Computer security audit for Gobierno Autónomo Descentralizado de Santa Ana de Cotacachi, based in the standard NTP ISO/IEC 17799:2007 and the methodology OSSTMM v2.

Edgar A. Maya, Daniel D. Jaramillo

***Summary*— This project exposes the process of conducting an audit of information security to the Gobierno Autónomo Descentralizado de Santa Ana de Cotacachi based in the standard NTP ISO/IEC 17799:2007 and the methodology OSSTMM v2 in order to detect possible vulnerabilities and deficiencies that may have the network and thus effectively determine the necessary steps to take.**

It's presented a set of recommendations establishing actions to undertake to help improve the level of information security, including security policies to minimize the risks that may arise in the future, to prevent attacks and improve network efficiency.

I. Introduction

Increased interconnectivity and the popularity of the Internet are offering all kinds of organizations with unprecedented opportunities to improve operations, significantly reducing paper use, in turn reducing costs by sharing information. However, the success of many of these efforts depends in large part on the ability of the organization to protect the integrity, confidentiality and availability of data and computer systems.

Although information security plays an important role in protecting data and assets of an organization, we often hear news about computer crimes, such as altering websites or data theft. Organisations need to be fully aware of the need to devote more resources to the protection of information assets and information security, information security should become a major concern of a company.

II. Computer Security

Due to advances in technology, and nature of communications, it is increasingly difficult to secure information so that its integrity is guaranteed.

In today's IT environment, organizations are increasingly dependent on their information systems. Information is an asset which, like other important business assets is very essential for the business and therefore needs to be suitably protected. This is especially important in the business environment where information is exposed to an increasing number of people and therefore a wider variety of threats and vulnerabilities. Threats, such as malware, hacking and denial of service attacks have become more common, and more and more sophisticated..

A. Audit

With the exploitation of Internet use in the last 10 years, both large and small companies, have been forced to secure their vital component is the technology of information. Currently companies, has valuable IT resources, such as computers, data networks, computer systems, etc.. To protect the assets of a company, it is suggested that at least has had a security audit, in order to get a clear picture of the security risks they face and know the best way to deal with these threats.

The purpose of a safety audit is not to blame or detracts from the design of a network, but to ensure the efficiency, integrity and compliance with security policies of the company. The audit provides the ability to test the systems, find and check risk controls are appropriate to mitigate exposure to different risk, it should be emphasized that security auditing is not just about how to run a number of hacker tools, in an attempt to enter the network.

Document received on July, 2014. This research has been made as a previous project to get the degree in the Electronics and Communication Network Engineering of the, Faculty of Applied Science (FICA), of the "Universidad Técnica del Norte".

E.A. Maya, Works at the "Universidad Técnica del Norte", 17 de Julio Avenue, "El Olivo" neighborhood, Ibarra-Ecuador (phone: 5936-2955-413; email: eamaya@utn.edu.ec).

D.D. Jaramillo, egresado de la Carrera de Ingeniería Electrónica y Redes de Comunicación (phone: 5936-2635-160; e-mail: davx_jra@hotmail.com.).

Features information security audit

The audit is systematic meaning that the results are due to a meticulous, methodical and planned by the auditor analysis, which ensures reliability.

The audit is fully independent since it is impossible for a company to evaluate themselves objectively.

Consider whether preventive measures aimed at controlling the risks of attacks or failures detected in the business, are effective or not, depending on the results.

The audit is responsible for analyzing the current state of the business to provide solutions to future without the need to find a culprit of possible flaws in the information technology.

The characteristics they can be graphically summarized in this scheme.

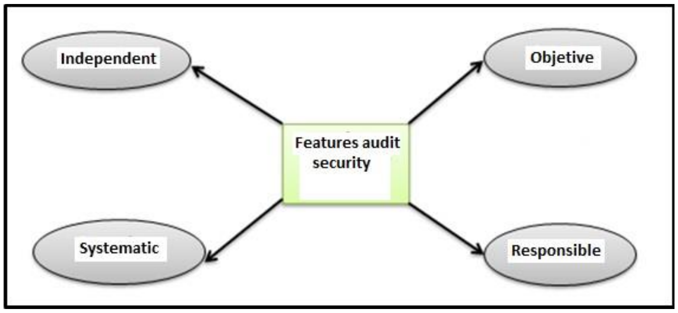

Fig. 1. Features audit computer security

B. NTP ISO/IEC 17799

ISO 17799 defines information as an asset that has value to the organization and therefore requires adequate protection. The purpose of information security is adequately protecting this asset to ensure business continuity, minimize damage to the organization and maximize return on investments and business opportunities.

