*. Technical Report Project: FP7-CASSANDRA. 2012. Available online: https://www.researchgate.net/publication/282845713_Common_Assessment_and_Analysis_of_Risk_in_Global_Supply_Chains (accessed on 28 May 2023).
75. Urciuoli, L.; Ekwall, D. The perceived impacts of AEO security certifications on supply chain efficiency—A survey study using structural equation modelling. *Int. J. Shipp. Transp. Logist.* **2015**, *7*, 1–20. [CrossRef]
76. International Criminal Police Organization. *Global Crime Trend Report 2022 INTERPOL*; International Criminal Police Organization: Lyon, France, 2022.
77. Moody's Analytics. The Top 10 Supply Chain Risks That Companies Face, Supplier Risk Management, Supply Chain. Available online: https://www.moodysanalytics.com/articles/2022/the-top-10-supply-chain-risks-that-companies-face (accessed on 3 November 2022).
78. What Inflation and Rising Prices Mean for Property Damage Insurance. Available online: https://www.zurich.com/en/commercial-insurance/sustainability-and-insights/commercial-insurance-risk-insights/what-inflation-and-rising-prices-mean-for-property-damage-insurance (accessed on 3 November 2022).
79. Volmar, G. Puntos de inflación—Dos países pueden tener el mismo porcentaje y sufrir trastornos diferentes. Available online: https://www.diariolibre.com/economia/columnistas/2022/01/31/el-impacto-social-de-la-inflacion/1614701 (accessed on 3 November 2022).
80. Global Slavery Index/Regional Findings the Americas. Available online: https://www.walkfree.org/global-slavery-index/findings/regional-findings/americas/ (accessed on 28 May 2023).
81. Gutierrez, X.; Wieser, P.; Hintsa, J. Voluntary supply-chain security programme impacts: An empirical study with BASC member companies. In *Risk Management in Port Operations, Logistics and Supply Chain Security*; Informa Law from Routledge: London, UK, 2007; pp. 31–35.
82. Hintsa, J. *Study on BASC-program in Latin America (2005–2007)*; Cross-Border Research Association (CBRA): Échandens, Switzerland, 2014.
83. Bichou, K. Risk-based Cost Assessment of Maritime and Port Security. In *Security and Environmental Sustainability of Multimodal Transport*; Bell, M., Hosseinloo, S.H., Kanturska, U., Eds.; Springer: Dordrecht, The Netherlands, 2010; pp. 183–211.
84. Costs and Benefits Survey. U.S. Customs Border and Protection. Available online: https://ctpatsecurity.com/wp-content/uploads/ctpat_css_survey-1.pdf (accessed on 28 May 2023).

85. Sheu, C.L.; Niehoff, B. A Voluntary Logistics Security Program and International Supply Chain Partnership. *Supply Chain Manag. Int. J.* **2006**, *11*, 363–374. [CrossRef]
86. Thibault, M.; Brooks, M.R.; Button, K.J. The Response of the US Maritime Industry to the New Container Security Initiatives. *Transp. J.* **2006**, *45*, 5–15. [CrossRef]
87. Gettinger, M. Everything You Need to Know about C-TPAT and Total Landed Cost. *ThomasNet Industry News*. 4 January 2021. Available online: https://www.thomasnet.com/insights/c-tpat-and-total-landed-cost/ (accessed on 28 May 2023).