Analysis of the Technical and Corporate Strategies Implemented to Combat Punishable Conducts That Have Affected the Cybersecurity of Personal Data in Financial and Telecommunications Organizations in Colombia During 2020

Wilson Pinzón Soler, Carlos Alberto Hurtado Martínez, Johemir Jesús Pérez Pertuz and Néstor Raúl Quiroz Cespedes

May 24, 2024

International Conference on Project Management 2024

Analysis of the technical and corporate strategies implemented to combat punishable conducts that have affected the cybersecurity of personal data in financial and telecommunications organizations in Colombia during 2020

Wilson Pinzón Soler

Carlos Alberto Hurtado Martínez

Johemir Jesús Pérez Pertuz

Néstor Raúl Quiroz Cespedes

Abstract:

Information security seeks to reduce, minimize and mitigate risks to an acceptable level of operation. This consists of avoiding latent threats or computer breaches that allow the commission of criminal conduct, and takes into account the complex surveillance necessary to provide users with an optimal level pf security with the aim of avoiding in its minimum cybercrime events and alien incursions that are every day risks in internet networks. In this era we cannot downplay that information is the most valuable asset for organizations and individuals, considered the oil of the future; information data is found in various forms: physical, digital, analog, verbal, written and transcribed: therefore, all kinds of thoughts or ideas have great value. Considering the value of the resources, the necessary security measures must be implemented to safeguard data and keep it secure in form and application.

Keywords: cybersecurity, cybercrime, information technology, information technologies

Analysis of the technical and corporate strategies implemented to combat punishable conduct that has affected the cybersecurity of personal data in financial and telecommunications organizations in Colombia during 2020

Resumen:

La seguridad de la información busca reducir, minimizar y mitigar en gran medida los riesgos hasta su mínima expresión hasta el punto de lograr un nivel aceptable donde no existan amenazas latentes o brechas informáticas que permitan la comisión de una conducta delictiva, teniendo en cuenta que es complejo conseguir una inmediata solución que proporciona a los usuarios un nivel óptimo con el objetivo de evitar en su mínima expresión los eventos y peligros que se presentan cada día en las redes e Internet. En esta era de la información no podemos olvidar que la información es sin duda el activo más valioso para las organizaciones y personas que podría ser considerado como el petróleo del futuro, y este dato se encuentra de diversas formas como: Física, digital, analógica, verbal, escrito y, por tanto, todo tipo de pensamientos o ideas son información y, como tales, tienen un gran valor. De esta forma, y considerando el valor de los datos, se deben implementar las medidas de seguridad necesarias con el objetivo de resguardar los datos y mantenerlos acorde a su importancia y aplicación.

Palabras clave: ciberseguridad, delito informático, tecnologías de la información

Introduction

We are currently immersed in an information age where data is a valuable asset, petroleum of the digital age, and as a result criminals are active at data mining, a persistent theft of data and metadata. With the leakage of information and the incorrect processing of personal data, crimes such as extortion, theft of monetary values, impersonations, irregular purchases, scams etc., are committed, a result of the misuse and mismanagement by the different entities, institutions and / or companies that collect such information. Vulnerability of systems is conducive to any cybercriminal who perpetuates a fraud or computer crimes, since not rigorously regulated. Also, citizens often provide personal data on web portals and applications, with total confidence in security, but without having any real proof that this data is not a gateway to crime, putting financial, personal and family safety at risk.

“To provide a context from global to the local and having as a frame of reference raised by the Colombian Chamber of Informatics and Telecommunications, in recent years cyber-attacks in the world have left losses close to 12 billion dollars, through the BEC modality or compromise of business accounts according to the FBI.” (Camara Colombiana de Informática y Telecomunicaciones, 2019).

The increase in cybercrime and victimization in cyberspace is a permanent concern since it is directly proportional to the habitual use and manipulation of Information and Communication Technologies (ICTs). This victimization can have different areas of impact, but beyond the diversity of scenarios of impact on cyber users, there is a common point that is in the use of the victim's personal data by cybercriminals.

