NORTH TECHNICAL UNIVERSITY

ENGINEERING SCIENCE APPLIED FACULTY

ENGINEERING IN ELECTRONICS AND COMMUNICATION NETWORKS CAREER

SCIENTIFIC ARTICLE:

GRADE JOB PRIOR TO THE OBTAINING THE TITLE OF ENGINEERING IN ELECTRONICS AND COMMUNICATION NETWORKS

THEME:

"PERIMETRIC SECURITY SYSTEM TO DATA NETWORK S.A FLORALP INDUSTRY IN IBARRA CITY BASED ON FREE SOFTWARE PLATFORM"

AUTHOR: GABRIELA JANETH LÓPEZ PAREDES

DIRECTOR: ING. SANDRA CASTRO

Ibarra – 2015

"PERIMETRIC SECURITY SYSTEM TO DATA NETWORK S.A FLORALP INDUSTRY IN IBARRA CITY BASED ON FREE SOFTWARE PLATFORM"

Gabriela J. López P.
North Technical University

Abstract — The massive use of computer services and networks as a means to transfer, process and store information in recent years has increased, transforming the information in all its forms and states in an extremely valuable asset which should be protected and secure to ensure integrity, availability and confidentiality.

Information security Systems can be a physical device or tool to safeguard a good, software or system that similarly help in some way to protect an asset that is not exactly something tangible, or security measure this is implemented it can be done via security policies based on standards to their creation.

The use of open standards contributes primarily on the economics of large and small businesses by allowing savings in licensing and hardware acquisition, since teams are reused due to handling and low resource consumption of applications installed in them

***Indexed terms* —ISO, IEC, IDS, DMZ, QoS.**

I. INTRODUCTION

T's a industry involved in the processing and marketing of dairy products specializing in craft mature cheeses, keeping original features and quality demanded by the market, ensuring a personal, fair and transparent relationship with its customers, suppliers, the community and the environment. FLORALP is an industry visionary, since its inception has innovated and grown through the years began preparing pasteurized milk and fresh cheeses.

Document received June 2015. This research was realized as a preliminary project to obtain the professional title of the Engineering in Electronics and Communication Networks Engineering Faculty of Applied Science career (FICA) North Technical University

G.J.López, it's going to graduate in Engineering in Electronics and Communication Networks career. (Phone number 5939-3078-067; e-mail: gaby_janeth_7hotmail.com).

Nowadays it has become the example of the dairy industry in the production of handmade aged cheeses as are Dutch cheese, cheddar, brie, camembert, gruyere, parmesan, Tilsiter, raclette, ricotta, mozzarella, butter, cream, cream cheese, yogurt, so on. These products you can find in the best supermarkets, hotels, restaurants, cafes, and industrially national level.

So the era of human development, processes, quality management, continuous improvement, the involvement where the decisive intervention support and execution of family members gravitated greatly in achieving the goals and objectives; strengthening internal communication channels and improving with worry permanent quality of life, knowledge and involvement of all employees in all areas.

So this form it's carries out a prospective international markets for natural products industry, always make mature cheeses defined in excellent quality cheeses such specialized niches and framed in a comprehensive management system to ensure the sustainability of the industry and satisfaction consumers.

II. THEORETICAL FOUNDATIONS NETWORK SECURITY

A. Computer Security

Computer security is focused on protecting the network infrastructure and everything related to this, so it guarantees the confidentiality, availability and integrity by protecting, classification and knowledge of impacts or damage potential threats or harmful intentions form indirect or direct to minimize risks.

Confidentiality

In computer security confidentiality means protection of information seeking prevent disclosure to unauthorized persons or systems, only allowing access to people who have their authorization.

Integrity

It means that the data values are maintained as they were intentionally placed in a system free of modifications.

Availability

The system must be kept working efficiently, be available for those who need to access it and be able to recover quickly in case of failure.

Authenticity

Allow ensure the origin of the information; the sender's identity can be validated so that it can be demonstrate what is, who say to be.

B. Weaknesses of an information system

The first three items form the triangle of weaknesses system [1]

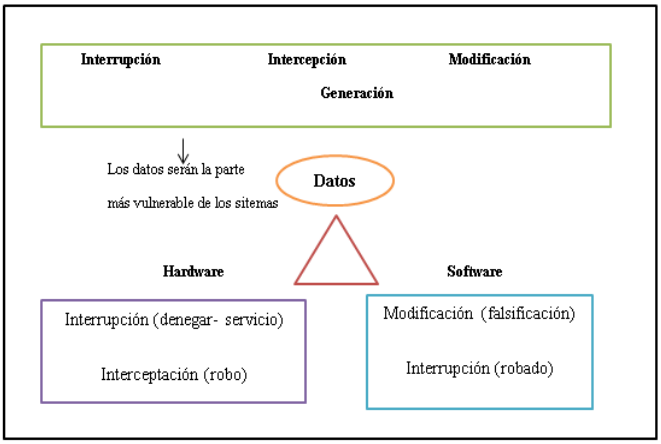


Figure 1. Triangle of weaknesses system
Source: Jorge Ramiro Aguirre. Electronic Book of Information Security and Cryptography.

- *Hardware*

May occur intermittent errors, loose connections, disconnection of cards.

- *Software*

May occur the subtraction of programs, erroneous execution, modification, defects in calls to the systems.

- *Data*

May occur Alteration of contents, introduction of false, fraudulent manipulation data.

- *Memory*

May occur of a virus, memory management, crash system.

- *Users*

May occur the suplantation of identity, unauthorized visualization access to confidential data.

C. Attacks and threats

Attack. - It's a method attempts to destabilize the functioning of the network trying to obtain unauthorized form the information.

Threats - It's anything that might interfere with the proper functioning of the network by exploiting the weaknesses of the system.

