



## CYBERCRIME AND THE INSECURITY OF AUTOMATED INFORMATION SYSTEMS DUE TO THE LACK OF DETECTION AND CONTROL OF COMPUTER INCIDENTS

SANTILLÁN MOLINA ALBERTO LEONEL<sup>1</sup>, VINUEZA OCHOA NELLY VALERIA<sup>2</sup>, BENAVIDES SALAZAR CRISTIAN FERNANDO<sup>3</sup>, SANTILLÁN OJEDA SALVATORE JOEL<sup>4</sup>

Universidad Regional Autónoma de Los Andes Santo Domingo. Ecuador.

<sup>1</sup>E-mail: us.albertosantillan@uniandes.edu.ec

ORCID: <https://orcid.org/0000-0001-8517-8980>

<sup>2</sup>E-mail: ub.nellyvinueza@uniandes.edu.ec

ORCID: <https://orcid.org/0000-0002-1348-5620>

<sup>3</sup>E-mail: us.cristianbenavides@uniandes.edu.ec

ORCID: <https://orcid.org/0000-0002-4326-2137>

<sup>4</sup>E-mail: ds.salvatorejso23@uniandes.edu.ec

ORCID: <https://orcid.org/0000-0003-4621-2132>

### ABSTRACT

*In 2019, Ecuador was the victim of a computer attack in which the personal data of the vast majority of Ecuadorian citizens were obtained. In the year 2021, the public company Corporación Nacional de Telecomunicaciones CNT, was the victim of a cyberattack using a computer virus called ransomware, hijacking the information of this company, denoting that the problem lay in the lack of public policies and technological infrastructure that allow a government that reduces the vulnerability of automated information systems in Ecuador. In this virtue, it was proposed as a research objective, to establish how the lack of detection and control of computer incidents influences the insecurity of automated information systems that allow the commission of cybercrimes. Within the qualitative research, the following methods were used: Historical-logical and analytical-synthetic, which was applied to the different definitions determined to frame the use of Information and Communication Technologies in cybercrime, as well as the state obligation to a government. secure email. Concluding that since cybersecurity is a set of tools that safeguards information through the use of guidelines, methods and practices to protect information, it is of paramount importance to design a strategic plan for the formation of an entity for the detection and control of computer incidents, to so that the violation of automated information systems can be significantly reduced.*

**KEYWORDS:** *Electronic government, cybersecurity, public policy, cybercrime*

### INTRODUCTION

Information and Communication Technologies use "devices that allow editing, producing, exchanging, storing and transmitting computer data, between different information systems", thus allowing the "intersubjective relationship" between people, thus developing globally an accelerated social, cultural, political, economic and financial growth, since it has provided greater operational ease through the use of these computer terminals, making everyday life much easier, with the journey of information and online commerce, thus benefiting all people in the information society and creating a "digital divide", much wider, given the technological difference and access to it. (Desongles Corrales, 2006, pág. 14) (Aboso, 2017, pág. 47) (Programa de las Naciones Unidas para el Desarrollo, 2002, pág. 47)

This ease with which digital operations are carried out, gave access to a new way of executing illicit activities with the violation of the security measures of automated information systems, consummating illicit behaviors that blur, with the entry of computer science, the interest of a quiet life in society.

The information society is a conglomerate that brings together different people, institutions, companies whose purpose is "the capture, storage and computer transmission of information produced in the social, cultural, economic and financial fields, which uses ICT to "create and disseminate these data through digital technologies". (Hilbert, 2009, pág. 27) (CEPAL, 2013, pág. 27)



This digital modernity allows the entry on the scene of ICT through the use of "digital platforms for the exchange of ideas and content, such as social networks", in web 2.0, which accelerates social, technological, industrial, financial and economic growth, which makes it attractive to citizens to be part of this community, and thus alleviate their hustle and bustle through this digital society, since "technology advances in the same way as society". (Cobo Romani, 2009, pág. 51)(Morgan, 1877, pág. 26)

This process that develops dynamically "in its social and economic globalization through the Internet that is interconnected by computers, telephones, interactive television, require computer security alternatives in response to the different forms of virtual crime." (Bremmer, 2010, págs. 86-91)

