Data-Driven Cyber Threat Intelligence: A Survey of Mexican Territory

M. A. Arturo E. Torres, Francisco Torres Guerrero, and Arturo Torres Budgud

Abstract Information technologies, as well as digital information and information assets, play a very important role today globally, which is why we have witnessed how publications related to cybersecurity incidents are increasing day by day; therefore, and in the face of the great growth of cyber threats, various researchers have dedicated a large part of their efforts to protect these information assets using intelligence sources to develop various techniques for understanding, evolving, detecting, and proactively responding against the cyber threats they face. For their part, companies, governments, and cybersecurity specialists have shown great interest in consuming these sources of intelligence called cyber threat intelligence (CTI), which consists of evidence-based knowledge, which includes context, mechanisms, actionable indicators, implications, and advice on an existing or emerging threat or danger to assets that can be used to inform decisions regarding the subject's response to that threat or danger. With a focus on the Mexican territory, this work aims to analyze the data obtained from CTI sources using the detection of perimeter cybersecurity devices (firewalls, intrusion prevention system, antivirus, honeypots, etc.), as well as the study of research related to cybersecurity predictions to point out the importance of having a model capable of making a possible prediction of cyber threats in Mexico. Challenges and future directions in this field are also discussed.

Keywords Information technology · Cybersecurity incidents · Cyber threats · Intelligence sources · Cybersecurity · Cyber threat intelligence (CTI) · Firewalls · Intrusion prevention system · Antivirus · Honeypots

M. A. A. E. Torres (✉) · F. T. Guerrero · A. T. Budgud
Universidad Autonoma de Nuevo Leon, San Nicolás de los Garza, N.L., Mexico
e-mail: arturo.torrescv@uanl.edu.mx; francisco.torresgrr@uanl.edu.mx; arturo.torresbg@uanl.edu.mx

F. Torres-Guerrero et al. (eds.), *2nd EAI International Conference on Smart Technology*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-031-07670-1_7

1 Introduction

With the constant use and dependence on technology, thanks to innovation and digital transformation, such as the Internet of Things (IoT) or cloud computing, it has become very important to have protection measures for our assets of digital information against cyber threats and/or cybercrime, which Cybersecurity Venture predicts that cybercrime will cost around $6 billion annually by 2021, making it more profitable than global trade in all major combined illegal drugs [1]. Likewise, in the Annual Risk Report 2020 [1] published by the "World Economic Forum" classifies cyberattacks as a latent risk to be prepared from, since the probability and impact on the economy caused by this phenomenon are only below risks such as natural disasters, crises due to lack of water, extreme climates, followed by risks such as infectious diseases, human-made environmental disasters, food crises, etc. In the same study [2], they talk about "the dangers of digital evolution" and how the IoT is also amplifying the potential of the cyberattack surface, estimating that today there are more than 21 billion smart devices or Internet of Things (IoT) worldwide and expected to double by 2025 [2], which have become tools used by cybercriminals, a case that occurred in late 2016, in which they launched a major attack known as distributed denial-of-service (DDoS), causing an interruption in Internet services that affected many companies, including Amazon, PayPal, Netflix, Spotify, and Twitter [3]. Likewise, *Forbes* magazine published [4] that researchers from the cybersecurity company F-Secure detected an increase of more than 300% in attacks on IoT devices in the first half of 2019 [5], while in September 2019, these devices were used to bring down page services such as Wikipedia through a distributed denial-of-service (DDoS) attack [6], and it is estimated that there will be an increase in the use of IoT devices as intermediaries between attackers and their victims.

According to the United States National Institute of Standards and Technology (NIST), cyber risk is defined as the risk of financial loss, operational interruption, or damage, due to the failure of the digital technologies used for informative and/or operational functions introduced to a system by electronic means without authorized access, for the use, disclosure, interruption, modification, or destruction of the systems [7]. The term cybernetic risk, or cyber risk, is closely linked to the concepts of cyber threat and cyberattack.

Given these incidents and the large number of cyber threats hovering around the Internet affecting different sectors of the industry, research has been conducted in sectors such as the health sector [8] which the authors indicate the health sector as a main target of cyberattackers for the theft of personal, critical, and confidential information; likewise, there are also cybersecurity investigations in other sectors such as manufacturing [9] where an investigation of cybersecurity in digital manufacturing systems is presented with a particular focus on the characterization of the system, identification of threats and vulnerabilities, attack scenarios, control methods, and risk determination techniques; we can also find investigations based on financial market reactions to a cybersecurity attack [11].

In these situations, the various communities, as well as manufacturers and cybersecurity researchers, have shown great interest in publishing their findings and research to the general public, resulting in a large amount of information that can be consumed by analysts to make important decisions about when carrying out a cybersecurity strategy, such as allocating resources, budgets, and prioritizing actions in the face of a cyber threat [10–12]. However, as of today, there are few threat prediction works that focus on perimeter security schemes based on the data collected by these devices.

The most widely used techniques to perform cybersecurity prediction focus on obtaining cyber threat intelligence (CTI) sources of information which consists of obtaining a data set of cybersecurity events to process and analyze with techniques such as data mining (DM) and machine learning (ML) to be able to make a decision based on the events or data obtained previously. Therefore, in a scenario where cyber threats can be predicted, any company and/or information technology providers, as well as users, could inform themselves and protect themselves from the impacts caused by cybersecurity threats.

And as we know, no system or device is perfect or can be considered 100% secure, and in the face of the great growth of everyday devices that connect to the network plus the dependency that we are generating towards them, we can consider that cyber threats are a constant that we must take into account at any time that we use a service or technology. That is why various studies have been carried out on the advances and developments of prediction of cyber threats and incidents, highlighting the study of [15], in which the authors present the compilation and investigation of schemes, methods, and data sets for predicting cybersecurity incidents of the latest generation, highlighting the existing work in this field. Likewise, the authors organize their research into six categories, according to the data sets used, such as reports and data sets of the organization, network data sets, synthetic data sets, web page data, social network data, and mixed-type data. Therefore, proactive prediction of cybersecurity threats and incidents is considered a potential and immediate problem to be solved. That is, the prediction of cyber threats is an area of research where there is a large area of opportunity to be studied and developed.

1.1 Contributions

In this research article, it is organized as follows:

- Section II aims to present the investigation of the current state of cybersecurity in Mexico in order to obtain an overview.
- The main contribution of Section III is the compilation and investigation of CTI schemes, methods, and data sets corresponding to the Mexican territory available to analyze in future investigations.
- Section V discusses the challenges and opportunities for future research in this area.
- Section VI presents the conclusions of the research article (Fig. 1).