Forms of menases

Attacks on security systems are very common at four categories of attacks as discussed:

Interruption
It's an attack face to the availability. This is when the system is destroyed or becomes unavailable. The disruption may be temporary or permanent depending on how serious the threat, these attacks are faster to identify but more difficult to solve for example the destruction of a hardware element such as a hard disk, cut a communication line.

Interception
It's unauthorized to be against safety system reliability attack, this is when an entity may be (person or computer program) accessing a resource unknown. Interception is the most difficult to detect threat, so it does not produce any change in the system.

Modification
This kind of attacks are dedicated to getting alter or manipulate the information in any way authorized this is not an attack on the integrity, mainly engaged intruders change the values of a file or delete information being used taking advantage of vulnerabilities security systems.

Generation
It's an attack on the authenticity; an unauthorized entity inserts counterfeit objects in the system. Examples of this attack are inserting false messages on a network or add records to a file. These attacks can be classified usefully in terms of passive attacks and active attacks.

D. Security Mechanisms

The security mechanisms are techniques used to implement a service, that is, it is one mechanism that is designed to detect, prevent or recover from a security attack. [2]

Prevention mechanisms
At this stage its take necessary actions to prevent possible intrusion or violation of safety, allowing for increased system reliability. These actions can be performed both at the level of software or hardware.

Detection mechanisms
They are used to detect security violations or attempted violations because if you do not realize the attack damage will be greater. Example, we have the audit programs.

Response mechanisms
They are applied when a violation is detected the system as it seeks to minimize the effects of an attack or problem and eventually return the system to its normal operating mode. Example, we have the copies of the security or additional hardware.

Mechanism of forensic analysis
Allow determines the actions made by the attacker from seeing that security holes have been used to make the team, to see the actions carried out in the system, thus preventing and detecting further attacks system.

E. Security Models

To the correct implementation of information security, we must establish and maintain actions that seek to meet the three requirements for information; these are availability, confidentiality and integrity.

Perimeter security
The model of perimeter security is one of the possible methods of defense of a system that strengthen the outer perimeter of the network infrastructure based on a set of strategies and measures that allow and denying access to a determine user.

Security by darkness
A system for darkness consist in maintain in secret the existence of the network, algorithms and protocols used, so that any system can be safe while anyone outside their group security implementation is allowed to know anything about their inner workings, an example of this security model is hiding passwords in binary files assuming that "nobody will never find".

Defense of profundity
The term defense in depth (sometimes called security in profundity or multilayered security) comes from a military term used to describe the implementation of security countermeasures to form a cohesive security environment without a single point of failure. The security layers that form the strategy of defense in profundity include deploying protective measures from external routers to the location of resources, through by all intermediate points [3]

F. Security Technologies

Security technologies are aimed at implementation of different integrated systems for information security is as follows: [4]

VPN.- A virtual private network (VPN) is a technology used by large companies to facilitate the extension of the public network, so that allows a secure connection without any risk restricting information to people outside the company or organization. [5]

NAT. - NAT has the task of translating the private IP network to a public IP so that the network can send packets to the outside; and then do it in reverse order, after translate the public IP, back to a private IP desktop.

Firewall.- is a system or group of systems (software or hardware) that allows or denies different services from the outside, that is, which is connected between the network and cable internet connection letting only authorized traffic from and outward as shown in Figure 2.

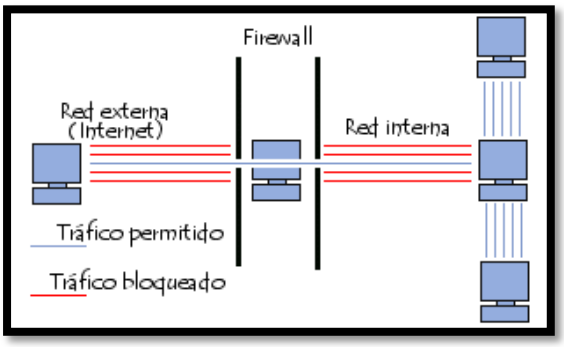


Figure 2. Implementation of a Firewall
Source: Security of Linux Rec overed from: Mohan, K., Seagren E .,& Alder R.(2008)

Intrusion detection systems
They are an essential part of the security firewall; monitor the activity of these systems in search of violations of security policies, such as denial of service attacks, subtraction or modification of information [6].

- ✓ HIDS (Host-Bases Intrusion-Detection System)
- ✓ NIPS (Network Intrusion Prevention System)
- ✓ NIDS (Network-Based Intrusion Detection System)

In the figure 3, its show the function of an intrusion detection system.

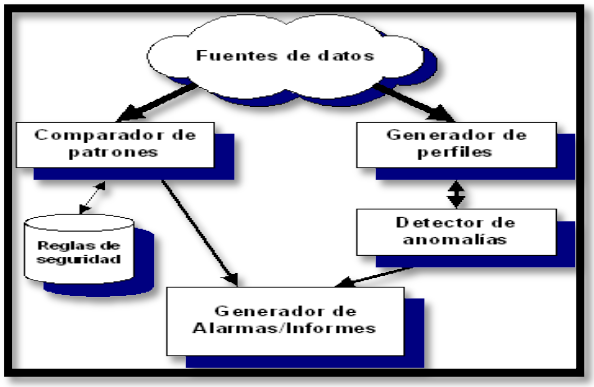


Figure 3. General scheme Intrusion Detector System
Source: Intrusion detection elements Recovered: http://www.dgonzalez.net/papers/ids/html/cap02.htm

G.Computer Security Standards

Security standards are a tool to support the management of information security, as the increasingly complex environments require models that manage technologies holistically; however, there are various models applicable to the security administration. [7]

International standard ISO/IEC 27001

According (International Standard ISO / IEC 27001), say that: International standards are a good guide that provides a model for implementing, operating, monitoring, reviewing, maintaining and improving a System Management Information Security (ISMS). The design and implementation of an organization's ISMS is influenced by the needs and objectives, security requirements, the processes employed and the size structure of the organization.

