Computer security audit following OSSTMMv3 methodology: study case.

Cristian L. Bracho, Fabian G. Cuzme
{clbrachoo, fgcuzme}@utn.edu.ec
Técnica del Norte University

***Abstract*— This article tries to explain the application process of an informatics security audit, taking as reference OSSTMM version 3 methodology recommendations in which are 5 fundamental channels. The article describes a practical environment case whit the finality of understand OSSTMM methodology applicability, taken as study case Decentralized Autonomous Government from Mira City. The methodology allows to measure the actual security of five different channels: human, physical, wireless communications, telecommunications and data networks; three important measures are considered for calculation of each channel: porosity (OpSec), controls and limitations too; in addition, the final results after to do an analysis allow to determine the numerical values of each of these items, for it is necessary to avail of methodology recommendations for types of tests to calculate them. The results obtained after to apply the methodology allow to understand deficiencies or excesses of security operational controls that exist in a company or organization in each channel, being an important point to control the vulnerabilities internally detected and to be able to solve them properly.**

Keywords: audit, channels, controls, limitations, OSSTMM, porosity, security.

I. INTRODUCTION

Justice administration in society has been profoundly transformed with the emergence of new information and communication technologies (ICTs); The ubiquitous computers interconnected in the worldwide network called the Internet are the most obvious sign of the impact it has today. According to [2], for telecommunications, commercial traffic and entertainment, these technologies are practically indispensable. Without the help of this invaluable tool, at present it is practically impossible to achieve acceptable and beneficial economic results, both for the administration in particular and for the administration of justice in society at large; Therefore, this principle is perfectly applicable to the Ecuadorian judicial system, which in order to fulfill its function of administering justice, must deal with information in increasing amounts.

Electronic medium has become a target to commit different illegal acts such as extortion, theft, fraud, phishing, among others [2]. Computer crime is difficult to understand since it is often considered as a neglected behavior by legislation, because it involves the use of various technologies for the achievement of crime.

Enrique Mafla, [3] expert in Computer Security, said that there are no secure computer systems. "They have even hacked the Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI)"

According to [3], Ecuador began to talk about cybercrime in 2009, since then, authorities have registered 3143 cases, which includes the reported robberies until the first quarter of 2011; but there would be an underreporting of those who did not report the loss. Pichincha is the province that registers most computer crimes, far above Guayas and the rest of the country; Being this province the one that has greater access to the Internet, contemplating about 30% of its connected population, followed by Azuay with 16%.

In 2011, the National Director of the Information Technology Unit of the Public Prosecutor's Office, said that until that date, the use of network-connected services was the main reason for the increase in cases of cybercrime, Unlawful amounts or values, electronic forgery of identity and computer damage (when the custodian is a public official) [3]

In an investigation carried out by [4], it is pointed out that in 2013 about 1013 frauds were committed through ATMs and web pages, cloning the magnetic strips of credit cards. Although there are no exact figures for the amount of money lost by this criminal mechanism, according to the Attorney General's Office, in Ecuador alone, cyber theft amounted to more than two million dollars, in addition, this same entity registered 530 crimes In the first five months of 2016 [5], 635 complaints were filed in the same period in the previous year, although the complaints presented a decrease, the figures would have to be evaluated for the remainder of the year [4].

As an intervention measure, in order to curb this criminal outbreak, the National Assembly of Ecuador has elaborated, within its new COIP (Organic Comprehensive Criminal Code), 6 regulations that seek to solve or to some extent curb the lack

Document received on May 31, 2017. This research was performed as a previous degree to obtain the professional title in the Electronic Engineering and Communication Networks major of the Faculty of Engineering in Applied Sciences from Técnica del Norte University.
C. L. Bracho, graduate of the Engineering Degree in Electronics and Communication Networks (telephone: + 5939-8557174; e-mail: clbrachoo@utn.edu.ec).
F.G. Cuzme, teacher of the Engineering Degree in Electronics and Communication Networks (telephone: + 5939-94564714; e-mail: fgcuzme@utn.edu.ec).

of effectiveness of the Administration of Justice Depending on these types of crimes. [2] states that it is imperative that the Administration of Justice elaborates and deepen the necessary rewards for the accreditation process of specialists in the field, given that even if there is a rule, if there is a lack of understanding in the application of the law in An illegal activity carried out by electronic means will not serve the new regulations.

