International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 23 (2018) pp. 16648-16655
© Research India Publications. http://www.ripublication.com

Approach to the State of the Art of Ciberdelincuence in Colombia

Miguel Hernández[1], Luis Baquero[1], Celio Gil[1], Daniel A. Cárdenas[1] and Alfredo Gil[1]

[1] Fundación Universitaria Los Libertadores, Bogotá D.C., Colombia.

Abstract

The objective of this article is to present an approach to the state of the art of cybercrime in Colombia, due to the progressive increase that Cybercrime has had in recent years, therefore, it is necessary to know what cybercrime and its types are, as well as the characteristics that identify a cyberdelicuent. The biggest attacks to the banking sector, to private entities and to the governmental sector are described during the period from 2014 to 2017, through statistics that illustrate this phenomenon that has taken more force every day, being one of the biggest scourges of the country. Also, it is described that the authorities in our country have done to face this problem, which is the most important legislation on the subject and how bills of the Budapest Convention will allow adopting measures to confront cybercrime, as well as establishing the due to controls in order to reduce the rate of incidents caused by this phenomenon. Although we are pioneers and leaders in Latin America, there is still much that needs to be done in terms of cybersecurity.

Keywords: Cybercrime, Cybercrime, Cybersecurity, Hacker, Computer crime

INTRODUCTION

In Colombia the term hacker is often heard when there is loss of information or an attack on a company, a social network or a bank account, but from the beginning we are misinformed, because according to the Royal Academy of the Spanish Language [1], Hacker is an "Expert person in the management of computers, who deals with the security of systems and developing improvement techniques". According to [2] this type of crime is called cybercrime which is an activity carried out by one or several people with knowledge in communication networks, with a great expertise in computer programming and use it as a criminal means to harm entities. Financial institutions, corporations, universities, government entities and the population in general.

According to Andrés Velázquez, there are two types of cybercriminals: the first are experts and commit crimes, the others know the vulnerabilities in a certain platform, organization or entity and take advantage of them for their benefit, these are called insiders; This second group is made up of employees of the same company who delete, damage, steal sensitive information in mass storage media and documents. For [3] within the crimes that most afflict Colombia are identity theft, cyber fraud, denial of service, information leakage, phishing, improper disclosure of content, child pornography, use of spyware, violation of copyright and Internet piracy.

1. THE CIBERDELINCUENCE

According to [4] cybercrime is largely made up of application developers and researchers who make up these criminal gangs, who are responsible for creating new innovative methods to enter without permission into data systems domains or exploit security vulnerabilities in operating environments, also take advantage of social engineering to infect computers through a range of tricks, hide information and resist the actions of system protectors or firewalls. But we also find skilled and restless students with extensive knowledge in operating systems and infrastructure, who want to test their skills by generating malware and targeting companies, and young people who want to experience this world of development with the help of the internet, as there are now numerous websites that explain how to create and develop computer viruses and how they can bypass antivirus software.

Cybercrime is part of cybercrime, but in many cases the investigations exaggerate with the threat of the impact of the damage it causes and in others the real risk to which the use of information and communication technologies (ICTs) entails is not perceived. Cybercrime represents 15% of the illegal acts committed to companies in Colombia, generating an economic damage close to 600 million dollars in the last year. Approximately 62% of affected companies take more than a month to detect it; even 10% do it a year after the attack was carried out [5]. By that time, correcting the security structure may take longer due to resource constraints.

The logic that this novelty lasts so long, is the revolution of ICT, as a broad, open and dynamic concept that encompasses all the elements and systems used today for the treatment of information, its exchange and communication in today's society, in which the phenomenon of Cybercrime is framed. Based on the figures presented above, it is assumed that cybercrime will continue to expand and evolve in the coming decades [6].

Cybercrime converts a citizen who interacts on the Internet, contacts others, sends messages, interacts in forums or shares their photos, as a possible target of a personal cyber-attack or their honor, intimacy, sexual freedom or similar legal. The same happens with other supranational institutions in relation to political or ideological cybercrimes committed with the intention of destabilizing a State or of spreading a specific political message taking advantage of the possibilities of massive communication offered by cyberspace [7]. For Ivan Dario Marrugo [8], a lawyer specializing in Telecommunications Law, the process of investigation and the expert and computer evidence is the main difficulty in processing this type of crime. In Colombia "only a few years ago we have an Administrative Procedure Law [9] and the

General Process Code (Law 1564) [10] that opened the possibility of admitting electronic evidence in this type of lawsuit".

