informatics

MDPI

Review

A Comprehensive Analysis of the Worst Cybersecurity Vulnerabilities in Latin America

Omar Flor-Unda [1], Freddy Simbaña [2], Xavier Larriva-Novo [3], Ángel Acuña [4], Rolando Tipán [4] and Patricia Acosta-Vargas [1,5,*]

[1] Ingeniería Industrial, Facultad de Ingeniería y Ciencias Aplicadas, Universidad de las Américas, Quito 170125, Ecuador; omar.flor@udla.edu.ec

[2] Maestría en Ciberseguridad, Universidad Internacional de la Rioja, 170525 Logroño, Spain; freddysantiago.simbana143@comunidadunir.net

[3] ETSI de Telecomunicación, Departamento de Ingeniería de Sistemas Telemáticos, Universidad Politécnica de Madrid, Avenida Complutense 30, 28040 Madrid, Spain; xavier.larriva.novo@upm.es

[4] Redes y Telecomunicaciones, Instituto Superior Tecnológico Bolivar, Ambato 180109, Ecuador; aacuna@institutos.gob.ec (Á.A.); rtipan@institutos.gob.ec (R.T.)

[5] Intelligent and Interactive Systems Laboratory, Universidad de Las Américas, Quito 170125, Ecuador

* Correspondence: patricia.acosta@udla.edu.ec

Abstract: Vulnerabilities in cyber defense in the countries of the Latin American region have favored the activities of cybercriminals from different parts of the world who have carried out a growing number of cyberattacks that affect public and private services and compromise the integrity of users and organizations. This article describes the most representative vulnerabilities related to cyberattacks that have affected different sectors of countries in the Latin American region. A systematic review of repositories and the scientific literature was conducted, considering journal articles, conference proceedings, and reports from official bodies and leading brands of cybersecurity systems. The cybersecurity vulnerabilities identified in the countries of the Latin American region are low cybersecurity awareness, lack of standards and regulations, use of outdated software, security gaps in critical infrastructure, and lack of training and professional specialization.

Keywords: cyberattack; cyber defense; cyber threats; cybersecurity; Latin America

Citation: Flor-Unda, O.; Simbaña, F.; Larriva-Novo, X.; Acuña, Á.; Tipán, R.; Acosta-Vargas, P. A Comprehensive Analysis of the Worst Cybersecurity Vulnerabilities in Latin America. *Informatics* **2023**, *10*, 71. https://doi.org/10.3390/informatics10030071

Academic Editor: Francisco José García-Peñalvo

Received: 23 June 2023
Revised: 15 August 2023
Accepted: 19 August 2023
Published: 31 August 2023

1. Introduction

The use of technology to perform personal and work tasks requires more extensive use of devices, applications, software, electronic systems, sensors, and technologies that allow information to be processed and that, without sufficient care and security measures, can be vulnerable to attack by cybercriminals. The use of smart devices tends to be ubiquitous, incorporating multiple devices employing the Internet of Things (IoT) and presenting risks associated with increased connectivity and automation [1]. Intelligent systems also show risks in their use in aircraft navigation systems [2] and autonomous vehicles [3], whose vulnerabilities, in addition to affecting the computer system, sometimes threaten the integrity and life of users, in addition to affecting the interests of large companies by causing poor customer satisfaction.

In Latin America, cyber threats have significantly impacted several governments and countries, such as Venezuela, Mexico, and Argentina [4]. Threats have been identified in public organizations [5], generating significant economic losses for regional governments and companies. Communication systems have also been affected by cyberattacks [6]. Cyberattacks have also affected banking and financial systems in Latin American countries, causing operational failures and uncertainty among the institution's customers [7].

Latin America and the Caribbean are regions in the initial phase of building and implementing cyber capabilities to combat cyberspace threats. The increase in these threats in Latin American countries has been associated with the lack of maturity of National

Cybersecurity Strategies (NSCs), which suggests aspects, such as the lack of development and application of policies and strategies, lack of investment, lack of multilateral international cooperation agreements, and the lack of training programs for cybersecurity professionals [8]. The increased frequency of cybercriminal attacks has led to a greater need to motivate awareness and implement defense mechanisms to mitigate these threats.

According to the report "Report on Cybersecurity and Critical Infrastructure in the Americas" by the Organization of American States (OAS) of 2015 [9], it mentions that in Latin America, there are several organizations that ensure cybersecurity, among them are: the Cybersecurity Working Group of the Asia-Pacific Economic Cooperation (APEC), the Group of Governmental Experts on Security in Information and Communication Technologies (GETIC), and the Regional Cybersecurity Center.

The report Cybersecurity Trends in Latin America and the Caribbean and Government Responses [10] noted that since 2012 cyberattacks on public and private entities or websites have grown to annual figures of more than 61%. Countries, such as Ecuador, Guatemala, Bolivia, Peru, and Brazil, were among the ten most affected by the malware. Similarly, Uruguay, Colombia, and Chile presented malware infection figures above the global average, which framed this region and Asia with the highest rates of computer viruses globally. In the last seven years, the use of cyberspace to carry out bank fraud has become a problem, given that it was estimated that 92% of financial institutions had presented a cyberattack, with a success rate of 37% [11].

The effects of the recent COVID-19 pandemic have strongly impacted cybersecurity in Latin America (Figure 1), with recurrent cases reported around trends [10] in attacks on individuals and organizations. From these events, reference documents were developed that promote cybersecurity culture to minimize the impact of these threats [12].

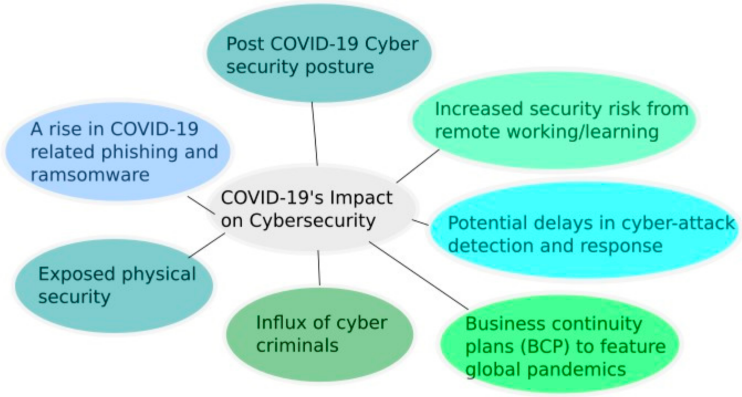
Post COVID-19 Cyber security posture
Increased security risk from remote working/learning
A rise in COVID-19 related phishing and ramsomware
COVID-19's Impact on Cybersecurity
Potential delays in cyber-attack detection and response
Exposed physical security
Influx of cyber criminals
Business continuity plans (BCP) to feature global pandemics

Figure 1. Trends in cybersecurity impacts caused by the aftermath of the COVID-19 pandemic.

Cybersecurity also considers aspects related to the digitalization of economies addressed by the Organization for Economic Cooperation and Development (OECD). The OECD and other influential organizations have recognized the dangers of a more digitalized economy [13] Institutional investment at all levels of government has been necessary to promote control strategies and generate policies to mitigate the impacts of cyber threats [14].

This article presents an overview of the impact of cyberattacks as well as the vulnerabilities that have been documented and that have affected the Latin American region. The Methodology Section describes the process by which the reference information was obtained. The section titled "Cyberattacks in Latin America" presents aspects, such as the most frequent types of attacks in the last five years, the most frequent attacks in Latin American countries, and cyberattacks through devices that use the Internet of Things (IoT). The section titled "Vulnerabilities to cyberattacks in countries of the Latin American region" describes the vulnerabilities that have been determined and documented: vulnerabilities in computer aspects, vulnerabilities by types of application, vulnerabilities in IoT devices, and vulnerabilities of a personal nature. It should be noted that the information and the scientific literature on these aspects does not present enough information, which is why official reports for the Latin American region and applications of companies recognized worldwide in the field of cybersecurity have been taken as a reference.

2. Methodology

This work was carried out through a systematic review whose dataset can be consulted in [12] The review of the scientific literature considered journal articles and conference papers. In addition to this, reports and documents issued by companies related to the development and dissemination of cybersecurity were taken into account, focusing on data obtained for the Latin American region. Scientific articles categorized in the first quartiles, Q1, Q2, Q3, and Q4, have been considered. The following terms were considered as inclusion criteria: "Cyberattacks, Latin America, vulnerability". PRISMA guidelines (Table A1 in Appendix A) have been considered for this systematic review. Five questions were asked to extract information from the reference documents: RQ1. What are the most frequent cyberattacks in Latin America? RQ2. What are the damages and consequences of cyberattacks in Latin American countries? RQ3. What importance has been given to cybersecurity in the governments of Latin American countries? RQ4. What are the cybersecurity vulnerabilities in Latin American countries? RQ5. What vulnerabilities affect IoT devices?

The search conducted in repositories and databases of the scientific literature was carried out considering the text strings presented in Table 1, identifying 606 related studies and from which the workflow presented in Figure 2 was carried out; they were reduced to 53 documents that were considered as a reference for the realization of this article.

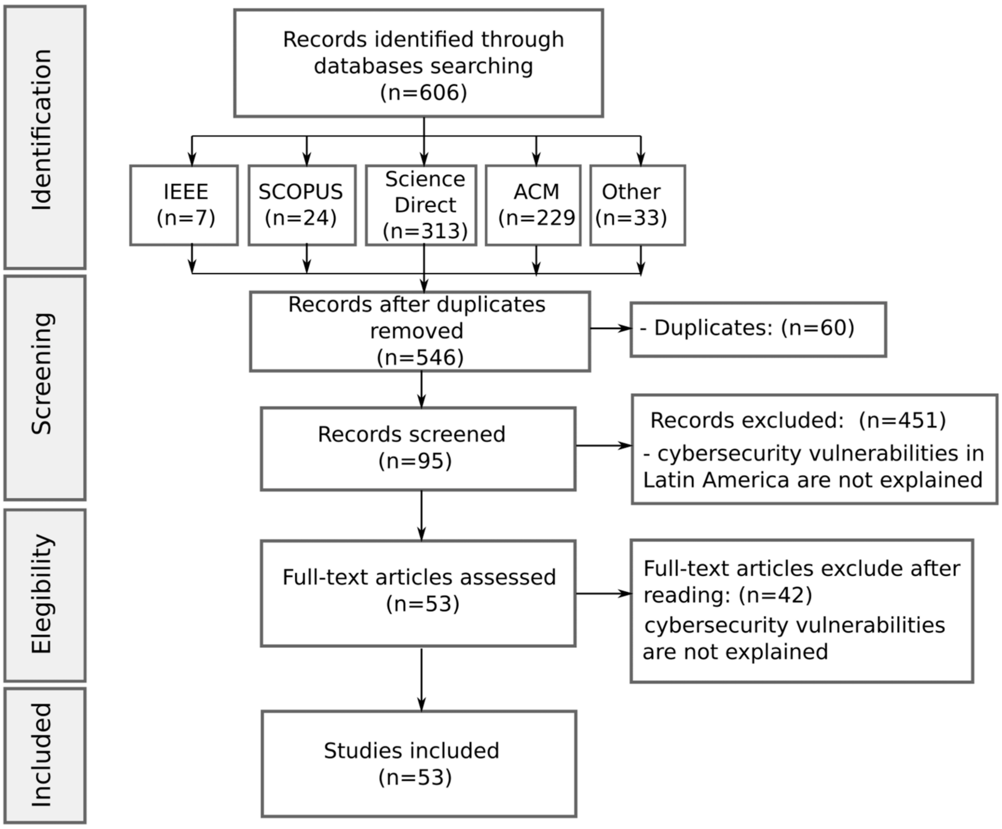
Identification
Screening
Elegibility
Included
Records identified through databases searching (n=606)
IEEE (n=7)
SCOPUS (n=24)
Science Direct (n=313)
ACM (n=229
Other (n=33)
Records after duplicates removed (n=546)
- Duplicates: (n=60)
Records screened (n=95)
Records excluded: (n=451)
- cybersecurity vulnerabilities in Latin America are not explained
Full-text articles assessed (n=53)
Full-text articles exclude after reading: (n=42)
cybersecurity vulnerabilities are not explained
Studies included (n=53)

Figure 2. Systematic review according to PRISMA methodology.

