UNIVERSIDAD MAYOR DE SAN ANDRÉS

FACULTAD DE CIENCIAS PURAS Y NATURALES

CARRERA DE INFORMÁTICA

TESIS DE GRADO

AUTENTICACIÓN PARA REDES INALÁMBRICAS WIFI CORPORATIVAS BASADO EN ÁREAS DE CONEXIÓN CON MIKROTIK

Tesis de Grado para obtener el Título de Licenciatura en Informática

Mención Ingeniería de Sistemas Informáticos

POR: DANY RUDDY HUAYHUA HUAYHUA

TUTOR METODOLÓGICO: M. Sc. FRANZ CUEVAS QUIROZ

ASESOR: M. Sc. ALDO VALDEZ ALVARADO

LA PAZ – BOLIVIA

2018

UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA DE INFORMÁTICA

LA CARRERA DE INFORMÁTICA DE LA FACULTAD DE CIENCIAS PURAS Y NATURALES PERTENECIENTE A LA UNIVERSIDAD MAYOR DE SAN ANDRÉS AUTORIZA EL USO DE LA INFORMACIÓN CONTENIDA EN ESTE DOCUMENTO SI LOS PROPÓSITOS SON ESTRICTAMENTE ACADÉMICOS.

LICENCIA DE USO

El usuario está autorizado a:

a) visualizar el documento mediante el uso de un ordenador o dispositivo móvil.
b) copiar, almacenar o imprimir si ha de ser de uso exclusivamente personal y privado.
c) copiar textualmente parte(s) de su contenido mencionando la fuente y/o haciendo la referencia correspondiente respetando normas de redacción e investigación.

El usuario no puede publicar, distribuir o realizar emisión o exhibición alguna de este material, sin la autorización correspondiente.

Gracias por enseñarme el valor de la educación y la creatividad. Por mostrarme que dónde hay voluntad, hay un camino.

AGRADECIMIENTOS

A Dios por brindarme la oportunidad de vivir una vida maravillosa.

A mi madre, por el incontable apoyo y por confiar en mí y en lo que hago, gracias por transmitirlo sin pronunciar palabra alguna.

A mi padre, por sus sabios consejos. Siempre serás un gran ejemplo de persistencia y constancia.

A mi tutor, M. Sc. Franz Cuevas Quiroz, por su guía, su apoyo y por compartir desprendidamente sus conocimientos, fundamentales para el desarrollo de la presente tesis.

A mi asesor, M. Sc. Aldo Ramiro Valdez Alvarado, por dedicar tiempo para dirigir el curso de la tesis, por su incontable paciencia, consejos, sugerencias y correcciones.

Al Ing. Omar Saire Aguirre, Gerente general de la empresa de servicios tecnológicos AGADON S.R.L. por compartir su sapiencia y experiencia, por su confianza y disposición de su equipo de profesionales para las pruebas experimentales.

A todas las personas que cada día alentaron mi viaje durante esta investigación y los años de universidad.

¡Muchas gracias!

RESUMEN

Las redes inalámbricas Wi-Fi corporativas utilizan e implementan protocolos de seguridad que permiten el acceso de los usuarios a la red y los recursos que esta brinda. Los protocolos de seguridad usan credenciales compuestas por un usuario y una contraseña, las cuales deben ingresarse cada vez que el usuario corporativo pierde la conexión de la red.

El presente trabajo propone un modelo de autenticación basado en PIN's de ingreso, los cuales serán utilizados durante y únicamente en la primera autenticación del dispositivo. El modelo propone también la implementación de áreas de conexión que permitan identificar cuándo un dispositivo se encuentra dentro y de esa manera autenticarlo de manera automática en la red corporativa. Así, cuando el usuario salga del área de conexión será desautenticado.

Otro aspecto que el modelo propone es el uso de *tokens* para agregar nuevos dispositivos, los *tokens* podrán únicamente agregar un dispositivo y además contarán con un corto tiempo de vida. Finalizado el tiempo o cumplida la acción de agregación, serán destruidos.

La validación del modelo se basa en el desarrollo de un prototipo deacuerdo a las especificaciones propuestas, utilizando la tecnología Mikrotik. Las pruebas se realizarán tomando como variable el tiempo de autenticación, dado que el grupo de estudio será sometido a dos pruebas, se utilizará un método estadístico que compare el antes y el después, a fin de medir el cambio.

Palabras clave: autenticación, redes inalámbricas corporativas, Wi-Fi, Mikrotik, PIN, áreas de conexión, token.

ABSTRACT

The wireless Wi-Fi corporate networks use and implement security protocols that allow users access to the network and the resources it provides. These security protocols use credentials composed by a user and a password, which must be entered each time the corporate user loses the network connection.

The present work proposes an authentication model based on entry PIN, which will be used during and only in the first authentication of the device. The model also proposes the implementation of connection areas that allow to identify when a device is inside and thus authenticate it automatically in the corporate network. When the user leaves the connection area will be no authenticate.

Another aspect that the model proposes is the use of tokens to add new devices, tokens can only add a device and also have a short life time. Once the time has expired or the aggregation action has been completed, they will be destroyed.

The validation of the model is based on the development of a prototype according to the proposed specifications, using Mikrotik technology. The tests will be carried out taking as a variable the authentication time, since a study group will be subjected to two tests, it will use a statistical method that compares the before and after in order to measure the change.

Keywords: authentication, corporate wireless networks, Wi-Fi, Mikrotik, PIN, connection areas, token.

INDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I

1 MARCO REFERENCIAL

1.1 Introducción

Las redes inalámbricas tienen una alta preferencia cuando se tratan de resolver problemas de conectividad en entornos corporativos. Así las autenticaciones principales se distinguen en dos grupos: autenticaciones a través del uso de credenciales y a través del uso de una clave inicial compartida (Ruz, Riveros, & Varas, 2012).