Adopt a model to be applied to ISMS processes, such as the PDCA model (Plan-Do-Check-Act). Figure 4 shows the development process of implementing an ISMS:

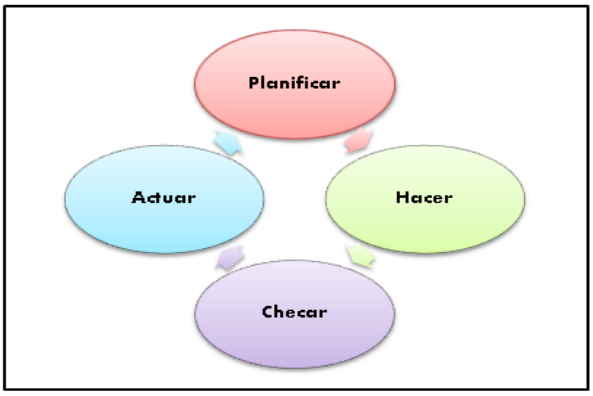


Figure 4. Development model PDCA
Source: Management Model (wall, 2010) Retrieved from:http://goo.gl/poG11L

PDCA model
Then we will describe the activities performed in each of the four phases of the PDCA cycle.

- Plan

This phase establishes policies, objectives, processes and procedures relevant to improve risk and improve information security. Security policies that consider the requirements which can then be approved by management or management.

- Do

This phase covers the implementation of the policies, controls, processes and procedures that reduce the risk to levels considered acceptable.

- Check

During this phase different types of reviews are carried out to verify the correct implementation of the system, ie, evaluate and measure the performance of the process compared to the policy objectives and thus report the results to management for review.

- Act

Take corrective and preventive actions based on an internal audit to improve the ISMS, communicate the actions and improvements to all interested parties with the appropriate level of detail and agree on how to proceed, it is also important to ensure that the best introduced achieve the objectives.

Areas and controls
The standard is being developed in 11 areas or domains that collect the 133 checks to follow.

- Security Policy.
- Organization of information security.
- Resource Management.
- Safety of human resources.
- Physical and environmental security.
- Management of communications and operations.
- Access control.
- Information systems acquisition, development and maintenance.
- Administration of security incidents.
- Managing business continuity.
- Legal framework and best practices.

III. ANALYSIS OF ACTUAL INFRASTRUCTURE FLORALP NETWORK DATA

A. Study of the Actual situation of the network

As shown in Figure 5 is a flat network which makes use of multiple IP's, along directions not have a hierarchical model so then each detailed networking equipment.

There are two routers a Cisco 1700 CLARO provider and provider Cisco1800 CNT which are owned by each provider.

On the distribution side there is a Cisco-Linksys WRT110 router where this makes use of one of the four IP's public, therefore, this channel will not be filtered by any safety equipment such as firewall IDS / IPS (System Intrusion Detection and Intrusion Prevention System), represents a great vulnerability in terms of traffic that can enter or leave through this link.

Two IP public's provider Claro are used, one for the service LIFESIZE and other IP for KYPUS server where this offers the service of Firewall designed to prevent unauthorized also access this equipment is connected to the switch Linksys SF

2000 which also provides the service of connecting users to the external network.

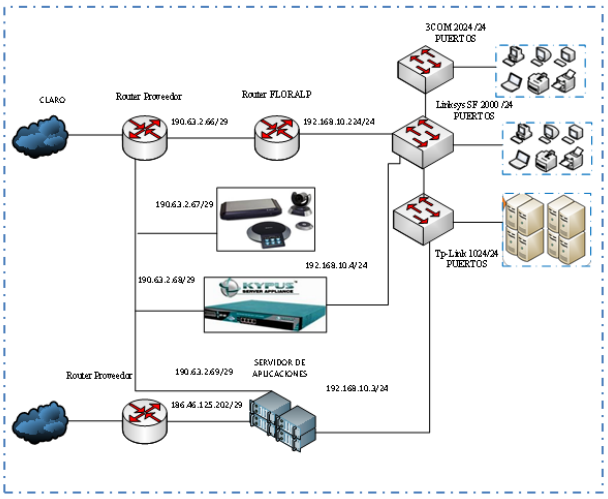


Figure 5. Network topology diagram
Source: Graphing Microsoft Visio 2010 by Gabriela López

In reference to the access distinguishes two layers: the first formed by 3Com 2024 switch that is located for the plant that is connected via fiber optics to the Linksys switch SF 2000 for administrative floor and the second by the Tp-Link switch 1024 for connecting servers, where they give service to users.

B. IP Address

The data network used FLORALP industry's 10 public IP addresses ranges described in Table 1 below.

Table 1. address IP's Public

PUBLIC IP	MASK	DESCRIPTION
190.63.x.x	255.255.255.0	FLORALP ROUTER
190.63.x.x	255.255.255.0	LIFESIZE
190.63.x.x	255.255.255.0	EXTERNAL NETWORK
190.63.x.x	255.255.255.0	APPEON
190.63.x.x	255.255.255.0	WITHOUT USE
186.46.x.x	255.255.255.0	APPLICATION SERVER
186.46.x.x	255.255.255.0	WITHOUT USE
186.46.x.x	255.255.255.0	WITHOUT USE
186.46.x.x	255.255.255.0	WITHOUT USE
186.46.x.x	255.255.255.0	WITHOUT USE

Source: Provided by the Systems Department.

C. User Access

Users when they handle the information are not responsible because they do not have any guidelines of security policy for protecting it. In addition, the information they hold is vulnerable because unauthorized people outside the industry have access without any problems, so they have no privilege during the time of use of FLORALP network.