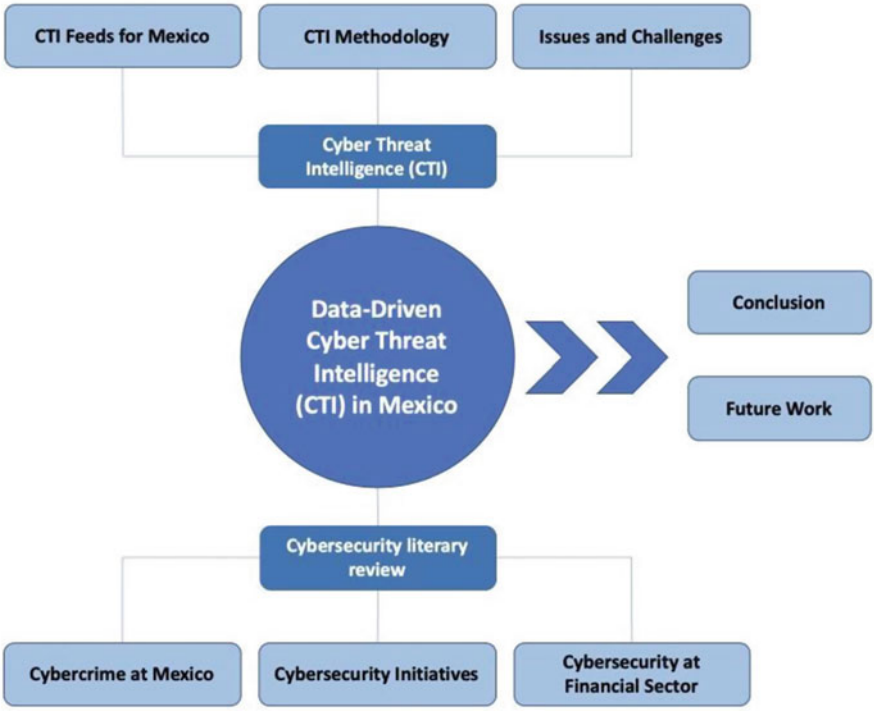

Fig. 1 Methodology

2 Current State of Cybersecurity in Mexico

In this section, a general vision of the current cybersecurity situation in the Mexican territory is presented, which aims to cover the different articles issued by consultancies in conjunction with the Mexican government, as well as studies on different sectors of the industry to have a broad overview of current cybersecurity in the country. For this study, we will use the term cybersecurity defined by the ISO/IEC 27032 standard as the preservation of the confidentiality, integrity, and availability of information in cyberspace, which in turn is defined as the complex environment that results from the interaction of people, software, and services on the Internet through technological devices and networks connected to it, which do not exist in any physical form [13].

Mexico is a country in constant industrial and technological development; however, there are certain emerging issues in the new industrial policies, which go beyond the traditional areas of promotion, protection, and industrial and service regulation. The Scientific and Technological Advisory Forum [14] published a document where issues such as the efficient use of energy and sustainable development are pointed out; competition in the national and international market; education and training; and promoting scientific research and technological development [15]. In

this same document, it is mentioned that said developments have been characterized by the dominance of foreign capital and technology and the low national added value. In contrast to what happened in China, South Korea, India, and other Asian countries, companies with national capital have not co-invested in Mexico with foreign companies, nor have they excelled in the development of their own technologies, or their exports (with the exception of the mining sector). Likewise, the great challenge of generating a successful economy where it is only based on foreign investment is mentioned, as has been understood in Mexico and other Latin American countries in recent years.

Cybersecurity in Mexico is an issue that has grown strong in recent years, and the cyberattacks that we have faced recently have had a significant national impact, and the media are increasingly taking more value on news related to the cybercrime [16, 20, 21]. In summary, it affects in some way all sectors of the country due to the rapid growth made up of technology, social networks, information systems, and the Internet, where Mexico achieves a 71% penetration among the population of people 6 years and older. With 79.1 million users connected, therefore, Mexican companies have adapted new business models, such as electronic commerce, in which it was revealed that 8 out of 10 Internet users of legal age have made a purchase online in the last year, in which 85% of online purchases in Mexico are made through smartphones, highlighting that already 2 out of 10 online buyers make some purchases on their Smart TV, reaching a value of more than 491 billion pesos and with a growth of 24% compared to 2017 [17]. This tells us about the adoption and constant use of digital media to consume a service or purchase a product in the Mexican territory where Internet users in Mexico spend 8 hours 20 minutes daily, 8 minutes more than in 2018 [23].

Almost all aspects of daily life in the country depend today on the use of information and telecommunications technologies, which favor and improve the lives of Mexicans as well as improve productivity by being able to improve and automate processes. As evidence of this, there has been an exponential growth in the use of devices connected to the Internet, and it is estimated that by 2025 there will be more than 300 million devices with access to networks in Mexico; this is 70% more than the 180 million documented in 2018 [18]. The increasing dependence on information technologies and the accelerated increase in cyber threats as well as cybercrime have forced Mexican companies in the public and private sector to increase their investments and budgets in strategies and cybersecurity controls with the main objective of being able to protect from these threats that affect the availability, confidentiality, and integrity of your information and your business. The financial sector is a critical system that has a high dependence on information technologies, since its transactions between clients, other institutions such as businesses and electronic payments are carried out digitally and in which studies have been carried out where the impact that occurs in a company when it is the victim of a cyber threat [11] it is shown. Likewise, different sectors of the industry have also adopted technology as a day-to-day tool to automate and optimize many of their critical processes where we have mentioned various scientific articles, which

seek to improve their detections and incident response process according to their sector [8, 9].

In February 2019, the Secretary of Communications and Transportation (SCT) [19] in conjunction with the Organization of American States (OAS) [20] published a study on the habits of users in cybersecurity in Mexico, in which more than 5 thousand people residing in different states of the republic were interviewed and in which the annual increase in users on the Internet stands out exponentially with a growth of 4.7% from 2015 to 2016 and an increase of 8.1% from 2016 to 2017. Where free Internet access is identified, as well as mobile device applications for minors as one of the most important concerns, since according to the study only 45% of adults monitor the content minors visit and/or consume and 37% declare the use of these mobile devices and applications as entertainment for their children without controlling the content or pages they relate to while accessing the Internet. Given this annual rise, immediate action is paramount regarding day-to-day activities since the study revealed that 42% of the participants indicated not knowing the permits required by the applications before installing them as well as more than 20% of the users accepted being victims of financial fraud through digital means mostly by email [21] using techniques such as phishing, which is defined by the Federal Police as a type of scam, whose objective is to obtain data, passwords, bank account numbers and credit cards, identity, or other data to be used fraudulently [22].

In the document issued by the McKinsey & Company consultancy in collaboration with COMEXI, cyber risks are pointed out as a new threat that we must face. Likewise, they define the concept of "cyber risks" as a set of possible damages that companies, governments, and members of society could suffer due to a failure or violation of the information technologies they use every day. This can be reflected in an impact of economic loss, damage to the reputation of a company or person, as well as in the loss of availability to provide a service or in making poorly informed decisions [18]. These can occur in various ways, such as a system error or vulnerability, some accidentally caused failure, or configuration error; however, the greatest damages usually arise from a cyberattack directed either by an external actor or some internal actor of the company. The term cyberattack is defined as an unauthorized attempt by some digital way to access a system, information, and/or resource in order to exfiltrate the information, compromise it, and affect its availability until it ends up extorting users and organizations and corresponds to the materialization of one or more cyber threats.