1.1. CLASSIFICATION OF CRIMES

According to [11] there is a series of computer crimes on which special care must be taken not to become a victim of these, among the most important we have:

- Crimes against the confidentiality, integrity and availability of data and computer systems:
  - Illicit access to computer systems.
  - Unlawful interception of computer data.
  - Interference in the operation of a computer system.
  - Abuse of devices that facilitate the commission of crimes.
- Computer crimes:
  - Computer falsification through the introduction, deletion or deletion of computer data.
  - Computer fraud through the introduction, alteration or deletion of computer data, or interference in computer systems.
  - Fraudulent data erasure or file corruption.
- Offenses related to content:
  - Production, offer, dissemination, acquisition of contents of child pornography, by means of a computer system or possession of said contents in a computer system or data storage medium.
- Offenses related to infractions of intellectual property and related rights:
  - In this group of crimes is the copying and distribution of computer programs, or hacking.

1.2. CHARACTERISTICS OF THE CIBERDELINCUENTE

1.2.1. ACTIVE SUBJECT

These people are those who possess certain computer features not very common to other criminals, these subjects are usually in the company managing sensitive and important information of their organization, their main skill is the management of computer systems, they are ready, determined, motivated and willing to accept technological challenges, according to [12] every day the criminals have been changing their characteristics and now the only difference is the crime they commit and the modality of it. That is, the person who enters a computer system without intending to commit a crime is different from that employee of a financial institution which diverts funds from the accounts of their clients to another.

1.2.2. PASSIVE SUBJECT

It is the victim of the crime, that is to say, on which falls the action of the active subject, these can be individuals, credit institutions, and governments. The passive subject is very important to study computer crimes, because through it you can know the different facts committed by criminals, with this actions can be prevented, because many of the crimes are discovered by chance due to ignorance of the modus operandi. Operandi of the criminals. According to [13] the lack of laws that protect victims, the lack of preparation on the part of the authorities to understand, investigate and apply the appropriate legal treatment and the fear of companies in reporting these crimes for the consequences and losses that may carry for which it is impossible to know the true magnitude of these computer crimes.

2. CIBERDELINCUENCE IN COLOMBIA

2.1. GENERAL CONSIDERATIONS

According to the report of the Colombian National Police [14], a service portal called @caivirtual 24/7 has been adapted, in order to provide attention to incidents that affect the citizenry in everything related to computer incidents. In this Center, which has the direction of the DIJIN, its main objective is the prevention, orientation and attention of incidents that affect the different public and private sectors, as well as, the citizens in general. Through the page www.caivirtual.policia.gov.co alerts are disseminated, such as those of the year 2014, in which 92% of them affected citizens, 5% to financial institutions and the rest shared by sectors of industry, technology, government and education as shown in Figure 1.

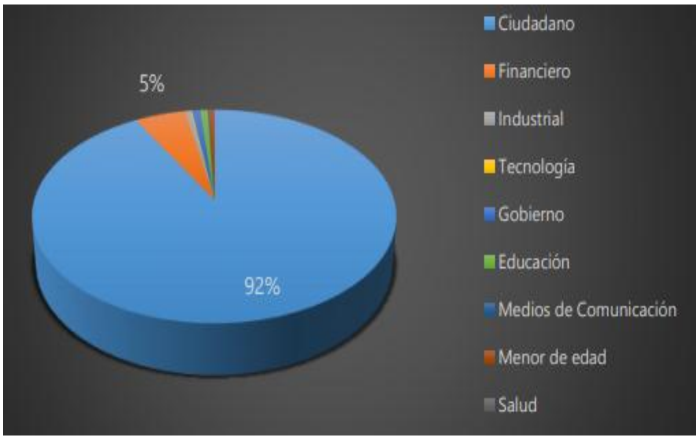


Figure 1. Statistics year 2014 taken from https://bit.ly/2IoIR14

For the year 2015, attacks on citizens were reduced to 63%, in financial institutions the percentage increased by 10% to the figures of the previous year, the industry by 5%, technology by

4%, the Government by 6%, Education 3% and the media and minors each with 2%, as can be seen in Figure 2.