Kaspersky Security Company, detected malware that has affected 140 organizations from 40 different countries, including the United States, France, Ecuador, Kenya and the United Kingdom, the five most affected countries. In Ecuador there are at least 9 institutions, according to this report [12]. This entails considering information security as an important point for organizations.

II. INFORMATIC SECURITY

It is common to speak of computer security and information security as if they were the same thing and, at first glance, it seems to be, especially considering that, thanks to the constant technological development, it tends to digitize all kinds of information and to manage it through a computer system [8]. However, although they have the need to work in harmony, each of these aspects has different objectives and activities.

Computer security refers to the set of policies, rules, standards, methods and protocols used to protect the computer infrastructure and all information contained or managed by it [7]. Not only should attention be paid to intentional attacks, but also to possible software or hardware malfunctions that attempt against security, trying to minimize the risks associated with accessing and using a certain system in an unauthorized way or Malicious to reveal, use, modify or accidentally or intentionally destroy the information contained therein. For this, the assets to be protected must be evaluated and quantified, and based on this analysis, implement preventive and corrective measures that eliminate or reduce the associated risks to manageable levels.

On the other hand, information security refers to all those measures that seek to protect the information in the event of any irregularity [7]. The main difference between computer security and information security is that the first is responsible for security in a computer environment and the second is interested in information in general, which can be stored both in a computer medium and in any other. For example, a manual of procedures written on paper, people's knowledge, blackboard writings, and discarded papers are important sources of information.

A. Computer Security Audit

A computer security audit or security audit of information systems is the study that includes the analysis and management of computer systems, performed by a person or group of people, called auditors, who may be of the staff or outside the staff. Organization; to identify and then correct the various vulnerabilities that could arise in a comprehensive review of workstations, communications networks or servers. [9]

The computer security audits at the time of their realization allow to know the exact situation of their information assets in terms of protection, control and safety measures and thus improve the profitability and effectiveness of the system, by exposing the Weaknesses and dysfunctions that are encountered in the process, and then draw up a final report indicating the action plans to eliminate such shortcomings as recommendations. [9]

To choose a suitable type of test, it is best to first understand how your modules are designed to work. Depending on the meticulousness, business, time allocation and audit requirements, the analyst can program the details of the same by phases, in the methodology OSSTMM version 3 there are four phases in its execution: Phase Induction, Interaction, Of Inquiry and of Intervention. [1]

Induction Phase

At this stage, the analyst begins the audit by understanding the requirements, scope, and limitations of the audit in that scope. Often, the type of test is best determined after this phase. [1]

Interaction Phase

In order for the security audit to be carried out correctly, an audit plan will need to be developed. The purpose of this planning is the collection of information from the organization and its computer systems to obtain comprehensive information of the area to be audited. The collection of information should be done through observations, interviews with the agents that interact with the system and with the request of documents and information to the responsible of the organization. With this, the auditor will be able to define specifically the general objective of the study, the scope that the audit should have and the program developed of the auditing tasks. [11]

Inquiry Phase

When the interaction phase is complete, the next step is to inquire. The investigation phase consists in the accomplishment of a series of tests whose results allow to detect weaknesses and strengths of the audited information system and justify the detection of the evidences. [11]

Intervention Phase

These tests focus on the resources of the objectives required in the application, which can be exchanged, changed, overloaded, or die due to penetration or interruption. This is often the final phase of a safety test to ensure that interruptions do not affect the responses of less invasive tests and because the information to do these tests may not be known until other phases have been carried out. [1]

B. Ecuadorian Legislation Regulating Computer Crime

Despite Ecuador's failure to take into account cybercrime in jurisprudence, Ecuadorian legislation currently protects laws and decrees that establish sections and specifications in accordance with the importance of information and technologies, Among them we have:

- Organic law on transparency and access to public information.
- Law of electronic commerce, electronic signatures and data messages.
- Intellectual Property Law.

- Special Telecommunications Law.
- Organic law on jurisdictional guarantees and constitutional control.
- Comprehensive Criminal Organic Code (COIP)

Based on statements by [6], the Departments of both the State Attorney General's Office and the Judicial Police serve as national contact points for formal or informal international cooperation based on trustworthy transactional networks between agents Of application of the Law; Which is possible through the application of Article 226 of the Constitution and the Law of Electronic Commerce Electronic Signatures and Data Messages.