From criminal deception through social networks to a cyber-attack with highly sophisticated malicious software, there is an impact on identification or access data. Thus, personal data is recognized as the most valuable asset in today's organizations and its protection is of vital importance for any Internet user.

In the national framework of Colombia, the Attorney General's Office assures that the number of losses is between 120 million to 5 billion pesos, depending on the size of the affected company. (Camara Colombiana de Informática y Telecomunicaciones, 2019).

“These figures were consolidated in the study of cybercrime trends in Colombia, led by the Security Applied to Business Strengthening (SAFE) program of the ICT Analysis and Creativity Tank (TicTac), which together with the Colombian Chamber of Informatics and Telecommunications (CCIT) and the Colombian Center for Cybersecurity Capabilities (C4) of the National Police seeks to “show the impact of the cybercrime phenomenon and raise awareness among companies to promote greater digital confidence to mitigate the risks of loss of information or money. “According to Alberto Samuel Yohai, president of the CCIT. Currently, 45.5% of complaints are made through virtual channels and in the course of 2019, 28,827 business cybersecurity incidents have been reported in the country, of which 17,531 cases have been reported to the Prosecutor's Office. (Camara Colombiana de Informática y Telecomunicaciones, 2019).

“From 2017 to date, 52,901 complaints were reported, of which the largest number of thefts are carried out by computer means (31,058), followed by identity theft (8,037); Bogota was the city that reported the most incidents (5,308), then Cali (1,190) and Medellin (1,186). Faced with this situation, Lieutenant Colonel Alex Durán, head of the Police Cyber Center, assured that “there has been an operational increase of 27.5% compared to 2018, materializing 241 arrests and 11 impact operations for different types of computer crimes contemplated in Law 1273 of 2009, as well as through the 24/7 Virtual CAI service, 12,959 incidents have been attended, increasing the service capacity by 53.7% compared to 2018”. (Camara Colombiana de Informática y Telecomunicaciones, 2019).

“In the country, malware attacks during the year grew by 612%, the amount paid for information ransom is between 32 million and 160 million pesos. Given this scenario, Colombia is among the countries that received the highest number of ransomware attacks in Latin America with a total of 252, which corresponds to 30% after Brazil and Argentina.” (Camara Colombiana de Informática y Telecomunicaciones, 2019).

Cyber Police Center.

Cyber Police Center is also responsible for responding to citizens through the “CAI Virtual” platform. Through this medium, the Colombian National Police received a total of 41,649 complaints. During the year, 190 arrests were made for cybercrimes, 42 of them for child pornography (Centro Cibernetico Policía Nacional Colombia, 2019).

“Unfortunately, we as citizens, when we moved from a physical to a digital environment, because of Covid, so abruptly, it did not allow us to have the necessary preparation in cybersecurity to be on the defensive in these types of cases. Not only in antivirus, but also in good computer security practices,”concluded Major Rodriguez. (Centro Cibernetico Policía Nacional Colombia, 2019).

“According to statistics from the Cybersecurity Center, during 2020, 6,541 web pages containing child sexual abuse material were blocked. Through the Virtual CAI, 13,339 complaints were handled. In addition, the computer forensic laboratory was able to analyze 720 malware samples, which are programs designed to damage your computer. A total of 389 phishing pages were suspended.” (Centro Cibernetico Policía Nacional Colombia, 2019).

Methodology

This descriptive research article uses the following analysis methodologies:

Literature review: This methodology involves collecting and analyzing relevant and up-to-date information on the topic of cybersecurity from academic sources, books, journal articles, technical reports, and other reliable sources. You can use this information to describe trends, best practices, emerging technologies, current threats, among other aspects.

Case studies: We perform a detailed analysis of actual cases of cybersecurity incidents, examining how they occurred, what vulnerabilities were exploited, the consequences, and lessons learned. This approach can provide a practical and applied view of the subject.