D. Network elements

The main network elements that are part of the infrastructure of the same are shown in Table 2 below.

Tabla 2. Descripción de los Rack's

Quantity	Network Element	Location
5	Physical servers	Rack 2
2	Router	Rack 1
1	Managed switch	Rack 1
1	Unmanaged switch	Rack 2
2	Unmanaged switch	Rack 3
1	Central PBX	Rack 1
	Equipment Provider	
2	CLARO	Rack 1
1	Router	
	ODF	
2	UPS	Rack 2
1	Monitors	Rack 2
	CNT Equipment Supplier	
1	Router	
1	ODF	Rack 2

Source: Provided by the Department of Systems

E. Servers

A server is a computer that is part of a network and provides services to other client computers, specializing in very high processing capabilities, responsible for providing different services to data networks, both wireless and wire-based; these servers have systems that allow them to resolve certain failures automatically and alert systems to prevent failures in critical operations data because they must be on 365 days a year, 24 hours a day.

- Domain Server
- Application Server
- Backups Server
- DHCP Server

F. *Measuring network traffic*

To have a real understanding of what is the current status of the network has conducted monitoring of each IP information to determine what ports and protocols are used within the internal network. To monitor has it taken into account different monitoring tools that can be used also must consider what kind of aspects are to be monitored, so among the most considered for the realization of this project are:

• *Bandwidth*

In Figure 6, the bandwidth consumption is observed for a month where you can see four peaks between the hours of

9:30 a.m. to 10:30 a.m., 11:30 a.m. to 12:30 p.m., 4:00 p.m. to 4:30 p.m. and 4:30 p.m. to 5:30 p.m. where more congested network information is performed.

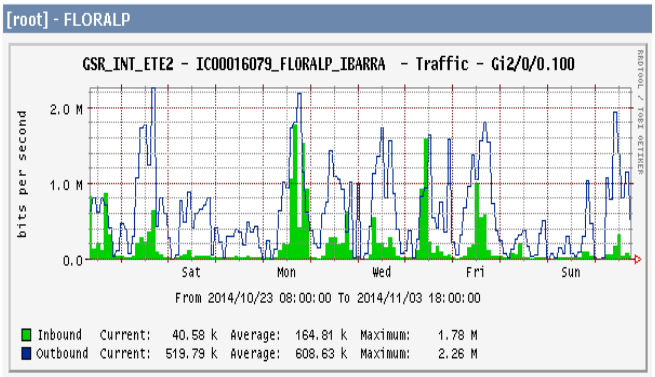


Figure 6. Bandwidth consumption for one month
Source: Results obtained using the MRTG monitoring software provided by a CLARO public IP.

- *Types of Ports and Protocols.*

The following Figure 7 a statistical table showing us what kinds of protocols are used by all users and belong in the range 192.168.10.0/24 is performed.

- *Services used*

The analysis of this parameter is performed by the data obtained from monitoring ports and protocols which contain the graphs of statistics that indicate the type most commonly used services within the network with which it is determined that the HTTP protocol SMTP, and POP3 have a high percentage on the basis that users make use of services provided by each as email, call or transfer files using Skype and access to server applications is done through a website.

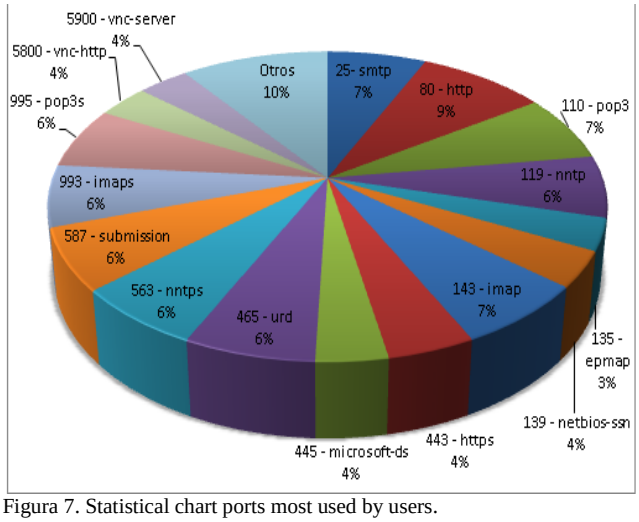


Figura 7. Statistical chart ports most used by users.
Fuente: Data obtains through the tools NTOP and Wireshark

IV. DESIGN PERIMETER SECURITY SYSTEM TO DATA NETWORK.

A. Approach security policies

Before making a design of a perimeter security system is important to know what resources and services are provided by the network. So you must perform a document attesting to all network security policies. This document will consist of controls and objectives using the PDCA model to establish the policies, management and accountability of the network, the design of a model of security and contingency plans or action plans in the event that security has been violated.

B. Security Policies

Security policies are rules that provide insight into the network behavior with regard to information security, each definition to perform procedures and plans that protect network resources both in losses and damages that may arise.

A very important part of policy development is that these should be well concise and effective because much depends on them that the industry can protect all your information. For the network administrator to draw up the document security policies should be aware of what services and resources are used by most users and thus allow you to prioritize which types of users can access and which will restrictions.