Multinational cooperation of multinational special groups may prove particularly useful; and indeed there are cases in which international cooperation has been very effective in resolving any particular type of electronic crime.

III. STUDY CASE

In this part, a brief description of the main data of importance of the Decentralized Autonomous Government of the Canton Mira (GADM-Mira) is made, based on the information provided by the person in charge of the Systems Area, who is in charge of managing the entire infrastructure of The data network the entity, and technical visits to the physical facilities where the different communication devices are located.

A. Current Active Network

The LAN network has been operating since the end of 2007 and taking into account that its current building was rebuilt, it was designed with new technological advances in mind and the use of a data LAN. The distribution of the structured cabling coming from the telecommunications room to the different floors of the building; But in spite of having the aforementioned ducts, for the new departmental departments that are being incorporated it is necessary to adapt new external routes of wiring, depending on the location conditions that are presented.

The LAN network is Ethernet type and has a topological tree-type distribution as shown in Fig. 2. At the time of its implementation, a network was considered that was scalable in time, with 75 network points for desktop and laptops.

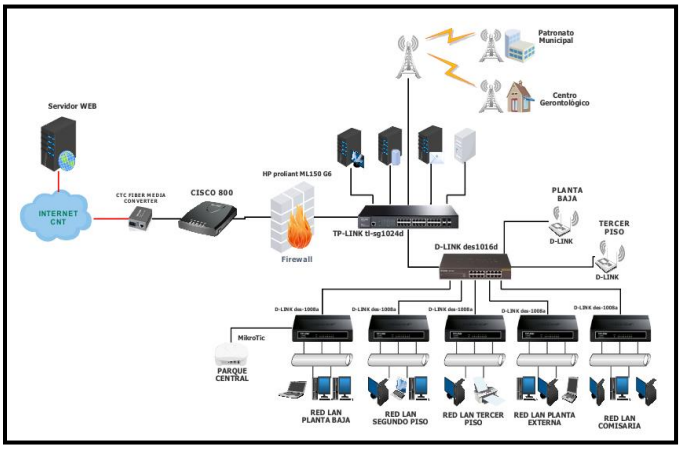

Fig. 1. Physical topology of the GADM-Mira LAN network

B. Routing equipment

GADM-Mira does not have its own routing equipment, it maintains a router provided by the company providing Internet services, which, besides providing a dynamic routing protocol, serves as an Internet connection to the LAN users Through the use of static routing.

C. WAN link

GADM-Mira has a contract for Internet services with the company CNT E.P. With a total bandwidth of 13 Mbps symmetrical through a single-mode Fiber Optic connection without backup, as can be seen in Fig. 3. In order to control the network traffic both in and out to and from the Internet, Makes use of the Firewall service.

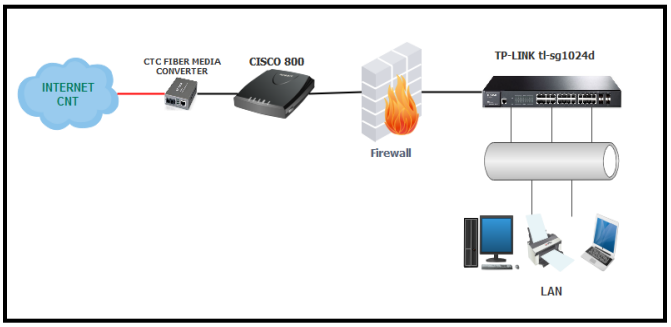

Fig. 2. GADM-Mira Internet connection

D. Addressing

Addressing assigned to GADM-Mira communication devices, computers and / or terminal devices makes use of Class C addressing, thus having 254 IP addresses available to hosts, to date no more than 100 addresses are required by the Fact of being a partially small network, but if it has been considered a percentage of scalability in the time.

E. Switching equipment

The GADM-Mira switching devices are non-administrable and are connected in a hierarchical order, based on the cascade model that starts with the core switch, then the distribution switch and finally the access switches, as shown in Fig. 2. If more ports are needed for workstations, a free port is left on the access switch and another access switch is connected to this port, forming a cascade; And thus the network is extended until the number of workstations required for each floor of the building can be satisfied.

