Model for the Implementation of Security in Wi-Fi Networks for SMEs

Diego Vega¹, Andrés Lozano¹, Fabián Blanco¹ and Fredys Simanca²*

¹Escuela de Comunicaciones del Ejercito, Bogotá, Colombia
²Universidad Cooperativa de Colombia, Bogotá, Colombia
*Email:fredys.simanca@campusucc.edu.co

Abstract. In the last decades, the computerized handling of data has played a fundamental role in different economic areas, since there are several technological instruments that help to speed up a number of processes, so it is of utmost importance to learn how to use these tools, otherwise the information would be compromised. This paper aims to present a model for small and medium enterprises, through a process of identification and analysis of security measures in companies, based on the study of each company and in relation to the size of each organization, allowing to know the concepts of network monitoring that are applied in the creation of strong security policies for their facilities.

1. Introduction
The evolution of technologies has allowed more accessibility to computer systems, these advances have allowed people to have any kind of information at their fingertips, causing in turn, a risk linked to security. The Internet has allowed the use of different communication tools, such as email, instant messaging, information in the cloud, connection with databases, thus opening possibilities for greater contact with customers, presenting better trends in the industry and all its competitive developments [1]. In this sense, it is important to have the data digitized, since computers are of great help to process data, both in the creation, editing and search of them, which helps the company to be more competitive and effective.

Behind the benefits that technologies offer, it is of great importance to consider the data security issues related to the information systems, gaining great importance the computer security. Nowadays, it is very easy to pass the security filters of the companies, in which the integrity of the network structure and the information is exposed. As it is expressed in [2], it is necessary to create a security culture in the companies, where the employees must know the importance of protecting the information, in addition to having restriction of sites that are not suitable, data protection policies, safe storage means and use of passwords.

It is important to emphasize that companies are migrating from a traditional wired network model to a wireless network model, which brings great benefits to the business, such as cost reduction, civil construction work and furniture adaptation. Based on this, the search for strategies that allow for greater security becomes an indispensable task in the control of cyber-attacks and information theft.

It should be noted that wired networks do not offer flexibility in connection, but are more secure for any organization [3] making it a transmission less vulnerable to communication processes, the wireless network allows the connection of a large number of computers that access it, physical obstacles and location, seeking that the solution to the difficulties of network security there are various protocols such
as WEP, WPA, and WPA2 that have an encryption, which seek that no person has access to the provider equipment. It is important to note that this must have sufficient security features and shielding required for the solution of these problems, therefore, this article will be a model for the implementation of Wi-Fi networks in SMEs in the city of Bogota.

1.1. State of the Art
Ronald Reagan, former president of the United States, could have been the creator, together with the CIA, of the first computer virus, with the aim of sabotaging the industries of the USSR with defective technology [4]; Kevin Mitnick, was the most famous computer hacker in the United States, for stealing files from prestigious companies and breaking into various systems, using various methods to prevent the security of computers [5]; Carnivore, an FBI program that allowed the reading of electronic messages and communications from alleged criminals, was severely criticized by privacy advocates [6]. These facts make it necessary to prepare companies for such situations, both through training and by providing technologies and implementing security policies that can help in these situations.

Reviewing previous studies, it is important to take into account that different espionage techniques have been perfected to allow any person to be a carrier of a malicious code, being a threat to companies and the information existing in them [1]. It is confirmed that the objective is to equip small and medium enterprises with few in-formation and communication technology personnel, with low-cost solutions that help evaluate the quality of its infrastructure, in order to detect possible errors in the architecture and security policies of its networks, thus obtaining results with simulations of the local networks allowing the traffic of the ports 80, 21 and 1024 for the exchange of file server-client.

However, there are companies that do not have the capital to invest in information and communication technology personnel or people to train their collaborators. Despite this, it is important to invest in technological resources that provide security and encryption in companies such as Backus, intrusion detection systems, fire-walls, taking into account personnel training, these being one of the main problems in information leakage in companies [7]. At present, the objective of information security should also cover the human resources of a company, as shown by news types, impersonation generated by a worker selling company information, including factors such as lack of knowledge of the laws protecting information, which vary depending on the country.