C. Development of controls and ISMS policies related to information security

Each of the policies pursued in this document is developed with the support of the Head of department. The different objectives, policies and controls used in this project are:

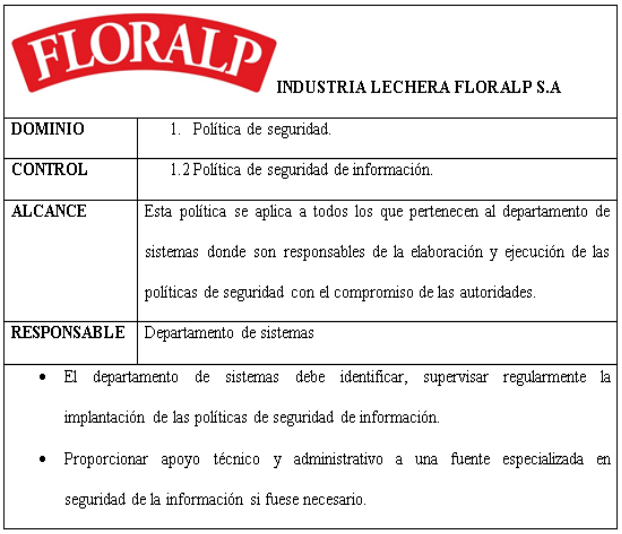
Goals
Create policies to ensure the proper use, handling, integrity, accuracy and preservation of information industry, and protect against modification, disclosure, manipulation or unauthorized or accidental destruction.

Ensure the privacy of personal, sensitive or critical information industry, its employees and their beneficiaries, thus providing penalties for misuse or loss of confidential information industry occurs.

Scope
These policies apply to all departments of the industry who have access to computer equipment and / or information systems, entering, create, process or have custody of information.

Responsibility
They are responsible for all managers and department heads, staff and employees to observe and enforce the policy of information security within the area of their responsibility and

therefore enforce the personnel under his charge. The following Figure 8 can watch a posed policy.



INDUSTRIA LECHERA FLORALP S.A

DOMINIO	1. Política de seguridad.
CONTROL	1.2 Política de seguridad de información.
ALCANCE	Esta política se aplica a todos los que pertenecen al departamento de sistemas donde son responsables de la elaboración y ejecución de las políticas de seguridad con el compromiso de las autoridades.
RESPONSABLE	Departamento de sistemas

- El departamento de sistemas debe identificar, supervisar regularmente la implantación de las políticas de seguridad de información.
- Proporcionar apoyo técnico y administrativo a una fuente especializada en seguridad de la información si fuese necesario.

Figure 8. Raised policy
Source: Approach to security policies FLORALP industry

D.Selection software firewall based on the IEEE 830 standard.

Analysis of possible solutions OPEN SOURCE

The possible solutions open source detailed.

- CentOS
- Ubuntu
- Debian

Qualification for each software solution for perimeter security
After performing the measurement at each requirement based on the IEEE 830 standard, we proceed to the respective comparison of each software solution for implementing the security system.

Table 3. Rating for each software solution

REQUIREMENT	CENTOS	UBUNTU	DEBIAN
REQ01	1	1	1
REQ02	2	2	2
REQ03	1	1	0
REQ04	2	1	1
REQ05	2	1	1
REQ06	2	1	1
REQ07	1	0	1
REQ08	1	1	1
REQ09	2	1	1
REQ10	1	0	1
REQ11	1	1	1
REQ12	1	0	1
REQ13	1	0	0
REQ14	1	0	0
REQ15	1	2	1
REQ16	0	0	1
TOTAL	**20**	12	14

Source: Compiled by author

Once the rating of each request made was observed that the highest scoring software is CentOS, reliability and stability of this tool allows the implementation of perimeter security system.

CentOS among its important features is highlighted by the high use as servers and high compatibility with operating systems, applications and services; greater reliability, communities, technical support for troubleshooting, efficiency of network management, a high degree of information processing and a wide range of platform support, therefore, CentOS makes the best option to solve Informatic security.

E. Selection software to intrusion detection system based on the IEEE 830 standard

Analysis of possible solutions OPEN SOURCE

The possible solutions open source detailed.

- SNORT
- SURICATA

Qualification for each software solution for perimeter security

After performing the measurement at each requirement based on the IEEE 830 standard, we proceed to the respective comparison of each software solution for implementing the security system

Table 4. Rating for each software solution IDS

REQUIREMENT	SNORT	SURICATA
REQ01	1	1
REQ02	1	0
REQ03	1	1
REQ04	2	1
REQ05	1	0
REQ06	0	1
REQ07	1	0
REQ08	2	1
REQ09	1	1
REQ10	1	0
REQ11	1	0
REQ12	1	1
REQ13	2	1

Sourse: Made by Author

Once it realized the qualification of each requirement is noted that the software with the highest score is Snort, the degree of integrity to the rest of IDS provides an effect to provide reliability and adaptability to different platforms or environments so it is a perfect addition to the system perimeter security.

Snort allows administrators and managers can observe and understand what they are told this tool revealing problems before loss occurs, So Snort makes the best choice for the detection and solution of anomalies within the network infrastructure.

V.IMPLEMENTATION OF PERIMETER SECURITY SYSTEM TO DATA NETWORK

The basis to the implementation of perimeter security system is the following points:

- Network Topology
- Addressing Plan
- Location servers and access points
- Analysis of network devices in order to identify the aspects of hardware and software that may affect the implementation

A. Design of the location of the perimeter firewall IP routing network cards firewall

For the new network design has it been considered a new IP address that allows the user to identify each server interface that is connected to the network infrastructure, remains a single network segment because the number of users isn't high, so, to avoid wasting IP's addresses.

Table 5. Addressing server Firewall

Equipment	Interface	IP	Mask	DNS
FIREWALL SERVER	eth0	190.63.2.66	/28	200.25.207.114
	eth1	192.168.20.1	/24	200.25.207.114
	eth2	192.168.20.254	/24	200.25.207.114

Source: Addressing IP realized by Gabriela López

Design and analysis of environment server of perimeter security

The perimeter firewall assumed important roles in the industry in this case is used as a firewall to establish a security methodology led to both internal and external traffic to the network. The network requirements are:

- Ensure access and reliability to the network.
- Maintain the confidentiality and integrity of information transmitted.
- Secure and fast access to internal servers.