The most representative computer crime given the technological form of its commitment is the hacking behavior, which is understood as the "violation of the security measures that are imposed on automated information systems, and access to it to execute espionage or computer sabotage". (Santillán Molina, 2015, pág. 67)

These security measures imposed to allow access to a system are: "voice pattern recognition, eye iris reader, facial biometric recognition, fingerprint, and username and password", and when these are violated, we are facing the crime of hacking. (Suarez, 2016, pág. 344)

Computer science as such is defined as the "science that studies techniques, processes and methods that aim to store, process and transmit information in digital format, while crime is defined as "the action typically unlawful and guilty, and imputable to the one who committed the act and therefore subject to a penalty". (Desongles Corrales, 2006, pág. 14)(Carranca y Trujillo & y Carranca y Rivas, 1991, pág. 223)

So it can be evidenced that effectively in this fourth industrial revolution, cybercrime is that typical, unlawful and culpable act, in which computer means are used for its commission and thus make itself worthy of a penalty.

"The purpose of Criminal Law is the subsidiary protection of legal assets", through the typification of conduct contrary to law, maintaining clearly the importance of the legal good, because it is "an abstract value of legally protected social order, in whose defense the community is interested, whose ownership may correspond to an individual or to the collectivity". (Roxin, 2013, pág. 323) (Jescheck, 2002, pág. 275)

In 2019, Ecuador was the victim of an attack on information processing systems, in which the personal data of Ecuadorian citizens were obtained, which is why the former President of the Republic Lic. Lenin Moreno Garcés issued a memorandum on September 0184, 2019, delivering to the Legislative Function a Draft Organic Law on Protection of Personal Data, that had as its purpose the protection of these, but that did not delve into issues of cyber security or programming, and that in general guarantees their security.

In 2021, the public company Corporación Nacional de Telecomunicaciones CNT was the victim of a cyberattack through the intrusion of a computer virus called ransomware, which is nothing more than the kidnapping of information that is stored in software.

The Ecuadorian State should establish an entity that is dedicated to the detection and control of the violation of automated information systems, both in public and private entities, and in this way can maintain an electronic government according to the information society of the 21st century, in order to protect those legal assets related to information technology such as: property, sexual integrity, intimacy, privacy and thus ensure the security of systems.

Therefore, it can be established that the research problem lies in the lack of public policies and technological infrastructure that allows an electronic government that reduces the vulnerability of automated information systems in Ecuador.

Therefore, the objective of this research is to establish how the lack of detection and control of computer incidents, influence the insecurity of automated information systems that allow the commission of cybercrimes.

#### METHODOLOGY

The research was qualitative in which the following methods were used:



1. Historical-logical method to identify the main lines of how Information and Communication Technologies are established, as well as the information society and computer crimes.
2. The Analytical-synthetic will be applied to the different definitions determined to frame the use of Information and Communication Technologies in cybercrime, as well as the state obligation to a secure electronic government.
3. As a scientific research technique, content analysis applied to different documentary sources related to information and communication technologies, information society, computer security, and secure electronic government will be used.

## RESULTS

Ecuador, through article 66.19 of the Constitution, guarantees individuals the right to the protection of their personal data, as well as the decision on the treatment of information, its collection, archiving and processing.

The Organic Law on Transparency and Access to Public Information published in Official Gazette 337 of March 18, 2004, in its fundamental part, provides that this legal system guarantees the fundamental right of individuals to information in accordance with the guarantees enshrined in the Constitution of the Republic of Ecuador, International Covenant on Civil and Political Rights, Inter-American Convention on Human Rights and other international instruments in force in Ecuador.

The Comprehensive Organic Criminal Code, which entered into force on August 10, 2014, typifies new behaviors related to computer crimes such as: a) the crime of disclosure of information and violation of privacy and privacy; (b) unlawful interception; (c) computer deception; (d) illegal marketing; (e) assistance and participation in computer crime; (f) illegal profits and electronic transfers; (g) destruction of classified information; (h) hacking and unauthorized access; (i) computer-based property crime; (j) illegal marketing; (k) misuse of mobile terminal equipment; and sexual offences involving automated information systems.