Table 1. Strings employed in the search for information across repositories and scientific literature databases.

Database	String Search	Studies Number
ACM	[Publication Title: cyber attack] OR [Publication Title: "Latin America"] AND [E-Publication Date: Past five years]	229
IEEE	search: cyber attack Latin America	7
Web of Science	cyber (Topic) and attack (Topic) and Latin America (Topic)	3
Scopus	TITLE-ABS-KEY (cyber AND attack OR threat AND Latin AND America)	24
Science Direct	Title, abstract, keywords: cyber threat Latin America	313
Manual Search	search: cyber attack Latin America	30
	Total number of studies	606

3. Cyberattacks in Latin America

This section addresses aspects related to cyberattacks that have affected countries in the Latin American region. The most frequent cyberattacks in the last five years have been considered, the attacks that have most affected each country, attacks on public and private organizations in countries of the region, and cyberattacks carried out through IoT devices.

3.1. Most Frequent Types of Attacks in the Last 5 Years

This section describes evidence of frequent cyberattacks in Latin American countries based on information provided by companies, such as Kaspersky Lab, reports submitted by government agencies of countries in the Latin American region, and information provided in the scientific literature considered in this review paper.

Table 2 presents the types of cyber threats that have strongly impacted Latin American countries in the last five years, according to information presented in [15,16] It also describes the impacts and how they affect and compromise systems by taking advantage of their vulnerabilities.

3.2. Cyberattacks in Latin American Countries

Despite the large number of countries that make up the Latin American region, there is socialized information regarding a few countries, such as those described in Figure 3. Official reports on cyberattacks in Latin America have considered the countries of Panama, Chile, Colombia, Ecuador, Argentina, Uruguay, Peru, Brazil, and Mexico. The attacks presented in Figure 3 show only the number of attacks regardless of the socio-economic impact and consequences they may cause in organizations and countries.

Cyberattacks have multiple variants, methods, techniques, and modes of execution, which evolve rapidly. From the information provided in [15], the graph presented in Figure 3 has been obtained, quantifying the occurrence of various types of cyberattacks for some countries in the region. The scale of events is considered between values of 0 and 5, in which zero represents the lack of cyberattacks and 5 represents a higher incidence on the generalized scale.

Figure 3 shows that the effects of data hijacking and identity theft have the highest values in the case of Ecuador. There is no direct evidence of considerable trends and variations in levels between countries and according to types of cyberattacks. Figure 3 highlights a lower impact on the effects of SSL communications. One of the least affected countries is Mexico, which shows a reduced value in all categories of cyberattacks. While Panama, Ecuador, and Uruguay add, in total, a more significant number of incidents.

The information provided in the scientific literature, official documents of related organizations [9,15–17], and reports of companies in the field of technology present multiple points of view on the impacts of cyberattacks that are sometimes limited to countries that have taken active measures to prevent and reduce risks and that have registered or documented these actions.

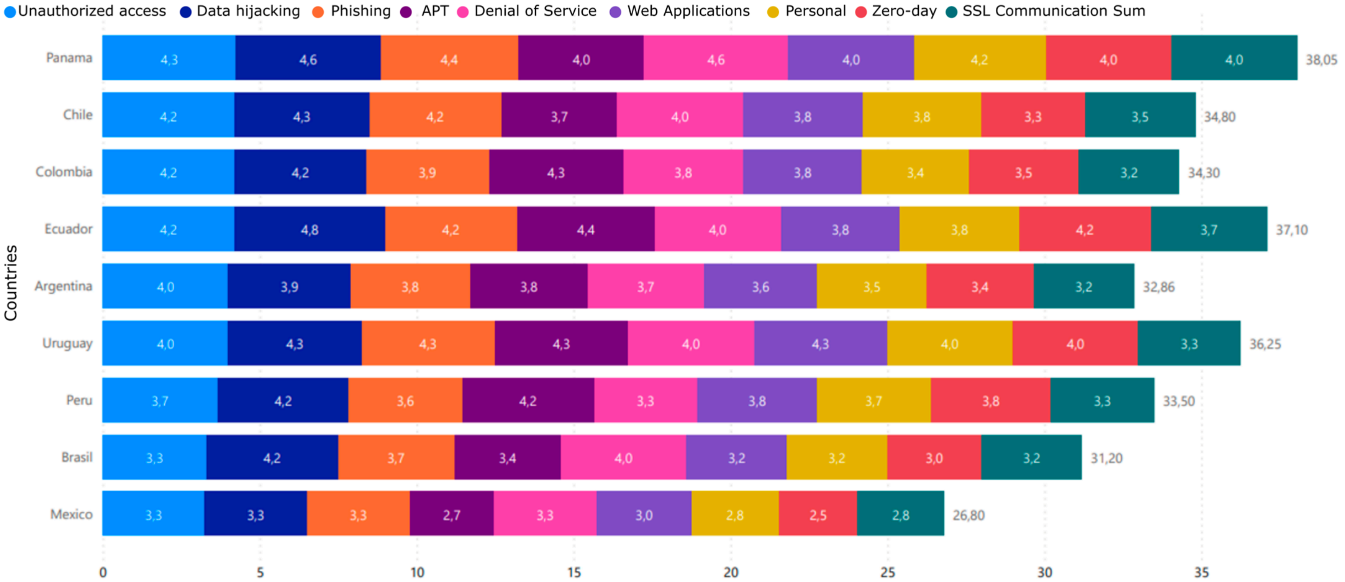

Figure 3. Levels of effects of cyberattacks in Latin American countries according to the type of threat.

Table 2. Types of attacks identified and that have impacted Latin America in the last five years.

Type of Attack	How It Operates	How It Affects
Denial of Service	A Denial of Service (DoS) attack aims to overwhelm a system's resources, rendering it unresponsive to legitimate requests. It alters DNS records to redirect traffic to a fake site, stealing sensitive data. The attacker impersonates IP addresses, seizing control of sessions between clients and servers.	The attack modifies DNS records, funnels traffic to a fraudulent site, and manipulates victim-server sessions by impersonating IP addresses. This floods the system with requests, preventing it from addressing valid demands and carrying risks, like data theft and breaches.
Phishing	Phishing impacts the security of personal and financial information. Tricking people into revealing sensitive data, like passwords or credit card numbers, leads to identity theft, financial fraud, and unauthorized access to accounts. It can also damage the reputation of impersonated organizations, leading to a loss of customer trust.	Phishing works by sending seemingly genuine emails with misleading links to fake websites. Victims are prompted to provide personal or financial information, which is then collected by attackers. Customized messages, tailored through research, enhance the effectiveness. Phishing occurs through emails, text messages, social media, or other electronic communication channels.
Personal	In this personal attack, exploiters manipulate system access to enact critical changes. Online harassers use digital platforms for defamation. Scammers extract bank info via deceitful calls, employing it for trickery. Attackers employ false emails for information extraction. Misuse of domains and trademarks seeks personal profit. Fake job and wage promises deceive through online resources.	Individuals can pose risks, accessing systems to make critical changes. Online harassment and slander also impact people. Scammers gather bank data through phone calls for deception. Fake emails seek information. Attackers misuse domains or trademarks for personal gain. False claims of employment and wages deceive via the internet.

Table 2. *Cont.*

Type of Attack	How It Operates	How It Affects
Ransomware	This malware restricts user access by blocking systems until a ransom is paid. “Ransomware-as-a-Service” facilitates fast attack creation using tools	Ransomware attacks affect victims and organizations significantly. Data restriction halts operations, affecting productivity. Victims face a dilemma: pay or risk data loss. Economic impact includes recovery costs and loss of trust. RaaS broadens risks by enabling less skilled attackers.
Unauthorized access	Unauthorized access to information systems breaches privacy and is a necessary step in committing various cybercrimes. Many of these crimes demand private or pertinent data [18].	Unauthorized access has significant consequences. It compromises privacy and data security for individuals and organizations. This can lead to theft of sensitive information, misuse of personal data, and potential for other cybercrimes reliant on illegally obtained information. Losing control over data can harm the reputation of involved parties and foster a climate of distrust in the online community.
Advanced persistent threat (APT)	An APT attack is stealthy in computer networks. The attacker gains and maintains unauthorized access, going unnoticed. They monitor, intercept, and transmit sensitive data. The goal is data theft, not causing disruptions [19].	An APT has serious consequences. It filters valuable data, exposing trade secrets, intellectual property, and personal information. It can erode trust, with legal and financial repercussions. Detecting and eliminating it is costly and time-consuming, impacting normal operations.
Web Applications	These threats target web applications, services, or mobile apps that utilize exposed or vulnerable APIs. Common vulnerabilities, like SQL injection, cross-site scripting (XSS), and content management systems (CMS), are prevalent in web application attacks. Mitigation includes formulating security policies, using a web application firewall (WAF), vulnerability scanning, and patching [20].	The effects of these attacks can be severe. Exploiting vulnerabilities in web applications can lead to data leaks, information theft, and compromised user accounts. This can significantly impact an organization’s reputation, user trust and potentially result in legal and financial consequences. The ongoing need to mitigate and patch against these threats can increase an organization’s workload and operational costs.
SSL communications	The SSL/TLS protocol is widely used to ensure data security. However, its broad adoption makes it attractive for discovering and exploiting vulnerabilities that can compromise the integrity and security of information [21].	The impact of SSL/TLS communication vulnerabilities can be significant. Exploiting these vulnerabilities could allow attackers to intercept, alter, or steal sensitive data transmitted over secure connections. This can lead to exposure of sensitive information, privacy breaches, and potential legal and financial consequences for affected organizations and users. Trust in online communication security can also be undermined, affecting the adoption and continued use of online services relying on SSL/TLS data protection.
Zero-day	A zero-day attack aims to execute malicious code in an application or system by exploiting vulnerabilities unknown to users and product manufacturers. These unpatched vulnerabilities make them especially dangerous [22].	Zero-day attacks have a significant impact. Exploiting unknown vulnerabilities without restrictions can lead to data theft, malware propagation, and overall system compromise. Lack of effective defenses increases risk, damaging reputation and resulting in legal liabilities for compromised data or unauthorized access.

Kaspersky Lab (2020) recorded more than 746 thousand malware attacks daily during the year 2020 in Latin America, which implies that nine malware cyberattacks are carried out per second. At the same time, it was detected that the three main countries with the highest incidence of cybercrime are Brazil (56.25% of the total in the region), Mexico (22.81%), and Colombia (10.20%). On the other hand, it is essential to highlight that of a total of 62 million attacks detected by this firm during 2020, 66% were linked to robberies of private and commercial entities, while the remaining 34% were related to criminal activities, hacktivism, and attacks on government systems [11].

Relevant data on cyberattacks have been collected on the German statistics portal [23] Table 3 summarizes the essential milestones in cyberattacks that have affected Latin America in the last three years.

Table 3. Important milestones recorded around cyberattacks that have affected Latin American countries in the last three years.