Los usuarios corporativos deben usar credenciales compuestas por un usuario y contraseña para acceder a la red, son ingresadas en un portal que captura la información, autenticando a los usuarios en caso de ser correctas. Los invitados o personas ajenas a la corporación utilizan una clave pre compartida para acceder a la red inalámbrica.

La generación de credenciales y autenticación en redes corporativas es un proceso recurrente que consume un intervalo de tiempo, que, aun siendo corto, puede destinarse para otras tareas.

Por otra parte, la red inalámbrica no suele contar con un registro activo de aquellos dispositivos que accedieron a la red, siendo en muchos casos información vital en caso de existir intrusiones, ya que puede brindar información de inicio para una posible investigación. Agregar la dirección física del dispositivo suele ser opcional, lo que añade vulnerabilidad a la red (Ballmann, 2012).

Otro aspecto que se debe tomar en cuenta es que, a diferencia de las redes cableadas, las redes inalámbricas pueden colaborar con un mayor alcance en distancia. Una mayor cobertura puede ser beneficiosa como también puede convertir la red vulnerable, también se debe notar que él área de cobertura y la velocidad de transmisión tienen una relación inversamente proporcional. A mayor distancia, menor la velocidad de transmisión (Cisco, 2017).

El presente trabajo plantea un modelo de generación y autenticación de credenciales que permita facilitar a los usuarios autenticarse de manera automática dentro de la red inalámbrica Wi-Fi corporativa, haciendo uso de la intensidad de señal del punto de acceso para definir áreas de autenticación, que colabore además con limitar el uso de la red inalámbrica corporativa dentro de los límites de las instalaciones.

1.2 Antecedentes

La transmisión de información a través de nodos inalámbricos en sus inicios fue descubierta por Alexander Graham Bell (1847-1922). En sus investigaciones publicadas describe la producción de una señal acústica por medio de la iluminación con radiación modulada de manera periódica en una celda cerrada, posteriormente fue nombrado como efecto fotoacústico (Bell, 1880). Durante ese mismo año, junto a Summer Tainter, crean un aparato de comunicación sin cables, el fotófono.

Rudolf Hertz (1857-1894) en el año 1888, realizó dos descubrimientos importantes: la propagación de las ondas electromagnéticas y el efecto fotoeléctrico. Los experimentos de Hertz en el campo probaron la existencia teórica de ondas electromagnéticas planteada por Maxwell (1831-1879) (Lamberti, 2009).

Guillermo Marconi en el año 1899 y a través del Canal de la Mancha logró establecer las primeras comunicaciones por radio, se transmitieron los primeros mensajes completos a través del Atlántico. Nikola Tesla desarrollaba la misma tecnología durante el mismo año y aunque perdió la patente de transmisión inalámbrica, fue años después de su muerte que se lo reconoció como padre de la radio (Cheney, 2009).

Se desarrollaron muchos avances durante la Segunda Guerra Mundial y en 1971 en la Universidad de Hawaii, la investigación en dirección de Norman Abramson logró crear el primer sistema de conmutación de paquetes por radio, llamado ALOHA fue la primera red de área local inalámbrica (WLAN) conformada por 7 estaciones situadas en distintas islas que podían comunicarse con un ordenador central, el principal problema que afrontaba el proyecto fue que las distintas estaciones solapen los mensajes entre sí (Márquez, Pardo, & Pizarro, 2001). Posteriormente un año después se realiza la conexión del proyecto a la ARPANET creada por el Departamento de Defensa de los EEUU.

En 1979 IBM logra transmitir información de manera local en una fábrica ubicada en Suiza, con la utilización de infrarojos, este fue considerado el punto de inicio para la evolución de las redes inalámbricas que se conocen hoy en día (Ochoa, 2010). En 1985 la Federal Communication Comission, agencia Federal de EEUU encargada de regular las telecomunicaciones asigna las bandas IMS (Industrial, Scientific and Medical) 902-928 MHz, 2.400-2.4835 GHz y 5.725-5.850 GHz a las redes electromagnéticas basadas en el espectro electromagnético.

Años más tarde en 1991 la IEEE con la norma 802 reconoció como redes LAN a aquellas redes que transmitían al menos 1 Mbps. La introducción al mercado se hizo esperar hasta que el cambio de ordenadores de escritorio a ordenadores personales móviles impulsó su implantación como una necesidad de conexión sin cables. En el año 1999 Nokia, 3com, Airones, Intersil, Lucent Technologies y Symbol Technologies se asocian bajo el denominado WECA (Wireless Ethernet Compatibility Aliance) y un año después implementan como estándar la norma IEEE 802.11b bajo el nombre de Wi-Fi (Wireless Fidelity) que sustituiría las capas físicas en la estructura Ethernet 802.3 (Griffith, 2002).

La evolución de las redes inalámbricas ha llevado a categorizarlas en cuatro grupos: WPAN (Wireless Personal Area Network) que aloja tecnologías como HomeRF, Bluetooth, ZigBee y RFID, utilizada para comunicar dispositivos en espacios cortos con tasas bajas en transmisión y consumo de energía. WLAN (Wireless Local Area Network) implementada para comunicaciones domésticas y empresariales. WMAN (Wireless Metropolitan Area Network, que se implementa para conexiones que necesitan una alta cobertura como interconexión de edificios en una ciudad. WWAN (Wireless Wide Area Networks) implementada para comunicaciones entre ciudades o países (Sharma & Dhir, 2014).