This standard provides recommendations for managing the security of information that can be used by those responsible for initiating, implementing or maintaining and improving security in an organization. Aims to provide a common basis for developing safety standards within organizations and be an effective practice of safety management.

Structure and Scope

This standard contains 11 security control clauses collectively containing a total of 39 main security categories and one introductory clause containing issues of risk assessment and treatment. The clauses are as follows:

- Security Policy;
- Organizing information security;
- Assets Management;
- Safety in human resources;
- Physical and environmental security;
- Communications and operations management;
- Access control;
- Acquisition, development and maintenance of information systems;
- Incident management information systems;
- Management of business continuity;
- Compliance;

Within each clause, the objectives of the various controls for information security are specified. For each of the controls also indicates a guide for implementation. For this project previously considered few are really applicable as required

C. OSSTMM Methodology

The OSSTMM was created by Peter Herzog of ISECOM organization in December 2000, this manual the only and the most extensive standard certificate available for development testing Internet Security Systems and Networks. In order that this manual always updated, ensures the organization to be aware of the changes taking place and new developments in the field of Information Security.

The OSSTMM serves as a comprehensive guide, with regard to the main aspects of information security of a company, thus allows authorized to conduct audits, staff can consult relevant information about its own security policies, this shows the flexibility of the manual.

Structure

Safety tests covering six sections corresponding to the six sections in this manual. Each section consists of several modules and each module indicates a series of tasks or tests to be performed; which cover the following areas.

- Information Security
- Process Safety
- Security in Internet technologies
- Secure Communications
- Wireless Security
- Physical Security

The outline of this manual is as shown in Figure 2.

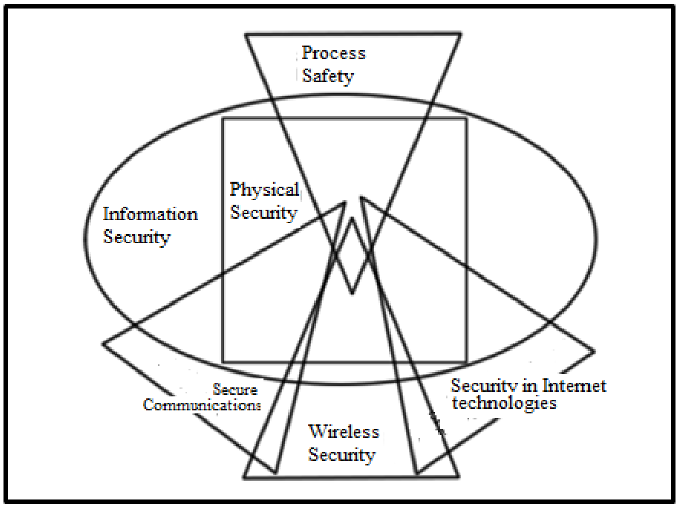

Fig. 2. Estructure of manual OSSTMM.

The OSSTMM care of the boundary conditions such as the testing process, ethics, analysis of test results and IT security with regard to the law, regulations and standards.

III. Analysis of the current situation

In this chapter the current network infrastructure data of the Government Municipal of Santa Ana de Cotacachi to October 2013 is described, the data are the result of information collected in collaboration with the department and the recognition of the physical facilities network.

A. Overview

The organizational structure of the Government Municipal of Santa Ana of Cotacachi is the vehicle that links the mission and institutional goals with the provision of services to the community Cotacachi, and is based on a process approach, products and services to ensure the organic system and continuity of municipal utilities.

B. Technical specifications

The GAD de Santa Ana Cotacachi is a public non-profit institution located in the Province of Imbabura in the city of the same name, located in the streets García Moreno and Gonzales Suarez.

At this point the physical location described the structure of the network of both internal and external data, computing resources and network links related institutions towards the town.

C. Network management system

This item management software, hardware equipment of the municipal GAD as well as antivirus management and administration of the department of computer.

D. Liability of officers of the IT department

Computer Department is comprised of the Head of IT, Head of Connectivity, and two computer analysts; the responsibilities assigned to each staff, are as follows: computer analysts perform software maintenance, hardware maintenance, user support, user account management, inventory, etc. The heads of computer usually responsible for the administrative, applications development, etc.