F. Servers

Basically the GADM-Mira makes use of 5 elementary services such as databases, Internet, Firewall proxy, web and hosting for email accounts; Of which only two (databases and the Internet) are physically located in the telecommunications room. The other three services are contracted to private companies: Proxy Firewall is a complement to the antivirus service provided by the company ESET Smart Security, web services and hosting for email accounts are provided by the company NIC.EC.

G. Wireless Links

GADM manages two main links, one of radiofrequency, with its respective back-up that is directed from the terrace of the building of the GADM-Mira, towards a small tower of 5m of height that is articulated in the terrace of the building of the former Patronato Municipal, in order to take advantage of the elevation of this infrastructure, where it is possible to better distribute several radio links to different institutions and agencies that are part of the administrative jurisdiction of the Institution, thus facilitating their connection to the Internet service. The other link offered by GADM-Mira is the one that is addressed to the citizenship for free, offering the free Internet service or Wi-Fi Zone in the central park of the city.

H. Software, Hardware and Antivirus Management

The management of the software is done manually in the computer that presents problems, or in the case that a new official goes to make use of it for which the following procedure must be followed: the person in charge of the Systems area notifies to the department of Human Resources To be assigned a user profile, if you are going to make use of any type of system or special application, is installed at that time, and to finish, the new employee must sign a computer use liability agreement.

The management of the hardware is carried out semi-automatically, so the records are taken with the help of an Excel sheet, where certain important characteristics such as: brand, model, etc. are recorded. In case of presenting problems with the computer equipment, an immediate solution is given in case the problem is not serious, otherwise the equipment is transferred to the computer department for repair. In the same way, systematic processes are carried out in case there is a need to cancel a computer equipment, once it has reached its useful life within the Institution.

For the management of Antivirus, a year ago was done by a server (RAID 0) for the administration of the antivirus and their respective updates on each of the computers; currently, both the installation of the entire antivirus package on each computer and its update are performed manually. The company that provides this service is ESET with a contract for a year, so the GADM-Mira has an original License granted by that private company so you only have to enter the password in the graphical interface of the antivirus and the service is dropped In full operation for a whole year.

I. Documentation

As tangible information in physical documents, GADM-Mira has the following documentation, which is accessible only with the consent of the System Area Manager:

- IP addresses Registration
- Inventories of computer resources
- Internet Use Manual
- Systems use confidentiality agreements
- Topological diagrams of the wired LAN
- Topological diagrams of the wireless LAN
- Structured wiring plans of the GADM building

IV. METHODOLOGY APPLICATION

It is necessary to indicate that the case study considered for the application of the present methodology is in order to obtain real results of the application of the same. However, the steps described here can be followed to adapt it to any organizational environment in which important information from a computer security audit is required, applying it in all areas of an organization.

The following is a brief description of 7 steps that should be followed to carry out a successful safety test [1]:

1. Define what you want to protect, i.e. assets. The protection mechanisms of these assets are the Controls, which will be tested to identify the Limitations.
2. Identify the area around assets, which should include protection mechanisms and processes or services built around the assets. This is known as the confrontation zone.
3. Define everything outside the confrontation zone that is necessary to maintain operational assets, such as: electricity, food, water, air, stable land, information, legislation and regulations; and the environments and things you can work with. This is known as the scope of the test.
4. Define how the scope interacts within itself and with the outside, for it is necessary to split assets within reach according to the direction of interactions such as: from the interior to the exterior, from the exterior to the interior, the interior to the interior , etc. This is known as the vectors, ideally, each vector should consider a separate test with a short duration, before the test environment presents notable changes.
5. Identify the equipment that will be needed for each test. Within each vector, interactions can occur at several levels, which are classified according to their function in five channels. The channels can best be seen in Table 1.
6. Determine the information you want to get from the test. The type of test must be defined individually, however [1] identifies six types: Shielding or Ethical Hacking, Black Box, Gray Box, White Box, Sequential and Investment; Depending on the amount of information that the auditor knows about the objectives and what the objective expects from the test, it should be defined individually that best suits the needs of the process to be developed in the assessment of Each of the channels.
7. Ensure that the security test complies with the judicial rules, in order to ensure that the process carried out does not lead to misunderstandings, confusion or false expectations.