Las estructuras empresariales tienen alta preferencia por la implementación de redes WLAN para comunicaciones internas dentro de sus espacios físicos y a través de los años han utilizado los variados protocolos de seguridad que este ofrece como ser el WEP que dado a sus vulnerabilidades fue oficialmente abandonada en 2004. El protocolo siguiente en uso sería WPA, que como se demostraría fue vulnerable a la Configuración de WPS, un sistema auxiliar desarrollado para simplificar la vinculación de dispositivos a puntos de acceso remotos. El avance en la creación de un nuevo protocolo, trajo la segunda versión WPA2 en 2004, que introdujo el Estándar de cifrado avanzado AES. Ya el protocolo WPA había introducido dos

modos de autenticación: el *personal* que utiliza un clave pre compartida y *enterprise* que utiliza una estructura EAP (Protocolo de Autenticación Extensible) que utiliza credenciales compuestas por un usuario y una contraseña para la autenticación de usuarios, posteriormente bajo estas características WPA2 sería el método más usado en entornos corporativos (Bartoli, Medvet, & Onesti, 2018).

Se detallan algunos trabajos relacionados a la presente investigación:

TITULO: Wireless authentication methods and apparatus

AUTOR: Daniel Vernon Bailey, John G. Brainard, Ari Juels, Burton S. Kaliski, Jr. AÑO: 2006

CATEGORÍA: Patente

Un primer dispositivo de procesamiento, que puede ser, por ejemplo, un token de autenticación inalámbrico o una etiqueta RFID, transmite información en una red inalámbrica de manera que emula las comunicaciones estándar de un punto de acceso de la red inalámbrica, aunque el primer dispositivo de procesamiento no es configurado para operar como un punto de acceso real de la red inalámbrica. Un segundo dispositivo de procesamiento, que puede ser, por ejemplo, una computadora u otra estación de la red inalámbrica, recibe la información transmitida y puede determinar a partir de ella que la información proviene de un punto de acceso emulado en lugar de un punto de acceso real. El segundo dispositivo de procesamiento responde a esta condición utilizando la información transmitida de una manera distinta de su utilización de información similar recibida desde el punto de acceso real de la red inalámbrica.

TITULO: System and method for device authentication in a dynamic network using wireless communication devices

AUTOR: Gary B. Jabara, Christos Karmis, David Brett Simon, Lloyd Frederick Linder

AÑO: 2009

CATEGORÍA: Patente

Se establece una red inalámbrica de corto alcance mediante comunicación directa entre dispositivos inalámbricos y puntos de acceso inalámbricos. Un dispositivo de comunicación

inalámbrica proporciona información de registro inicial a una red y se convierte en un dispositivo registrado. Se descarga una API al dispositivo inalámbrico para permitir la autenticación automática del dispositivo para futuras comunicaciones. Cuando un dispositivo registrado ingresa a un lugar, al menos un punto de acceso detectará automáticamente el dispositivo inalámbrico y extraerá los datos de identificación necesarios para permitir la autenticación del dispositivo. Se pueden proporcionar mensajes personalizados al dispositivo inalámbrico. Si el dispositivo inalámbrico ingresa a un lugar diferente, incluso en otra ciudad o estado, los datos de registro pueden ser extraídos automáticamente por un AP y proporcionados a una red en la nube para su autenticación. Los dispositivos autenticados reciben una lista de proveedores autenticados y proveedores no autenticados cerca de la ubicación actual del dispositivo autenticado.

TITULO: Secure authentication using mobile device

AUTOR: David M. T. Ting, Michael C. Bilancieri, Edward J. Gaudet, Jason Mafera AÑO: 2011

CATEGORÍA: Patente

Las realizaciones representativas de la autenticación segura incluyen la recepción, por un servidor, de información desde un dispositivo móvil que identifica (i) el dispositivo móvil y (ii) una etiqueta de identificación leída por el dispositivo móvil; acceder, por el servidor, a una base de datos para identificar (i) un usuario asociado con el dispositivo móvil, (ii) un dispositivo seguro asociado con la etiqueta identificadora, y (iii) una política de seguridad asociada con el dispositivo seguro; y si la política permite el acceso del usuario identificado al dispositivo seguro identificado, lo que hace que el acceso al dispositivo seguro sea otorgado al usuario.

TITULO: Method of device authentication and application registration in a push communication framework

AUTOR: Venkateswara R. Gaddam, Shahid Ahmed, Sankar SHANMUGAM, S M Masudur Rahman

AÑO: 2011

CATEGORÍA: Patente

Un sistema de servidor y un dispositivo móvil establecen un marco de datos de inserción para la comunicación. El dispositivo móvil incluye un cliente de inserción y ejecuta una o más aplicaciones que requieren comunicaciones de datos de inserción. El cliente de inserción transmite una autenticación de dispositivo y una solicitud de validación de aplicación a un servidor de inserción. Después de que el servidor de inserción autentica y valida con éxito el dispositivo y la aplicación, el cliente de inserción recibe un identificador de sesión para establecer una conexión de comunicación persistente con el servidor de inserción. Una vez establecido, un servidor de aplicaciones puede enviar datos al dispositivo móvil a través de la sesión de comunicación persistente. El identificador de sesión permanece válido durante un período de tiempo prolongado y permite al cliente de inserción mantener y restablecer las conexiones de inserción con el servidor de inserción durante el período de tiempo prolongado.

TITULO: Wireless multi-factor authentication with captive portals

AUTOR: Lawrence T. Belton, Brian Beaty, Timothy H. Morris, Douglas S. Rodgers, Lynn Allen Smith

AÑO: 2012

CATEGORÍA: Patente

Se describen sistemas y métodos para la autenticación de red multifactorial independiente del dispositivo. En algunas realizaciones, una conexión de red inalámbrica puede autenticar un dispositivo a través de medios de autenticación seguros con un certificado que confirma la identidad de un dispositivo. Después de autenticar el dispositivo, se puede pedir a un usuario que proporcione credenciales en un portal cautivo. El portal cautivo puede ser inaccesible para dispositivos que aún no se hayan autenticado utilizando un certificado. Después de proporcionar credenciales aprobadas al portal cautivo, el usuario puede acceder a la red. Esta realización y las realizaciones adicionales se integran fácilmente en redes inalámbricas privadas y otras.