The United Nations Office on Drugs and Crime in 2013, established the points that determined the increase in cybercrime as well as the risks and threats that were in the cyber world, thus detailing the following findings:

1. The existence of diversity of national laws; 2. Reliance on traditional means of international cooperation to address cybercrime; 3. The location of digital evidence has to be dealt with in the legislatures due to the impossibility of obtaining it; 4. Lack of organization regarding the investigation and obtaining of electronic evidence; 5. Lack of resources for the investigation of cybercrimes in developing countries; 6. Strengthening cybercrime prevention in all countries. (Ministerio del Interior de la República del Ecuador , 2020, pág. 38)

Ecuador developed the National Plan for Citizen Security and Peaceful Social Coexistence 2019-2030, in which it proposed specific objectives to confront organized crime and cybercrime, so within the seventh objective it provides: "Implement strategic anticipation in public actions, to face risks and threats fundamentally related to organized crime, money laundering, transnational crime, terrorism and cybercrime"; Objective No. 6 also mandates "strengthening the information system with the standardization and quality of data and statistics responsible for security and justice." (Ministerio del Interior de la República del Ecuador , 2020, pág. 39)(Ministerio del Interior de la República del Ecuador , 2020, pág. 39)

## DISCUSSION

Information and Communication Technologies are a set of technical resources and instruments that allow the interconnection between computer devices that aim to "edit, produce, store, exchange and transmit data between different information systems, which allow communication and personal interaction as a tool for exchange and dissemination as well as the management of access to knowledge". (Cobo Romani, 2009, pág. 312)

ICTs in this 21st century have allowed the development of societies in a much more accelerated way, their growth has been beneficial for each of the people in their intersubjective relationships, which have allowed to have more ease for the management of their daily activities, so we have the use of



the internet, the satellite phone, The cell phone with which communication is in real time from one point to another.

The constant management of this technology has allowed the formation of the "information society" as a system of exchange of data of a social, political, and cultural nature, which includes automated information systems as an interactive entity that allows the compartment of information by the cybernetic triad, this is by computer means, Telematics and telecommunications. (Cumbre Mundial Sobre la Sociedad de la Información, 2005)

The development of societies with the use of ICT as well as the automation of public or private operations, have allowed a growing illicit activity to obtain an economic or material benefit, once the extraction or improper handling of computer data as such is effected, which requires the application of cybersecurity measures to safeguard computer data as well as the information of users and their environment.

Cybersecurity is the set of "tools that aim to safeguard information through the implementation of guidelines, risk management methods as well as practices to protect information in the cyber environment and the properties of computer security". (Caro, 2011, pág. 61)

The advances in information and communication technologies that are taking place day by day, have demanded that hackers explore new techniques with the use of more effective tools when executing acts that violate the security of systems, so we have the use of the Botnets virus that is nothing more than "a network of computers interconnected and infected by malware programs" that aim to launch attacks of Denial of service so that the system is saturated and security measures are disabled and that would allow access to the system. (European Union Agency for Cybersecurity, 2019, pág. 2)

Therefore, it is necessary to apply a public policy that analyzes the social and cyber reality in both public and private institutions that use information and communication technologies, in order to establish a secure electronic government that guarantees the protection of cyberspace, as well as establish strategies and objectives that guarantee the cybersecurity of their critical infrastructures and that they can detect in an accurate way, attacks on automated information systems.

## CONCLUSIONS


One of the solutions to the present research problem would be to design a strategic plan for the formation of an entity for the detection and control of computer incidents, so that the violation of automated information systems can be significantly reduced, and that covers not only public but also private entities, with the aim of protecting those legal assets that are related to computing.

The lack of a technological infrastructure that reduces the vulnerabilities of the systems is of paramount importance, since it has been possible to demonstrate how computer incidents in the Republic of Ecuador violate automated information systems in public and private institutions and companies, and thus avoid the commission of computer crimes.