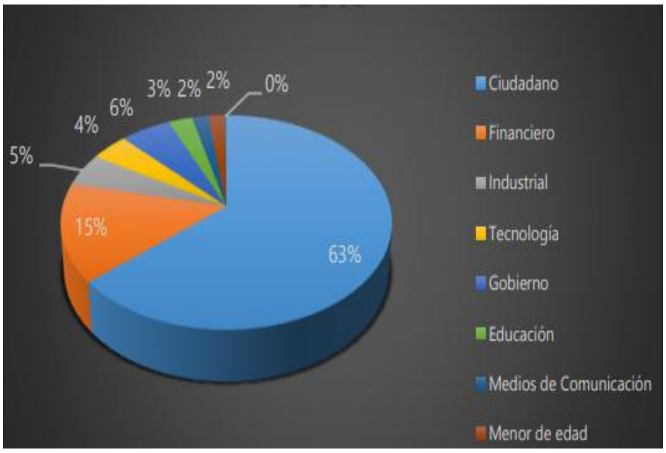


Figure 2. Statistics year 2015 taken from https://bit.ly/2IoIR14

For 2016, citizens and some organizations adopt security policies which help a large decrease in attacks as reflected in the reports of that year, which yielded the following figures: citizens 57%, financial 14% and the government 2%, but increased in the Industry 7%, technology 8%, Education and media each with 4%, and minors 3%, as can be seen in Figure 3.

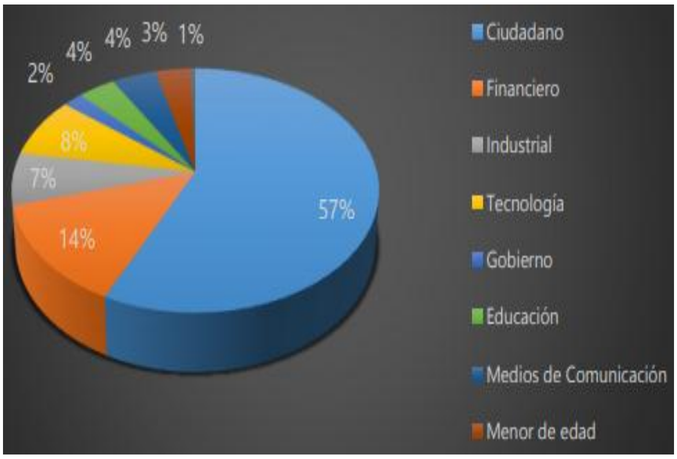


Figure 3. Statistics year 2016 taken from https://bit.ly/2IoIR14

In the year 2017 Cybercrime increased by 28.30%, the commercialization of illegal products such as narcotics, stolen goods, fraudulent documents, among others, have been favored by the consolidation of cryptocurrencies as the preferred means of payment for crime. The integration of children and adolescents on the web, resulted in criminal actions against their lives and the integrity of them, in this activity generated the following indicators: 508 alerts generated, 2,987 interactions published on social networks, 15 groups identified worldwide on Facebook [15], 3 groups eliminated in Colombia (Facebook) and 4,123 users who were denied access to these groups and one (1) INTERPOL global alert (purple circular), as we see in the figure 4.

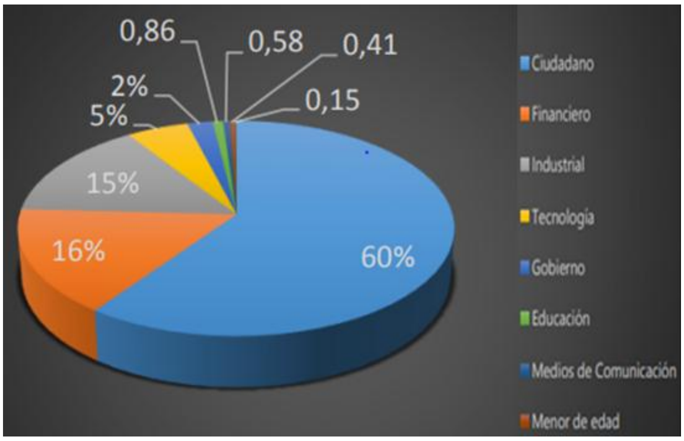


Figure 4. Statistics year 2017 taken from https://bit.ly/2zHtmco

The panorama of cybercrime in Colombia is reflected in figure 5, where in the main cities more than 75% of subscribers of fixed internet are concentrated and the highest index of inhabitants per city [16]. The following figures indicate that 60% of scams correspond to fraud by buying or selling products through the Internet (3846 reports), 16% to scams by phone calls (Vishing), 13% correspond to scams through text messages or chats (Smishing), 8% of scams are associated with Nigerian letters, 2% correspond to fraudulent offers of leases of rest estates by internet (tourist packages), 1385 cases of sim card impersonation, while government computer attacks with backdoor mode was caused by malware infection and RAT (Remote Access Tool).