2.1 Cybercrime in Mexico

As mentioned throughout this document, in recent years, the evolution and technological dependence at a global level has had an accelerated growth, which although it offers us many advantages also carries risks for the daily use of technology and information that we enter to be able to use it, for example, an application to go to the movies, buy a pantry or food or transport, you can ask for personal and financial

information to be able to use it and even administrator permissions on your devices, access to your location, photos, and others; another example is the exponential use of social networks, which today is estimated that an average user in Mexico spends up to 8 hours connected to the Internet and uses more than three social networks (Facebook, Twitter, Instagram, Twitch, TikTok, etc.) in a day [23]. This added to the lack of security measures by users when entering unknown sites or installing applications without reading or understanding the permissions or risks involved, increases the risk of contracting an infection and spreading some type of computer threat within of its devices that can trigger a cybercrime having as a victim some user or institution.

The term cybercrime or cybernetic crime is a form of crime that uses both the Internet and technology as a means of committing some unlawful act that may harm integrity, confidentiality, or availability. Some problems related to this type of crime are fraud, information hijacking (ransomware), phishing, malware distribution, distributed denial-of-service (DDoS) attacks, piracy, child exploitation, information theft and/or identity theft, as well as privacy breaches when confidential information is lost or stolen; they become increasingly common in our society, and this has alerted governments and organizations globally to increase their investments in cybersecurity controls to deal with it. According to the generally accepted international classification, we present some of the terms and concepts of cyber threats defined by the NIST [23].

Cyber threats	Description
Malware	Simplified term to denote "malicious code" and consists of software intended to carry out an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of an information system. Within this category are mainly the following types
Virus	Hidden and self-replicating section of computer software, which spreads by infecting (i.e., by inserting a copy of itself into another program and becoming part of it). A virus cannot run alone; requires your host program to run to activate it
Spyware	Software that is secretly or surreptitiously installed in an information system to collect information about individuals or organizations without your knowledge
Adware	Software that automatically plays, displays, or downloads advertising material to a computer after installing the software or while using the application. The malicious program is designed to display unwanted advertisements on the victim's computer without their permission, pop-ups or advertisements are uncontrollable and tend to behave erratically, they usually appear many times on the screen, and it is tedious to close them

(continued)

Cyber threats	Description
Rootkit	A set of tools used by an attacker after gaining root-level access on a host to hide the attacker's activities on the host and allow him to maintain root-level access to the host through secret means. In other words, it allows a hacker to remotely access or control a computing device or network without being exposed. They are difficult to detect because they are activated even before the operating system starts
Trojan horse	Computer program that seems to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes exploiting legitimate authorizations from an entity that invokes the program
Worm	It is the simplified term to denote "write once, read many"; it consists of a computer program that can be run independently, can propagate a full version of itself to other hosts or networks, and can destroy a computer's resources. In other words, it is malicious code that is also copied and spread to other computers, a system, or a network
Ransomware	It is a virus that prevents the user from accessing the files or programs, and for its elimination, it is required to pay a "ransom" through certain online payment methods. Once the amount is paid, the user can resume using their system
Keylogger	A program designed to record which keys are pressed on a used computer keyboard, to obtain passwords or encryption keys
Botnet	It is a network of devices that has been infected with malicious software, such as a virus. Attackers can control a botnet as a group without the owner's knowledge in order to increase the magnitude of their attacks. Often a botnet is used to overwhelm systems in a distributed denial-of-service (DDoS) attack
Phishing	A technique of trying to acquire sensitive data, such as bank account numbers, through a fraudulent request in an email, or on a website, in which the perpetrator is posing as a legitimate business or reputable person
Man-in-the-middle attack (MitM)	A MitM attack is when an attacker disrupts communication between two users, posing as both victims to manipulate them and gain access to their data. Users are not aware that they are actually communicating with an attacker and not with each other
Distributed denial-of-service (DDoS) attack	A denial-of-service attack floods systems, servers, or networks with traffic to drain resources and bandwidth. As a result, the system cannot fulfill legitimate requests. Attackers can also use multiple compromised devices to launch this attack. This is known as a distributed denial-of-service attack
SQL injection	It occurs when an attacker inserts malicious code into a server that uses Structured Query Language (SQL). They only succeed when a security vulnerability exists in the software of an application. Successful SQL attacks force a server to provide access or modify data
Zero-day attack	An attack that exploits a previously unknown hardware or software vulnerability. Using outdated (unpatched) software opens up opportunities for criminal hackers to exploit vulnerabilities. A zero-day vulnerability can occur when a vulnerability is made public before the developer has implemented a patch or solution

Cybercrime has become one of the most important security issues that will continue to emerge as a critical problem for years to come. Among the different attacks, the use of techniques to exploit a vulnerability is of special interest due to its negative impact on the economy. In the last decade, cybercrime has transformed from a low-volume crime to a high-volume crime. During that time, the perpetrators have switched from specialized individuals to expert attackers who have established organized structures to carry out some structured cyberattack. Likewise, cyberattacks are considered one of the risks with the greatest impact in the coming years, according to the "Global Risk Report 2019," which presents the results of the last "global risk perception survey," in which nearly a thousand decision-makers from the public sector, private sector, and academic and civilian society evaluate risks faced by the world [24].

In Mexico, various studies related to cybercrime have been carried out, explaining that this phenomenon has become something much more complex and of greater impact, where it is estimated that more than 80% of Mexican companies are victims of cyberattacks by at least once a year, which positions Mexico as one of the ten countries with the highest number of cyberattack attempts and cyber threats globally [25]. In 2017, 33 million Mexicans (50% more than in 2016) were victims of some cybercrime-related cyber threat, that is, one in four inhabitants of the country. At the same time, the economic impact of these crimes is estimated to have amounted to 7.7 billion dollars, 40% more than the previous year [18], being human behavior (negligence or malicious acts of workers) one of the main factors of these cyber risks.

In Mexico, we have witnessed an increase in cyber threats that have affected different sectors of the industry in recent years, such as the one that affected the National Electoral Institute (INE) in 2016, where it was possible to violate a hosted database in the Amazon Web Services (AWS) cloud, in which data from more than 93.4 million Mexicans was exposed [26]. Another case in 2018 where it was revealed that some cyberattackers violated some financial institution systems that interacted with the Electronic Payments System (SPEI), which resulted in the theft and loss of approximately 300 million pesos from different locations, in which the attackers created fake accounts to send fraudulent payment instructions through a malicious code, tricking financial institutions to send transactions from Banco de Mexico through SPEI, as it usually does. As a result of this, various companies were affected, such as AXA Seguros, which reported inconsistencies related to the payment system, and its operative field declared that the attack was aimed to their connection systems with the SPEI platform causing an economical loss of approximately 57 million pesos [27, 34].

As detailed in the McKinsey & Company document in collaboration with COMEXI [18], there are groups called hacktivists for the purposes of carrying out a cyberattack with the main objective of making a political declaration or protest towards a government or institution. In 2012, the Cyber Protesta Mexicana group carried out a simultaneous cyberattack, where protest messages were published on at least 10 government, political party, and press websites. This group, which had similarly attacked in 2009, positioned it cyberattack as a peaceful protest against

the country's political situation, in which its activities have become global notes [28]. In Mexico alone, during the fourth quarter of 2019, cyber fraud increased 36% compared to the same period of the previous year, representing an approximate amount of 11,171 million pesos, and only 45% were rewarded and 86 out of 100 cyber frauds were able be resolved in favor of the affected user according to the document prepared by the Comision Nacional para la Proteccion y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) based on the claims with monetary impact presented by the clients of Banco de Mexico contained in the Regulatory Report R27 (CNBV) [29].