Surveys and interviews: We get direct feedback from cybersecurity experts or industry professionals and conduct surveys from structured interviews. This allows the gathering of opinions, experiences, and perceptions on various aspects of cybersecurity, which enriches the article with practical and current points of view.

Trend analysis: A trend analysis can be conducted in the field of cybersecurity, using data and statistics gathered from reliable sources such as reports from security companies, government agencies and international organizations. This approach allows identification and description of current and emerging trends in cybersecurity threats, technologies, and practices.

Comparative study: We may compare different cybersecurity approaches, technologies, or strategies to identify their strengths, weaknesses, and areas of application. This approach can help readers understand the different options available and make informed decisions on how to improve the security of their systems and data.

Results

The growing use of the digital environment in Colombia to develop economic and social activities generates uncertainties and risks inherent to digital security that must be managed on an ongoing basis. Failure to do so may result in the materialization of threats or cyber-attacks, generating undesired economic or social effects for the country, and affecting the integrity of citizens in this environment, (Ministry of Information and Communication Technologies, 2016).

The approach of the cybersecurity and cyber defense policy, so far, has focused on counteracting the increase of cyber threats under the objectives of (I) defense of the country; and (II) fight against cybercrime. Although this policy has positioned Colombia as one of the leaders in this area at the regional level, it has neglected risk management in the digital environment. This approach is essential in a context in which the increased use of ICTs for the development of economic and social activities has brought with it new and more sophisticated ways of affecting the normal development of these activities in the digital environment. A fact that demands greater planning, prevention, and attention from the countries. (Ministry of Information and Communication Technologies, 2016).

According to the Faculty of Political Science and International Relations of the Pontificia Universidad Javeriana, to talk about digital security is to understand the Internet as a real scenario (like the home or the street), where actual situations are experienced. Care must be taken to avoid risk situations, such as, for example, the loss of work information when the computer is damaged or lost, the access of other people to accounts in social networks or bank transactions that are recorded on the cell phone, among others. (Universidad Pontificia Javeriana, 2019) In addition to these physical risks, we find the risks in the security of our personal data information in the different systems or databases, where they are registered to acquire a service.

According to what is proposed by the Pilot University of Colombia, it can be indicated that there are several definitions of cybersecurity. In a Secure conference meeting, where security professionals from ISACA (Information Systems Audit and Control Association) participate, gives a definition of cybersecurity: "Protection of information assets, through the treatment of threats that put the information that is processed, stored and transported by information systems that are interconnected." (Universidad Piloto de Colombia - Valoyes Mosquera Amancio, 2019)

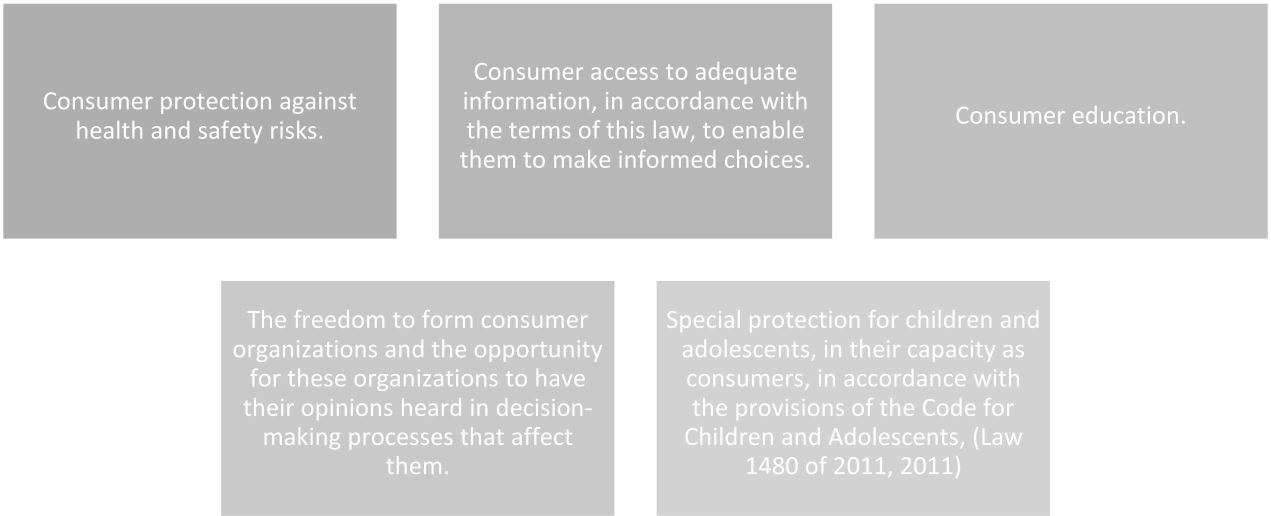
ISO 27001 defines the information asset as the knowledge that an organization has a value, while the information systems are the applications, services, information technology assets or other components that allow its management. (Technical Standard NTC-ISO/IEC Colombiana 27001, 2006)