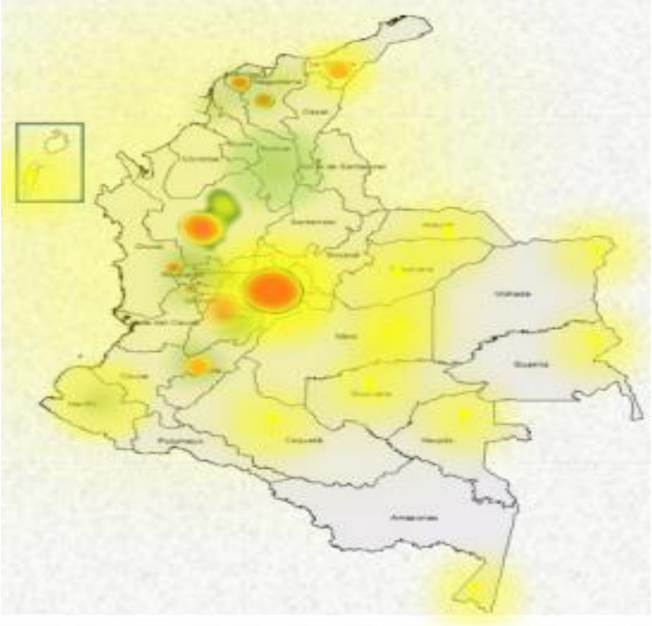


Figure 5. Heat map. Taken from https://bit.ly/2zHtmco

3. CIBERDELINCUENCE IN BANKING ENTITIES

3.1.1. IDENTITY THEFT MODALITY

The financial sector is the most affected with this modality, since cybercriminals use identities daily to access credit cards or indebtedness slots, these attacks are generated by the loss of documents, leakage of internal, external information or Social Engineering. In Colombia, in the window from 2014 to 2015, 12,923 cases were registered for violation of Law 1273 of 2009, of which 1,299 were for identity theft, this being 11% of the complaints. It is also known that criminals acquire cellular telephony, data, equipment, purchases of air tickets, household appliances, goods and services, therefore, it is recommended that before the loss of personal or bank documents should be reported immediately to the entities charged with in order to block bank cards, tokens and / or pins [17].

3.1.2. PHISHING MODE

Phishing "is a method that cybercriminals use to deceive you and get you to reveal personal information, such as passwords or credit card information, social security and bank account numbers" [18]. This is done by text message to the cell phone, phone call, websites simulating your bank, in pop-up windows that come out on your computer and sending emails, the person diligence all your data without realizing that you may be committing a crime with your information [19]. Phishing cannot be eliminated, but it can be avoided by not replying to text messages or the links that arrive to your email, not giving information by phone, not opening attachments of unsolicited emails, and as a protection measure it is recommended to change periodically the password and protect it, finally, validate well the URLs that are of the site where they are going to enter.

ASOBANCARIA through a study of the Organization of American States (OAS) and Symantec signaled that cyber fraud in Colombia is a phenomenon equivalent to US $ 461 million each year. In countries like Brazil, this scourge costs the economy US $ 8,000 million and in Mexico about US $ 3,000 million. The entire financial system invests many resources each year in technology to carry out transactions, likewise banks continue to increase the budget in security measures and policies, but also customers have an obligation to take more care of the tools that banks give as a means of payment to avoid cybercrime. ASOBANCARIA maintains that customers are the weakest links in the chain [20], of which 30 percent of attacks are against natural persons and 70 percent against companies.

3.1.3. SKIMMING MODE

This modality is well known in Colombia and is the cloning of credit or debit cards, it consists of duplicating one card in another with the same information obtained from yours. According to [21] in Colombia, 84 incidents were recorded in 2016 and 23 in the course of 2017, with the growth of international bands from countries such as Romania, which arrive in the country with a high influx of tourists and install high-tech devices. like micro cameras and microphones in the ATMs. These cards are standardized by ISO 7810, have dimensions and characteristics such as name of the entity, name of the owner, date of validity of the same, the signature of the carrier, also have a PIN code, a key to operate ATMs, a security code and a magnetic strip where the data is saved under the ISO 7813 security standard [22]. Criminals can adapt parts (as illustrated in Figure 6) where they install sensors to capture the information of the magnetic strips and spy cameras where they take the bill from the account holders and hours later remove these objects and extract the information to make the respective cloning.