Aspect	Description
Countries in Latin America most targeted by cyberattacks in 2020	As of September 2020, a significant portion of cyberattacks in the Latin American countries under scrutiny focused on Brazil, with nearly 56 percent of the attacks targeting users or infrastructures. Mexico followed closely, with approximately 28 percent of the attacks directed toward its users. Colombia took third place, which experienced over 10 percent of the cyberattacks.
Distribution of human-initiated cyberattacks originating from Latin America in the second half of 2021 by device	In the latter half of 2021, a significant majority of human-initiated cyberattacks linked to Latin America, precisely about 72 percent, were identified as originating from mobile devices, while approximately 28 percent were reported to have developed from desktop computers. Moreover, the attack rates observed in Latin America surpassed the global average across all channels.
The cyber-attack rate in Latin America compared to the global average in the second half of 2021 by channel	In the latter half of 2021, Latin America experienced a significantly higher incidence of cyberattacks than the global average. The rate of attacks originating from mobile browsers surpassed three percent, exceeding the worldwide average of 2.4 percent. Furthermore, the region recorded the highest rate of cyberattacks from desktop computers, reaching four percent, while the global average stood at 1.8 percent.
Year-on-year change in the volume of cyberattacks originating in Latin America in the second half of 2021 by type	In the second half of 2021, there was a year-on-year growth of 455 percent in automated bot-driven cyberattacks from Latin America. Additionally, during the same period, there was a year-on-year growth of almost 140 percent in human-initiated attacks. Furthermore, attack rates in Latin America exceeded the global average across all channels.
Countries and territories with the highest risk of local malware infections in Latin America in Q2 2020	In the second quarter of 2020, approximately 26 percent of computer users in Bolivia who utilized Kaspersky Lab's security products were targeted by local malware threats. Ecuador and Cuba followed closely, with 24.3 percent and 23.5 percent of users facing at least one regional malware threat. Furthermore, during that same period, Ecuador also ranked among the Latin American countries with a high incidence of malware attacks on mobile users.
The proportion of internet users attacked by malware in selected Latin American countries and territories in the second quarter of 2020	In the second quarter of 2020, around six percent of internet users in Brazil, who utilized Kaspersky Lab's security products on their computers, experienced web-based malware attacks. On the other hand, Mexico had a 4.6 percent rate of internet users targeted by trojans during that period. Mexico also ranked third among Latin American countries, with a significant percentage of mobile users being attacked by malware.
The proportion of mobile users attacked by malware in selected Latin American countries in the second quarter of 2020	During the second quarter of 2020, around nine percent of mobile users in Argentina, who used Kaspersky Lab's mobile security products, encountered malware attacks. Similarly, nearly 4.5 percent of mobile users in Peru experienced the same problem. The complete expansion of mobile internet in Latin America is anticipated to persist.

Table 3. *Cont.*

Aspect	Description
The most common malware strains in Latin America in the first half of 2020, by a percentage of malware attacks	In the first half of 2020, Emotet stood out as Latin America's most common type of malware. It accounted for nine percent of all malware attacks in the region. The open-source miner XMRig followed closely behind, responsible for seven percent of the detected attacks.
Countries in Latin America and the Caribbean are the most affected by phishing attacks in 2020	In 2020, Brazil and Venezuela had the highest number of users targeted by phishing attacks in Latin America and the Caribbean, with 19.94 percent and 16.84 percent, respectively. These phishing attacks expose users to malicious software, including ransomware, which encrypts data and demands payment for its release. Brazil also experienced the highest number of ransomware attacks among all countries in the region that year.
Latin American countries with the highest proportion of users attacked with ransomware in 2020	From September 2020 onwards, Brazil stood out as the country in Latin America with the highest percentage of unique users affected by ransomware, with nearly 46.7 percent of users falling victim to these attacks. Mexico followed closely behind in second place, with approximately 22.6 percent of users being targeted, while Colombia ranked third, with over eight percent of users experiencing ransomware attacks.
Latin American countries most attacked by cyber miners in Q2 2020	During the second quarter of 2020, Bolivia experienced the highest mining attacks among computer users who relied on Kaspersky Lab's security products in Latin America. These attacks accounted for approximately 1.22 percent of the cases. A malicious mining attack occurs when online currency, cryptocurrency, is illicitly mined from a device. Furthermore, Bolivia also ranked as the Latin American country with the highest risk of local malware infections during that period.
Latin American countries were the most attacked by web applications in June 2019	Based on the recorded web application attacks in June 2019, Brazil endured the highest volume of attacks within seven days among Latin American countries. Approximately 8.3 million attacks were directed toward websites in Brazil. Argentina, taking second place, faced nearly 1.8 million attacks.
Leading IT security incidents among Latin American companies in 2021	According to a 2021 survey conducted among security professionals in various Latin American companies, 24 percent of the participants disclosed that their organizations had experienced malware infections. Additionally, 17 percent reported social engineering attacks, whereas 13 percent reported unauthorized access to their business applications and/or databases.

3.3. Cyberattacks on Public and Private Organizations in Latin America

Cybercrime is a global phenomenon that has repercussions in both the private and public spheres of nations. Cybercriminals pursue financial benefits and carry out attacks targeting geostrategic structures to serve the interests of the state. Due to the dispersed nature of threats, the actors involved, and their targets, cybercrime affects different regions differently. In the case of Latin America, there is a unique regional profile in terms of the threat of cybercrime, given that the socio-economic challenges affecting the region uniquely shape experiences in the cyber field [24]. Several government agencies in Latin America have been targeted by ransomware attacks in recent months, with the latest victims being Chile and the Dominican Republic.

In 2022, multiple attacks on critical infrastructure improved essential services for the population, which generated significant consequences in the face of disruptions. In addition, it includes services that handle substantial volumes of citizens' personal data that can be used to carry out cybercriminal activities, such as identity theft or social engineering attacks [25].

Costa Rica fell victim to large-scale ransomware attacks initiated by the group dubbed Conti, in April 2022. The cyberattack involved 27 ministries in a series of interrelated attacks that began at Costa Rica's Ministry of Finance. Conti's action left parts of Costa Rica's digital infrastructure paralyzed for months while at the same time disrupting public health care and the salaries of some public sector workers [26].

One of Argentina's largest internet service providers, Telecom Argentina, also suffered a major ransomware attack involving around 18,000 computers in 2020. In this incident, hackers demanded a $7.5 million ransom while employees were prevented from accessing internal databases and VPNs [27].

Cybersecurity strategies in the water sector in Latin America and the Caribbean are currently being developed and implemented, constituting a current vulnerability. This vulnerability of the industry jeopardizes the water security of each country. Several elements have been identified that can be attacked by cybercriminals, such as meters that are part of intelligent water management systems, applications that allow the provision of services, and that operate through the use of information and communication technologies [28].

Public institutions in middle-income and developing countries in Latin America are affected by cybercriminals who extort government entities, as is the case with the judicial system in the Argentine city of Córdoba. Attackers destroyed a flood monitoring system in the Indian state of GOA. In addition to this, there were also disruptions at Zambia's central bank [29].

Some services that support booking travel, flights, hotels, and other tourism-related activities are often used for cybercriminal activities. They are scammed through these portals in which people book and plan their trips, tempted by reasonable costs and opportunities, contributing a value of 30 to 50% of the total cost [30]. In addition to this way of accessing money for a service that is not provided, these portals have access to the private information of users and, sometimes, to their credit card numbers, with which fraudulent purchases are made without the consent of users.

According to [31]. some of the most common cyberattacks faced by financial institutions are credential theft and identity fraud to gain unauthorized access to bank accounts and economic systems. Data manipulation and theft have also been used to commit fraud and extortion.

Industrial sectors and economic activities linked to the internet or digital services in Latin America faced significant losses and risks due to cyber threats, resulting in approximately USD 1 trillion in cyber defense expenditures in 2019. In addition, cyber threats are perceived as the main risk in cyberspace by private and governmental entities in Latin America and the world [8].

Brazil was the country most affected by cyberattacks in Latin America in 2020, with 55.97% of attacks targeting that country, followed by Mexico with 27.86% and Colombia with 7.33%. Brazilian companies detected social engineering (phishing) and malware attacks. In 2018, Mexico suffered a phishing attack that affected several banks and businesses, resulting in the loss of millions of dollars. In 2017, a malware campaign known as "Operation Blockbuster" affected several companies and organizations in Latin America, including telecommunications companies in Brazil and Mexico.

In 2016, Banco de Chile suffered a malware attack that affected its online payment systems. In 2015, the government of Venezuela fell victim to a distributed denial of service (DDoS) attack that affected several government websites. In 2014, the National Bank of Costa Rica suffered a malware attack that affected its online payment systems [24].

In Mexico, the Bank of Mexico (Banxico) was the victim of a cyberattack in which 836 bank accounts of 10 different institutions were victims of fraud, and the attack had a cost of approximately MXN 300 million (almost USD 16 million). In Brazil, Banco Inter was apparently hacked and confidential information leaked, causing an 11% drop in market shares. In Chile, Banco de Chile was also the target of a cyberattack, where hackers stole CLP 10 million [25].

In September 2020, Brazil had the highest proportion of unique users attacked with ransomware in the region, with almost 46.7% of users infected. Mexico ranked second, with approximately 22.6% of users attacked, followed by Colombia, with more than 8% of affected users. In addition, the document mentions specific cases of ransomware attacks in the region, such as the attack on Panama's Ministry of Social Development in January 2021, which affected its network infrastructure and backup systems [26].

The Latin American and Caribbean region has experienced a number of cyberattacks in recent years, including attacks on banks, governments, and businesses. The most common attacks evidenced for countries in the Latin American region correspond to ransomware and phishing [32].

3.4. Cyberattacks through IoT Devices

The rise of IoT devices has expanded the reach of cyber threats, as evidenced by the case of the powerful Pegasus spyware in Mexico. Developed by NSO Group, this software has targeted various figures, including politicians and activists, and researchers investigating the disappearance of students. In an incident revealed by the University of Toronto's Citizen Lab, the Group of Independent Experts (GIEI) was attacked in 2016 with poisoned text messages seeking to install spyware. This highlights the subtlety with which attackers leverage user interactions to infiltrate IoT devices [27]. This case highlights the urgency of addressing vulnerabilities in IoT devices. The cybersecurity of these devices is essential to prevent intrusions and unauthorized access to sensitive information. As IoT becomes more deeply integrated into our lives, data protection and privacy must be priorities, and collaboration between governments, businesses, and cybersecurity experts needs to be strengthened to ensure a safe and trusted digital environment.

Cyberattacks through IoT devices have significant impacts on cybersecurity and privacy due to the interconnection of multiple devices. The growing number of internet-connected devices, such as security devices, medical health tracking, entertainment, and home automation, has created an ecosystem prone to vulnerabilities. In Latin America, cybercriminals target hospitals and other IoT devices, posing serious threats to users' privacy and security. Vulnerabilities, such as lack of computational power, poor encryption in data transmission, insecure internet applications, and lack of authentication and authorization expose these devices to cyberattacks [25].

Deep learning has been employed to detect cyber threats in the mobile cloud with an impressive accuracy of 97.11% (Analysis of Cyberattacks in Public Organizations in Latam). These initiatives seek to reduce the risk of attacks and protect the integrity of electoral processes, a particularly relevant issue in Latin America, where the possibility of voting systems being attacked has been identified, jeopardizing the integrity of information crucial for the exercise of democracy [28].

In addition, it has been recognized that Latin America faces similar challenges to other regions in terms of the security of IoT devices. Lack of security patches, inadequate implementation of security measures, and exposure to cyberattacks, malware, and hackers are shared concerns (Lack of Technological Innovation in IoT in Colombia). The lack of technological innovation in the region has impeded progress in the field of IoT, with cooperation between companies and governments being crucial to boost investments in a solid and secure communications infrastructure that is current with the digital age [29].