Basic description of the work environment of the perimeter firewall

The perimeter firewall will be in the midst of the router CLEAR provider, the switch Linksys Switch SF 2000/24 and ports10 TP-LINK 24 / 100Mbps, this server will have three network interfaces, WAN call will be sticking up the Internet, the other is called DMZ where are located all servers in the industry and the latest is called LAN interface that will handle the internal network where all users are located and identified wireless devices within the network. As it's shown in the Figure 9.

Firewall server

Iptables rules to be applied to ensure internal and external network are:

- Allow traffic to the internal interface.
- Allow internal traffic.
- Make masking the external network to the internal and vice versa.
- Allow access from LAN to WAN via the following ports.
  - ✓ HTTP www Port
  - ✓ FTP Port
  - ✓ SSH Port
  - ✓ POP3 and SMTP e-mail Port
  - ✓ Design of network topology HTTP www Port.
  - ✓ FTP Port
  - ✓ SSH Port
  - ✓ POP3 y SMTP e-mail Port

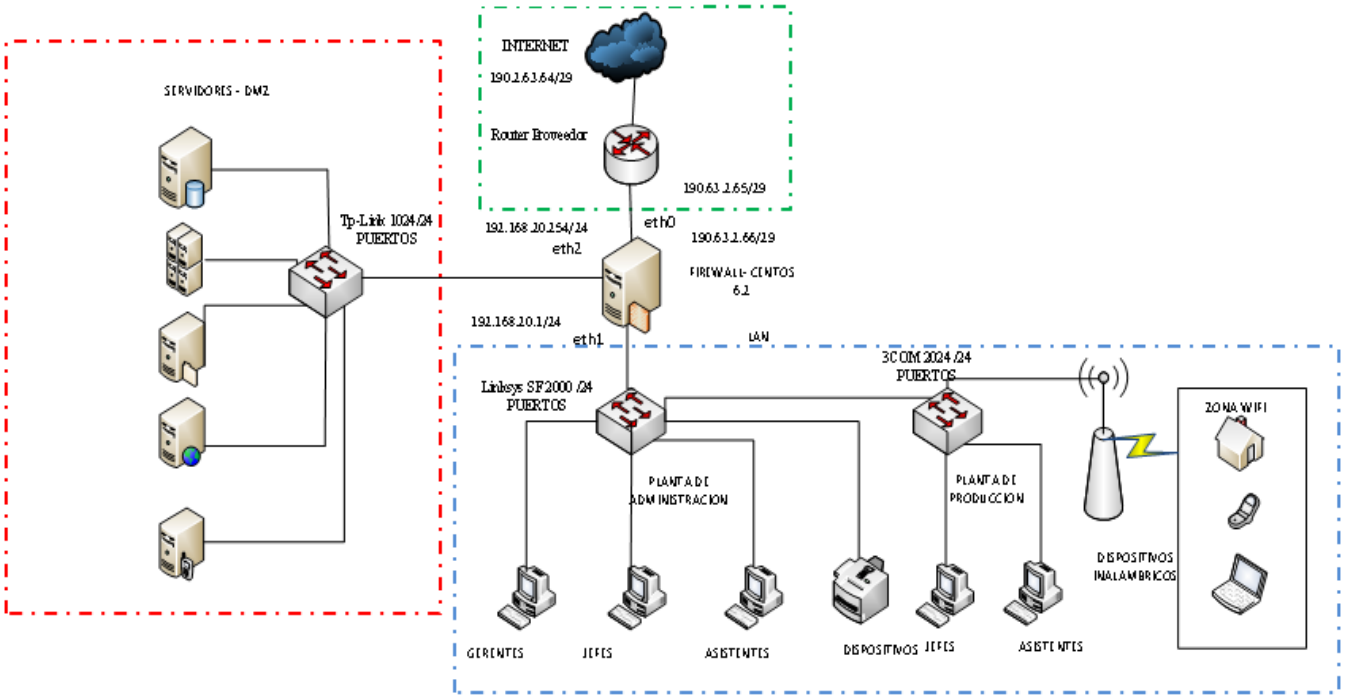


Figure 9. Design of network topology
Source: Graphic in Microsoft Visio 2010 realized by Gabriela López

B. Location of the IDS inside the network topology

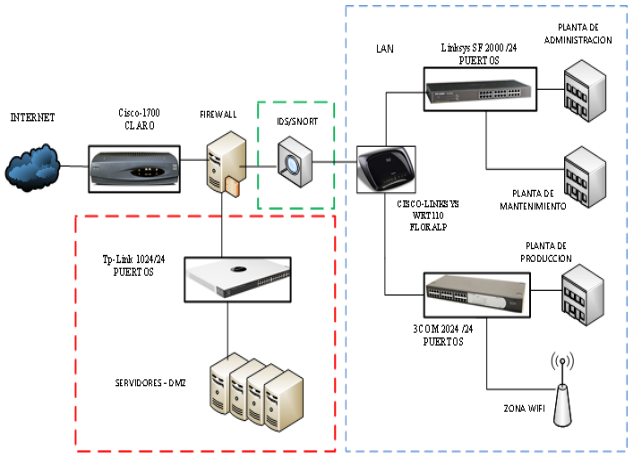


Figure 10. Location of IDS
Source: Graphic in Microsoft Visio 2010 realized by Gabriela López

Requirements for the installation of snort

Apache.- It's a HTTP web server platforms open operating systems such as UNIX and Windows NT code. Its purpose is to provide a safe and efficient current server that provides HTTP services and configurable PHP support for database applications like MySQL (Camelo, 2010).

PHP.- It's an open source language very popular especially suited for Web development, including its important features is compatibility with databases like MySQL.

MySQL.-It's a relational database management system, multithreading and multi-user database, which uses output module alerts provided by the IDS. You need to have alerts stored in a database to maintain good system performance.

BASE.-It's a PHP web interface for managing in an easy form and comfortable databases generated by IDS security, firewalls, and monitoring tools.