IV. Vulnerability testing

This chapter describes the vulnerabilities found in the data network of the Autonomous Decentralized Government Municipal of Santa Ana de Cotacachi, for which we used the software described Backtrack and has been based on the precepts of OSSTMM methodology.

A. Information Security

The information security describes the competitive intelligence GAD Municipal of Santa Ana Cotacachi, detailing the same infrastructure that has in the area of information and intellectual information of each of the people who are part of the support department computer.

B. Process safety

Consists of a series of testings access privileges for the organization and its assets from a fraudulent position, using phone, chat, newsletters, interviews, mail, etc.

C. Safety in internet technologies

An analysis of the security of information technologies such as network survey, identifying services systems, Internet applications, routing, password encryption, denial of service testing is performed, and evaluation of policies security.

D. Secure comunications

The testing of the communication security is to check the operation of the PBX, and FAX modem, with the aim of finding an abnormality.

E. Wireless Security

Is to verify the security of wireless networks such as WiFi networks, Bluetooth, RFID, infrared etc.

F. Physical security

Is to evaluate the security of GAD Municipal of Santa Ana Cotacachi and computer goods, verifying the security of their physical perimeter, and evaluate the conditions of the region to natural disasters.

V. Specific correction

This chapter discusses a number of recommendations establishing actions to take, how to improve information security, including security policies to minimize the risks that may arise in the future, based on NTP-ISO/IEC 17799: 2007.

A. Security policies

After reviewing the diagnosis of which was the subject chapter 4, it was noted that information security is scarce, vulnerable to failure, considering that the main objective of the department of Computer Science of GAD Municipal of Cotacachi is to have continuity service that provides a daily Citizenship canton has developed a series of recommendations to improve the quality of service provided in the GAD Municipal of santa Ana Cotacachi.

B. Organizational aspects for safety

Whereas the GAD Municipal of Santa Ana of Cotacachi, when there is no process for handling the information department information suggests developing a bakery that lets users know the importance of processes and procedures to follow when process information for it to be reliable, for which it has established a schedule in which it could disseminate the above policies, which are of importance to employees.

TABLE I
SCHEDULE BROADCAST SECURITY POLICES

SCHEDULE BROADCAST SECURITY POLICES		
Date	***Department***	***Hours***
4-08-14	Mayor and councilors	15:00
5-08-14	Overall coordination	15:00
6-08-14	General secretariat	15:00
7-08-14	Financial management	15:00
8-08-14	Administrative management	15:00
11-08-14	Development planning local	15:00
12-08-14	Works and publics services	15:00
13-08-14	Social management and interculturality and human rights.	15:00

C. Asset management

To keep track of assets that are used in network of the GAD Municipal of Santa Ana of Cotacachi, the IT department in conjunction with inventory and warehouse, label each of the equipment delivered, so information was recorded as the name responsible asset location, physical description, at the given serial number.

The information collected will be stored physically and digitally, for which the IT department should design a program that allows the entry and storage of information, so that it can be processed easily and quickly by the staff responsible for carrying record.

D. Safety human resource

The personnel working in the technical department, it has been doing for several years, each has the experience necessary for the position they hold, the work is done full time and only have signed the contract for services .

They recommend, include in the employment contract, a confidentiality agreement, to ensure that the same employees not to reveal information concerning the institution, and remember that to violate this agreement THEY MAY BE subject to the laws that are in force.

E. Physical and environmental security

Concerning the physical security teams used the network user GAD Municipal Santa Ana of Cotacachi, not visible to the public, each of these are protected by a desk, most are within offices, same as for the income need to have the key which allows access.

Servers, which allow the implementation of different IT services that is handled in the GAD Municipal Santa Ana of Cotacachi, are in a room that has a door that the only security it offers is the veneer.

He recommends that the gateway access security is implemented through biometrics, access code, among others, in addition to changing the door, the other to provide security may be a steel door designed for bathrooms quipos since that in which the door currently is glass and aluminum.

F. Communications and operations management

Network Administration and Management of GAD Municipal Santa Ana of Cotacachi

Currently the computer systems that are handled by the GAD Santa Ana Cotacachi, can be evaluated as good, but the performance of the network tends to have problems because the network equipment such as routers and switches do not have an ideal setup and administration network, the network currently GAD Municipal Santa Ana of Cotacachi is configured as shown in Figure 3.