Very often, SMEs choose Wi-Fi models as the main network topology, without thinking about encryption and decryption techniques of passwords. New applications are created with the ability to violate wireless systems, and as security there are different encryption systems that vary in their level of security and characteristics.

It should be noted that the WIFI networks [8] are wireless networks based on radio emissions, which allow users to use in a limited environment, with similar foundations unlike wired networks, and this technology is based on the IEEE 802.11 standard.

Looking for a solution, the recognition of the security of the protocols of the data transmitted by a WLAN so that they cannot be decrypted by someone outside the network, as expressed in Table 1 [9], this must have an encryption and key management algorithm.

| Encryption            | Security |
|-----------------------|----------|
| WEP Wired Equivalent Privacy | Very low |
| WPA Wifi Protect Access | Very low |
| WPA2                  | Low      |
| WPA-PSK               | Intermediate |
| WPA2-PSK              | High     |
| WPAWPA2-PSK           | Very High |
According to [10], in order to secure a wireless network, it is important to know what the types of attacks are:

Passive. This is where information, spying, eavesdropping, wardriving and pass-words are obtained.
Active. Modify and create false transmission data flows, to impersonate or col-lapse the network.

Based on the above, companies must audit their networks in order to create security protocols on the network or hardening that prevent unauthorized access to computers or servers. According to [11], the aim is to secure the system by reducing vulnerabilities through the elimination of software, services, users, unnecessary system files, as well as closing ports that are not in use.

For [12], one of the main threats that can affect a wireless network is: Wi-Fi pass-word cracking, fake hotspots, malware placement, spying, data theft, inappropriate and illegal use and bad neighbours.

Wireless networks are being used in different business environments, to reduce wiring and structure costs. It is essential to carry out an analysis on network security, to avoid information theft or computer attacks that can affect the proper functioning, so this article presents an analysis of the SMEs in Bogota against the management of wireless networks in order to provide a guide for the implementation of Wi-Fi network security.

2. Materials and Methods

This section describes the materials and methods for the security analysis of Wi-Fi networks in SMEs, and expands on the methodology and design used to carry out this analysis, which served to carry out the different practices and data analysis.

2.1. Design of the Model

For the design of the model, information was collected to allow the study of the problem, in which data of great importance was gathered on how companies use computer security systems in the use of Wi-Fi networks.

For this phase, the consulted literature included a compilation of different problems that could occur in the security of Wi-Fi networks in SMEs and the legal measures on data theft and virtual security. With the results found in the research, it was possible to develop the guide for the implementation of security policies, in order to control access to Wi-Fi networks in companies.

2.2. Research

The research was carried out in the city of Bogota. 108 SMEs that had technology areas or departments were surveyed, conducting a pilot survey to determine whether or not the implementation of the proposed model was required. In this way, a diagnosis was made to determine the level of security of Wi-Fi networks and which controls should be implemented.

Two surveys were designed, the first one for filtering with 12 questions and the second one for diagnosis with 34 closed questions, regarding aspects such as system security, guest and employee access to the wireless network, technology used and control techniques for mobile services access, as well as the existence of internal security protocols and policies.

2.3. Analysis

The results obtained from the 108 surveys carried out on the SMEs showed that 80% of them use a network design for corporate use, the rest do not use it for that purpose.

Of the companies that use network design, 59% have not implemented the WLAN and continue with the traditional wired network model. 38.8% believe it is important to have a systems department that manages the WLAN networks, but 41% do not have qualified personnel for the administration and implementation of the Wi-Fi network. According to these results, companies do not take the necessary measures to prevent cyber-attacks since 51% of companies do not believe they are vulnerable to any type of attack.

Based on the previous results, it is necessary to create a model of implementation of Wi-Fi network security in SMEs, seeking to make an analysis of the risks that a company can have, being 69% of the
total companies surveyed those willing to implement the proposal of work and make the respective diagnosis.

3. Results
As a result of the needs of businesses with regard to the security of Wi-Fi networks, given the conditions mentioned above, it is necessary to have a baseline that meets the needs of small and medium businesses. This is how the following objective was set: to select from the guide provided by NIST 800-153 [13], the recommendations applied to Wi-Fi networks in small and medium businesses in Colombia.