VI. TESTS AND RESULTS

The respective functionality testing each of the services implemented in the data network, in order to observe and verify proper performance is realized. For this purpose, it intends to make the simulation of certain computer attacks and the establishment of a set of rules to filter specific traffic

A. Development of squid testing service.

Access the web page defined in the file youtube.com social sites.

Then you enter the website www.youtube.com defined in the file social sites because there is competition, as shown in the

following Figure 64 the denial of this page where your IP address is a wizard.

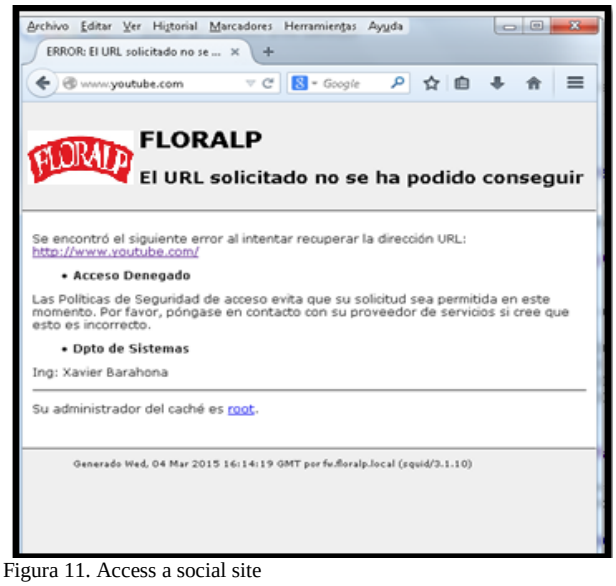


Figura 11. Access a social site
Fuente: Capture Screen access to word youtube

B. Penetration Test

To continue it's simulated many informatics attacks which are usually committed within the information security including: DoS attacks, ARP drainage and brute force. Moreover they listed the steps and tools that make use for execution within the data network of FLORALP industry.

To realize these tests should be considered in this case software has been chosen Kali Linux which is nothing more than a free advanced distribution based on Debian to penetration testing and security audits.

The penetration test is done through a series of stages for simulating attacks in controlled scenarios allowing evaluating the safety of the security system, so, finding the weak and vulnerable points of the network.

In the following figure 13 indicates the phases of a penetration test.

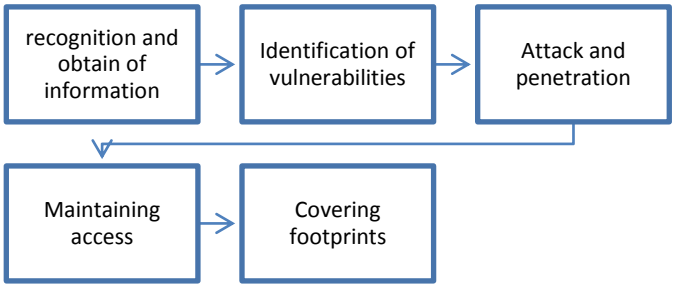


Figure 12. Anatomy of a penetration test
Source: Computer Attacks, Recovered of http://goo.gl/VCc6Ef

Exploration phase

Port scanning and host

This is made by Kali Linux tool where you can view that host are using the following command.

nmap –sn 192.168.20.1/24

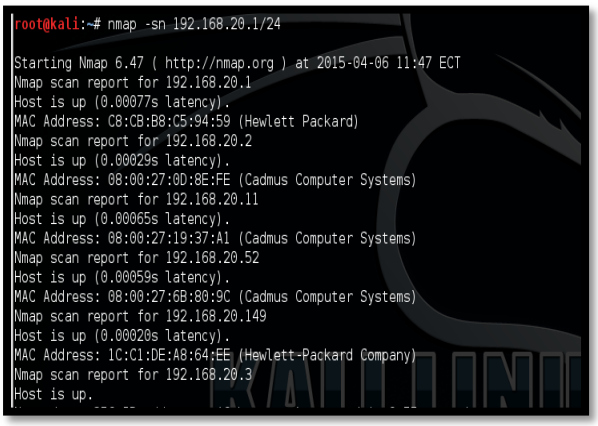


Figure 13. Scan of host through Nmap
Source: Exploration of host through Kali-Linux

In the figure 15 shows the deployment of alert Snort:

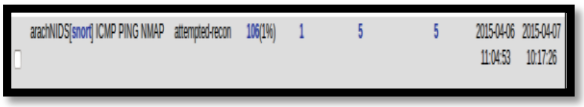


Figure 14. Alert in Snort
Source: Capture of the alert by Snort

After to realize different attacks, before told Snort above all anomalies identified thus gives us a statistical of the scanning of anomalies through its sensors.

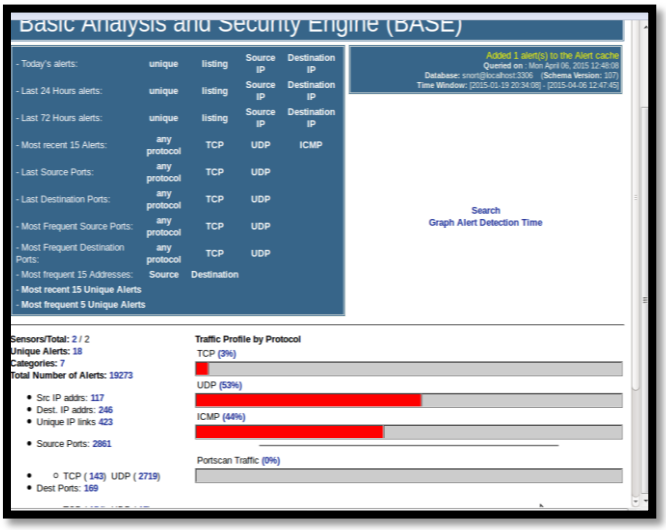


Figure 15. Alert in Snort
Source: Capture of the alert by Snort

To say penetration test relates allowed certain techniques offered Kali Linux simulate an environment for execution of internal attacks, where they were discovered by certain common tests such as denial of service, drainage ARP and brute force attacks where they succeeded because the network at that time didn't count with any security

VII. ECONOMIC ANALYSIS

A. Budget reference

To give a solution low-cost to the industry with a reference budget of equipment, installation, configuration of perimeter security system is done. This project to have a system under free software, which is a safe and free platform, allows a reliable and economical alternative.