As a legal framework, we can state that the laws governing the protection of personal data in Colombia (also with international reference) results in the fundamental support to protect the security of personal data. Consider the document "CONPES 3701 DE 2011 - Guidelines for Cybersecurity" and Cyberese's, which aims to seek and generate policy guidelines on cybersecurity and cyberese's aimed at developing a national strategy to counteract the increase in computer threats that affect the country. (Virtual, 2018)

It is also important to highlight the law governing the protection of personal data, which is of vital importance in the development of the legal framework through which legal certainty is provided and a new protected legal asset is created - called "of the protection of information and data," and systems using information and communication technologies are fully preserved, among other provisions. (Virtual, 2018)

Law 1480 of 2011 - Consumer Protection by Electronic Means has a great impact on the Colombian legal framework. The law establishes security in electronic transactions, and guarantees the effectiveness and free exercise of consumer rights, as well as protects respect for the individual’s dignity and economic interests, especially about:

Figure 1. - *Consumer Protection by Electronic*



Consumer protection against health and safety risks.

Consumer access to adequate information, in accordance with the terms of this law, to enable them to make informed choices.

Consumer education.

The freedom to form consumer organizations and the opportunity for these organizations to have their opinions heard in decision-making processes that affect them.

Special protection for children and adolescents, in their capacity as consumers, in accordance with the provisions of the Code for Children and Adolescents, (Law 1480 of 2011, 2011)

Organic Law 1581 of 2012 develops the constitutional right of all persons to know, update and rectify the information that has been collected about them in databases or files, and the other rights, freedoms and constitutional guarantees referred to in Article 15 of the Political Constitution; as well as the right to information enshrined in Article 20 of the same law.

Area of application: The principles and provisions contained in this law shall apply to personal data recorded in any database that makes them susceptible to processing by public or private entities, (Law 1581 of 2012, 2012).

Decree number 1317 of June 27, 2013 (Colombia, 2013) The purpose of this Decree is to partially regulate Law 1581 of 2012, by which general provisions for the protection of personal data are issued, considering the following:

Definitions. In addition to the definitions set forth in Article 3 of Law 1581 of 2012, for the purposes of this Decree the following shall be understood as:

Analysis of current regulations in Colombia	
1. Privacy notice: Verbal or written communication generated by the responsible party, addressed to the Data Subject for the processing of personal data, through which he/she is informed of the existence of the information processing policies that will be applicable, the form of access to the same and the purposes of the processing that is intended to be given to personal data (Law 1581 of 2012, 2012).	2. Sensitive data: Sensitive data are those that affect the privacy of the Data Subject or whose improper use may generate discrimination, such as those that reveal racial or ethnic origin, political orientation, religious or philosophical convictions, union membership, social, human rights, organizations or organizations that promote the interests of any political party or that guarantee the rights and guarantees of opposition political parties, as well as data related to health, sex life and biometric data. (Law 1581 of 2012, 2012).
3. Public data: Data that is not semi-private, private, or sensitive. Public data, among others, are data related to the marital status of individuals, their profession or trade, and their status as a merchant or public servant. By their nature, public data may be contained, among others, in public records, public documents, official bulletins and gazettes and duly enforceable court decisions that are not subject to reserve. (Law 1581 of 2012, 2012).	4. Transfer: The transfer of data occurs when the Data Processor and / or Data Processor, located in Colombia, sends the information or personal data to a recipient, who in turn is the data controller and is inside or outside the country. (Law 1581 of 2012, 2012).
5. Transmission: Processing of personal data that involves the communication of such data within or outside the territory of the Republic of Colombia when it is intended to be processed by the processor on behalf of the controller (Law 1581 of 2012, 2012).	6. Collection of personal data. In development of the principles of purpose and freedom, the collection of data must be limited to those personal data that are relevant and appropriate for the purpose for which they are collected or required in accordance with current regulations. Except in the cases expressly provided for in the Law, personal data may not be collected without the authorization of the Data Subject (Law 1581 of 2012, 2012).

Note: The table shows the researcher's analysis of the Colombian regulations on data protection. Source. Own elaboration, 2024.

The analysis of technical and corporate strategies implemented to combat punishable behaviors that have affected personal data cybersecurity reveals that a multi-faceted approach is crucial in mitigating cyber threats. The implementation of robust technical strategies such as encryption, access controls, and incident response plans is essential in preventing data breaches. Additionally, corporate strategies such as employee training, risk assessments, and compliance with regulatory frameworks are vital in fostering a culture of cybersecurity awareness and accountability.

The findings of this analysis highlight the importance of a proactive and adaptive approach to cybersecurity, one that leverages cutting-edge technologies, robust policies, and employee engagement to stay ahead of evolving cyber threats. By adopting a comprehensive and integrated approach, organizations can effectively combat punishable behaviors, protect personal data, and maintain the trust of their customers and stakeholders.

Ultimately, the success of cybersecurity strategies hinges on the ability of organizations to stay vigilant, adapt to emerging threats, and prioritize the protection of personal data as a core aspect of their operations. By doing so, organizations can ensure the confidentiality, integrity, and availability of personal data, thereby fostering trust, credibility, and long-term success in an increasingly digital and interconnected world.

Conclusions

In 2020, Colombia, like many other countries, faced significant cybersecurity challenges, particularly within financial and telecommunications organizations. This is an analysis of the technical and corporate strategies implemented to combat punishable conduct affecting the cybersecurity of personal data in these sectors.

Financial and telecommunications organizations in Colombia are subject to regulatory frameworks aimed at protecting personal data and ensuring cybersecurity. These regulations, such as Colombia's Data Protection Law and guidelines from regulatory bodies such as the Superintendencies Financier de Colombia (SFC) and the Commission de Regulation de Comunicaciones (CRC), set standards for data security practices and require reporting of security breaches. Compliance with these standards is a pillar of the strategies implemented.

This includes implementing robust security measures, increasing awareness and training programs for employees, collaborating with law enforcement agencies, and continuously updating cybersecurity protocols to stay ahead of evolving threats. By taking these proactive steps, organizations can better protect personal data and mitigate the risks associated with cybercrime in the future. It is imperative for organizations to prioritize cybersecurity and work together to safeguard sensitive information from malicious actors.

After analyzing the technical and corporate strategies implemented to combat criminal behaviors affecting the cybersecurity of personal data in financial and telecommunications organizations in Colombia during 2020, it is evident that a multi-faceted approach is necessary. By combining advanced technical measures with strong corporate policies and procedures, organizations can better protect sensitive information from cyber threats. It is crucial for these organizations to continuously update and adapt their strategies to stay ahead of evolving threats in the digital landscape. Ultimately, a comprehensive and proactive approach is essential to safeguarding personal data and maintaining trust with customers in the financial and telecommunications sectors in Colombia.