The implementation model is composed of 4 phases:

**Phase 1:** Diagnostic survey. A form was used to develop the diagnosis.

**Fill out a survey.** It allows to fill out the survey for the first time, it is divided into several sections to have detailed information about the company: a) Identification of the company, b) Identification of the elements of study, c) Infrastructure, d) Security analysis and e) Security policies.

**Consult diagnosis.** Results can be consulted with the company’s NIT. A risk assessment matrix is presented according to the answers given in the survey.

**Phase 2:** Recommendations for the implementation of infrastructure for Wi-Fi networks. This phase shows a basic network architecture for an SME company; the main components of the network were clearly and precisely defined (see Figure 1).

![Figure 1. Architecture of a Wi-Fi Network.](image)

Based on the above, the aim is to identify the function that each of the computers fulfills within the network (Table 2).

**Router.** Equipment in charge of routing traffic to allow navigation towards the internet

**Firewall.** Allows traffic from the internal network to the external network and vice versa, filters traffic by port, host or network segment

**Layer 3 Switch.** It has the same function of Router, but with several ports which allow direct connection with devices, such as servers, Wi-Fi controllers, firewall, Layer 2 switches, etc.

**Layer 2 Switch.** Connects end devices through Ethernet ports

**Wireless access point or Access Point.** Interconnects wireless communication equipment, propagates SSIDs or network names.

**Encryption password.** WIFI network password and each encryption is specified.
Proxy server. Intermediary between end users and the external network or Inter-net, filters the content of the network.

DHCP Server. Manages the delivery of IP addresses to network devices.

FTP server. Uses file transfer protocols.

Table 2. Basic Network Architecture for SMEs.

| Basic Network Architecture for SMEs | Not important | 2 | 3 | 4 | 5 |
|------------------------------------|--------------|---|---|---|---|
| Router                             |              |   |   |   | X |
| Switch                             |             | X |   |   |   |
| Access Point                       |             | X |   |   |   |
| Controller                         |             | X |   |   |   |
| DHCP Server                        |             |   | X |   |   |
| FTP Server                         |             |   | X |   |   |
| Proxy Server                       |             |   | X |   |   |
| Firewall                           |             |   |   |   | X |

Phase 3: Recommendations for Wireless Local Area Network Security. This phase establishes practices to be developed by the NIST (National Institute of Standards and Technology) [13] to implement the configuration of wireless networks. It also provides different recommendations at the level of security in the Wi-Fi network.

Configuration design. The IEEE 802.11 WLAN security configuration is performed. Figure 2 shows a simplified view, showing that the security of the components depends directly on their configuration.

Monitoring. It explains about the two types of safety supervision, evaluation and continuous monitoring.

The evaluation determines the degree of effectiveness of an entity, and is carried out periodically, for example, every year, or quarterly.

Figure 2. Simplified view of WLAN architecture.
The continuous monitoring allows the awareness of information security, vulnerability and different threats, its objective is to carry out a continuous monitoring of the security of networks, information and systems of the organization.

**Phase 4:** Templates for the creation of security policies applicable to SMEs. In this phase, formats are created for the development of security policies that can be applied to small and medium-sized companies. It includes a set of bases to define strategies, guidelines, procedures, codes of conduct and standards (Figure 3).

| POLITICA DE ACCESO A REDES Y RECURSOS DE RED | COD | WIFI-07 |
|---------------------------------------------|-----|---------|
| Fecha de elaboración                         | Definir fecha |
| Versión                                      | 1.0 |
| Fuente                                      |      |

**Figure 3. Monitoring format.**

4. **Discussion**

The importance of networks for the good functioning and communication of a company should be emphasized. Networks are constantly developing in order to improve security, speed and transmission capacity, depending on the appropriate use given to them to access good service and security, Therefore, it is necessary, as mentioned in this article, to create a model for network security, in this case of Wi-Fi networks in SMEs. The migration from traditional wired networks to WLAN networks not only requires updating and the service provider, it is also necessary to have the technological means to establish security in companies.