Despite efforts to address these vulnerabilities, successful cyberattacks on IoT devices have been demonstrated. Examples of hacked routers, media centers, televisions, and even refrigerators highlight the seriousness of the situation and the need to strengthen security on these devices [30]. In this context, greater interest on the part of governments to promote technological advances in IoT is essential, encouraging research in universities and local companies to improve competitiveness and security in the region [29].

Cyberattacks through IoT devices in Latin America have a significant impact on cybersecurity, privacy, and the integrity of systems, highlighting the need to address these vulnerabilities effectively and collaboratively.

4. Vulnerabilities to Cyberattacks in Latin American Countries

This section presents the vulnerabilities identified for the countries of the Latin American region that correspond to computer aspects, according to the type of application, in IoT devices of a personal nature and some trends with respect to new vulnerabilities identified in the scientific literature.

4.1. Computer Vulnerabilities in Countries of the Latin American Region

In order to visualize the main vulnerabilities in the computer aspect and their impact in countries of the Latin American region, the information provided in the biweekly reports that the division for Latin America of the company Securesoft publishes through its webpages and in which it addresses the cases of incidents in cyberattacks and providing alternative solutions to solve these vulnerabilities has been taken into account. Based on the information supplied by Securesoft Cyber Intelligence's bi-weekly reports [29–31,33–49]. Figure 4 represents the attack targets and vulnerabilities that affected organizations have identified due to cyberattacks. They have been considered as reference information to the new vulnerabilities presented according to the Securesoft division for Chile, Colombia, Peru, and Ecuador.

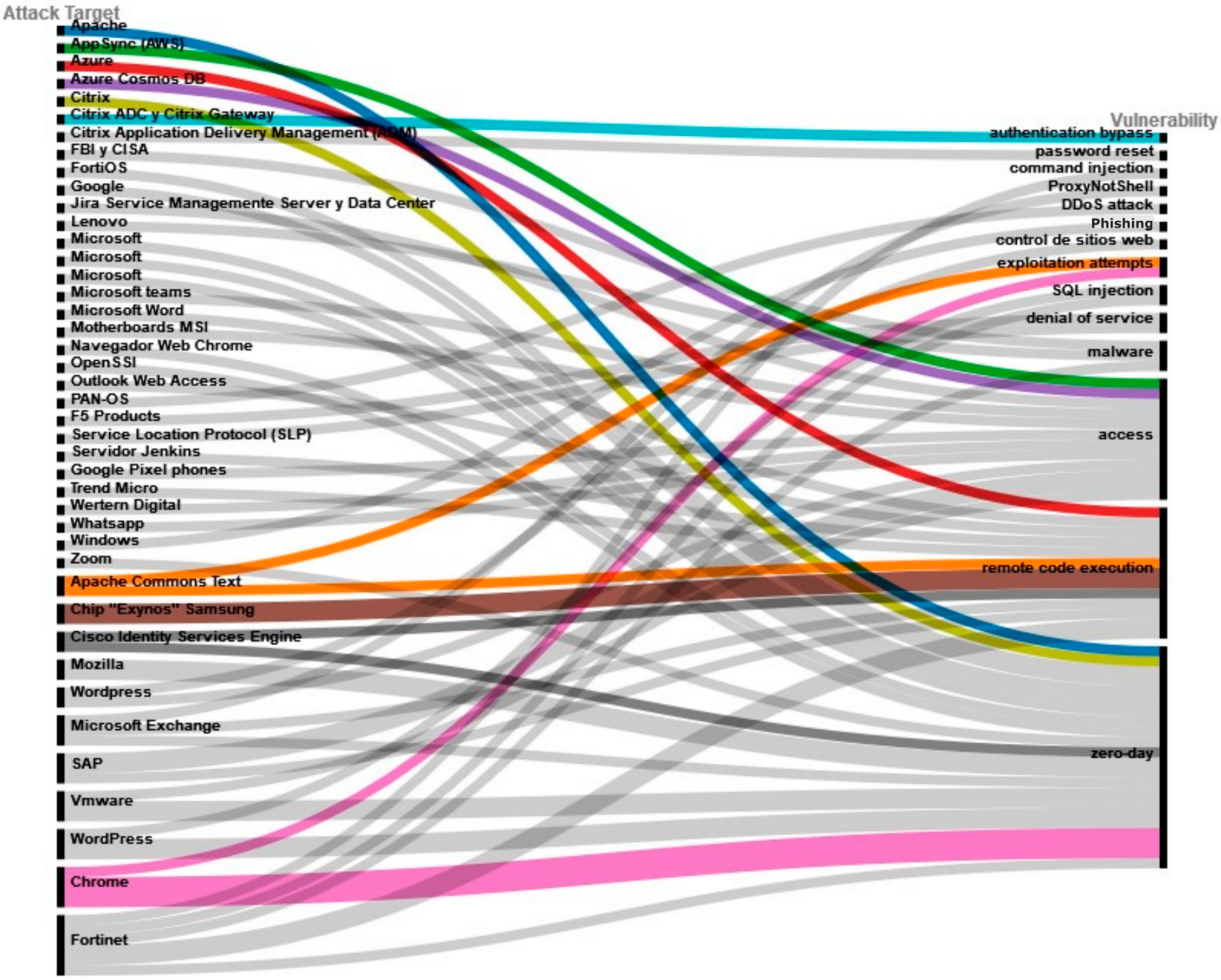

Figure 4. Vulnerabilities identified in attacks on operating systems, applications, websites, social networks, platforms, and database networks, according to the reports of the last year of the company Ciberinteligencia Securesoft.

Figure 4 most significantly illustrates how organizations, applications, websites, browsers, devices, operating systems, protocols, platforms, servers, and data centers present vulnerabilities that are eventually updated with security options by organizations affected by a variety of attacks that reveal a number of vulnerabilities of which the most frequent are zero-day: remote code execution, access, malware, denial of service, and SQL injection.

Baseline information shows evidence of a continuous effort in updating security systems that run alongside computer applications and whose updates are sometimes made in short times of one or two weeks in most cases.

As for the cyberattacks produced in recent years and according to the telemetry of the ESET company, attacks on critical infrastructures have not yet been identified, although there is a large amount of evidence showing the effects that government agencies have faced concerning destabilization attempts in Latin American countries [50].

Software used by organizations or personal computers can have bugs or vulnerabilities in their operating systems, which are exploited by cybercriminals who find predictive entry routes to carry out attacks with malicious code, information theft, or intrusions. More frequently in organizations and, according to the ESET telemetry report of the year 2021, in which the record of reported vulnerabilities was broken with more than twenty thousand records (60 verified daily news), Android applications, website plug-ins, among others, presented an average criticality of 5 and 6 points out of 10 according to the CVSS score (or Common Vulnerability Scoring System). The most affected products were document readers, database applications, server and service administrators, development tools, and multipurpose corporate applications. Five exploits were identified in the Latin American region; these malicious codes targeting existing vulnerabilities in versions 2003 (Windows, Microsoft, Redmond, WA, USA) and 2008 (Mac, Apple, Cupertino, CA, USA), 2019 versions of Microsoft Exchange, Windows 7, Server 2003, Server 2008, and Windows Office in their interpretations of 2003, 2007, and 2010 [29].

Through the use of the application of Ciberamenzas in real time of free access and enhanced by the company Kaspersky [51]. the values obtained that correspond to the most frequent threats in the last 30 days have been consulted and are presented in Figure 5 for the countries of Argentina, Bolivia, Brazil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Mexico, Panama, Paraguay, Peru, Dominican Republic, Uruguay, and Venezuela. In most countries, except Paraguay, Peru, and Uruguay, the vulnerabilities correspond to MSOffice.CVE (Microsoft Office) and Multi.desert.gen (file system). As for Panama, the most frequent vulnerability is HTTP. CVE (Apache server) allows a request smuggling attack.

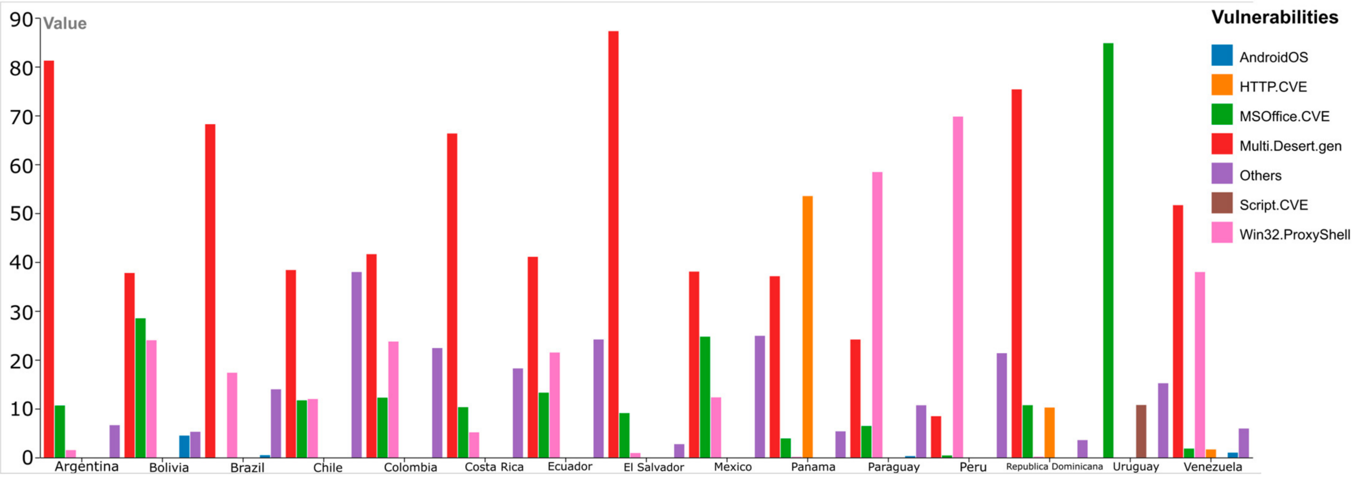

Figure 5. Vulnerabilities by type of computer application.

4.2. *Vulnerabilities by Computer Application Type*

Similar to the rest of the world, applications are exploited by cybercriminals due to their vulnerabilities and wide diffusion in the countries of the Latin American region and the rest of the world.

Work computers and devices, such as tablets on which multiple applications are used to execute tasks, use applications that attackers exploit, as some applications and software have vulnerabilities. There is clear evidence of significant exposure of Microsoft Office applications, which, despite being reliable and long-standing applications, are prone to mishandling by users, who have access to their privileges and settings, which is why attackers prefer to use these applications [48].

Because applications, such as Office, Adobe reader (PDF), and browsers run on operating systems, cyberattackers use vulnerabilities in operating systems and applications to access and exploit sensitive information.

As shown in Figure 6, it is evident that IoT devices, which use Microsoft Office applications, have potential risks along with the use of browsers and the Android operating system. They are also mentioned to have vulnerable applications, file managers in PDF format, Adobe Flash, and Java applications.