According to several studies carried out since 2019 by Fortinet and its research laboratories, FortiGuard, Mexico is the country that presents the highest number of cyberattacks in Latin America [30]. This represents a great challenge for Mexican users and companies that face this new wave of digital crime every day.

2.2 Cybersecurity Initiatives in Mexico

Although different agencies can independently implement cybersecurity initiatives, the organization and integration of these efforts requires an agency that can properly manage them. Given this, in 2017, the government of Mexico issued the National Cybersecurity Strategy [31], which establishes the vision of the Mexican State in the matter, taking into account the impotence of information and communication technologies (ICT), the risks associated with the use of technologies and cybercrimes, as well as the need for a general culture of cybersecurity. The general objective of this strategy is to identify and establish cybersecurity actions applied to the social, economic, and political spheres that allow the population and public and private organizations to use and take advantage of ICT in a responsible manner for the sustainable development of the Mexican State.

On the other hand, the Mexican legal framework also typifies cybercrime, although in a decentralized manner, however, there is a legal framework for the protection of personal data by the Federal Law on Protection of Personal Data Held by Private Parties (LFPDPPP) [32], which specifies in its Article 7 that the collection of personal data should not be done through deceptive or fraudulent means, as well as Article 20, which dictates that security breaches occurred at any stage of the treatment that affect in a way the proprietary or moral rights of the owners will be informed immediately by the person responsible to the owner, so that the latter can take the corresponding measures to defend their rights and Article 58. The owners who consider that they have suffered damage or injury to their property or rights as a result of noncompliance with the provisions of this law by the person in charge or the responsible may exercise the rights that they deem pertinent for the purposes of the corresponding compensation in terms of the corresponding legal provisions. There is also a General Law on the Protection of Personal Data in Possession of Obligatory Subjects (LGPDPPSO) [33] which contains specific topics on technological issues, cloud computing, and security specified in Article 3, where technical security

measures are defined as a set of actions and mechanisms that use technology related to hardware and software to protect the digital environment of personal data and the resources involved in its treatment. As well as in the LFPDPPP it is also specified in Article 19. The person responsible must not obtain and process personal data, through deceptive or fraudulent means, privileging the protection of the interests of the owner and the reasonable expectation of privacy. These legal frameworks have as their main objective the obligation of every entity, which handles personal data, to establish and maintain technical and physical administrative security measures. These allow to protect personal information against damage, loss, destruction, use, access, or unauthorized treatment. The legal framework also specifies confidentiality obligations, which define the specific cases in which private information may be shared with other entities, and the precautions due for that transaction. For the implementation of data security measures, those responsible must consider the existing risk, the possible consequences for the data owners, and the technological development that is available. The National Institute for Transparency, Access to Information and Protection of Personal Data (INAI) develops and publishes material to assist organizations that handle personal data and thus fulfill its responsibilities. Any organization that does not adhere to this legal framework is subject to sanctions, but these can be reduced if the authority considers that the organization followed the recommendations of the INAI.

It should be noted that a cyberattack is not considered a crime in the legislation of our country, that is, only those that are considered computer crimes, since there is no legislation on cybersecurity, for example, the theft of wireless networks (Wi-Fi) is not considered a computer crime; however, there are some that can be reported, for example, theft of data and personal information or cyberbullying [34, 35]. Given this, the Government of the State of Mexico, through the Secretariat of Security of the State of Mexico, created the Cybernetic Prevention and Investigation Unit or Cyber Police, whose main objective is to prevent, attend, and combat incidents that are committed through digital means, such as fraud, extortion, identity theft, sexual exploitation, harassment, animal abuse, and sale of prohibited substances and weapons, among others. This unit works 24 hours a day, 365 days a year, through its three areas of operation: citizen attention and cyber patrol, technological laboratory, and prevention of cybercrime [36]. On the other hand, in Mexico, some of the main universities already offer careers or educational programs in cybersecurity (e.g., UNAM, ITAM, ITESM, IPN, UNITEC). It should be noted that the Autonomous University of Nuevo León (UANL) offers the Bachelor of Security in Information Technology in which agreements have been made with the cybersecurity firm Fortinet to include its Fortinet Network Security Academy (FNSA) program, which provides academic institutions (high schools, colleges and universities, and nongovernmental organization (NGO) focused on career readiness), with the resources necessary to facilitate Fortinet's industry-recognized certification curriculum.

2.3 Cybersecurity in the Mexican Financial System

In Mexico, cybersecurity strategies have only recently been agreed for the financial sector and for the country in general, due to the fact that in 2017, Mexico ranked seventh among the 20 most important markets in the world in terms of adoption of FinTech companies, defined as the proportion of the adult population that has used at least two services of companies classified as FinTech in the last 6 months [37]; this makes for a more efficient and inclusive sector than that of some years ago; however, in addition to the growth of new industries, such as FinTech, the risk of cyberattacks on the financial sector has also increased. Given the accelerated increase in cyberattacks on the financial sector, in October 2017, the Cybersecurity Forum "Strengthening Cybersecurity for the Stability of the Mexican Financial System" was held [45]. This forum brought together authorities, representatives of financial institutions, and national and international experts to analyze best practices at the international level to strengthen cybersecurity measures, set an agenda, and coordinate efforts between authorities and the private sector, and communicates the Principles for Strengthening the Cybersecurity for the Stability of the Mexican Financial System [38]:

1. Adopt and keep updated policies, methods, and controls to identify, evaluate, prevent, and mitigate cybersecurity risks, which are authorized by the highest decision-making governing bodies and permeate all levels of the organization.
2. Establish secure mechanisms for the exchange of information between the members of the financial system and the authorities, about attacks occurred in real time and their mode of operation, response strategies, new threats, as well as the results of investigations and studies, that allow entities to anticipate actions to mitigate the risks of cyberattacks; the foregoing, protecting the confidentiality of the information.
3. Promote initiatives to update regulatory and legal frameworks that support and converge the actions and efforts of the parties, considering best practices and international agreements.
4. Collaborate in projects to strengthen the security controls of the different components of the infrastructures and operating platforms that support the country's financial services, promoting the use of information technologies to prevent, identify, react, communicate, typify, and make a common front in the face of present and future threats.
5. Promote cybersecurity education and culture among end users and the staff of the institutions themselves that, through continuous training, result in active participation to mitigate the current risks of cyberattacks.

However, the National Banking and Securities Commission (CNBV) in collaboration with the Organization of American States (OAS) [39] revealed that 100% of Mexican financial entities and institutions affirm that they identified some type of digital security event, that is, successful attacks and/or failed attacks that attempted to violate them. The most commonly identified digital security events during 2018

were malware with 56%, targeted phishing with 47%, and breach of security policies with 31%. Likewise, it is highlighted that 19% of financial entities and institutions daily identify the occurrence of events of some type of cyber threat, taking into account one of the main reasons why attacks are carried out in this specific sector. They are mainly for economic reasons. Likewise, in this study, it is mentioned that the main cybersecurity actions carried out by Mexican financial institutions consist of implementation of controls such as firewalls (85%), automated antimalware consoles (76%), automated backups (68%), and network security (VPN, NAC, ISE, IDS/IPS, web filtering, secure email, etc.) (54%). Therefore, we can assume that there is a great opportunity for development in the area of research and development in technological and cybersecurity fields in Mexico.