TABLE 1
CHANNELS CLASSIFICATION

Type	Channel	Description
Physical security (PHYSSEC)	Human	It comprises the human element of communication where the interaction is both physical and psychological.
	Physic	It comprises the tangible element of safety where the interaction requires physical effort or a transmitter of energy to manipulate.
Wireless Security (SPECSEC)	Wireless	It comprises all electronic communications, signals and emanations taking place on the electromagnetic spectrum EM.

Security in Communications (COMSEC)		It comprises all telecommunication networks, digital or analog, where the interaction is carried out through a telephone determined or similar to the lines of the public telephone network.
	Telecommunications	
	Data Network	It comprises all electronic systems and data networks where the interaction is carried out through an established cable and wired network lines.

A. Safety Metrics

The information of each of the audited channels is summarized in the Rav, which is nothing more than the balance of porosity, controls and limitations. It should be noted that for calculation of the final value of the current security can be done in two ways: one manually (applying various formulas), or automated (using an Excel sheet).

The Rav spreadsheet can be downloaded from the official ISECOM website (http://www.isecom.org/research/ravs.html), in which the numerical values of each item must be entered and the value Of the current security is obtained automatically.

To calculate the numerical value of the current security of each channel, which is the measure that allows to evaluate the percentage of efficiency of the operational controls implemented for each one, it is necessary to take into account the recommendations dictated by the methodology to separately weighting each one Of the items for which it is composed [1]:

- Porosity: Is measured as the sum of visibility (P_V), access (P_A) and confidence (P_T).
- Controles
  - ✓ Class A: authentication (LC_{Au}), indemnification (LC_{Id}), resilience (LC_{Re}), subjugation (LC_{Su}), continuity (LC_{Ct}).
  - ✓ Class B: non-repudiation (LC_{NR}), confidentiality (LC_{Cf}), privacy (LC_{Pr}), integrity (LC_{It}) and alarm (LC_{Al})
- Limitations: vulnerabilities (L_V), weakness (L_W), concerns (L_C), exposures (L_E) y anomalies (L_A).

To find the values of weakness and concern it is necessary to refer to Figure 3, from which the following criteria are taken:

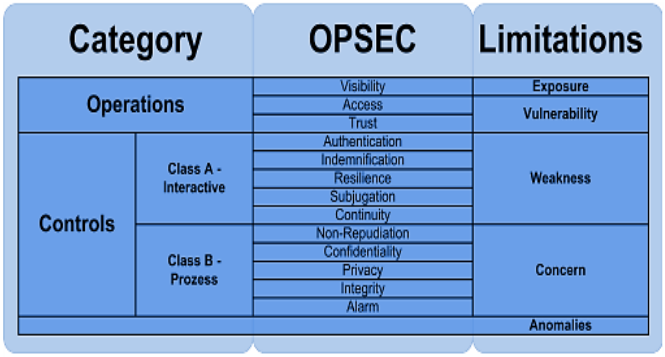

Fig. 3. Porosity, Controls and Limitations Relationship

Weakness is calculated by accounting for each defect or error in interactive or Class A controls: $(FC_{Au})(FC_{Id})(FC_{Re})(FC_{Su})(FC_{Ct})$ Thus:

$$\boldsymbol{L_w = FC_{Au} + FC_{Id} + FC_{Re} + FC_{Su} + FC_{Ct}}$$

The concern is calculated by posting each defect or error in the process or Class B controls: $(FC_{NR})(FC_{Cf})(FC_{Pr})(FC_{It})(FC_{Al})$ Thus:

$$\boldsymbol{L_C = FC_{NR} + FC_{Cf} + FC_{Pr} + FC_{It} + FC_{Al}}$$

The current security value is measured based on a reference level of 100rav, where more than 100rav means that a cost is too much spent on controls, and less than 100rav means that the operational controls adopted by the entity protect the entire system Of the audited channel, but with several limitations.

Performed Tests

For this section it is necessary to indicate that only one example of the use of the RAV spreadsheet in the human channel is shown, for the other channels the procedure to follow is the same.