Detail total cost referential

The total cost benchmark for the implementation of perimeter security system has taken all the equipment and tools were new, whereas in case of implementation in another branch.

The total project is the sum of the components for installation of perimeter security system is $ 4,946.00 if not count on the teams.

But it is important to reuse technology so have not taken certain equipment because existing within the network infrastructure and the cost would be in a total of $ 2,180.00 All prices are subject to change, given that they were listed with the date of May 2015

B. Cost-benefit

Cost-benefit calculation

For the cost benefit analysis of the project it is necessary to analyze the costs incurred in implementing perimeter security system and the benefits generated by the project to its implementation by making use of existing technology, for which we use the following equation*:*

$$\frac{B}{C} = \frac{\sum Benefits}{\sum Costs\ and\ Expenses}$$

After to analyze of the cost, spend and benefits generate the project applied the formula for determining the cost benefit, for which are used the following evaluation parameters:

Replacing the values in the formula are:

$$\frac{B}{C} = \frac{\sum Beneficios}{\sum Costos\ y\ Gastos}$$

$$\frac{B}{C} = \frac{2766.00}{2180.00}$$

$$\frac{B}{C} = 1{,}2$$

All results obtained indicate that it's feasible and profitable implement this present project.

Beneficiaries

Security usually isn't an investment that generates a profit, this is loss prevention. In other words, when you invest in security, the institutions do not expect profits, the goal is to reduce risks to information, in order to minimize the amount of data loss thanks to the investment made.

The beneficiaries of this system would be all users who belong to the various departments that make use of the services offered by the data network because all the information you are driving, and would be better protected.

Other benefits are the restrictions on user access to sites that eventually generate damage and limiting the use of bandwidth for applications that are keys to the industry.

Thanks to the use of free software provides high-level services without paying any price to the acquisition of allowing himself to be very competitive with paid software.

CONCLUSIONS

Must have theoretical bases to give us enough information about what are the main characteristics of a perimeter security system as the basis for the realization of this project, because this will be a source for future research interested about security of information.

The analysis of the type of traffic that is circulating inside the network infrastructure allows us to know the services and protocols that each user handle, so, you can determine the requirements for the design of perimeter security system .

To design of perimeter security system has taken into account the ISO / IEC 27001norm to the development of security policies, because a process of continuous improvement that allows us to have an agile and flexible scheme that follows meets the requirements of the industry.

The analysis of different software platforms based on the IEEE 830 standard software requirement specifications allows selection of the best alternative that meets the design requirements perimeter security system.

The use of free software in private institutions has become a fundamental factor in the management, administration and security of information technology because it uses very few

resources of memory, processor and disk space of the computer, allowing the reuse of resources and reduction of costs by the industry by not having to acquire new equipment.

Through implementation service Proxy Cache Squid allows content filtering and caching capacity, it succeeded in increasing the response time in navigation and avoid saturation of the internet channel, keeping a real-time monitoring and statistics daily navigation.

Snorts are IDS software great acceptance, powerful and free allowing us to know when it is being attacked by sensors that realize constant monitoring.

The IDS integration identified successfully simulated attacks with tool, Kali-Linux ethical hacker, which is widely used for a penetration test on the network, verifying their efficiency against a series of tests with diverse techniques.

We are conscious there isn't a system that provides complete protection, but to continuous improvement and adoption of methods and standards of information security is maintained an acceptable level of security reduces the risk of the network.

REFERENCIAS

[1] Aguirre, J. R. (2006). Libro Electrónico de Seguridad Información y Criptografía. Madrid-España.

[2] Estrella. (Abril de 2010). Mecanismos de Seguridad. Recuperado el Septiembre de 2014, de http://www.buenastareas.com/ensayos/Mecanismos-De-Seguridad/229947.html

[3] VINUEZA, T. (2012). HONEYNET VIRTUAL HÍBRIDA EN EL ENTORNO DE RED DE LA UNIVERSIDAD TÉCNICA DEL NORTE DE LA CIUDAD DE IBARRA. Ibarra.

[4] Manuel, I. L. (30 de Mayo de 2013). SliderShared.com. Recuperado el 31 de Marzo de 2014, de http://es.slideshare.net/MelvinBrian/seguridad-en-profundidad

[5] MICHILENA, M. A. (2013). METODOLOGÍA DE SEGURIDAD INFORMÁTICA CON BASE EN LA NORMA ISO 27002 Y EN HERRAMIENTAS DE PREVENCIÓN DE INTRUSOS PARA LA RED ADMINISTRATIVA DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA. Ibarra.

[6] Seguridad, F. d. (s.f). Fundamentos de Seguridad Informatica. Recuperado el Octubre de 2014, de http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/Estandares.php

[7] Torres, V. (13 de Marzo de 2012). Ciber Informatico. Recuperado el 6 de Abril de 2015, de http://ciberinfosystem.blogspot.com/2012/03/anatomia-de-un-ataque.html

Gabriela J. López P.

She was born in Ibarra – Ecuador January 5 1989. Realized her primary studies at "María Angélica Idrobo". In 2006 years she got her Bachelor's title in mathematics physical sciences at "Teodoro Gómez de la Torre" high school. Nowadays, almost over Engineering in Electronics and Communication Networks career at North Technical University Ibarra city.