3 Cyber Threat Intelligence

Given the accelerated growth of cyberattacks, as well as the constant development and use of new digital platforms, organizations face more complex challenges every day when it comes to monitoring their information, that is, each application, device, or process that interacts with technology generates digital information that each, in turn, represents an event (log) in a system that cybersecurity analysts should take into account to monitor any type of suspicious activity; however, as we have mentioned, the constant use, evolution, and dependence of technology have resulted in an impressive amount of information, including possible threats that in many cases exceed analysts' analytical skills and risk omitting or reporting this information as noise. Likewise, cyber threats are becoming increasingly complex, developing new ways to violate systems using new techniques, as well as the ease of use of tools that allow any user to be able to generate these types of threats with very little effort and cause a high impact. Given this, the main challenge lies in being able to transform all this information into something actionable that can be used to make decisions for senior management, for example, being able to prioritize activities and allocate budget or personnel based on the impacts that can be had based on the collected data. This requires not only the time and/or effort of the IT or cybersecurity team but also organization, collaboration between the different areas, experience, and resources allocated by senior management to carry out these investigations successfully. This leads us to what is called cyber threat intelligence (CTI), which is defined as evidence-based knowledge, which includes context, mechanisms, indicators, implications, and practical advice, about an existing or emerging threat or danger for assets that can be used to inform decisions regarding the subject's response to that threat or danger [40]; on the other hand, SANS [41] defines CTI as analyzed information about the capabilities, opportunities, and intentions of adversaries that meets specific requirements determined by an interested party.

3.1 CTI Processes and Methodology

One of the main points that needs to be understood in this area is the difference between data, information, and intelligence to understand CTI. Therefore, we can define data as an individual element that contains information, either from a system, action, or executed process, that is, individual elements with a specific meaning. On the other hand, we can define the term threat as the possible danger that can be used to exploit an existing vulnerability with the intention of causing damage to systems, networks, or entire organizations. CTI is defined as information on how to detect and defend against cyber threats by aggregating data analysis and evaluation information with meaning.

The CTI cycle is a process to generate accurate and actionable information for the organization [41]. It begins with a planning phase, in which the intelligence questions or requirements that need to be answered are generated. When the requirements are known, the next phase is collection, the collection of data to help answer the questions and meet the requirements. The next phase is processing, where the data is put into a usable format for analysis. This leads to the fourth phase, analysis, in which the data is synthesized to identify responses to intelligence requirements. The last phase is dissemination, where the findings are captured in the correct format to reach the intended audience described in the planning phase. It is important to keep in mind that although the intelligence cycle is a cyclical process, sometimes it is necessary to go back in the process; for example, if during the analysis phase it is determined that additional information is needed or if the information should be processed in a different format, it is important to return to the appropriate previous step so that the final result is an informed and accurate analytical finding. So, as an example of where and how intelligence really adds value to the organization, it will basically give us visibility. It will allow the threat intelligence analyst to add value very quickly, timely, and actionable information that can be fed to defense teams across various roles within the organization and to IT operations people to execute and configure any necessary controls to reduce the risk of an incident and/or cyber threat. Therefore, organizations with CTI processes focus on understanding the cyber threats they face with the primary goal of providing actionable and valuable information to help defend against those threats that put the organization's information at risk.

3.2 CTI Mexico Feeds

As mentioned above, the key to be able to carry out a good CTI process is the definition of sources and collection of information; that is, once the requirements have been identified, the next step is to identify how to obtain access to the information that will help answer to the requirements. These sources of information are called intelligence feeds, which emit relevant information for analysts to

consume it in different ways. In this same article, SANS [41] shows which are the intelligence sources that organizations consume the most in order to carry out CTI.

Sources for gathering intelligence	2020
Open-source or public CTI feeds (DNS, MalwareDomainList.com)	74.30%
Threat feeds from CTI-specific vendors	68.90%
Threat feeds from general security vendors	68.50%
Community or industry groups such as Information Sharing and Analysis Centers (ISACs) and Computer Emergency Readiness Teams (CERTs)	68.20%
Security data gathered from our IDS, firewall, endpoint, and other security systems	63.40%
External sources such as media reports and news	63.10%
Incident response and live forensics	63.10%
SIEM platform	62.00%
Vulnerability data	60.60%
Network traffic analysis (packet and flow data)	57.00%
Forensics (postmortem)	56.40%
CTI service provider	45.90%
Application logs	44.40%
Other formal and informal groups with a shared interest	43.30%
Closed or dark web sources	42.10%
Honeypot data	29.90%
Shared spreadsheets and/or email	21.00%
Other	1.50%

Sources for Gathering Intelligence [41]

This definition can be explained with an example from the perspective of the analysis of cyber incidents in such a way that the data can be such as the IP, the domain, the URL, or the email that can be collected from the systems or sources of information opened on the Internet like Google. In addition, the information can be described as the exploited URL for phishing, the domain that spreads the malicious code, and the IP that establishes C&C communication with the malicious code [50]. Cyber threat intelligence is the result of comprehensive analysis reporting that a group of cybercriminals is targeting primarily financial entities, and it was recently discovered that malicious code was a variant of some previously seen threat. Therefore, actions are required to block the IP address of the C&C server frequently used by malicious code. There are different types of tools that can provide very relevant information to organizations regarding feeds for CTI, which aim to be able to carry out the mentioned intelligence phases, to deliver information already processed to organizations with the main objective of sharing information, cybersecurity studies, and findings to help organizations protect their information and minimize the risk of a vulnerability. Given this, organizations and/or companies dedicated to cybersecurity have adopted the use of CTI in their tool sets and are complemented by products or services that provide information already digested or

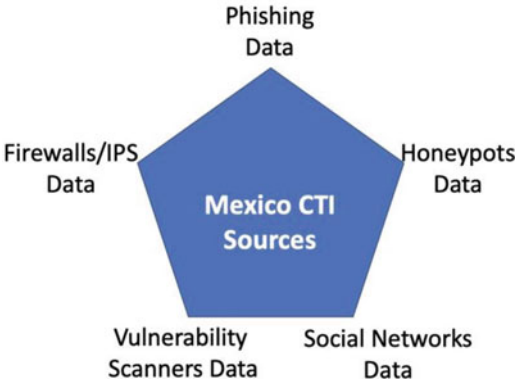

Fig. 2 CTI sources for Mexico

consumable by CTI [42–44], including social media platforms such as Facebook, has launched its ThreatExchange project [45] to share information about CTI, as well as studies related to the extraction of CTI through Twitter [46, 47]. One of the most relevant phases of the intelligence life cycle [41] focuses on being able to collect information related to relevant threats according to the population to be protected in order to understand the risks, threats, and requirements to be investigated; therefore, we will mention some of the platforms that can be used to collect relevant information to Mexico.

As mentioned above, there are various platforms and/or services available to collect relevant information on threat trends, a specific threat, as well as the techniques they use; but what intelligence sources are available that provide information for the Mexican sector? In this document, the contribution is to show some of the platforms that provide information about cyber threats that occur in Mexico and that can be used to generate relevant and actionable information in an organization, that is, using the information collected as a starting point of any malware trend or cyber threat that has occurred or that is targeting Mexico, categorizing them into five sections (phishing, firewall/IPS, honeypots, vulnerability/scanners, and social network data) so that organizations can carry out an investigation on said cyber threat to understand its objective, techniques, and procedures to measure its impact on the business, with the main objective of converting this information into a cybersecurity strategy to reduce the risk of any incident to the organization (Fig. 2).