Human Security Testing

En primer lugar, para tener un punto de partida para evaluar este canal fue necesario aplicar una encuesta a 10 empleados que interactúen en mayor frecuencia con el Área de Sistemas del GADM-Mira, mismos que se encuentran comprendidos por los departamentos del proceso habilitante de apoyo tomados de su Organigrama Institucional por Procesos.

To calculate the value of porosity in this channel, it was necessary to apply various social engineering techniques such as: direct observation, observation and persuasion, and false telephone calls; This in order to obtain the visibility, access and trust values, which are summarized in the following table.

TABLE 2
POROSITY CALCULATION

POROSITY or Op-Sec		
Ítem	**Test**	**Total**
Visibility	Accounting for which departments or areas of the GADM-Mira are authorized to perform interactions with the telecommunications room	5
Access	Accounting for scenarios where an interaction can occur without requiring an authorization from the employee guarding the information generated on your workstation	4
Trust	Accounting for access to the information or physical assets of employees who did not generate or are responsible for them respectively	3

The next step to define the RAV is to calculate the controls, which are nothing more than the safety mechanisms set in place to protect operations, the results of these operational measures are summarized below in the table below.

TABLE 3
CONTROLS CALCULATION

CONTROLS		
Interaction or Class A controls		
Ítem	**Test**	**Total**
Authentication	Accounting for methods by which you can interact with reception staff	4
Indemnification	Accounting for legal documents that GADM-Mira employees must submit to safeguard information generated or handled by their employees	4
Resilience	Accounting for employees that allow unauthorized access to the assets of the telecommunications room	1
Subjugation	Accounting for assets that can be communicated through channels in which controls are not needed can be circumvented or ignored	0
Continuity	Accounting for personnel who generate conflicts regarding access delays	1
Process or Class B Controls		
Ítem	**Test**	**Total**
Non-repudiation	Accounting for those in the reception staff to properly identify and record access to or interactions with GADM assets	2
Confidentiality	Accounting for communication segments with staff within reach that are efficient	3
Privacity	Accounting for efficient methods to ensure this control	1
Integrity	Account for the efficient methods applied by GADM to protect and ensure that the information of the physical assets can not be changed, switched, re-directed or invested without the parties having knowledge of it.	2
Alarm	Accounting for the use of warning systems or alarm systems throughout the scope	3

Then, the Limitations, which are calculated individually, should be weighted, for them the procedure shown in the following table was followed.

TABLE 4
LIMITATIONS CALCULATION

LIMITATIONS		
Ítem	**Test**	**Total**
Vulnerabilities	Accounting for faults or errors by which a person or process can gain or deny access to others	2
Weakness	Accounting for possible faults or errors that may occur in Class A controls	3
Concern	To account for possible defects or errors that may occur in Type B controls	3
Exposure	Accounting for unjustified actions, failures or errors that provide direct or indirect visibility of assets within the scope	3
Anomalies	Post unknown items that can not be taken into account in normal GADM operations	3

Once all the individual values of each item have already been obtained, they must be entered in the blank spaces provided in the Rav spreadsheet, and then the other values will be displayed automatically, as shown in Figure 4.