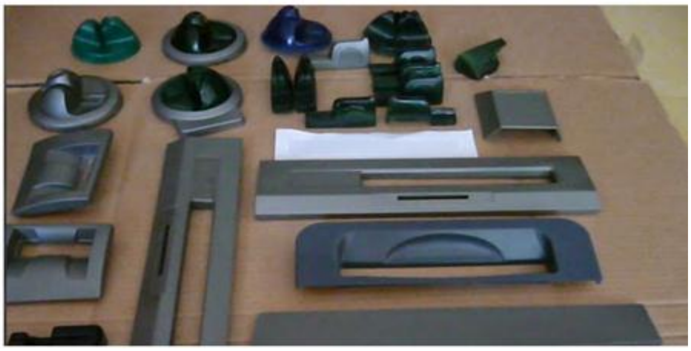


Figure 6. Objects that modify the criminals taken from https://bit.ly/2SnAvrR

4. CIBERDELINCUENCE IN PRIVATE ENTITIES

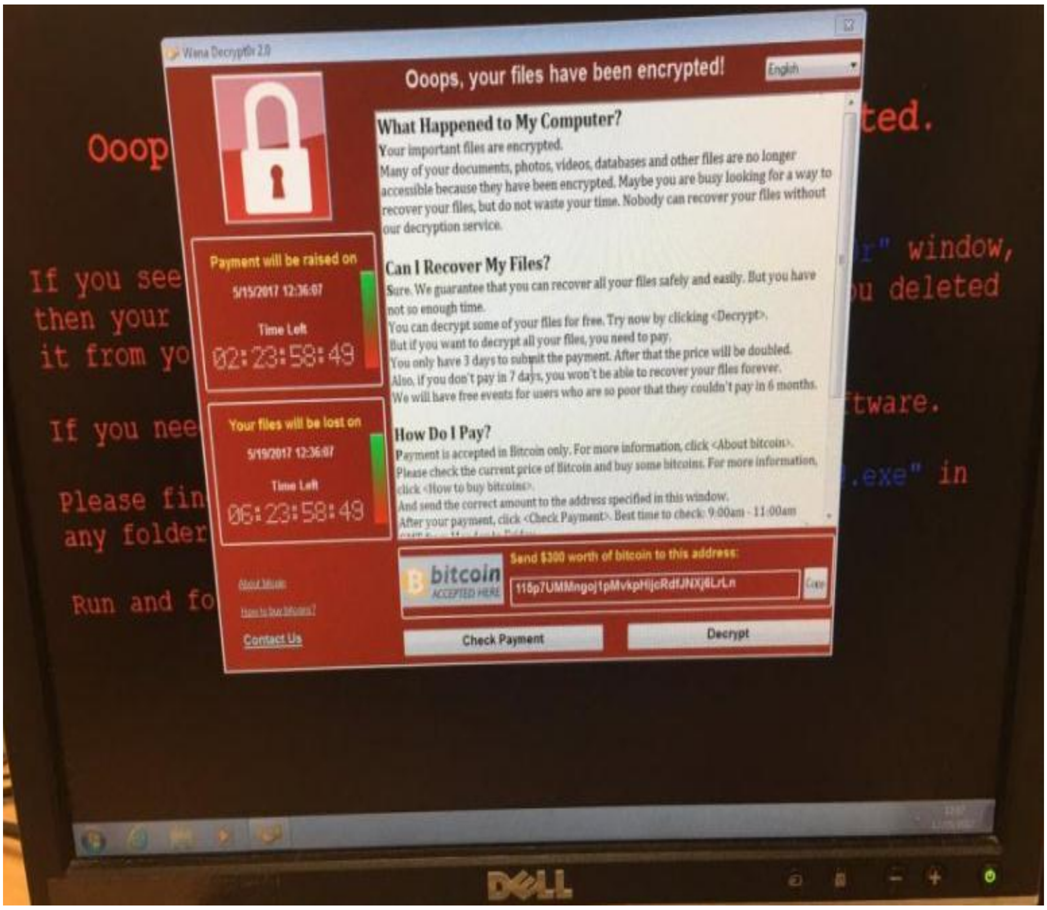
4.1. CORPORATE MAIL SUPPLY

Also known as Business Email Compromise Attacks (BEC), according to [23] it is an attack made by phishing cybercriminals intercepting the email inbox, which is studied to pass through spam filters, analyze the information of the company, look for employees in social networks, and then these criminals pass themselves off as executives sent similar emails to try to get an employee, client or provider to transfer funds or confidential information to places or accounts where they indicate them. In the article entitled: "Cybercrime in 2017: the threat grows over Colombia", the magazine [24] indicates that losses were registered for 380 million pesos and that this figure grew from 5 to 28 percent of the total during 2017.

4.2. RANSOMWARE

After Windows (Microsoft) issued a patch to update a vulnerability named Eternal Blue which had the operating system generated the attack known as Ransomware, according to [25] is a software with which cybercriminals infect computers, this has the ability to block a device from a remote location and encrypt the files by removing control of all information, then request the payment of a ransom, said payment is made through a virtual currency.