References

[1] Camara Colombiana de Informática y Telecomunicaciones. (1 de octubre de 2019). *Tendencias del cibercrimen en colombia 2019 -2010*. (T. Tac, Editor) Obtenido de Camara Colombiana de Informática y Telecomunicaciones: https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

[2] Centro Cibernetico Policía Nacional Colombia. (20 de octubre de 2019). *Tendencias Cibercrimen Colombia 2019 - 2020*. Obtenido de https://caivirtual.policia.gov.co: https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

[3] Colombia, C. d. (27 de junio de 2013). *Disposiciones Generales para la protección de datos personales*. Obtenido de Congreso de la República: http://www.lasallecucuta.edu.co/infopdf/decreto1377.pdf

[4] Consejo Nacional de Política Económica y Social República de Colombia. (14 de julio de 2011). *Documento CONPES 3701*. Obtenido de https://colaboracion.dnp.gov.co/: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

[5] Eset Miguel Angel Mendoza. (16 de 06 de 2015). *Ciberseguridad Seguridad de la Información We live Security*. Obtenido de https://www.welivesecurity.com/laes/2015/06/16/ciberseguridad-seguridad-informaciondiferencia/.

[6] Ley 1480 de 2011. (12 de Octubre de 2011). *Por medio de la cual se expide el estatuto del consumidor y se dictan otras disposiciones*. Obtenido de https://www.sic.gov.co/: https://www.sic.gov.co/sites/default/files/normatividad/042017/Ley_1480_Estatuto_Consumidor_2.pdf

[7] Ley 1581 de 2012. (17 de octubre de 2012). *LEY ESTATUTARIA 1581 DE 2012.* Obtenido de Título I Objeto, Ámbito de aplicación y definiciones: https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf

[8] Mendoza, M. (16 de junio de 2015). *¿Ciberseguridad o seguridad de la información? Aclarando la diferencia*. Obtenido de https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/

[9] Ministerio de Tecnologías de la Información y las Comunicaciones. (11 de abril de 2016). *https://colaboracion.dnp.gov.co/.* Obtenido de Política Nacional de Seguridad Digital: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

[10] Ministerio de Tecnologías de la Información y las Comunicaciones. (1 de Mayo de 2019). *Guía para el uso y aprovechamiento de Datos Abiertos en Colombia*. Obtenido de https://herramientas.datos.gov.co: https://herramientas.datos.gov.co/sites/default/files/Guia%20de%20Datos%20Abiertos%20de%20Colombia.pdf

[11] Norma Técnica NTC-ISO/IEC Colombiana 27001. (2006). *Tecnología de la Información Técnicas De Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.* Obtenido de International organization for standardization. Information Technology. Security Techniques. Information Security Management Systems. Requirements. Geneva, ISO.: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

[12] Universidad Piloto de Colombia - Valoyes Mosquera Amancio. (26 de junio de 2019). *CIBERSEGURIDAD EN COLOMBIA*. (U. P. Colombia, Editor, & V. M. Amancio, Productor) Obtenido de http://repository.unipiloto.edu.co/: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6370/CIBERSEGURIDAD%20EN%20COLOMBIA.pdf?sequence=1&isAllowed=y

[13] Universidad Pontificia Javeriana. (1 de junio de 2019). *COLOMBIA: ¿ES UN ESTADO EFECTIVO EN TÉRMINOS DE SEGURIDAD DIGITAL CON ÉNFASIS EN EL SECTOR PRIVADO?* (2016, Editor, Colnodo, Productor, & Universidad Pontificia Javeriana Bogotá D.C.) Obtenido de Facultad de Ciencias Políticas y Relaciones Internacionales: https://repository.javeriana.edu.co/bitstream/handle/10554/46540/TRABAJO%20DE%20GRADO.pdf?sequence=1&isAllowed=y

[14] Virtual, C. (Productor), & YouTube, C. V.-C. (Dirección). (2018). *Violación de datos personales en Colombia* [Película]. Obtenido de https://www.youtube.com/watch?v=5lrh2llhHbg: http://censavirtual.edu.co/