For this, we will cover some of the main areas of intelligence interest; among them there are cyber threat trend platforms based on detections of cybersecurity events from perimeter devices (firewalls, IPS, EPP, etc.), such as Fortinet Threat Intelligence Insider Latin America [48], a quarterly threat trend tool by FortiGuard Labs [42]. For ten countries in the Latin American region, including Mexico, which has data collected and analyzed from millions of daily cybersecurity events detected by sensors deployed in the region, it also offers data on cyber threat trends by country and information on the ten main cyberattacks for the countries of the region, in the category of malware, exploits and botnets, as well as regional executive summaries of the main areas of risk and vulnerabilities identified, as well

as security tips and key findings, in addition to the possibility to download this information in PDF format, which is updated quarterly in the three main languages of the region (English, Portuguese, and Spanish). Another CTI source that offers information on vulnerabilities and visibility of devices exposed to the Internet in the Mexican sector is the Shodan search engine [49]; that is, if a device is directly connected to the Internet (from small desktop computers to nuclear power plants, etc.), Shodan consults it to obtain the public information available on that device, in which various studies about the risks that exist on devices exposed to the Internet have been carried out [50]. Shodan recently added panels and exposition of Internet availability for certain countries, including one for Mexico [51], which shows the number of industrial control systems exposed in the country, as well as the most relevant vulnerabilities. In addition, a general search was made in this tool using the "country:" MX "" filter, which gave us a total result of 4,880,789 devices exposed to the Internet [52], of which cities such as CDMX (616,591), Zapopan (212,236), Guadalajara (189,331), Monterrey (180,109), and San Luis Potosí (88,374) stood out.

On the other hand, there are various platforms made up of a network of honeypots, which are nothing more than devices exposed to the Internet that work as decoys to attract cyber threats and to monitor the techniques used by these cyber threats, such as Bad Packets Cyber Threat Intelligence [53], which has a global network of honeypots that detect the activities of active botnets, which are scanning the Internet and/or participating in malicious activities, also have honeypots deployed in Mexico [54], which can provide information on cyber threats that target our country, in which said tool has been used for different studies to monitor botnet campaign traffic by scanning devices exposed to the Internet [55] and the profiling of critical industrial systems (ICS) exposed on the web [56]. Likewise, platforms were also found that provide intelligence feeds related to fraudulent websites, better known as phishing, such as APWG [57]who mention in their Phishing Activities and Trends report for the first quarter of 2020 that country code domains (ccTLDs), such as .UK for the UK and .MX for Mexico, were approximately 44% of the domains in the world at the beginning of the first quarter, but only 27% of the domains in the first quarter sample. Another platform from which phishing information can be downloaded is OpenPhish [57], which offers different plans for the use of its platform, from downloading URLs for free to detailed information on each site. It should be noted that using the free phishing site download offered by the platform [58], at least 15 sites with the domain ".mx" and 2 with the word "mexico" were found in the URL that have been detected with some malicious activity. Another tool that can provide intelligence on malicious sites for Mexico is URLhaus, which offers feeds of malicious sites that can be downloaded, and for Mexico, 291 URLs were found classified as phishing or malicious [59].

Social media platforms allow users and organizations to communicate and share information. For security professionals, it could be more than just a network tool; that is, it can be an additional source of valuable information on topics from vulnerabilities, exploits, and malware to threat actors and anomalous cyber activities. For example, Twitter and Facebook are not just a platform for sharing

content, promotion, or social networks. There are open-source intelligence tools (e.g., TWINT [60] and ThreatExchange [61]) that can scrape data or publicly available Twitter streaming application programming interfaces (APIs) that can collect sample data for analysis. We also saw that bots shared the latest indicators of compromise (IoC) and even threat detection rules. In fact, there is publicly available information on how Twitter bots can be used to monitor Internet of Things (IoT) devices. There are also open-source honeypots that can log data on Twitter.

There are cloud-based threat intelligence platforms, such as the IBM X-Force Exchange [62] that allows you to use, share, and act based on threat intelligence. This platform allows you to quickly investigate the latest cyber threats in the industry based on tags, hashtags, or indicators as well as adding actionable intelligence or collaborate with other cybersecurity analysts; it also shows us different options for malware, analysis, profiles, etc. On this platform, 35 cyber threats were found by performing a search with the tag "Mexico" which allowed us to carry out a search for 35 cyber threats documented on this platform, of which only 12 were related to Mexico in 2020. On the other hand, cybersecurity organizations have created real-time cyber threat maps, to provide an overview of the attacks and their relationship between countries; for example, Live Cyber Threat Map is a free Check Point page that shows malware attacks in real time, phishing and exploit in the world, as well as statistics. By focusing on Mexico (by clicking on the map) [63] shows us the trends of cyber threats in the last 30 days: banking Trojans (1.2%), botnet (6.2%), cryptominer (3.6%), mobile (6.5%), and ransomware (0.3%). Another threat map that can provide relevant information for Mexico is the A10 company DDoS map [64], which indicates that in Mexico there are more than 115,000 devices that can be used as weapons to carry out a distributed denial-of-service (DDoS) attack, 21,097 hosts identified and infected with DDoS malware (called drones), 2,884 identified hosts that are carrying out malicious activity (called abuse), 5,760 publicly exposed and vulnerable DNS servers to be exploited by an amplification attack, as well as NTP servers (1,608), SSDP (26,421), SNMP (27,375), and TFTP (28,527), among others. Additionally, a service was found that its main function is to be a search engine for servers and services as its support for IPv6 generating intelligence; with this information, it obtains an analysis and evaluates the risk exposure of organizations in real time [65, 66].

4 Conclusion

This document compiled the most relevant information, as well as the current situation in Mexico using, for the most part, documents issued by the Mexican government. This attracts attention, since there are various studies, initiatives, and strategies under development in the country. Likewise, it was found that performing a CTI strategy requires great demand and constant development by any organization, whether it involves personnel or technology with advanced analysis and detection capabilities, as well as a framework of references and processes to obtain the

knowledge for the prevention of cyber threats with the main objective of obtaining evidence that can positively influence the decision-making of the organization; therefore, experience, skills, and information sources of a security team define its ability to produce accurate and actionable cyber threat information [67]. Given this, we were able to find different intelligence sources related to information for Mexico, which will be analyzed in future work and dictate the ability to generate a threat detection model based on the evidence collected from the sources described in this document. It is also clear that there are numerous positive trends in the community, such as more organizations producing intelligence rather than just consuming it. But there are also many challenges, such as getting the right staff and training to conduct cyber threat intelligence. Tools and data sources will always be vital to the process, but the world of intelligence analysis is intrinsically analyst driven, and an approach is rightly placed there. Sharing not only adversarial IoC and TTP, but also analytical processes, will help the community continue to grow. Some sharing processes include strategies to measure the effectiveness of a CTI program [41].