Under this statement it can be established from the practical field, that the constitution of a government entity that detects and controls computer incidents that allow for the intrusion of automated information systems, through the violation of computer and information security measures, would guarantee the reduction of hacks, ransomware, espionage and computer sabotage, and therefore will make Ecuador a country with a more secure electronic government.

## BIBLIOGRAPHIC REFERENCE

- [1] Aboso, G. (2017). *Cyber Criminal Law. Cybercrime and criminal law in the modern information society and communication technology*. Buenos Aires: Editorial BdeF. Ltda.,.
- [2] Bremmer, I. (November-december de 2010). *What information technology can and Cannot Do, Foreign Affairs. Democracy in Cyberspace.*, 89(6), 86-91.
- [3] Caro, M. J. (2011). *Scope and scope of National Security in Cyberspace*. *Revista Cuadernos de Estrategia*, 49-82. Retrieved from <https://dialnet.unirioja.es/servlet/revista?codigo=7646>
- [4] Carranca & Trujillo, R., & Carranca & Rivas, R. (1991). *Mexican Criminal Law*. Mexico: Temis.
- [5] ECLAC. (2013). *Pathways to an Information Society in Latin America and the Caribbean. Economic Commission for Latin America and the Caribbean.*, 27.

- 
- [6] Cobo Romani, J. (2009). *The concept of information technologies. Benchmarking on the definitions of ICT in the knowledge society.* Zer Magazine, 312.
- [7] World Summit on the Information Society. (2005). *World Summit on the Information Society.* Geneva: World Summit Geneva 2003-Tunis 2005,. Retrieved from [http://www.itu.int/net/wsis/documents/doc\\_multi.asp?lang=es&id=1161|0](http://www.itu.int/net/wsis/documents/doc_multi.asp?lang=es&id=1161|0)
- [8] Desongles Corrales, J. y. (2006). *Basic Computer Skills.* Seville : Editorial MAD, .
- [9] European Union Agency for Cybersecurity, (. (January 20, 2019). *European Agency for Cyber Security.* Obtained from ENISA: <https://www.enisa.europa.eu/events/botnets>
- [10] Hilbert, M. (2009). *The information society in Latin America and the Caribbean. Development of technologies and technologies for development.* Santiago, Chile: Ediciones ECLAC, Economic Commission for Latin America and the Caribbean.
- [11] Jescheck, H.-H. y. (2002). *Treatise on Criminal Law, General Part,.* Granada: Editorial Comares S.L.,.
- [12] Ministry of the Interior of the Republic of Ecuador . (April 02, 2020). *National Plan for Citizen Security.* Obtained from the National Citizen Security Plan: [https://www.ministeriodegobierno.gob.ec/wp-content/uploads/2019/08/PLAN-NACIONAL-DE-SEGURIDAD-CIUDADANA-Y-CONVIVENCIA-SOCIAL-PACI%CC%81FICA-2019-2030-1\\_compressed.pdf](https://www.ministeriodegobierno.gob.ec/wp-content/uploads/2019/08/PLAN-NACIONAL-DE-SEGURIDAD-CIUDADANA-Y-CONVIVENCIA-SOCIAL-PACI%CC%81FICA-2019-2030-1_compressed.pdf)
- [13] Morgan, L. H. (1877). *Ancient Society.* New York: H. Holt and company. .
- [14] National Cyber Security Centre. (25 de enero de 2018). *The Cyber threat to UK business, London 2018.* Obtenido de National Crimen Agency: <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/178-the-cyber-threat-to-uk-business-2017-18/file>
- [15] United Nations Development Programme. (2002). *Report on Human Rights in Venezuela 2002. Information and Communication Technologies at the service of development.* Caracas: UNDP.
- [16] Roxin, C. (2013). *Criminal law. General part. Fundamentals. The Structure of Crime Theory.* Madrid: Thomsom-Civitas.
- [17] Santillán Molina, A. (2015). *Computer Law, a civil, criminal and commercial approach.* Quito: Editorial Jurídica del Ecuador.
- [18] Suarez, A. (2016). *Manual of computer crime in Colombia. Dogmatic analysis of Law 1273 of 2009,.* Bogotá: Universidad Externado de Colombia,.