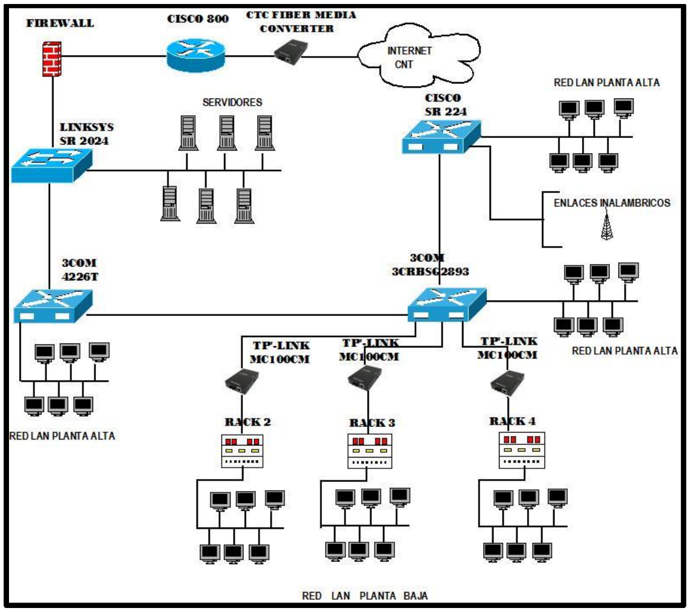

Fig. 3 Network diagram of GAD Municipal of Santa Ana of Cotacachi

It suggests a reorganization in the network equipment in order to have better management of equipment, and the performance of the network is reflected in the excellence of the service provided to the citizens of Canton Cotacachi, preventing collection systems, collections among others are offline, for them it has redesigned the network, by implementing VLANs and subnets performing, taking into account the hierarchical levels that should have network equipment.

It has taken the class C network 192.168.0.0/24 which 254 computers are available in order to optimize the number of usable networks and host, considering it is a relatively small network.

The network segmentation is performed using the VLSM tool in order to avoid wasting network addresses, subnets that allow obtaining the network administrator provide broadcast containment and low-level security on the LAN. To perform this segmentation is taken into account the number of hosts per rack and the number of servers.

VLANs seven is designed, in order to reduce the collision domain, constant requests ARP messages that can flood a network, with a significant number of host, for it smaller diffusion domains is created. In each of the VLANs are assigned different units according to their function, information handled and where they are.

Once designed segmentation subnets and vlans for each unit the correct distribution of network devices such as switches and router is made to keep the network operational and functioning properly, in Figure 4, it can display the appropriate configuration network for GAD Municipal of Santa Ana of Cotacachi.

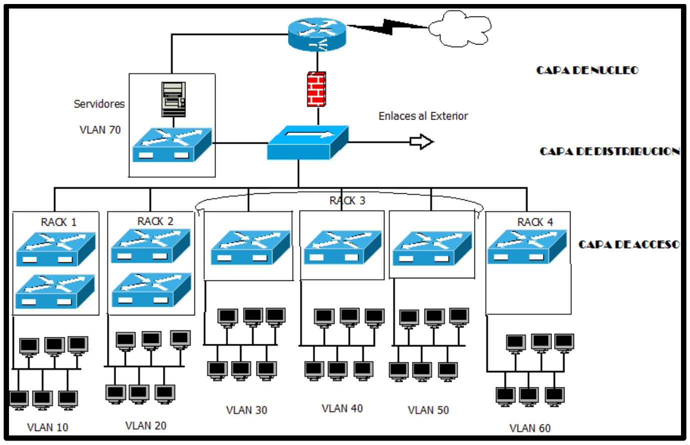

Fig. 4. Diagram Reorganization GAD Municipal Santa Ana of Cotacachi

As seen in the figure of redesigning the network, the network devices such as router and switch are distributed hierarchically, this allows for an easily understandable network and define functions in each layer also allows easy configuration if it is necessary.

Safety Management In Wireless Networksz

SSID of the Access Point with Santa Ana Cotacachi is recommended to use a strong password, it should be at least eight characters and consist of lowercase and uppercase letters, numbers and symbols like `~! @ # $% ^ & * () _ - + = {} [] \ |:; "'<>, /,.? Password it should be changed regularly, so it can get it easily avoided if a victim of an attack.

SSID of the Access Point Systems is recommended to configure a security key that is similar to those previously mentioned because when it does not has password features. Users who wish to connect to this network must request their password in the Computer Science Department.

The Access Point with SSID Wifi_Parque_MC recommended to assigning port Rack 3 to this port must be assigned a new VLAN 80, to keep the users connecting from the isolated park in the municipal system and thus avoids any intrusion through the wireless network to the internal network of the Municipal

Protection Threats

Website cotacachi.gob.ec

According to the result of the vulnerability scanner for this website as seen in section 3.4.1.1, the page has the vulnerability that is known as password guessing at logon; it is recommended to implement the following security type.