TITULO: Method for adaptive authentication using a mobile device

AUTOR: Mourad Ben Ayed

AÑO: 2013

CATEGORÍA: Patente

Un método para facilitar el inicio de sesión utilizando autenticación adaptativa. El método utiliza diferentes métodos de autenticación y diferentes métodos de protección de datos dependiendo de la ubicación del usuario, la disponibilidad de la red, la importancia de los datos.

1.3 Planteamiento del Problema

El uso de redes inalámbricas para el acceso a datos e información cada vez se vuelve más común y preferido en estructuras corporativas, debido a que este tipo de conexiones no necesita ningún tipo de cableado estructurado para transmitir el flujo de información (Carballar, 2010).

Los usuarios atribuyen un incremento a la productividad estrechamente relacionada a la movilidad y flexibilidad que estos ofrecen (Lee, Su, & Shen, 2007). Este tipo de redes además presentan muchos beneficios económicos para la empresa ya que el costo en comparación a la instalación de una estructura de datos cableada es menor (Sharma & Dhir, 2014).

Para acceder a estas redes inalámbricas corporativas, es necesario que el usuario cuente con unas credenciales, estas están compuestas por un nombre de usuario y una contraseña, información que se ingresa en un portal web de autenticación Hotspot - Radius.

Por otra parte, la autenticación de invitados en redes inalámbricas corporativas no exige credenciales, se facilita el acceso a través de la creación de una red independiente que se asemeja a una doméstica. Los invitados usan una única clave de pre compartida PSK, que puede presentar riesgos con respecto a la seguridad de la red a largo plazo, ya que no se tiene ningún tipo de control sobre la difusión de la misma (Castro, 2005).

El registro y generación de credenciales para usuarios corporativos suele presentar un problema, el tiempo de registro. Tomando en cuenta que en un futuro el usuario podría perder alguna información acerca de las credenciales proporcionadas, lo que implicaría producir un nuevo registro.

Por otra parte, no se cuenta con un control sobre las conexiones existentes de usuarios corporativos ya que no existen áreas de autenticación, que permitirían controlar las conexiones dentro y fuera de los límites de las instalaciones.

Se han identificado los siguientes problemas:

- El proceso de registro y generación de credenciales para el acceso inalámbrico es manual lo que puede ocasionar una pérdida de tiempo para los operadores de red.

- Las credenciales pueden ser usadas en cualquier dispositivo, lo que podría ocasionar un uso indebido por la difusión descontrolada de credenciales y la falta de registros de dispositivos.
- Si durante el registro se empareja un dispositivo, el operador puede ingresar erróneamente la información del dispositivo, la corrección puede causar pérdida de tiempo.
- Las credenciales generadas contienen contraseñas cortas, el acceso a la red podría ser vulnerado por un ataque de diccionario.
- La autenticación de usuarios suele ser un proceso recurrente, lo cual suele ser molesto para los usuarios.
- Se puede realizar el uso de la red más allá de los límites de las instalaciones.
- La información de dispositivos conectados no se guarda en ningún registro, que podría colaborar en investigaciones forenses en caso de intrusiones.
- No se tiene un registro de dispositivos conectados a la red inalámbrica, por lo que en caso de intrusiones no se cuenta con ninguna información de respaldo.

A consecuencia se define el problema principal de la siguiente manera:

1.3.1 Problema Central

¿Cómo mejorar el proceso de autenticación en redes inalámbricas Wi-Fi corporativas de modo que este sea flexible para los usuarios y mantenga el estándar de seguridad?

1.4 Definición de Objetivos

1.4.1 Objetivo General

Plantear un modelo de autenticación para redes inalámbricas Wi-Fi corporativas que genere y autentique credenciales de manera automática utilizando el control por áreas de conexión.

1.4.2 Objetivos Específicos

- Desarrollar un prototipo basado en las especificaciones del modelo propuesto.
- Automatizar el proceso de registro y generación de credenciales.
- Emparejar un único dispositivo a la credencial por medio del uso de un PIN durante el primer uso.

- Obtener la información del dispositivo de manera automática durante el emparejamiento con la credencial a fin de evitar errores de escritura.
- Generar contraseñas de mayor longitud.
- Automatizar el proceso de autenticación por medio del reconocimiento de áreas de conexión.
- Controlar el acceso a la red corporativa a través del uso de la intensidad de señal del punto de acceso.
- Limitar el uso de la red corporativa dentro de las instalaciones y áreas definidas.
- Producir un registro de todos los dispositivos conectados, resguardando la información como la fecha y hora de acceso.

1.5 Hipótesis

Un modelo de generación y autenticación automática de credenciales en redes inalámbricas Wi-Fi corporativas, basado en el control por áreas de conexión con Mikrotik, produce una ganancia del 45% en tiempo de autenticación sin afectar el nivel de seguridad.

1.6 Justificación

La generación de credenciales para el acceso a redes inalámbricas corporativas pasa por un proceso donde el usuario debe asistir donde un operador de redes, durante el procedimiento el operador genera de manera manual los dos componentes de la credencial, usuario y contraseña. Agregar la dirección física del dispositivo es opcional durante el procedimiento, esto puede presentar pros y contras, como, por ejemplo, si no se agrega la dirección física del dispositivo la clave puede ser usada en varios dispositivos y no se debe generar una nueva credencial por cada nuevo dispositivo. En caso de agregarse la dirección física el entorno de conexión es más segura, pero con la desventaja de que la credencial está ligada necesariamente a un dispositivo.

De un modo u otro el problema principal que se enfrenta el usuario corporativo es la autenticación recurrente. La autenticación se valida a través de un portal web generado por el tipo de autenticación WPA2-Enterprise donde se ingresan las credenciales. El procedimiento puede tomar algunos segundos, un intervalo de tiempo corto que podría ser utilizado en otras tareas dentro de la empresa. Además de convertirse en un procedimiento molesto, puesto que los usuarios desean disponer de una conexión sin tantos requerimientos.