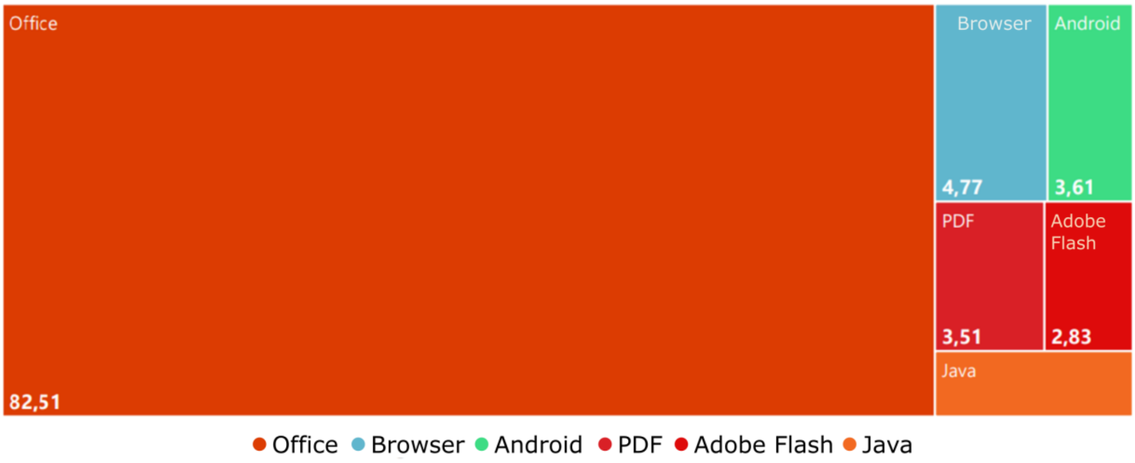

Figure 6. Vulnerabilities by type of computer application.

4.3. Vulnerabilities in IoT Devices

Vulnerabilities in cybersecurity, due to the connection of multiple IoT devices, are open doors for attackers who can access devices connected to the internet, such as security devices, medical devices, health tracking devices, entertainment devices, and home automation devices. In Latin America, one of the most interesting targets for crime is hospitals. In addition, IoT devices are vulnerable to attacks and hijacking of systems, which implies severe consequences for the privacy and security of users [25].

IoT devices in Latin America present the same vulnerabilities as in other parts of the world, such as the lack of security patches, the lack of implementation of security methodologies, and the exposure to computer attacks, malware, malicious software, and hackers. In addition, it is mentioned that the lack of technological innovation has prevented the positioning of Colombia in Latin America, and globally in terms of IoT, it is important to consider the cooperation of public and private companies to encourage manufacturers to invest in a solid and secure communications infrastructure that fits the demand and is at the forefront of the digital era.

Some vulnerabilities in IoT devices, such as a lack of computational power, a lack of encryption in data transport, insecure internet applications, and a lack of authentication and authorization to send and deliver data, allow them to be susceptible to cyberattacks [49].

Vulnerabilities to cyberattacks have been identified that can affect the integrity of electoral processes in Latin America. Voting systems are put at risk by attackers who compromise the integrity of the information necessary for the exercise of democracy [34].

Some IoT devices that were hacked in attacks carried out in the years of 2013 and 2014 include routers, media centers, televisions, and even refrigerators. There is no list of specific devices, but it is studied according to the number of IoT devices connected to the internet and their security vulnerabilities [35].

In Latin America, as in the rest of the world, IoT devices have created new challenges in cybersecurity, as these devices are designed to collect and transmit large amounts of data, increasing the risk of cyberattacks. IoT devices often have security vulnerabilities due to a lack of standards and regulations, making them more susceptible to attacks [50]. In addition, IoT devices can be used as backdoors to access other connected systems on the network.

Because there are currently a large number of bank transfers made with mobile devices (61%), there are concerns about the growing number of payment platforms and the growing use of IoT devices. Despite this, cyberattacks carried out through cell phones do not appear to be the most frequent due to the guarantees that the operating companies provide to their users so that they can trust their services and continue using them.

Some risks presented in Figure 7 have been identified in relation to cyberattacks that occur exclusively on cell phones. Some of these risks aim to access sensitive information using smartphones to access bank accounts or make fraudulent transactions [51]. There is little information on attacks on mobile cellular devices; global statistics do not record the most frequent attacks by region for Latin American countries in recent years.

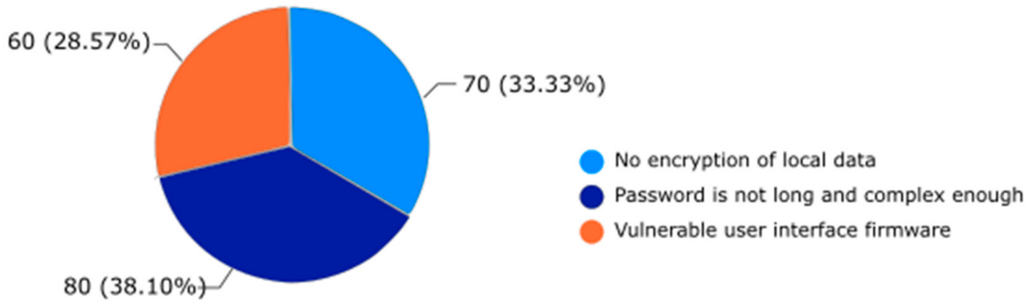

Figure 7. Principal vulnerabilities in IoT devices.

According to reports from the company Kaspersky, the number of malware attacks in general for the Latin American region is 2300 attacks per minute. Phishing scams are one of the most important and frequent vulnerabilities in the countries of this region. Most previous attacks have been carried out through cell phone use [52]. The most attacked countries are Brazil and Ecuador, which occupy the sixth and eighth positions in the global list of the top ten phishing attacks through smartphones.

IoT devices are vulnerable due to processes in which no human actions are performed and run with applications and communications networks. There is the vulnerability of these devices as they are prone to losing connectivity, for example, in the case of smartphones, in which they can lose connectivity due to wireless interruptions, as well as the fact of not having enough power in the battery of the device. IoT devices are extremely susceptible to eavesdropping, and their ubiquitous characteristic makes security crucial [53].

To reduce vulnerabilities in the use of mobile devices, Cloud Deep learning has been used to detect cyber threats with an accuracy of 97.11% (Analysis of Cyberattacks in Public Organizations in LATAM). It is essential to consider the cooperation of public and private companies to incentivize manufacturers to invest in a robust and secure communications infrastructure that meets the demand and is at the forefront of the digital age. In addition, it is mentioned that the lack of interest on the part of the government has caused few technological advances in IoT in the region, so universities and local companies should be encouraged to research these technologies to improve productivity and make the region more competitive [35].

According to [15]. IoT device vulnerabilities can be grouped in percentages and their main reasons, as shown in Figure 7.

Some risks presented in Figure 8 have been identified in relation to cyberattacks that occur exclusively on cell phones. Some of these risks aim to access sensitive information using the smartphone to access bank accounts or make fraudulent transactions [32]. There is little information about attacks on mobile cellular devices; global statistics do not record the most frequent attacks by region for Latin American countries in recent years.

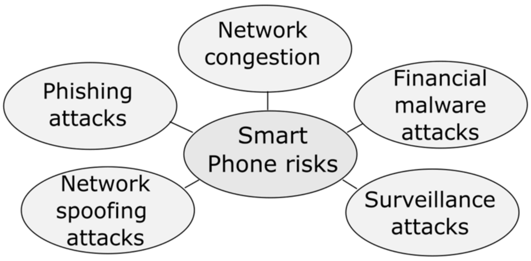

Figure 8. Top threats affecting smartphones.

4.4. Vulnerabilities to Cyberattacks Due to Personal Factors

The attitude of the inhabitants and governments of Latin American countries towards cyberattacks is crucial to achieve better results and reduce the impact of cyber vulnerabilities. Figure 9 presents the results obtained in [9]. whose study addresses aspects, such as Cybersecurity Policy and Strategy, Cyber Culture and Society, Education–Training, and Cybersecurity skills. Figure 9 shows an assessment of the government's mindset or awareness of cyber threats, user awareness, and professional training for some of the countries in the region.

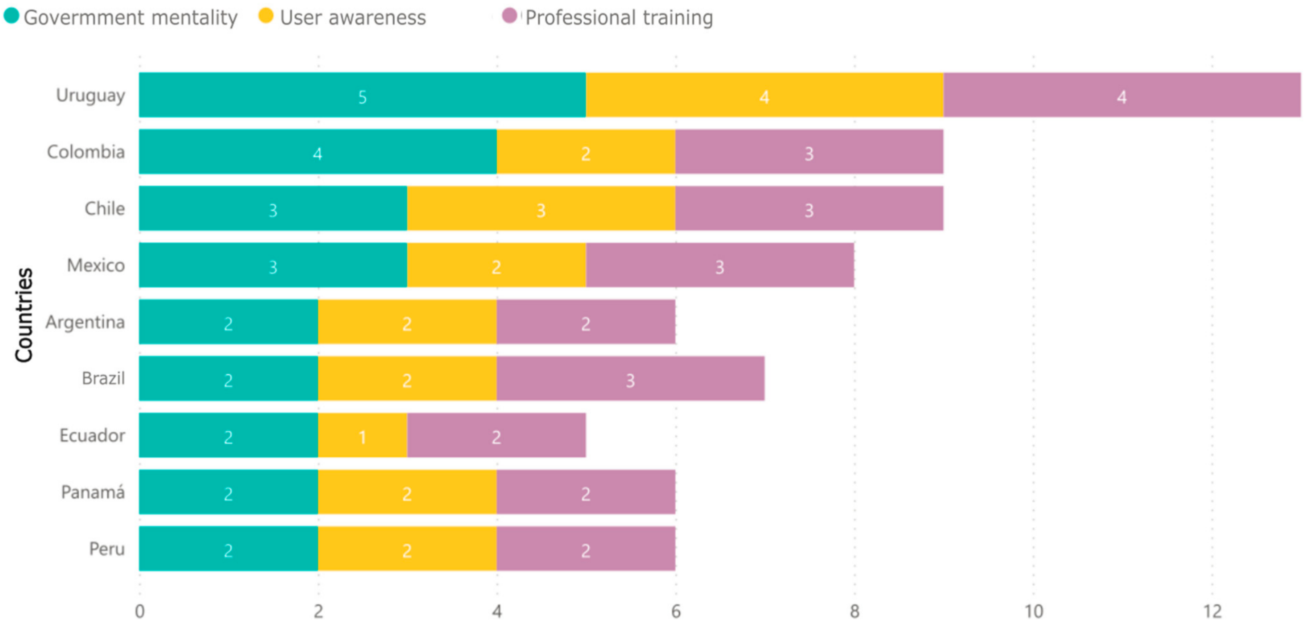

Figure 9. Factors that identify the response of some countries in the Latin American region to cyberattacks.

Significant differences are evident between the countries, highlighting a better attitude on the part of the Uruguayan government and its inhabitants, who show a greater interest and importance for the levels of professional training, as well as a greater knowledge of the users and their respective governments. Colombia and Chile have similar levels in terms of professional training in cybersecurity, while Ecuador presents in this evaluation, the lowest levels in all three areas. Government mentality, user awareness, and professional training are decisive factors when facing cyberattacks in both public and private companies.

Considering the number of organizations that have reported cases of cyberattacks in Latin American countries [15]. from this information, Figure 10 has been created. Uruguay stands out as one of the countries with the highest number of incidents, followed by Peru and Colombia. The corrective actions handled in Argentina are much more effective than those in other countries, as they allow a recovery time of 11 min, which is relatively shorter than those carried out in Peru and other nations.