The organizations must bear in mind the risk that exists in front of the problems that are presented cybernetically. For this, establishing security criteria becomes important, with the use of the model for the implementation of security of Wi-Fi net-works, the companies will make a diagnosis on the threats that can present and how a continuous monitoring could be made looking for minimizing risks.

5. **Conclusions**

The advances of the WLAN networks have allowed the improvement of the connections in the business scope, the reduction of costs of wiring and infrastructure has allowed that it is welcomed in the handling of the organizations being conscious of the necessity to protect the information from the threats to which they are exposed. Therefore, it becomes necessary to establish parameters of security in the network for the care of the information and the use that is given with the wireless connections of third parties.

According to the study conducted, it became evident that the companies in the city of Bogotá that were surveyed are aware of the importance of using wireless net-works for business use, although there are no clear criteria in the design of computer security parameters, creating the need to hire qualified personnel and establishing protection guidelines.

The purpose of using the implementation guide of Wi-Fi network security in SMEs is to allow the application and correction of controls to prevent cyber-attacks or access to unauthorized persons who may steal important information for criminal purposes. Due to this, the use of tools and monitoring is necessary to reduce risks based on information security, which aims to protect attributes related to confidentiality, integrity and availability of this, guided by ISO7IEC 27001 [14]. Therefore, the
fundamental support to reach protection levels is the awareness of the personnel and the adequate use of the information resources, adopting protection mechanisms should not be considered a high investment when protecting the organizations, considering these they should take into account legal and regulatory aspects by the information security management.

References

[1] Martínez K and Pacheco J 2009 Firewall – Linux: Una Solución De Seguridad Informática Para PYMES Revista UIS Ingenierías, pp. 155-165
[2] Contreras S P G 2017 Fuga de información la mayor amenaza para la imagen corporativa Universidad Militar Nueva Granada
[3] Monsalve J A, Aponte F A and Chaparro F 2015 Análisis de seguridad de una muestra de redes WLAN en la ciudad de Tunja, Boyacá, Colombia Dyna 82(189) 226-232
[4] El país 2004, elpais.com 27 02 2004. Available: https://elpais.com/internacional/2004/02-27/actualidad/1077836408_850215.html.
[5] Orantes K 2019, estrategiaynegocios.net 05 10 2019. [En línea]. Available: https://www.estrategiaynegocios.net/centroamericaymundo/1324152-330/kevin-mitnick-de-hacker-a-mr-seguridad.
[6] El país 2005 Elpais.com 19 01 2005. [En línea]. Available: https://elpais.com/tecnologia/2005/-01/19/actualidad/1106126878_850215.html.
[7] Borghello C F 2009 Segu-Info 14 12 2009. [En línea]. Available: https://www.segu-info.com.ar/articulos/93-informes-estudios-seguridad-informacion.htm.
[8] Huidrobo J M 2005 Wi-Fi. Conectividad en todo lugar y momento Manual formativo de ACTA, 35 33-39
[9] Mendoza C, Rodriguez L M And Aguilar M 2017 Análisis de seguridad en redes inalámbricas de las MiPyME y propuesta de mejora (Revista Iberoamericana de Producción Académica y Gestión Educativa)
[10] Gonzalez A, Beltran D. And Fuentes R 2016 Propuesta De Protocolos De Seguridad Para La Red Inalámbrica Local De La Universidad De Cienfuegos (SciELO Revista Universidad y Sociedad) 8(4) 130-137
[11] Swat Security 2019 Fortalecimiento de la seguridad [En línea]. Available: http://www.swatsecurityit.com/nuestro-servicios/hardening-o-aseguramiento/
[12] Alonso R 2016 Principales amenazas para la seguridad de las redes inalámbricas 18 01 2016. [En línea]. Available: https://www.networkworld.es/seguridad/principales-amenazas-para-la-seguridad-de-las-redes-inalambricas.
[13] Souppaya M and Scarfone K 2012 Guidelines for Securing Wireless Local Area Networks (WLANs) SP 800-153, (Gaithersburg: Computer Security Division)
[14] Norma ISO 2006 Norma Técnica Ntc-Iso/Iec Colombiana 27001, Bogota: Icontec