In Colombia, according to [26], the director of the Cybernetic Center of the Police, reported that the attack was named Wanna Cry, this being a classification of Ransomware, the Police received 7400 reports where 11 private sector companies were affected.



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/15/2017 12:36:07
Time Left
02:23:58:49

Your files will be lost on
5/19/2017 12:36:07
Time Left
06:23:58:49

Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Figure 7. Message issued in the attack taken from https://bit.ly/2QwaQA0

For the director of this center Colonel Fredy Bautista [27], the malignant program, arrived in a massive way to Colombia through a suspicious email that had as its subject "Online banking transfer" and as sender had a Mexican financial entity, this same He argued that Colombia was the fourth country most affected by the attack and explained that the victim has 3 hours, time that is given to pay US $ 300 in bitcoins, and the second that gives 24 hours and must pay US $ 600 to avoid the loss of information, as can be seen in figure 7.

5. REGULATIONS AND LEGISLATION AGAINST CIBERDELINCUENCE

5.1. BUDAPEST CONVENTION

The members of the Council [28] and the private sector met to create cooperation to combat or control cybercrime, where they highlighted the importance of information manipulation, confidentiality, integrity and the availability of computer systems, networks and data, defined some terms and decreed some measures to defend and prosecute these criminals. As a result of this cooperation we have the following definitions: "A computer system is any device connected in a network or isolated", "a computer data is any information, concept or program stored in a system", "a service provider is an entity private or public that offers service or storage of data for possible communication between users through a system ", legal and criminal measures will be taken for illegal access and interception, interference in data and system, abuse of devices, falsification of information, computer fraud, child pornography, infringement of intellectual property and related rights.

5.2. LAW 1273 PROTECTION OF INFORMATION AND DATA

According to [29] in Colombia, Law 1273 of 2009 is in force, which modifies the penal code and creates a legal right called "Protection of information and data", which is divided into two chapters: One that says textually: "Of the attacks against the confidentiality, the integrity and the availability of the data and the computer systems" and two that says: "Of the computer attacks and other infractions". This law was created to condemn cybercriminals if they are found infringing it, in table 1 you can observe the penalty for these infractions.

Table 1: Law 1273 2009, Source: authors

Of attacks against the confidentiality, integrity and availability of data and computer systems			
		NAME OF ARTICLE	PENA
Article	269th	Abusive access to a computer system	Prison between 48 to 96 months and a fine of 100 to 1000 minimum wages.
	269B	Illegitimate obstruction of computer system or telecommunication network	
	269C	Interception of computer data	Prison between 36 to 72 months.
	269D	Computer damage	Prison between 48 to 96 months and a fine of 100 to 1000 minimum wages
	269E	Use of malicious software	
	269F	Use of malicious software	
	269G	Impersonation of websites to capture personal data	
Of the computer attacks and other infractions			
Article	269I	Theft by computer and similar means	Prison between 48 to 120 months and a fine of 200 to 1500 minimum wages.
	269J	Non-consensual transfer of assets	Prison between 36 to 96 months.

5.3. CONPES

Colombia is a reference in South America thanks to the dedication to combat cybercrime, this policy is embodied in two documents of the National Council of Economic and Social Policy (CONPES). According to [30], the CONPES is made up of state entities, private companies, the community and infrastructure operators, and focuses on cyber threats in the fight against Cybercrime, in the 2016 version, they include the theme of risk management.

6. ORGANISMS AGAINST THE CYBER-LEADERSHIP

6.1. POLICE CYBERNETIC CENTER

It is an incident response group created by the national police according to [31] to meet "the needs of prevention, care and investigation of events and incidents of computer security." It coordinates management mechanisms with the use of standards and good practices in order to protect the technological infrastructure, has strategic alliances with private entities, public and national and international organizations to mitigate the impact caused by attacks generating alerts, announcements and communications that allow prevent associated risks in the use of new information technologies.

6.2. COLCERT

COLCERT [32], is the entity "responsible for the coordination of Cybersecurity and National Cyber Defense, which will be framed within the Missionary Process of Management of Security and Defense of the Ministry of National Defense". The main purpose is the coordination of actions for the protection of critical infrastructure of the State against possible emergencies with cyber attacks, to meet this objective has a series of services to public and private companies in order to prevent computer threats by sensitizing and training with documentation to the civil servants of the same one, executing security policies so that the companies can defend themselves against incidents of Cybersecurity in infrastructure and thus, develop and promote procedures, protocols and guides of good practices and recommendations for the suitable detection in the computer science crimes and In addition, it supports the State and national agencies to prevent and investigate each of the cybercrimes committed.