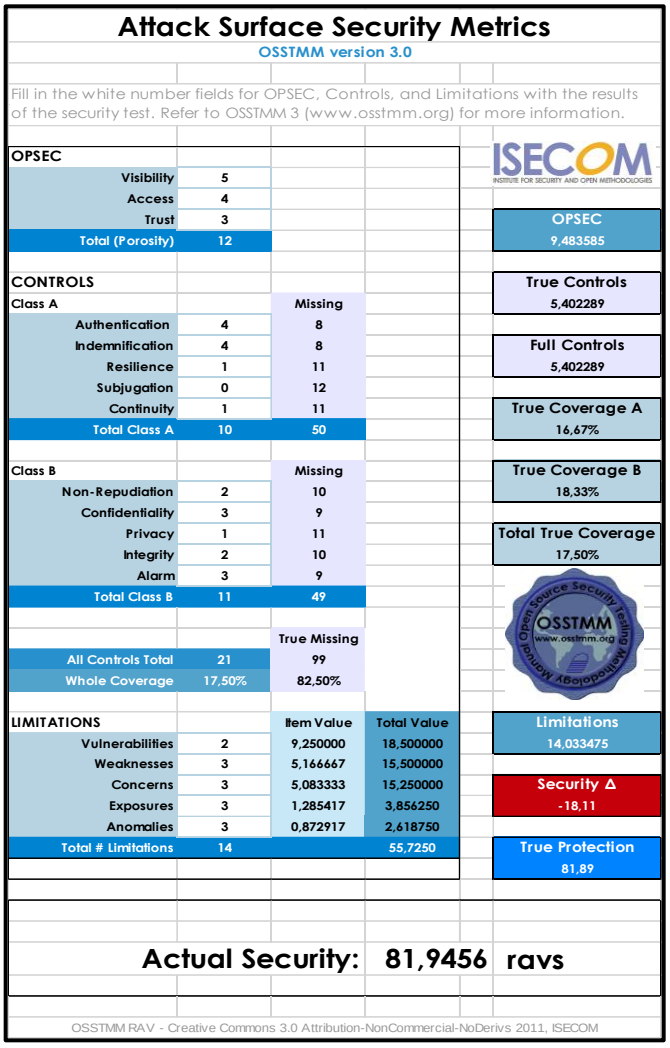

Fig. 4. Results obtained in the audit of the human channel in the GADM Mira

Results of Physical, Wireless and Data Network Security Testing

The following table summarizes the numerical values obtained for Porosity, Controls and Limitations, after having performed the different tests that it dictates [1].

TABLE 5
NUMERICAL VALUES OF OPERATIONAL METRICS

OPERATIONAL SAFETY			
Channel / **Ítem**	**Physic**	**Wireless**	**Data Network**
Visibility	11	4	21
Access	13	3	20
Trust	0	1	1
CONTROLS			
Channel / **Ítem**	**Physic**	**Wireless**	**Data Network**
Authentication	1	5	6
Indemnification	8	0	9
Resilience	5	1	4
Subjugation	1	0	2

Continuity	9	1	1
Non-repudiation	1	0	1
Confidentiality	1	1	0
Privacity	2	2	19
Integrity	3	2	0
Alarm	0	0	2
LIMITATIONS			
Channel Ítem	**Physic**	**Wireless**	**Data Network**
Vulnerabilities	7	0	25
Weakness	4	3	7
Concern	2	2	4
Exposure	3	0	2
Anomalies	0	1	1

Telecommunications Security Testing

For this particular channel, [1] recommends that the attack vectors for this channel are:

- PBX testing
- Voice mailbox Testing
- FAX and Modem surveying, polling, and testing
- Remote Access Services (RAS) testing
- Backup ISDN lines testing
- Voice over IP testing
- X.25 packet switched network testing

Para este canal solo existen dos objetivos que pueden ser probados dentro del GADM-Mira ya que solo se cuenta una central telefónica analógica y un sistema de fax; de los cuales, la central telefónica no sería considerada como un dispositivo de telecomunicaciones ya que está limitada para uso exclusivo dentro del espacio físico del GADM.

Consequently, for this channel, it will appeal to the resource that dictates [1] to report it as an "untested objective", because the environment of the test does not allow to gather the necessary information to issue a report that yields results according to the current reality of GADM-Mira. It is best to take this aspect for future tests, and if you have the necessary vectors to test, you must issue a criterion on the degree of safety that will have this channel.

V. RESULTS

There are two expressions that allow an interpretation of the values obtained in the current security of the audited channel, the first is Security Δ as shown in figure 4 marked red, which is nothing more than the balance between values (+) Or negative (-), the following aspects can be considered: a positive delta shows how much is spent on controls Or even if the excess spending is too much in one type of control; A negative delta shows a lack of controls or they control themselves with limitations that can not adequately protect the target.

The limitations that were identified in the analysis of results of the methodology giving them a priority order are firstly the financial type for not allocating the necessary resources to the systems department so that the necessary controls are implemented and secondly are the competencies Strategic because there are no plans for continuous training for staff that must provide security to the institution's information, as well as create access policies to network resources.

The other expression allows to analyze the risk of the attack surface is the Current Security whose values can be seen in table 6, where on average for the four audited channels has a numerical value of approximately 80 ravs, which translates into a Deficiency of about 20%; And therefore it can be ensured that there is a considerable percentage of vulnerabilities within the security system that is managed within the Institution.