Por otra parte, eliminar tales requerimientos podría bajar el nivel de seguridad en la red, ya que el protocolo WPA2-Personal utiliza una clave compartida PSK, la cual es difícil de controlar en términos de difusión. Tal difusión, podría incidir en pérdidas económicas para la empresa, ya que un tercero podría tomar provecho de la situación. La productividad de la empresa está relacionada a la productividad de sus usuarios y la productividad de los mismos está relacionada a una conexión estable proporcionada por la empresa. La participación de un tercero incide directamente en la productividad de la empresa partiendo en un inicio desde el desvío de recursos de red.

De este modo se plantea un modelo de generación y autenticación de credenciales que beneficie al usuario corporativo, con respecto a tiempos de autenticación, sin tener la necesidad de reducir el nivel de seguridad de la red inalámbrica.

1.7 Alcances y Límites

Se definirán una serie de aspectos que se tomará en cuenta durante el desarrollo de este trabajo, intentando ser lo más puntual posible, a fin de no colocar expectativas que superen el modelo propuesto:

1.7.1 Alcances

A continuación, se plantean algunos alcances puntuales con relación a la propuesta:

- El modelo se encargará de monitorear el estado del punto de acceso y las solicitudes de dispositivos que se encuentren dentro del área de autenticación.
- La atención de solicitudes se manejará a través de operaciones FIFO.
- El modelo generará una credencial genérica durante el primer uso basada en la información del usuario y la del dispositivo.
- El modelo asignará contraseñas de mayor longitud.
- El modelo realizará el uso de *tokens* para autenticar nuevos dispositivos de una misma cuenta de usuario.
- El modelo autenticará y desautenticará dispositivos dentro de los parámetros establecidos con el uso de la intensidad de señal medida en dBm.
- El modelo usará una base de datos no relacional para almacenar toda la información relacionada con las operaciones.

- El modelo hará uso de un servidor el cual monitoreará el estado del punto de acceso durante intervalos de tiempo inicialmente establecidos.

1.7.2 Límites

El presente trabajo tiene como límites los siguientes aspectos:

- El modelo no trabaja con un conjunto de puntos de acceso, siendo que específicamente está desarrollado para trabajar con uno.
- El modelo no modifica ninguna propiedad de los dispositivos, sólo hace lectura de su información.
- El modelo no identifica intentos de intrusión en la red.
- No aplica inteligencia artificial para la selección de usuarios, dispositivos conectados o que se conectaron anteriormente.
- El modelo no es capaz de interpretar un ataque dentro de la red inalámbrica.
- El modelo no incluirá ninguna interfaz de administración de la red, dispositivos conectados, activos, inactivos ni huéspedes.
- El modelo no es portable dado que es un servidor el que almacena el software, por lo tanto, es el servidor el que conecta con el punto de acceso para su control y monitoreo.
- El modelo no mejora ni modifica la señal del punto de acceso, sólo realiza su lectura.
- El modelo no genera los PIN's de acceso iniciales para el emparejamiento de dispositivos. Los cuales deben ser generados previamente junto a la información relacionada a los clientes en la base de datos.
- El modelo trabajará con equipos de la marca Mikrotik, que están dedicados a cubrir un mercado *Small-Business*.

1.8 Aportes

1.8.1 Práctico

El modelo mostrará una alternativa de autenticación automatizada similar a la WPA-Personal sin modificar el nivel de seguridad que entrega el modo de autenticación WPA2-Enterprise, permitiendo así continuar con el uso de credenciales pero que al mismo tiempo facilite al usuario conectarse a la red inalámbrica sin hacer uso recurrente del portal de autenticación.

Otro aspecto importante es el de la utilización de la intensidad de señal dentro del modelo, para las conexiones entrantes y salientes en el punto de acceso inalámbrico, lo que permitirá añadir un mayor control sobre el uso de la red inalámbrica corporativa, a fin de evitar que personas ajenas a la empresa hagan uso indebido de la misma.

1.8.2 Teórico

Establecer un modelo como base para futuras investigaciones en el campo, que permita operar la generación y autenticación de usuarios no sólo con tecnologías actuales como ser Mikrotik dedicadas a entornos *Small Business*. Esto permitirá extrapolar el concepto y aplicarlo a redes de empresas más grandes, facilitando así el trabajo con un grupo de usuarios mayor.

1.9 Metodología

1.9.1 Muestra

La población o grupo de estudio para la investigación serán los usuarios que utilizan una red inalámbrica Wi-Fi corporativa, esta población utiliza credenciales como medio de acceso, bajo el protocolo WPA2-Enterprise.

Dado que la investigación trabajará con el análisis en un único nodo y no en una red completa, la muestra estará relacionada a la cantidad de usuarios que el nodo puede soportar entregando una conexión estable, lo cual son aproximadamente 20 usuarios.

Para la verificación de resultados, se usará el mismo grupo de usuarios inicial, para poder comparar el comportamiento anterior y el obtenido bajo la propuesta del modelo.

1.9.2 Método y Medios de Investigación

El desarrollo del presente trabajo se adecua a la metodología experimental cuantitativa de acuerdo a las siguientes características:

- Los indicadores tienen valores numéricos que pueden ser traducidos a tablas y funciones estadísticas para poder observar su comportamiento.
- Los valores de entrada de los indicadores como fuerza de señal, asignación IP están sujetos a la experimentación entre los distintos dispositivos que solicitan acceso y la red inalámbrica que los acoge.
- Se considera experimental dado que el investigador interviene y manipula la variable de estudio.

- El investigador realiza una planificación por lo cual adquiere un estado prospectivo.

El trabajo tiene un grado de abstracción aplicado, generando así pocos aportes de conocimiento científico a nivel teórico, esto se debe a que el modelo se implementará con una tecnología específica, por lo cual no se intenta demostrar un teorema sino producir un comportamiento.

Por consecuencia, el presente trabajo se adecua a la investigación exploratoria dado que no existen muchas fuentes de información en esta línea.