4.1 Challenges and Future Work

The next steps in this and future investigations include identifying the intelligence sources necessary to carry out a predictive model based on data and evidence collected for the Mexican sector; even specific adjustments can be planned to identify the circumstances of the data collected. In addition, studies will be carried out on the technology of processing large amounts of data and information on cyber threats, as well as data mining analysis techniques, the analysis of correlation between the data with the main objective of processing the CTI information collected to estimate a forecast of cyber incidents based on evidence from intelligence sources.

References

1. W.E. Forum, «World Economic Forum Global Risks Perception Survey 2019–2020,» 2020. [En línea]. Available: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf
2. I. (. D. Corporation)., «The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast,» 2019. [En línea]. Available: https://www.idc.com/getdoc.jsp?containerId=prUS45213219
3. Gartner, «Leading the IoT: Gartner Insights on How to Lead in a Connected World.,» 2017. [En línea]. Available: https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf
4. Z. Doffman, «Cyberattacks on IoT Devices Surge 300% in 2019, 'Measured in Billions', Report Claims",» Forbes, 2019. [En línea]. Available: https://www.forbes.com/sites/zakdoffman/2019/09/14/dangerous-cyberattacks-on-iot-devices-up-300-in-2019-now-rampant-report-claims/#43ec06af5892
5. F-Secure, «ATTACK LANDSCAPE H1 2019,» 2019. [En línea]. Available: https://blog-assets.f-secure.com/wp-content/uploads/2019/09/12093807/2019_attack_landscape_report.pdf

6. A. Venkat, «Wikipedia Investigates DDoS Attack,» Bankinfosecurity.com, Information Security Media Group (ISMG), 2019 September. [En línea]. Available: https://www.bankinfosecurity.com/wikipedia-investigates-ddos-attack-a-13049
7. NIST, «COMPUTER SECURITY RESOURCE CENTER,» NIST, [En línea]. Available: https://csrc.nist.gov/glossary/term/cyber_risk. [Último acceso: 19 May 2020]
8. C. S. F. B. J. T. &. M. D. K. Kruse, «Cybersecurity in healthcare: A systematic review of modern threats and trend,» Technology and Health Care, 2017
9. D. R. A. Z. W. F. F. L. P. F. X. &. T. J. Wu, «Cybersecurity for digital manufacturing,» Journal of Manufacturing Systems, 2018
10. Fortinet, «Fortinet Threat Intelligence,» Fortinet, [En línea]. Available: https://www.fortinet.com/fortiguard/threat-intelligence/threat-research.html. [Último acceso: 03 May 2020]
11. Cisco, «Cisco Cybersecurity Report Series,» Cisco, [En línea]. Available: https://www.cisco.com/c/en/us/products/security/security-reports.html#~more-reports. [Último acceso: 03 May 2020]
12. Fireeye, «M-Trends 2020,» Fireeye, [En línea]. Available.: https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html. [Último acceso: 03 May 2020]
13. ISO27000, « ISO/IEC 27032:2012 — Information technology — Security techniques — Guidelines for cybersecurity,» ISO/IEC, [En línea]. Available: https://www.iso27001security.com/html/27032.html. [Último acceso: 19 May 2020]
14. F. C. y. C. Teconologico. [En línea]. Available: http://foroconsultivo.org.mx/. [Último acceso: 08 May 2020]
15. I. a. d. i. y. t. d. México, «Foro Consultivo Cientifico y Tenologico,» 2018. [En línea]. Available: https://foroconsultivo.org.mx/proyectos_estrategicos/img/8/17.pdf. [Último acceso: 07 May 2020]
16. F. Staff, «Cibercrimen afecta a uno de cada cuatro mexicanos, según aseguradoras,» forbes Mexico, 05 May 2019. [En línea]. Available: https://www.forbes.com.mx/cibercrimen-afecta-a-uno-de-cada-cuatro-mexicanos-segun-aseguradoras/. [Último acceso: 08 May 2020]
17. E. s. C. E. e. M. 2. D. t. entrega, «Asociacion de Internet MX,» Diciembre 2019. [En línea]. Available: https://irp-cdn.multiscreensite.com/81280eda/files/uploaded/Estudio%20de%20Comercio%20Electro%CC%81nico%20en%20Me%CC%81xico%202019.pdf. [Último acceso: 08 May 2020]
18. P. d. c. e. México, «Comexi,» Junio 2018. [En línea]. Available: https://consejomexicano.org/multimedia/1528987628-817.pdf. [Último acceso: 08 May 2020]
19. G. d. Mexico, «Secretaria de Comunicaciones y Transportes,» [En línea]. Available: https://www.gob.mx/sct. [Último acceso: 12 May 2020]
20. OEA. [En línea]. Available: http://www.oas.org/es/. [Último acceso: 12 May 2020]
21. H. d. l. u. e. c. e. M. 2019, «Gobierno de Mexico,» 2019. [En línea]. Available: https://www.gob.mx/cms/uploads/attachment/file/444447/Estudio_Ciberseguridad.pdf. [Último acceso: 12 May 2020]
22. P. Federal, «¿Conoces qué es el Phishing?,» Gobierno de Mexico, 08 Enero 2019. [En línea]. Available: https://www.gob.mx/policiafederal/es/articulos/conoces-que-es-el-phishing?idiom=es. [Último acceso: 12 May 2020]
23. NIST, «NIST Information Technology Laboratory,» NIST, [En línea]. Available: https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary. [Último acceso: 19 May 2020]
24. T. G. R. R. 2020, «The Global Risks Report 2020,» 16 January 2020. [En línea]. Available: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf. [Último acceso: 12 May 2020]
25. R. C. M. 2018, «Willis Towers Watson,» 04 December 2018. [En línea]. Available: https://www.willistowerswatson.com/es-MX/Insights/2018/12/riesgo-cibernetico-mexico-2018. [Último acceso: 13 May 2020]
26. J. Arreola, «Padrón electoral en la nube: ¿ciberproblemas a la mexicana?,» Forbes Mexico, 26 April 2016. [En línea]. Available: https://www.forbes.com.mx/padron-electoral-la-nube-ciberproblemas-la-mexicana/. [Último acceso: 13 May 2020]