6.3. COMMAND CIBERNÉTICO (CCOC)

COMANDO CIBERNETICO JOINT [33], is a group created by the Colombian Armed Forces, being a group of experts in engineering from various branches such as: telecommunications, aviation and intelligence, whose objective is to address the issues of cyber defense, ensuring security by means complying with the law, responding to cyber attacks, ensuring the protection of critical infrastructures and defending military computer networks, training public and private entities to create security policies and safeguarding information against potential threats.

7. CONCLUSIONS

Colombia has been a target country of many crimes and malicious people who come from other parts of the world with the interest of harming both businessmen, industrialists and financial entities, for this reason it is important that each sector knows their weaknesses and becomes aware of the importance of taking care, safeguarding and not spreading important information about companies, maintaining up-to-date security policies and being informed of new attack models by cybercriminals.

The statistics presented show how this scourge has increased year after year, which is why the Ministry of Justice, Defense and Information and Communication Technologies (ICT) presented a bill to the Congress of the Republic, to join the Budapest Convention with the primary objective of reducing the rate of cybercrime. It also aims to increase cooperation between the States and the private sector by improving research techniques, under this measure will create a network that will operate 24/7, both in the national and international territory to detect and prosecute cybercriminals.

Colombia, as a country interested in reducing this problem, has formulated security policies, establishing controls on infrastructure, raising awareness among companies on the importance of safeguarding their information systems, implementing good practices techniques and having adequate personnel to manage the systems of information and thus, protect your data. As new information systems, new mobile applications, the future of the internet of things are designed and implemented, cyber criminals also develop new methods to generate their attacks and ask for large amounts of money for the kidnapping of information. which increases the risks before a system that is very vulnerable.

8. REFERENCES

[1] Royal Spanish Academy. (2017). Hacker Retrieved on 01.02.2018, Hacker:
http://dle.rae.es/?id=JxlUKkm

[2] Rondón, M. F. (1 of 04 of 2014). blogs Retrieved on the 24 of 01 of 2018.
http://mariafernandainformaticajep.blogspot.com.co/

[3] Colombia Digital. (01 of 05 of 2013). In Colombia, crimes are investigated computer Retrieved on 08 of 02 of 2018 https://colombiadigital.net/actualidad/articulos-informativos/item/4810-en-colombia-se-investigan-los-delitos-informaticos.html

[4] Kaspersky Lab. (217). Cybercrime and Cybercrimes Retrieved on February 18, 2018, from Cybercrime and Cybercrimes.
https://www.kaspersky.es/resource-center/threats/computer-vandalism

[5] Portfolio. (06 of 04 of 2016). Cybercrime does not segment: we are all vulnerable. Retrieved on January 20, 2018.
http://www.portafolio.co/opinion/otros-columnistas-1/ciberdelincuencia-colombia-perdidas-anuales-155222

[6] Linares, F. M. (2012). Cybercrime: Phenomenology and criminology of crime in cyberspace. Retrieved on 02 02 02 2018
https://www.marcialpons.es/static/pdf/9788415664185.pdf

[7] Digital magazine (18 of 05 of 2016). Retrieved on 02 02, 2018.
https://revistadigital.inesem.es/informatica-y-tics/

[8] Garcia, C. P. (1 of 05 of 2013). In Colombia are computer crimes investigated? Recovered the 2018 of 01 of 24, of In Colombia the computer science crimes are investigated?
https://colombiadigital.net/actualidad/articulos-informativos/item/4810-en-colombia-se-investigan-los-delitos-informaticos .html

[9] Law 1437 of 2011. CONGRESS OF THE REPUBLIC by which the Code of Administrative Procedure and Administrative Litigation is issued. https://www.ramajudicial.gov.co/documents/10228/2045451/LEY+1437+DE+2011+PDF.pdf/7f84163f-0261-4790-b67b-83012cb70a62?version=1.1

[10] Law 1564. In Colombia, computer crimes are investigated.
https://colombiadigital.net/actualidad/articulos-informativos/item/4810-en-colombia-se-investigan-los-delitos-informaticos.html

[11] Díaz, I. M., & Saavedra, M. G. (2013). Cybercrime Recovered on 01 of 02 of 2018, of Cybercrime:
http://www.redipd.org/actividades/seminarios_2008/common/102008/doc_4_2.pdf

[12] Lopez, S. L. (01 of 01 of 2014). Possible subjects of computer crimes. Retrieved on 01 of 02 of 2018.
http://www.informatica-juridica.com/trabajos/posibles-sujetos-de-los-delitos-informaticos/