TABLE 6
FINAL RESULTS

ANALYSIS VALUES					
Channel Item	**Human**	**Physic**	**Wireless**	**Data Network**	**Average**
OpSec	9.48	11.43	8.43	12.29	10.41
Limitations	14.04	16.12	11.76	20.10	15.51
True Controls	5.4	6.21	4.34	6.99	5.74
Δ Security	-18.11	-21.34	-15.85	-25.39	-20.17
True Protection	81.89	78.66	84.15	74.61	79.83
Actual Security	81.95 ravs	78.79 ravs	84.26 ravs	74.81 ravs	79.95 ravs

VI. CONCLUSIONS

The applicability of the methodology OSSTMM version 3 allows to know punctual results on the channels in which a greater attention is required, so as to be able to provide a timely solution to certain vulnerabilities that may occur within the organizational environment, either due to financial, human, Procedures or strategic, normative; As well as poor application of security controls that may be underutilized.

The fact that the methodology separates into individual channels the tests that must be performed is very beneficial, not only for the auditor; But also for the institution since this allows to know for sure where part of the infrastructure of the network security system is a greater number of vulnerabilities and thus to be able to apply the necessary corrective methods in the channel that needs it.

The channel in which the most time was invested was the data network channel, this being due to the fact that it was necessary to first apply an interview to the GADM Systems Director of Canton Mira, in order to have a starting point, With relevant information on said channel; And secondly because it was necessary to execute several applications of the audit software (Kali-Linux), in order to obtain as much information as possible the communications equipment that make up the data network of the Institution.

Within the scope of computer audits there are a number of methodologies that can be taken as a reference to obtain results on the security of information maintained by a certain organization, in such a way must make a technical analysis of which provides better performance to perform An evaluation not only qualitative but also quantitative of the security mechanisms in force in the Institution.

VII. REFERENCES

[1] P. Herzog, OSSTMM 3. Manual de la Metodología Abierta de Testeo de Seguridad, New York: ISECOM, 2010.

[2] E. Chiluiza, «Los delitos informáticos en el COIP,» *La Verdad*, 10 01 2015.

[3] Diario La Hora, «Se disparan los delitos informáticos,» *La Hora*, 21 Agosto 2011.

[4] AGN, «En Ecuador, aumentan los delitos cibernéticos,» *El Mercurio*, 02 01 2015.

[5] El Telégrafo , «En Ecuador, el 85% de los delitos informáticos ocurre por descuido del usuario,» *El Telégrafo*, 16 08 2016.

[6] S. Acurio del Pino, «inforc ECUADOR,» 29 02 2012. [En línea]. Available: http://www.inforc.ec. [Último acceso: 05 05 2017].

[7] G. A. Toth, «Implementación de la guía NIST SP800-30 mediante la utilización de OSSTMM,» Neuquén, 2014.

[8] G. Escrivá, R. Romero, D. Ramada y R. Onrabia, Seguridad Informática, Madrid: Macmillan Iberia, 2013.

[9] J. Costas Santos, Seguridad Informática, Madrid: Ra-Ma Editorial, 2010.

[10] ISACA, COBIT 5 para Seguridad de la Información, Madrid: ISACA Framework, 2012.

[11] E. Chicano Tejada, Auditoría de seguridad informática, Andalucía: IC Editorial, 2014.

[12] Karpesky Lab, «Karpesky,» 2017. [En línea]. Available: http://media.kaspersky.com/en/business-security/fileless-attacks-against-enterprise-networks.pdf.

VIII. BIOGRAPHY

Cristian L. Bracho. He was born on December 26, 1990 in Mira city; Carchi Province. He completed his primary studies at the Rafael Arellano School, his secondary studies at the U.E. León Rúales and is currently a graduate of Técnica del Norte University.

He took several courses at Técnica del Norte University: build and give maintenance to computers, 2008; Linux Basic, 2016; Databases, 2016.

Fabian G. Cuzme. He was born on November 14, 1985 in Portoviejo city, his secondary studies were made in the school Dr. Bruno Sánchez Carreño of the same city. Engineer in Computer Systems of the Technical of Manabí University. Magister in Communication Networks of the Pontifical Catholic University of Ecuador. He is currently teaching at the Técnica del Norte University in the Engineering Career in Electronics and Communication Networks.