1.9.3 Metodología Sistémica

El desarrollo del presente trabajo utilizará la Metodología Sistémica para plantear el modelo de autenticación propuesto. Las fases propuestas por la metodología de acuerdo al concepto propuesto por Churchman y Ackoff (Churchman, Ackoff, & Arnoff, 1957) son:

- Formulación del problema, donde describiremos el problema identificado.
- Construcción de un modelo, donde se realiza el análisis de las variables que intervienen y las cuales pueden ser modificadas.
- Obtención de una solución, el cual en nuestra investigación será un diagrama que muestre el nuevo comportamiento deseado bajo el problema.
- Prueba del modelo y la solución, aquí se añadirá el aporte realizado por Goode y Machol que en 1957 propusieron la construcción de un prototipo para su posterior evaluación.
- Implantación y control de la solución, que nuevamente en base al trabajo de Goode y Machol sugieren la: Prueba, Entrenamiento y Evaluación, donde en el presente trabajo pasaremos a afinar el prototipo basado en el modelo propuesto (Goode & Machol, 1957).

Una vez completado los pasos anteriores, se podrá realizar un análisis de los resultados obtenidos en campo, como consecuencia de aplicar el modelo a la muestra de estudio.

CAPÍTULO II

2 MARCO TEÓRICO

2.1 Redes Inalámbricas

Los diferentes tipos de redes inalámbricas pueden ser clasificados en cuatro extensas categorías: redes inalámbricas de área personal, redes inalámbricas de área local, redes inalámbricas de área metropolitana y redes inalámbricas de red amplia. La clasificación de las redes se encuentra categorizada de acuerdo al alcance de transmisión de datos y cada una de ellas se encuentra dentro de la familia IEEE 802 (Ciampa, 2013).

2.1.1 Wireless Personal Area Network (WPAN)

Se extienden por pocos metros y son de uso personal. Administra conexiones entre teléfonos celulares, computadoras, PDA, dispositivos de audio e impresoras. Utilizan el protocolo de comunicación IEEE 802.15.

2.1.2 Wireless Local Area Network (WLAN)

Utilizado para establecer comunicaciones entre ordenadores, es capaz de soportar una red de usuarios locales, utiliza el protocolo de comunicación IEEE 802.11.

2.1.3 Wireless Metropolitan Area Network (WMAN)

Establece comunicaciones inalámbricas en áreas metropolitanas e incluye tecnologías como WiMAX *(Worldwide Interoperability for Microwave Access)*, utiliza el protocolo IEEE 802.16.

2.1.4 Wireless Wide Area Network (WWAN)

Hace uso de redes de comunicaciones móviles como: GPRS, EDGE, GWM, HSPA y 3G entre algunos para transferir datos. Utiliza el protocolo de comunicación IEEE 802.20.

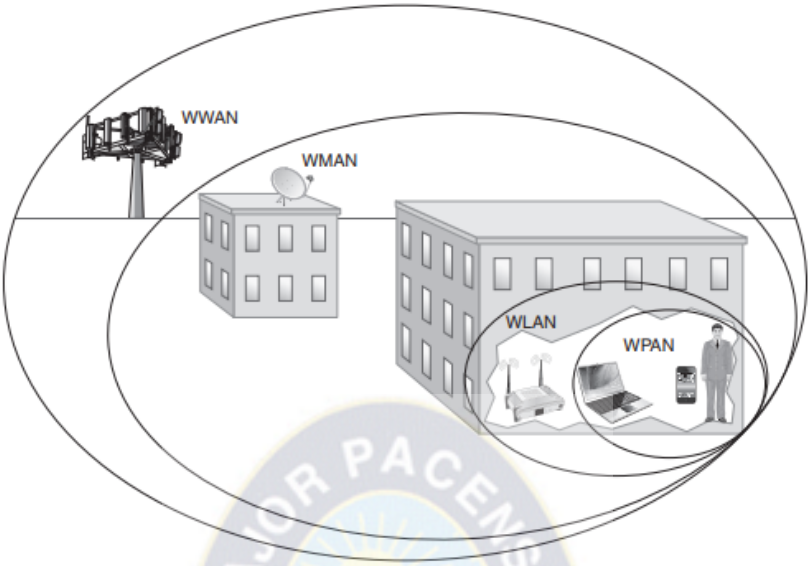


Figura 2.1: Áreas de cobertura de redes inalámbricas

Fuente: (Ciampa, 2013)

2.2 Red Inalámbrica Wi-Fi

Una red Inalámbrica denominada WLAN, es una red local de acceso inalámbrico que permite a las computadoras, móviles y otros dispositivos, conectarse entre sí a través de radio frecuencias, lo que permite a los usuarios poder trasladarse de un lugar a otro evitando que se utilicen cables como en la infraestructura Ethernet tradicional (Cárdenas, Molina, & Armijos, 2017).

El término Wi-Fi hace referencia a la expresión *Wireless Fidelity* que traducida significa fidelidad inalámbrica. Es usado como denominación general para los productos que incorporan cualquier variante del estándar inalámbrico 802.11, que permite la creación de redes locales inalámbricas (*Wireless Local Area Networks).*

Durante sus primeros años del término en uso, se hacía referencia únicamente al estándar 802.11b, con la aceptación prácticamente universal de varios de sus derivados como ser los estándares 802.11a, 802.11g, 802.11n, el término fue generalizado haciendo referencia al conjunto.

Wi-Fi llegó a convertirse en un estándar gracias a su asequibilidad al brindar acceso de banda ancha. Durante el 2004, las comunicaciones sin cable llegaron a ser requeridas y según la

previsión de analistas en el mercado éste generaría 1.739 millones de euros al formar parte de la estrategia de operadoras, fabricantes e integradores de sistemas en Europa (COIT, 2004).

2.2.1 Estándar IEEE 802.11

El 802.11 forma parte de la familia 802, que hace referencia a una serie de tecnologías para uso en redes inalámbricas.