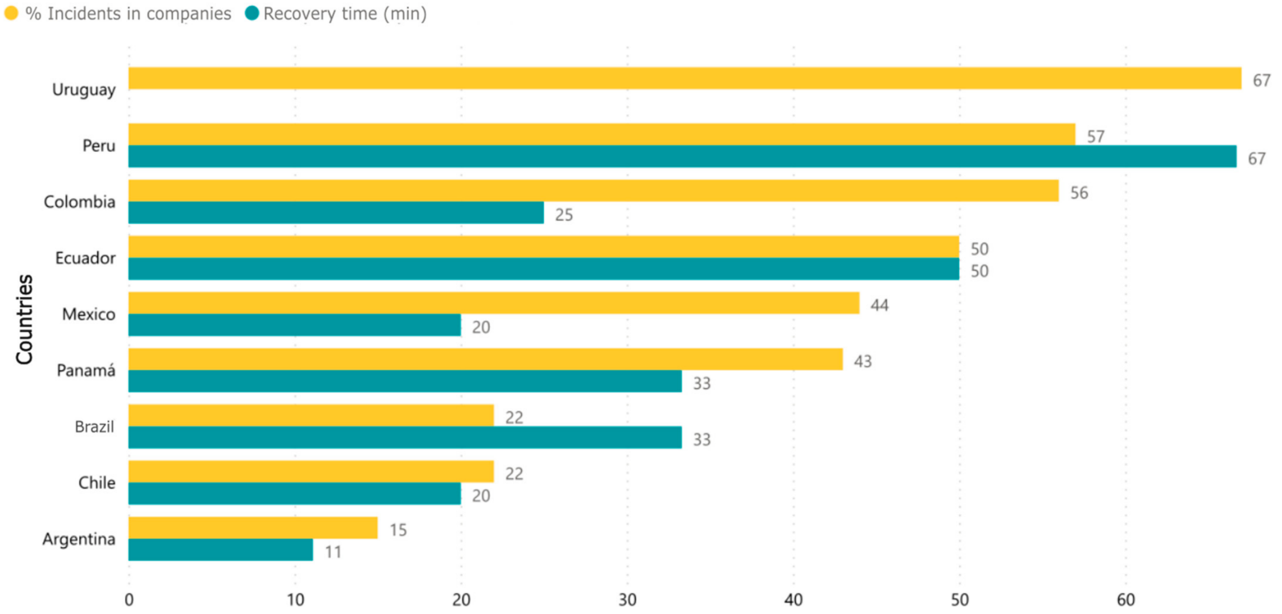

Figure 10. Incidents due to cyberattacks in Latin American companies (%) and recovery times (min).

5. Government Response to Mitigate the Effects of Cyberattacks

With the aim of reducing the negative impacts suffered by the public and private services of the nations, the efforts of the governments of Latin America have raised some government measures and cybersecurity laws.

The governments of Latin American countries have taken steps to strengthen their cybersecurity. In Argentina, a National Cybersecurity Directorate has been established, and laws have been enacted to regulate cybersecurity [21]. In Mexico, the police are responsible for cybersecurity, and the country has participated in international initiatives to combat cybercrime. In Venezuela, “a cybersecurity roadmap has been established, and a government agency has been created to coordinate the response to cyberattacks” [54].

Uruguay has created the National Cybersecurity Incident Response Center (CERTuy) to coordinate efforts to respond to security incidents. Argentina has created the National Program for Critical Infrastructure, Information, and Cybersecurity to protect critical infrastructure and promote collaboration between the public, civil, and private sectors [55]. Colombia has been the first country in the region that has led and taken as a priority the aspect of cybersecurity over the other countries in the region [56].

Organizations, such as the Inter-American Development Bank and the International Telecommunication Union, often provide support by facilitating countries’ efforts to implement effective cybersecurity measures [57]. It is important to note that the specific strategies and approaches used with the support of the international community may vary as they are influenced by various socio-economic and political factors [58].

The report “Cybersecurity in Latin America and the Caribbean 2020” highlights that governments in the region have given increasing importance to cybersecurity in recent years. There has been a significant increase in the adoption and revision of national cybersecurity strategies that address the security of all governments and society. National cybercrime laws have been implemented or adapted in developing countries that previously did not have such laws. This demonstrates the commitment of governments to address cybersecurity challenges and protect their citizens and their critical infrastructure [59].

It is important for governments to advance national cybersecurity strategies to minimize the vulnerabilities, risks, and threats inherent in the confidential information of their public services [4]. For this reason, the work must be coordinated with public authorities, universities, society, and international organizations [60]. It has become relevant to sensitize multiple strategic sectors about the importance of cybersecurity. However, greater efforts are required to fill the large gap that exists around this issue [61].

The problems in utilities are vulnerability to cyberattacks, weak security defenses, and a lack of consideration for cybersecurity in IoT environment designs. Therefore, it is possible to infer that major vulnerabilities could include a lack of adequate security measures on IoT devices, a lack of data encryption, a lack of strong authentication and authorization, and a lack of regular security updates.

In the study presented in [62]. it is mentioned that the cybersecurity commitment in Latin America is less than 0.70. Brazil and Uruguay are between 0.60 and 0.70, indicating that they have improved their national cybersecurity strategies. Colombia remains at an average of 0.58, while Paraguay has improved in 2018. Ecuador is between 0.35 and 0.47, with a slight improvement in its strategies. These data suggest that cybersecurity vulnerabilities in Latin America may include a lack of effective implementation of security measures, deficiencies in cybersecurity-related legislation and regulation, and a lack of cybersecurity awareness and training in public organizations. It is important to note that this information is based on data provided that does not cover all potential cybersecurity vulnerabilities in Latin America [62].

6. Trends in Cybernetics Vulnerabilities

The growing development, use, and implementation of applications with artificial intelligence has made it possible to improve cybersecurity in several ways, such as early detection of threats, identification of patterns of malicious behavior, threat prediction, automation of security tasks, user authentication, and protection of critical systems. AI can also help security teams analyze large amounts of security data and make more informed and accurate decisions. AI can improve the efficiency and effectiveness of security systems by reducing threat response time and minimizing the risk of human error [58]. Some of the future trends in cybersecurity include the use of deep learning techniques and neural networks to improve threat detection, the application of AI techniques to improve the protection of critical systems and the automation of security tasks, the use of AI techniques for user authentication, and the identification of malicious behavior patterns. Cybersecurity is expected to become an increasingly important part of business and government strategy, with more investment being made in the training and education of cybersecurity professionals.

The applicability of artificial intelligence in Industry 4.0 refers to the incorporation of digitalization in industrial activity, integrating physical and virtual components. This allows for greater data capture, transport, storage, and analysis. Connected products, machines, and equipment become sources of data and information to support decision-making. Intelligent manufacturing processes use artificial intelligence in automation systems for machine interaction. Intelligent automation platforms play a key role in obtaining, processing, and interpreting data generated in industrial production.

Artificial intelligence is being implemented in Industry 4.0 to provide information to track all activities in the manufacturing process and improved to manage the increase or decrease in production, considering demand, with the aim of reducing downtime to ensure constant efficiency of the production line. This can also help detect and prevent potential cyberattacks in industrial production [63].

7. Discussion

Cybersecurity is an aspect that has gained importance in recent decades for governments and organizations of the countries of the Latin American region [11]. The increasing digitalization and greater use of communication technologies imply the use of computer programs that bring vulnerabilities exploited by cybercriminals in the area and the rest of the world [10].

It is evident in the scientific literature, official reports, communications, and websites of brands related to cybersecurity that the governments of Latin American countries do not give relevant importance to computer security and its implementation, despite the growing threats in the last decade. The most frequent vulnerabilities identified for organizations and individual attacks are generated by malware attacks, phishing, and identity theft [15,16].

In Figure 4, it can be seen that professional training and user awareness on issues of importance in the use of cybersecurity systems is relatively low; considering their evaluations on five points, it can be seen that Uruguay has a better level in these two aspects. The results of Figure 4 mean that government systems and organizations do not have the tools and systems to face cyber challenges and threats without being able to respond efficiently to these attacks. For Figure 4, the response time to the attacks shows that only Argentina, Chile, and Mexico have been able to give a better efficient response over time.

Internet of Things (IoT) devices often present weak security due to inadequate standards and regulations. This lack of protective measures makes them more prone to attacks [25]. In addition, IoT devices can be leveraged as entry points for unauthorized access to other interconnected systems in the network. In other words, its vulnerability can be used as a form of unwanted access to other connected systems. One of the open doors that cybercriminals take advantage of is vulnerabilities in the Office operating system [29]. Android operating system, browsers, and pdf file readers, which are often used on smart and mobile devices.

There is no consensus in the reference sources on the statistics, reports, and reports presented by agencies that study cyber-attack impact. Each evaluates the parameters they consider appropriate to apply in their studies independently.

Considering that applications, operating systems, devices, platforms, and applications have vulnerabilities, such as those identified in Figure 8 that are created from the information provided in the reports of the company Ciberinteligencia Securesoft, the most frequent vulnerabilities in these attacks correspond to zero-day threats, remote code execution, access, and malware.

Figure 11 presents a word cloud obtained from the keywords of the documents cited in this review. A strong influence of cyber vulnerabilities and threats is appreciated with the use of devices with the Internet of Things, cyber-physical systems, security, artificial intelligence, and the term resilience.

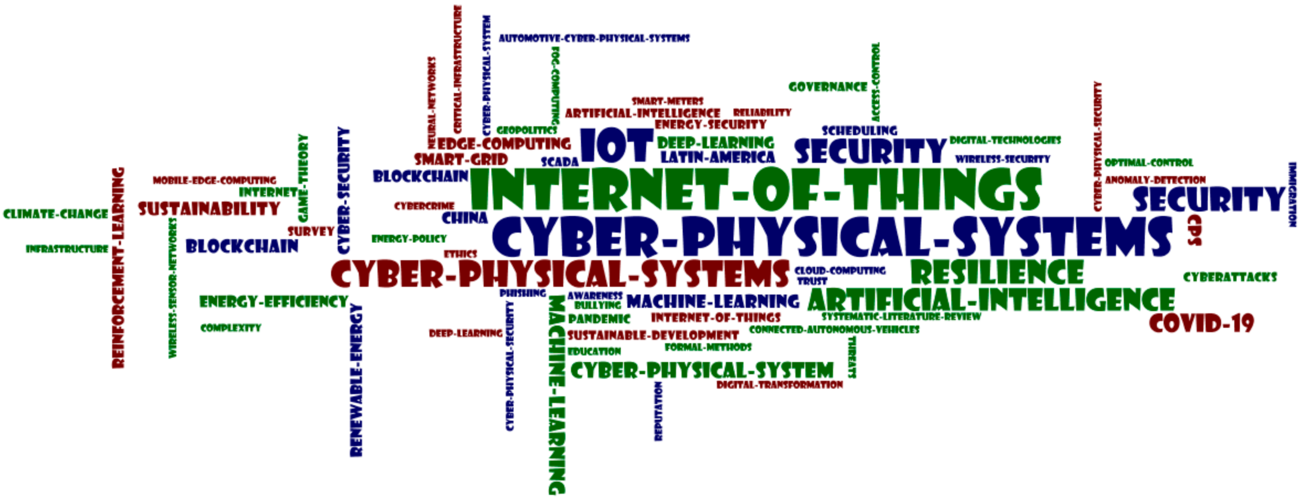

Figure 11. A cloud of words was obtained from the keywords in the articles referenced to realize this review.

Cybercriminals have embraced AI to make attacks effective without revealing their identities for cyberattacks and cybersecurity systems. Some of these attacks are associated with using chatbots, sending fraudulent emails, and using high-level programming to obtain passwords. Many organizations already use AI to detect and respond to cyber threats more effectively [63].