Website cotacachienlinea.gob.ec

According to the result of the vulnerability scanner for this website as seen in section 3.4.1.1, the page has the vulnerability that is known as password guessing at logon, it is recommended to implement the following security type.

The website is designed in joongla platform to patch this vulnerability is recommended to follow the following steps:

- Login to the website as administrator
- Go to Extensions - Manager plug-ins.
- Find a plug-in: System - Brute Force Stop
- Activate the plug-in
- The window where it can change the number of login attempts, locking time ip, and the option to send an email if the website is blocked appears.
- Save the changes and close

We recommend placing a smaller number of attempts to 5 and the blocking time is at least an hour, so we can say that the site is deemed safe.

G. *Access control*

To provide the necessary security to the information circulating within the network of the GAD Municipal of Santa Ana of Cotacachi should have a record of those who use computer systems that privileges are, and if the position he played in the municipality has been completed, remove from privileged users, to avoid undue network access.

Knowing the information flowing through the network of the GAD Municipal Santa Ana of Cotacachi, is confidential, it is recommended that all those with access to information systems, sign a pledge, it forces them not to reveal personal passwords, to third parties and also the group passwords, even more professionals working in the iT department will be in the ability to access all systems and know the password for all users.

H. *Acquisition and maintenance of systems development*

It should be consideration given to the acquisition of software warranty offered by the manufacturer, so it meets standards and recommendations that ensure information security.

Prior to the acquisition is recommended that a study of the benefits and disadvantages that each provides, in order to adapt it to systems that are operational.

It is necessary that the developed resources Municipal GAD Santa Ana Cotacachi, software is tested, to check the safety thereof for which the IT department is responsible for checking that meets the standards rules international security, since the information used in the network of the municipality is also on the Internet.

I. *Incident Management Information*

Its need to keep track of each of the events raised within the municipality, this will be useful to detect vulnerabilities on the network, and preventing possible security attacks of the same, to keep proper record has recommended the use of the template shown in Table 2.

TABLA II
TEMPLATE FOR REGISTRATION OF EVENTS

Template for registration of Events	
Number of Event	
Equipment Affected	
Departament	
Office	
Númber team	
Time	
Date	
Personal injury reporting	
Observations	
Signature of the responsible	

VI. CONCLUSIONS

The development of this project has been a great deal of work and time, as it has had to investigate topics such as management, security and safety audit and various computer security standards, which could be analyzed that there a security scheme that covers entirely possible risks, however it is can be prepared and ready to react quickly to threats and vulnerabilities that may arise in the field of computing.

It was found that the active computer that has the GAD municipal handle information that is very important for the citizens of Canton, this is because increasingly, the main services offered by the agency are dependent on computer systems, which is why the need for a security audit system network, and the efficient management of ICT is one of the main strategic objectives of the municipality.

The good performance of a company is due to the efficiency of their computer systems; a company can have people first, but if an error-prone, vulnerable and unstable computer system has and if not a balance between these two things, the company can never provide a quality service. Regarding the work of the audit itself, it can highlight that accurate knowledge of computer security, reliability, capacity, thoroughness and responsibility; computer security audit should be done by highly responsible people, and made a wrong audit can bring drastic consequences for the audited company.

VII. ACKNOWLEDGMENT

It is necessary to implement the recommendations drafted in the fifth chapter of this thesis project in order to improve the level of information security and optimize the resources of information technology.

It is recommended that the computer department staff is trained in safety and control technology that based on the knowledge gained expose appropriate new technologies for safe keeping of information that is handled daily in the municipality strategies.

It is recommended that the IT department to support the GAD municipal of Santa Ana of Cotacachi adopted as a best practice planning and conducting periodic audits taking into account that the standards are evolving and changing to ensure that the objectives related to security information are being met.