[13] Legislation and Computer Crimes - The Offender and the Victim. Retrieved on February 14, 2018.
https://www.segu-info.com.ar/delitos/delincuenteyvictima.htm

[14] National Police. (12 of 2017). Balance cybercrime in Colombia 2017. Retrieved on 07.02.2018. https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_2017.pdf

[15] Digital magazine (18 of 05 of 2016). Retrieved on 02 02, 2018. The blue whale, challenge of the fire fairy)
https://www.colombiadigital.net/creador-la-ballena-azul-se-declara-culpable-incitacion-al-suicidio/

[16] National Police. (03 of 2017). Report threats of cybercrime in Colombia 2016 - 2017.
https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

[17] National Police. (01 of 06 of 2015). Identity theft. Retrieved on 02 02, 2018, from Identity theft.
https://caivirtual.policia.gov.co/sites/default/files/bacif_002_9_0.pdf

[18] Avast (2015). Phishing Retrieved 02 of 02 of 2018
https://www.avast.com/es-es/c-phishing

[19] Villacrés, E. J., Molina, M. I., & Miguez, M. B. (09 of 2014). Cybercrime is an evil that affects current society. Retrieved February 02, 2018. http://www.egov.ufsc.br/portal/sites/default/files/ciberdelincuencia_un_mal_que_afecta_a_la_sociedad_actual.pdf

[20] LOZANO, B. G., & CAICEDO, D. P. (21 of 09 of 2017). Technical and legal challenges against cybercrime in the Colombian banking sector. Retrieved on 02 02, 2018. http://repository.unad.edu.co/handle/10596/13387

[21] ENTER.CO MAGAZINE. (31 of 03 of 2017). The new target of cybercriminals in Colombia are companies. Retrieved on February 14, 2018. http://www.enter.co/chips-bits/seguridad/empresas-el-nuevo-blanco-de-los-cibercriminales-en-colombia/

[22] PAUS, L. (06 of 04 of 2015). What is a skimmer and how to protect your credit card? Retrieved on February 14, 2018. https://www.welivesecurity.com/la-es/2015/04/06/que-es-skimmer-como-proteger-tarjeta/

[23] Harnedy, R. (09 of 2016). What is a commercial email compromise attack? Retrieved on February 14, 2018. https://blog.barkly.com/what-is-a-business-email-compromise-bec-attack-and-how-can-i-stop-it

[24] Week. (28 of 12 of 2017). Cybercrime in 2017: the threat grows over Colombia. Retrieved on February 14, 2018, from http://www.semana.com/nacion/articulo/cibercrimen-en-colombia-balance-de-2017/551979

[25] Panda security. (13 of 11 of 2013). What is a Ransomware? Retrieved on February 14, 2018. https://www.pandasecurity.com/spain/mediacenter/malware/que-es-un-ransomware/

[26] The Colombian. (May 16, 2017) Thousands of Wanna Cry cyber attacks have been reported in Colombia. Retrieved on February 14, 2018. http://www.elcolombiano.com/tecnologia/miles-de-ciberataques-wanna-cry-se-han-reportado-en-colombia-CX6541325

[27] El Espectador. (May 17, 2017) This is how Wannacry arrived in Colombia. Retrieved on February 14, 2018. https://www.elespectador.com/noticias/judicial/asi-llego-wannacry-colombia-articulo-694262

[28] Council of Europe. (23 of 11 of 2001). Convention on cybercrime Retrieved on 01 of 02 of 2018. http://www.human-rights-education.com/wp-content/uploads/2017/04/Convenio-sobre-cibercrimen-del-Consejo-Europeo.pdf

[29] CONGRESS OF THE REPUBLIC. (31 of 01 of 2018). LAW 1273 OF 2009. Retrieved on February 16, 2018. https://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

[30] Dialog. (09 of 11 of 2017). Armed Forces of Colombia counteract cybercrime. Retrieved on February 16, 2018. https://dialogo-americas.com/es/articles/colombian-armed-forces-counter-cybercrime

[31] CSIRT. (2017). Computer Security of the National Police. Retrieved on February 18, 2018. https://cc-csirt.policia.gov.co/Publicaciones/quienes_osomos

[32] Cybernetic Emergency Response Group. (12 of 07 of 2017). Retrieved on February 18, 2018. http://www.colcert.gov.co/index.php

[33] Dialogue. (01 of 04 of 2013). Colombia Takes on the Cybernetic Challenge Retrieved on February 18, 2018. https://dialogo-americas.com/es/articles/colombia-asume-el-desafio-cibernetico