In Latin America, various actions have been implemented to promote cybersecurity awareness. These actions include education and training programs to promote cybersecurity awareness in different sectors, such as academia, business, and government. These programs provide knowledge about cyber threats, best practices, and protective measures. Awareness campaigns have been proposed to inform the public about cyber threats and how to protect themselves. Organizations responsible for responding and advising against cyber incidents (CERT, Computer Emergency Response Team) have been implemented. Governments have implemented legal frameworks and regulations to strengthen cybersecurity. These regulations establish security requirements for organizations, promote personal data protection, and facilitate cooperation between the public and private sectors on cybersecurity. We have collaborated to exchange information between countries in Latin America and other world regions on cybersecurity issues, achieving cooperation agreements, participating in joint activities to respond to incidents, and adopting international security standards.

The growing threat of cyber vulnerabilities has highlighted the imperative need to develop robust solutions and effective countermeasures to safeguard security in the digital environment. In this process of adapting to new technologies, Latin America faces emerging risks in cyberspace that must be addressed urgently. Various documents and analyses highlight a series of proposals to meet this challenge. Standardization in cyber threat reporting, along with the utilization of tools, such as web application firewalls and scanning for web application vulnerabilities, emerge as effective methods to mitigate security breaches and strengthen online defenses [1].

The region has also explored specific models to protect itself and detect threats in its key sectors. An example is the proposal of a model of protection against cyberattacks in public organizations in Latin America. This approach aims to minimize the disruption of public services and is supported by the presentation of an algorithm in the form of a flowchart to reduce vulnerability to cyberattacks. In the banking sector, an innovative model is proposed that drives the responsibility of banks to create secure online experiences. This is based on security policies supported by information technology and the incorporation of behavioral studies and models based on artificial intelligence to identify early threats and the negligence of users [57].

The importance of a national approach and international collaboration to address cyber vulnerabilities in Latin America is undeniable. The specific challenges of the region require understanding the level of risks and threats, creating national cybersecurity strategies, and establishing legal frameworks to combat cybercrime. In addition, multilateral cooperation and the training of cybersecurity professionals are key pieces in this puzzle. Despite the uniqueness of each country, collaboration between more experienced nations in the field can provide valuable guidelines and best practices to deter, defend and adapt to cyberattacks, especially those of extraterritorial origin [8].

Awareness and capacity building in cybersecurity are fundamental pillars to strengthen online defenses in Latin America. Proposals, such as the creation of threat analysis units and cybersecurity websites managed by public authorities, as well as the strengthening of social and cultural awareness in the cyber sphere, aim to raise the digital resilience of the region. Regional cooperation in sharing information and best practices in cybersecurity, as well as the development of national strategies addressing both technological readiness and online user behavior, are essential elements for strong and adaptive cybersecurity. Ultimately, Latin America must adopt a comprehensive and collaborative approach to address cyber vulnerabilities and build a safer cyberspace successfully.

8. Conclusions

The vulnerabilities identified in Latin American countries are low awareness of cybersecurity, a lack of sufficiently implemented standards and regulations, the use of updated software, security gaps in critical infrastructures, inadequate training and specialization, and an incidence of advanced persistent threats (ATP). The vulnerabilities above are not unique to Latin America.

Latin America faces significant challenges regarding vulnerabilities to cyberattacks on government agencies and attacks on individuals. The multiple vulnerabilities present in government organizations, companies, and organizations are attractive to national and international cyberattackers who take advantage of the multiple vulnerabilities of computer applications as a gateway to circumvent security and obtain information.

In recent years, actions and programs have been implemented to promote awareness of cybersecurity in countries of the Latin American region. Vocational training programs have been included. Investing in cybersecurity education, training, and awareness at the individual, enterprise, and government levels is critical.

The cyberattacks that have been carried out on government agencies in Latin American countries have put critical infrastructure at risk, delaying the execution of essential processes and affecting financial systems, confidential databases, control systems of public services, and personal information, putting citizens and the integrity of multiple institutions and companies at risk.

Countries, such as Uruguay, Chile, Brazil, Colombia, and Mexico lead in implementing cybersecurity measures. Uruguay has been recognized for its comprehensive approach, national strategy, and emphasis on awareness and training. Chile has established a specialized agency and promoted public–private cooperation. Brazil has a national strategy, incident response centers, and international cooperation. Colombia has created a specialized agency and works on public–private partnerships. Mexico has boosted cybersecurity with a national strategy and awareness campaigns. Each country approaches cybersecurity uniquely, but all demonstrate notable progress in the region.

The convergence between artificial intelligence and cybercrime has transformed the cyber-attack landscape, allowing criminals to exploit vulnerabilities without revealing their identity. However, the response has been blunt, with organizations leveraging AI to detect and counter threats effectively. In Latin America, a multifaceted approach to cybersecurity awareness has emerged, encompassing education, training, and government initiatives. Legal frameworks and international cooperation have been instrumental in strengthening the region's defenses.

It becomes imperative to invest in and pay attention to cybersecurity in key sectors, such as public organizations and banking. The prevailing need for a collaborative national and international approach is evident to address the unique challenges posed by cyber vulnerabilities. By fostering awareness, capacity, and resilience, Latin America can lay the foundation for a safer digital future through comprehensive, collaborative, and adaptable cybersecurity strategies.

Author Contributions: Conceptualization, O.F.-U. and F.S.; methodology, O.F.-U.; software, Á.A. and R.T.; validation, O.F.-U., X.L.-N. and P.A.-V.; formal analysis, P.A.-V.; investigation, O.F.-U. and F.S.; resources, Á.A. and R.T.; writing—original draft preparation, O.F.-U. and P.A.-V.; writing—review and editing, X.L.-N., P.A.-V. and O.F.-U.; visualization, F.S. and O.F.-U.; supervision, X.L.-N.; project administration, O.F.-U.; funding acquisition, P.A.-V. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Universidad de Las Américas-Ecuador, as part of the internal research project INI.PAV.22.02.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sets for the review are available at [63] Flor, Omar; Acuña, Angel; Acosta-Vargas, Patricia (2023), "Vulnerabilities Ciberdefense in Latin America", Mendeley Data, V1, doi: 10.17632/ydgj5vg7kh.1.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Table A1. Preferred Reporting Items for Systematic Reviews and Meta-Analyses Extension for Scoping Reviews (PRISMAScR).

Section	Item	PRISMA-ScR Checklist Item	Reported on Page #
Title			
Title	1	Identify the report as a scoping review.	1
Abstract			
Structured summary	2	Provide a structured summary that includes (as applicable): background, objectives, eligibility criteria, sources of evidence, charting methods, results, and conclusions that relate to the review questions and objectives.	1
Introduction			
Rationale	3	Describe the rationale for the review in the context of what is already known. Explain why the review questions/objectives lend themselves to a scoping review approach.	2
Objectives	4	Provide an explicit statement of the questions and objectives being addressed with reference to their key elements (e.g., population or participants, concepts, and context) or other relevant key elements used to conceptualize the review questions and/or objectives.	2-3-4
Methods			
Protocol and registration	5	Indicate whether a review protocol exists; state if and where it can be accessed (e.g., a web address); and if available, provide registration information, including the registration number.	4-7
Eligibility criteria	6	Specify characteristics of the sources of evidence used as eligibility criteria (e.g., years considered, language, and publication status) and provide a rationale.	4
Information sources *	7	Describe all information sources in the search (e.g., databases with dates of coverage and contact with authors to identify additional sources), as well as the date the most recent search was executed.	4
Search	8	Present the full electronic search strategy for at least one database, including any limits used, such that it could be repeated.	3, 4
Selection of sources of evidence †	9	State the process for selecting sources of evidence (i.e., screening and eligibility) included in the scoping review.	4
Data charting process ‡	10	Describe the methods of charting data from the included sources of evidence (e.g., calibrated forms or forms that have been tested by the team before their use and whether data charting was performed independently or in duplicate) and any processes for obtaining and confirming data from investigators.	3
Data items	11	List and define all variables for which data were sought and any assumptions and simplifications made.	-
Critical appraisal of individual sources of evidence §	12	If performed, provide a rationale for conducting a critical appraisal of included sources of evidence; describe the methods used and how this information was used in any data synthesis (if appropriate).	-
Synthesis of results	13	Describe the methods of handling and summarizing the data that were charted.	19

Table A1. *Cont.*

Section	Item	PRISMA-ScR Checklist Item	Reported on Page #
Results			
Selection of sources of evidence	14	Give numbers of sources of evidence screened, assessed for eligibility, and included in the review, with reasons for exclusions at each stage, ideally using a flow diagram.	19
Characteristics of sources of evidence	15	For each source of evidence, present characteristics for which data were charted and provide the citations.	-
Critical appraisal within sources of evidence	16	If performed, present data on critical appraisal of included sources of evidence (see item 12).	15, 16
Results of individual sources of evidence	17	For each included source of evidence, present the relevant data that were charted that relate to the review questions and objectives.	
Synthesis of results	18	Summarize and/or present the charting results as they relate to the review questions and objectives.	
Discussion			
Summary of evidence	19	Summarize the main results (including an overview of concepts, themes, and types of evidence available), link to the review questions and objectives, and consider the relevance to key groups.	15
Limitations	20	Discuss the limitations of the scoping review process.	4
Conclusions	21	Provide a general interpretation of the results with respect to the review questions and objectives, as well as potential implications and/or next steps.	21, 22
Funding			
Funding	22	Describe sources of funding for the included sources of evidence, as well as sources of funding for the scoping review. Describe the role of the funders of the scoping review.	22

JBI = Joanna Briggs Institute; PRISMA-ScR = Preferred Reporting Items for Systematic reviews and Meta-Analyses extension for Scoping Reviews. * Where *sources of evidence* (see second footnote) are compiled from, such as bibliographic databases, social media platforms, and Web web sites. † A more inclusive/heterogeneous term used to account for the different types of evidence or data sources (e.g., quantitative and/or qualitative research, expert opinion, and policy documents) that may be eligible in a scoping review as opposed to only studies. This is not to be confused with information sources (see first footnote). ‡ The frameworks by Arksey and O'Malley (6) and Levac and colleagues (7) and the JBI guidance (4, 5) refer to the process of data extraction in a scoping review as data charting. § The process of systematically examining research evidence to assess its validity, results, and relevance before using it to inform a decision. This term is used for items 12 and 19 instead of "risk of bias" (which is more applicable to systematic reviews of interventions) to include and acknowledge the various sources of evidence that may be used in a scoping review (e.g., quantitative and/or qualitative research, expert opinion, and policy documents). #: page number.