VIII. REFERENCES

[1] Aldaz, K. (Julio, 2011). Normas de Auditoria. Alcance de la auditoría informática. Retrieved from: http://normasauditoria.blogspot.com/2011/07/alcance-de-la-auditoria-informatica.html

[2] Antonio Villalón Huerta *El sistema de gestión de seguridad de la información* Retrieved from:: http://www.shutdown.es/ISO17799.pdf

[3] Apaza, G. (Junio, 2011). Seguridad en Servicios TCP/IP. Retrieved from: http://www.sistemas.edu.bo/mreynolds/Redes2/SEGURIDAD%20TCP - IP_2.pptx

[4] Benavidez, E. (Junio, 2011). Seguridad Informatica: Que es la seguridad Informatica Retrieved from:: http://seguridadinformaticaais.wordpress.com

[5] Bisogno, M (Octubre, 2004). Metodología para el Aseguramiento de Entornos Informatizados" Project of titillation: Universidad de Buenos Aires

[6] Cerra, M. (2010). *200 respuestas de seguridad*. Argentina: USERSHOP

[7] Comité Técnico de Normalización de Codificación e Intercambio Electrónico de: Datos, (2007). Perú. *Norma Técnica Peruana NTP-ISO/IEC 17799. Reseña Histórica*. (p. iv).Lima (2a ed.).

[8] Daniel. Sf. Vulnerabilidades en las redes TCP/IP. Recuperado de: http://dnl-skm.blogspot.com/2011/07/vulnerabilidad-tcpip.html

[9] Del Peso, E. Ramos. M. (2010). *El documento de seguridad: Análisis técnico y jurídico*. Madrid: Díaz de Santos como se realiza la auditoria

[10] Dias, G. (2010). *Redes de Computadoras*. Retrieved from: http://webdelprofesor.ula.ve/ingenieria/gilberto/redes/08_capaTransporteUDP.pdf

[11] Economia, sf. Economia Aida. Estandares auditoría informática. Retrieved from: https://sites.google.com/site/economiaaida/estandares-auditoria- informatica

[12] Eleclibre. (Enero, 2011). Sistemas y mecanismos de proteccion. Retrieved from: http://eleclibre.blogspot.com/

[13] Flores, B. (Noviembre, 2010). Riesgos de Auditoria. Cuando se debe aplicar una auditoria informatica. Retrieved from: http://dfloresysbonilla.blogspot.com/

[14] Galisteo, D. Moya, R. sf. Seguridad en TIC. Man in the middle Ataque y deteccion. Retrieved from: http://issuu.com/arrayl/docs/mitm

[15] García, J. (2008). *Ataques contra redes TCP/IP*. Recuperado de: http://www.intercambiosvirtuales.org/tag/ataques-contra-les-redes-tcpip

[16] Gonzáles, H. (2013). UTTN-TICS. Unidad III Auditoria. Retrieved from: http://uttn-tics.wikispaces.com/Unidad+III.+Auditoria

[17] Jauregui, I. (2009). *SNIFFING DE REDES*. Retrieved from: http://toma37.blogspot.es/1241710200/

[18] Jiménez, E. (sf). Riesgos potenciales en los servicios de red. Retrieved from: http://esperanza7989.files.wordpress.com/2011/11/6-riesgos-potenciales-en-los-servicios-de-red.pdf

[19] Kioskea (Diciembre, 2012). Ataques por desbordamiento de buffer. Retrieved from: http://es.kioskea.net/contents/19-ataques-por-desbordamiento-de- bufer

[20] Martínez, J. E. Giraldo, C. A. (2009). *Auditoría de seguridad Informática*. Retrieved from: http://artemisa.unicauca.edu.co/~ecaldon/docs/audit/ponencia_PASSWORD_siti2004.pdf

[21] Tony, (febrero, 2011). Gestión de servicios de tecnologías de la información. Retrieved from:http://mymusicismydrug.blogspot.com/2011/02/unidad-1gestion-de-servicios-de.html

[22] Victoria, M. (2011). *Metodología para el Aseguramiento de Entornos Informatizados.* Retrieved from: http://es.scribd.com/doc/36819948/32/vulnerabilidades-a-nivel-fisico

IX. Biographies

Edgar A. Maya A. Born in Ibarra , province of Imbabura on April 22, 1980. Computer Systems Engineer of the “Universidad Técnica del Norte” in 2006. Currently, teacher of the Electronics and Communication Network Engineer Career (UTN), Ibarra-Ecuador, and studying for a Master degree in Communication and Networks (3 semester), Pontificia Universidad Católica del Quito- Ecuador.

Daniel D. Jaramillo R. Born in Otavalo – Ecuador. Imbabura on june 18, 1986. Son of Alfonso Jaramillo and Rosa Remache. He studied in the ´´Instituto Técnico Superior Otavalo´´ ITSO.

He studied Electronics and Communication Network Engineer at the ´´Universidad Técnica del Norte´´ Ibarra-Ecuador.