27. A. México, «Comunicado Oficial: Sin afectaciones a datos o recursos de asegurados: AXA,» 23 Octubre 2018. [En línea]. Available: https://axa.mx/web/blog/postura-de-axa-mexico. [Último acceso: 19 May 2020]
28. N. Rial, «Mexican hackers attack official sites,» New Europe, 17 September 2012. [En línea]. Available: https://www.neweurope.eu/article/mexican-hackers-attack-official-sites/ . [Último acceso: 15 May 2020]
29. CONDUSEF, «FRAUDES CIBERNÉTICOS TRADICIONALES,» 2020. [En línea]. Available.: https://www.condusef.gob.mx/?p=estadisticas. [Último acceso: 18 May 2020]
30. Fortinet, «Threat Intelligence Insider Latin America,» Fortinet, 10 April 2020. [En línea]. Available: https://www.fortinetthreatinsiderlat.com/. [Último acceso: 20 May 2020]
31. E. n. d. Ciberseguridad, «Gobierno de Mexico,» 2017. [En línea]. Available: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf. [Último acceso: 23 May 2020]
32. L. F. D. P. D. D. P. E. P. D. L. PARTICULARES, «http://www.diputados.gob.mx/» 2010. [En línea]. Available: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf. [Último acceso: 23 May 2020]
33. L. G. D. P. D. D. P. E. P. D. S. OBLIGADOS, «http://www.diputados.gob.mx/,» 2017. [En línea]. Available: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf. [Último acceso: 23 May 2020]
34. G. d. Mexico, «¿Has sufrido acoso cibernético? ¡Identifica sus modalidades y protégete!,» [En línea]. Available: https://www.gob.mx/conavim/articulos/has-sufrido-acoso-cibernetico-te-decimos-a-donde-acudir. [Último acceso: 20 May 2020]
35. Excelsior, «Cómo denunciar delitos cibernéticos en México,» Excelsior, 05 May 2019. [En línea]. Available: https://www.excelsior.com.mx/hacker/como-denunciar-delitos-ciberneticos-en-mexico/1311256. [Último acceso: 20 May 2020]
36. S. d. Seguridad, «Unidad de Prevención e Investigación Cibernética,» Gobierno del Estado de México, [En línea]. Available: https://sseguridad.edomex.gob.mx/seguridad-publica-transito/policia-cibernetica. [Último acceso: 21 May 2020]
37. R. N. d. I. Financiera, «cnvb.gob.mx,» 2019. [En línea]. Available.: https://www.cnbv.gob.mx/Inclusi%C3%B3n/Documents/Reportes%20de%20IF/Reporte%20de%20Inclusion%20Financiera%209.pdf. [Último acceso: 25 May 2020]
38. C. N. B. y. d. Valores, «Foro de Ciberseguridad,» 2017, 2020 23 Oct. [En línea]. Available: https://www.gob.mx/cnbv/articulos/foro-de-ciberseguridad. [Último acceso: 25 May]
39. T. S. O. I. T. C. M. F. SYSTEM, «http://www.oas.org/,» 2019. [En línea]. Available: http://www.oas.org/en/sms/cicte/Documents/reports/The-State-of-Cybersecurity-in-the-Mexican-Financial-system.pdf. [Último acceso: 26 May 2020]
40. R. McMillan, «Definition: Threat Intelligence,» Gartner Research, 2016 May 2013. [En línea]. Available: https://www.gartner.com/en/documents/2487216/definition-threat-intelligence
41. 2. S. C. T. I. (. Survey, «https://www.sans.org/,» 2020. [En línea]. Available: https://www.sans.org/reading-room/whitepapers/analyst/2020-cyber-threat-intelligence-cti-survey-39395. [Último acceso: 27 May 2020]
42. Fortinet, «FortiGuard Labs,» Fortinet, [En línea]. Available: https://fortiguard.com/. [Último acceso: 01 06 2020]
43. C. systems, «Talos,» Cisco systems, [En línea]. Available: https://talosintelligence.com/. [Último acceso: 01 06 2020]
44. Fireeye, «Mandiant Threat Intelligence,» Fireeye, [En línea]. Available: https://www.fireeye.com/solutions/cyber-threat-intelligence.html. [Último acceso: 01 06 2020]
45. Facebook, «ThreatExchange Documentation,» Facebook, [En línea]. Available: https://developers.facebook.com/docs/threat-exchange/v2.12. [Último acceso: 06 01 2020]
46. P. K. D., V. M., A. J., T. F. Sudip Mittal$_*$, «CyberTwitter: Using Twitter to generate alerts for Cybersecurity Threats and Vulnerabilities,» 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), 2016
47. G. C. T. I. f. T. U. N. Classification, «Gathering Cyber Threat Intelligence from Twitter Using Novelty Classification,» 2019. [En línea]. Available: https://www.researchgate.net/publication/

334223932_Gathering_Cyber_Threat_Intelligence_from_Twitter_Using_Novelty_ Classification. [Último acceso: 01 06 2020]
48. Fortinet, «Fortinet Threat Intelligence Insider Latin America,» Fortinet, 27 11 2019. [En línea]. Available: https://www.fortinetthreatinsiderlat.com/es/Q1-2020/MX/html/trends#trends_position. [Último acceso: 01 06 2020]
49. Shodan, «What is Shodan?,» [En línea]. Available: https://help.shodan.io/the-basics/what-is-shodan. [Último acceso: 05 06 2020]
50. A. A. a. I. Alsmadi, «IoT and the Risk of Internet Exposure: Risk Assessment Using Shodan Queries,» 2019 IEEE 20th International Symposium on A World of Wireless, Mobile and Multimedia Networks, 2019
51. Shodan, «Mexico Internet Exposure Dashboard,» [En línea]. Available: https://exposure.shodan.io/#/MX. [Último acceso: 05 06 2020]
52. Shodan, «Shodan,» [En línea]. Available: https://www.shodan.io/search?query=country%3A%22MX%22. [Último acceso: 05 06 2020]
53. B. Packets®, «Bad Packets® Cyber Threat Intelligence,» [En línea]. Available: https://badpackets.net/threat-intelligence/. [Último acceso: 05 06 2020]
54. B. Packets®, «Mirai-like Botnet Hosts,» Bad Packets®, [En línea]. Available: https://mirai.badpackets.net/accounts/login/?next=/%3Fpage%3D27651%26sort%3Dcountry. [Último acceso: 05 06 2020]
55. A. K. M. V. G. a. T. M. O. P. Dwyer, «Profiling IoT-Based Botnet Traffic Using DNS,» 019 IEEE Global Communications Conference (GLOBECOM), 2019
56. V. G. a. T. M. Angelos K. Marnerides, «Identifying infected energy systems in the wild,» de e-Energy '19: Proceedings of the Tenth ACM International Conference on Future Energy Systems, Phoenix AZ, 2019
57. P. Feeds, «openphish,» [En línea]. Available: https://openphish.com/phishing_feeds.html. [Último acceso: 06 06 2020]
58. openphish, «https://openphish.com/feed.txt,» [En línea]. Available: https://openphish.com/feed.txt. [Último acceso: 06 06 2020]
59. URLhaus, [En línea]. Available: https://urlhaus.abuse.ch/feeds/country/MX/. [Último acceso: 07 06 2020]
60. N. Young, «github.com,» [En línea]. Available: https://github.com/twintproject/twint. [Último acceso: 07 06 2020]
61. Facebook, [En línea]. Available: https://developers.facebook.com/programs/threatexchange/. [Último acceso: 07 06 2020]
62. IBM, [En línea]. Available: https://www.ibm.com/mx-es/security/xforce. [Último acceso: 07 06 2020]
63. checkpoint, «Live Cyber Threat Map,» [En línea]. Available: https://threatmap.checkpoint.com/. [Último acceso: 07 06 2020]
64. A10, «DDOS WEAPONS INTELLIGENCE MAP,» [En línea]. Available: https://threats.a10networks.com/. [Último acceso: 07 06 2020]
65. mrlooquer, [En línea]. Available: https://mrlooquer.com/. [Último acceso: 08 06 2020]
66. M. Muñoz, M. Peralta, C.Y. Laporte, «nálisis de las debilidades que presentan las Entidades Muy Pequeñas al implementar el estándar ISO/IEC 29110: Una comparativa entre estado del arte y el estado de la práctica,» RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação,, pp. 85–96, 2019
67. V. M. a. S. Bromander, «Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence,,» 2017 European Intelligence and Security Informatics Conference (EISIC), 2017