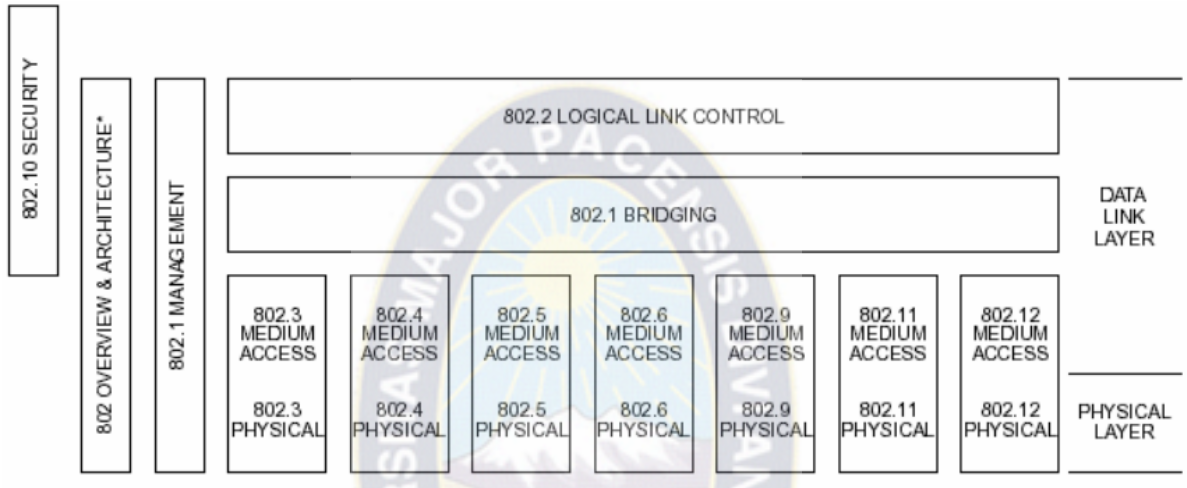


Figura 2.2: Relación entre los miembros de la familia 802

Fuente: (COIT, 2004)

El estándar 802.11 utiliza la Capa de enlace de datos (MAC) y la capa física (PHY). También tiene algunos estándares derivados, llamados estándares físicos, que operan en distintos rangos de velocidad de transferencia.

2.3 Componentes de una red inalámbrica

Para establecer la comunicación inalámbrica entre varios dispositivos y una red, son necesarios tres componentes, tarjetas inalámbricas NIC (*Network Interface Controller),* un *router* y un punto de acceso inalámbrico denominado AP.

2.3.1 Tarjetas inalámbricas WNIC

Las Wireless *Network Interface Controller o WNIC* son como su traducción al español indica, tarjetas de interface de red inalámbricas. Cada tarjeta posee un número de serie de un código único llamado “acceso a los medios” abreviado como MAC. Estas tarjetas trabajan a nivel de la capa 1 y 2 del modelo OSI y usan una antena para comunicarse vía radiación electromagnética.

En una computadora tradicionalmente se conecta a través del bus de datos PCI. Existen otros modelos que incorporan portabilidad como los USB WNIC (Khan, 2010).

- **MAC**

  Hace referencia a un número único que identifica un equipo en una red. Cada tarjeta *ethernet, bluetooth,* tarjeta de red inalámbrica, entre algunos, contienen esta dirección física. Esta no puede ser modificada y se asemeja a un número de identificación que usamos para acceder a los servicios cotidianos, pero se conoce como huella digital para los medios electrónicos (Pannell, 2018).

  Las especificaciones de para construir la dirección MAC puede ser MAC-48, EUI-48 y EUI 64, todas validadas por la IEEE (Symantec, 2018). Estos están diseñados para ser globalmente únicos. Un ejemplo, la construcción de 48 bits de espacio contiene potencialmente 2^{48} o 281,474,976,710,656 posibles direcciones MAC.

  La Figura 2.3 muestra la especificación de las direcciones MAC organizados por octetos, donde los primeros tres octetos hacen referencia al identificador único dentro de la organización a la cual pertenece la tarjeta de red (*OUI – Organisationally Unique Identifier)* y los siguientes tres octetos hacen referencia al controlador de interfaz de red (*NIC – Network Interface Controller)* (IEEE, 2018).

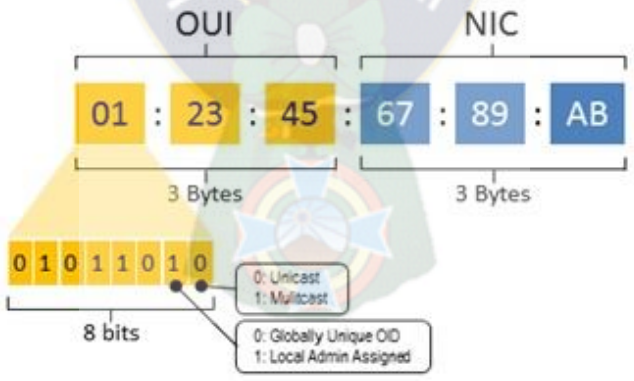


Figura 2.3: Distribución de octetos especificación MAC-48

Fuente: (Pathsolutions, 2018)

La inclusión de la dirección MAC en los dispositivos de interfaz de red, se realiza con la inclusión de una pegatina o *sticker* que tiene impresa la dirección MAC entre otras especificaciones adicionales del fabricante.

Figura 2.4: Etiqueta de un UMTS router con dirección MAC

Fuente: (Kiddle, 2018)

2.3.2 Router

Los *routers* analizan los datos que se envían a través de una red, realizan el empaquetado de datos y los envían a otra red. Se puede especificar qué computadoras tienen más prioridad que otras dentro de la misma red.

Son utilizados para brindar el acceso a internet a varios usuarios. Éste actuará como distribuidor y se encarga de elegir la mejor ruta de desplazamiento para que la información pueda ser recibida rápidamente (Cisco, 2018).