References

1. Kettani, H.; Cannistra, R.M. On Cyber Threats to Smart Digital Environments. In Proceedings of the 2nd International Conference on Smart Digital Environment, Rabat, Morocco, 18–20 October 2018; pp. 183–188. [CrossRef]
2. Dave, G.; Choudhary, G.; Sihag, V.; You, I.; Choo, K.-K.R. Cyber security challenges in aviation communication, navigation, and surveillance. *Comput. Secur.* **2021**, *112*, 102516. [CrossRef]
3. Parkinson, S.; Ward, P.; Wilson, K.; Miller, J. Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2898–2915. [CrossRef]
4. Solar, C. Cybersecurity and cyber defence in the emerging democracies. *J. Cyber Policy* **2020**, *5*, 392–412. [CrossRef]
5. Toapanta, S.M.T.; Cobeña, J.D.L.; Gallegos, L.E.M. Analysis of Cyberattacks in Public Organizations in Latin America. *Adv. Sci. Technol. Eng. Syst. J.* **2020**, *5*, 116–125. [CrossRef]
6. Gutierrez, L.H.; Berg, S. Telecommunications liberalization and regulatory governance: Lessons from Latin America. *Telecommun. Policy* **2000**, *24*, 865–884. [CrossRef]
7. Alghazo, J.M.; Kazmi, Z.; Latif, G. Cyber security analysis of internet banking in emerging countries: User and bank perspectives. In Proceedings of the 2017 4th IEEE international conference on engineering technologies and applied sciences (ICETAS), Salmabad, Bahrain, 29 November–1 December 2017; pp. 1–6. [CrossRef]
8. Antonio, J.M.A. La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas. *Rev. Estud. Segur. Int.* **2020**, *6*, 17–43. [CrossRef]
9. Tricco, A.C.; Lillie, E.; Zarin, W.; O'Brien, K.K.; Colquhoun, H.; Levac, D.; Moher, D.; Peters, M.D.; Horsley, T.; Weeks, L.; et al. PRISMA Extension for Scoping Reviews (PRISMAScR): Checklist and Explanation. *Ann. Intern. Med.* **2018**, *169*, 467–473. [CrossRef] [PubMed]
10. Antonio, J.M.A. Hechos ciberfísicos: Una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. *Rev. Latinoam. Estud. Segur.* **2019**, *25*, 24–40. [CrossRef]

11. Pawlak, P.; Barmpaliou, P.-N. Politics of cybersecurity capacity building: Conundrum and opportunity. *J. Cyber Policy* **2017**, *2*, 123–144. [CrossRef]
12. Flor, O.; Acuña, A.; Acosta-Vargas, P. *Vulnerabilities Ciberdefense in Latin America, Version 1*; Mendeley Data: Quito, Ecuador, 2023. [CrossRef]
13. Díaz, R.M. State of Cybersecurity in Logistics in Latin America and the Caribbean. Comisiòn Económica para América Latina y el Caribe 2021. Available online: http://repositorio.cepal.org/handle/11362/47655 (accessed on 20 June 2023).
14. Organization of American States. *Tendencias en la Seguridad Cibernética en América Latina y el Caribe y Respuestas de los Gobiernos*; Trend Micro: Hong Kong, China, 2013.
15. Abu Issa, H.; Ismail, M.; Aamar, O. Unauthorized access crime in Jordanian law (comparative study). *Digit. Investig.* **2019**, *28*, 104–111. [CrossRef]
16. Alshamrani, A.; Myneni, S.; Chowdhary, A.; Huang, D. A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1851–1877. [CrossRef]
17. Delloite. COVID-19s Impact on Cybersecurity. Available online: https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html (accessed on 20 June 2023).
18. Hummelholm, A. Cyber Threat Analysis in Smart City Environments. In Proceedings of the European Conference on Cyber Warfare and Security (ECCWS 2018), Oslo, Norway, 28–29 June 2018.
19. Ćurguz, J. Vulnerabilities of the SSL/TLS Protocol. In *Computer Science & Information Technology (CS & IT)*; Academy & Industry Research Collaboration Center (AIRCC): Banja Luka, Bosnia and Herzegovina, 2016; pp. 245–256.
20. Hindy, H.; Atkinson, R.; Tachtatzis, C.; Colin, J.-N.; Bayne, E.; Bellekens, X. Utilising Deep Learning Techniques for Effective Zero-Day Attack Detection. *Electronics* **2020**, *9*, 1684. [CrossRef]
21. Bolgov, R. The UN and Cybersecurity Policy of Latin American Countries. In Proceedings of the 2020 Seventh International Conference on eDemocracy & eGovernment (ICEDEG), Buenos Aires, Argentina, 22–24 April 2020; pp. 259–263. [CrossRef]
22. Most Targeted Countries by Cyber Attacks Latin America 2020. Statista. Available online: https://www.statista.com/statistics/818412/latin-american-countries-highest-share-cyber-attacks/ (accessed on 20 June 2023).
23. Vinueza, J. Nuevo Ransomware Como Servicio. 16 May 2023. Available online: https://csirt.celec.gob.ec/en/contenidos/alertas/514-nuevo-ransomware-como-servicio-michaelkors-dirigido-a-sistemas-linux-y-vmware-esxi (accessed on 20 June 2023).
24. SIM Swap Fraud Grows as the Biggest Cybersecurity Threat. Available online: https://www.dnkinfotelecom.com.br/en/sim-swap-fraud-grows-as-the-biggest-cybersecurity-threat/ (accessed on 20 June 2023).
25. Toapanta, S.M.T.; Pesantes, R.P.R.; Gallegos, L.E.M. Impact of Cybersecurity Applied to IoT in Public Organizations in Latin America. In Proceedings of the 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, UK, 27–28 July 2020; pp. 154–161. [CrossRef]
26. Foldvari, A.; Biczok, G.; Kocsis, I.; Gonczy, L.; Pataricza, A. Impact Assessment of IT Security Breaches in Cyber-Physical Systems: Short paper. In Proceedings of the 2021 10th Latin-American Symposium on Dependable Computing (LADC), Florianópolis, Brazil, 22–26 November 2021; pp. 1–4. [CrossRef]
27. Sancho, C. Ciberseguridad. Presentación del dossier/Cybersecurity. Introduction to Dossier. *Rev. Latinoam. Estud. Segur.* **2017**, *20*, 8–15. [CrossRef]
28. 10 Most Common Types of Cyber Attacks Today—CrowdStrike. Available online: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/ (accessed on 20 June 2023).
29. SecureSoft. Securesoft 54 Biweekly Cyber Intelligence Report. Available online: https://goo.su/HQwJ9KL (accessed on 1 June 2023).
30. SecureSoft. 55 Biweekly Cyber Intelligence Report. Available online: https://goo.su/ZPfxZ (accessed on 1 June 2023).
31. SecureSoft. 56 Biweekly Cyber Intelligence Report. Available online: https://goo.su/e0KFSRc (accessed on 1 June 2023).
32. Donoso, M.C. Cuán importante es la seguridad cibernética para lograr la seguridad hídrica? *Rev. Cienc. Ambient.* **2022**, *56*, 284–297. [CrossRef]
33. SecureSoft. 57 Biweekly Cyber Intelligence Report. Available online: https://goo.su/URUTp8 (accessed on 1 June 2023).
34. SecureSoft. 58 Biweekly Cyber Intelligence Report. Available online: https://goo.su/edMq (accessed on 1 June 2023).
35. SecureSoft. 59 Biweekly Cyber Intelligence Report. Available online: https://goo.su/88lxRGj (accessed on 1 June 2023).
36. SecureSoft. 61 Biweekly Cyber Intelligence Report. Available online: https://goo.su/lmqjOg (accessed on 1 June 2023).
37. SecureSoft. 62 Biweekly Cyber Intelligence Report. Available online: https://goo.su/tHxb (accessed on 1 June 2023).
38. SecureSoft. 63 Biweekly Cyber Intelligence Report. Available online: https://goo.su/FmvR (accessed on 1 June 2023).
39. SecureSoft. 64 Biweekly Cyber Intelligence Report. Available online: https://goo.su/F5FzT (accessed on 1 June 2023).
40. SecureSoft. 65 Biweekly Cyber Intelligence Report. Available online: https://goo.su/zJ7v9 (accessed on 1 June 2023).
41. SecureSoft. 66 Biweekly Cyber Intelligence Report. Available online: https://goo.su/PW7ipc (accessed on 1 June 2023).
42. SecureSoft. 67 Biweekly Cyber Intelligence Report. Available online: https://goo.su/YzgdNK (accessed on 1 June 2023).
43. SecureSoft. 68 Biweekly Cyber Intelligence Report. Available online: https://goo.su/WNTj (accessed on 1 June 2023).
44. SecureSoft. 69 Biweekly Cyber Intelligence Report. Available online: https://goo.su/lgGYC19 (accessed on 1 June 2023).
45. SecureSoft. 70 Biweekly Cyber Intelligence Report. Available online: https://goo.su/IQsYxN (accessed on 1 June 2023).
46. SecureSoft. 71 Biweekly Cyber Intelligence Report. Available online: https://goo.su/2zJFf (accessed on 1 June 2023).
47. SecureSoft. 72 Biweekly Cyber Intelligence Report. Available online: https://goo.su/nA73 (accessed on 1 June 2023).

48. SecureSoft. 73 Biweekly Cyber Intelligence Report. Available online: https://shorturl.at/finB0 (accessed on 1 June 2023).
49. SecureSoft. 74 Biweekly Cyber Intelligence Report. Available online: https://goo.su/7wUpBe (accessed on 1 June 2023).
50. ESSET 2022. ESET-Security-Report-LATAM202. Available online: https://goo.su/AXeiDL (accessed on 15 May 2023).
51. Cyberthreat Real Time. Available online: https://cybermap.kaspersky.com (accessed on 1 June 2023).
52. Geluvaraj, B.; Satwik, P.M.; Kumar, T.A.A. The Future of Cybersecurity: Major Role of Artificial Intelligence, Machine Learning, and Deep Learning in Cyberspace. In *International Conference on Computer Networks and Communication Technologies*; Smys, S., Bestak, R., Chen, J.I.-Z., Kotuliak, I., Eds.; Lecture Notes on Data Engineering and Communications Technologies; Springer: Singapore, 2019; Volume 15, pp. 739–747. [CrossRef]
53. Toapanta, S.; Peñafiel, L.; Mafla, L. Prototype to Mitigate the Risks of the Integrity of Cyberattack Information in Electoral Processes in Latin America. In Proceedings of the 2019 2nd International Conference on Education Technology Management (ICETM'19), Barcelona, Spain, 18–20 December 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 111–118. [CrossRef]
54. Jimenez, E.; Yepez, R.; Giraldo, J.; Rojas, I. Valley of Death: Factors Hindering the Success of Technological Innovations. *Rev. CEA* **2021**, *7*, e1926. [CrossRef]
55. Kalhoro, S.; Rehman, M.; Ponnusamy, V.; Shaikh, F.B. Extracting key factors of cyber hygiene behaviour among software engineers: A systematic literature review. *IEEE Access* **2021**, *9*, 99339–99363. [CrossRef]
56. De Azambuja, A.J.G.; Plesker, C.; Schützer, K.; Anderl, R.; Schleich, B.; Almeida, V.R. Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey. *Electronics* **2023**, *12*, 1920. [CrossRef]
57. Creado, Y.; Ramteke, V. Active cyber defence strategies and techniques for banks and financial institutions. *J. Financ. Crime* **2020**, *27*, 771–780. [CrossRef]
58. Ataque del Ransomware LockBit Afectó al Poder Judicial de Chile | WeLiveSecurity. Available online: https://www.welivesecurity.com/la-es/2022/09/28/ataque-ransomware-lockbit-poder-judicial-chile/ (accessed on 20 June 2023).
59. Fraud and Cybercrime in Latin America: An Evolving Threat Landscape—Blueliv.—Kippeo Technologies. Available online: https://kippeo.com/fraud-and-cybercrime-in-latin-america-an-evolving-threat-landscape-blueliv/ (accessed on 20 June 2023).
60. Niño, F.Y.A. Ransomware, una amenaza latente en Latinoamérica. *Intersedes* **2023**, *24*, 92–119. [CrossRef]
61. Organization of American States. *Report on Cybersecurity and Critical Infrastructure in the Americas*; Trend Micro: Irving, TX, USA, 2015.
62. Buzzio-Garcia, J.; Salazar-Vilchez, V.; Moreno-Torres, J.; Leon-Estofanero, O. Review of Cybersecurity in Latin America during the COVID-19 Pandemic: A brief Overview. In Proceedings of the 2021 IEEE Fifth Ecuador Technical Chapters Meeting (ETCM), Cuenca, Ecuador, 12–15 October 2021; pp. 1–5. [CrossRef]
63. Kaur, R.; Gabrijelčič, D.; Klobučar, T. Artificial intelligence for cybersecurity: Literature review and future research directions. *Inf. Fusion* **2023**, *97*, 101804. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.