Figura 2.5: Router Cisco Modelo RV180W Wireless Multifunction

Fuente: (Cisco, 2018)

2.3.3 Punto de Acceso Inalámbrico

Conocido como *Wireless Access Point* por sus siglas en inglés, se hace referencia de forma abreviada como WAP o AP.

Es un dispositivo de red que administra equipos de comunicación inalámbricos. Permite conectar varias máquinas sin la necesidad de un cable lo que otorga mayor portabilidad. Uno de sus objetivos principales es la conexión estable sin limitar demasiado el ancho de banda.

Estos dispositivos permiten la conexión inalámbrica de computadoras, tabletas, o *smartphones* con una red. Los equipos WAP también se conectan a una red cableada, pudiendo transmitir la información de manera indistinta entre ambas redes: inalámbrica y cableada.

Los equipos WAP son asignados con una dirección IP como cualquier dispositivo, ya que cuentan también con un identificador único MAC. Esto permite su configuración para poder conectar adicionalmente otros dispositivos WAP y formar una red más grande. Una red con varios dispositivos WAP permite realizar *roaming.*

Los puntos de acceso crean una red de área local inalámbrica denominada WLAN, este punto de acceso se conecta a un *router*, un *switch* o un *hub* por un cable Ethernet. De esta manera proyecta una señal Wi-Fi para la transmisión de información (Linksys, 2018).

Figura 2.6: Mikrotik Router – Access Point RB2011UiAS-2HnD-IN

Fuente: (Mikrotik, 2018)

- **SSID**

  Es el nombre con el cual se identifica la red Wi-Fi. El nombre viene preestablecido de fábrica, pero puede modificarse al acceder al panel de administración del punto de acceso.

2.3.4 Antenas

Son un elemento importante dentro de las redes inalámbricas, ya que se encargan de transformar la energía de corriente alterna, en un campo electromagnético para poder completar la transmisión de información y de manera inversa lo realiza para poder recibir información. De este modo los equipos que pueden comunicarse (Onofre, 2013).

- **Potencia – dBm**

  La potencia de emisión de una antena se encuentra medio en unidades de *dBm*, los valores de recepción de señal ligados a la distancia tienen relación estrecha con la potencia de la antena. La siguiente tabla muestra valores medidos en dBm donde claramente se observa que 0 es el valor óptimo de recepción (Soldo, 2013).

Tabla 2.1: Interpretación de valores aproximados dBm

dBm	Descripción
-80	Es la señal mínima aceptable para establecer la conexión, puede ocurrir caídas de enlace.
-70	Enlace normal-bajo, es una señal medianamente buena, aunque se pueden sufrir problemas con lluvia y viento.
-60	Enlace bueno, ajustando TX y *basic rates* se puede lograr una conexión estable al 80%.
-40 a -60	Señal idónea con tasas de transferencia estables.
-1 a -39	Señal excelente, muy difícil de conseguir en un entorno normal.
0	Señal ideal, lograda sólo en laboratorio.

Fuente: (Comunidad UBNT, 2016)

Los valores que se encuentran por debajo de -80 dBm son considerados de baja cobertura o con pérdida de señal, sin cobertura.

2.4 Protocolos de Cifrado

El cifrado de datos dentro de una red inalámbrica juega un papel muy importante. Muchos *routers* o *access point* brindan protocolos de cifrado tales como WEP, WPA o WPA2, como principales para codificar la información que se transmite por la red inalámbrica, aunque existen

métodos alternativos como el filtrado de MAC, que pueden añadirse a los anteriores protocolos para incrementar el nivel de seguridad en la red.

a) WEP

El cifrado de datos es de 64 y 128 bits, fue introducido en el año 1999, originalmente diseñado para proporcionar el mismo nivel de confidencialidad que una red cableada. Durante el año 2001, varias vulnerabilidades fueron encontradas por analistas criptográficos (Chaabouni, 2006). Actualmente se encuentra en desuso y no se recomienda configurar equipos con este protocolo de cifrado.

b) WPA

Fue publicado debido a las vulnerabilidades encontradas en el protocolo de seguridad WEP. El protocolo fue diseñado para soportar un servidor de autenticación, que comúnmente es un servidor RADIUS. El protocolo además conserva el modo de autenticación por clave única (*Pre-shared key)* e incorpora el llamado *Temporal Key Integrity Protocol (TKIP),* que cambia las claves dinámicamente conforme el sistema es utilizado. WPA es el protocolo reforzado de WEP, ya que lo fortaleció con una clave de 128 bits y un vector de inicialización de 48 bits (Wi-Fi Alliance, 2003). También se han descubierto vulnerabilidades, por lo que no se recomienda su uso.

c) WPA2

El protocolo de seguridad provee un nuevo esquema de encriptación conocido como AES y el gobierno de los Estados Unidos fue el primero en adoptarlo. La nueva característica logro definir dos modos de autenticación en el nuevo protocolo que se encontraban presentes en su antecesor: Personal y Enterprise.

- ✓ **WPA2-Personal**

  Implementado en el protocolo WPA como WPA-PSK, utiliza una clave compartida. Pasó a llamarse Personal por el uso casi estandarizado que se hacía en hogares.

- ✓ **WPA2-Enterprise**

  Hace referencia al uso de credenciales con claves únicas, muy extendido en redes corporativas y gubernamentales. Las credenciales se componen por un usuario y una contraseña y son administradas por un servidor RADIUS.

En octubre de 2017 fue descubierta una vulnerabilidad a través de un nuevo método de ataque llamado “Reinstalación de clave KRACK”. El autor Mathy Vanhoef autor de la investigación, asegura que la vulnerabilidad puede ser parcheada (Key Reinstallation Attacks, 2018).

d) WPA3

Es desarrollado luego de descubrirse la vulnerabilidad en WPA2, la clave de cifrado se incrementa a 192 bits y se mantiene los 48 bits de inicialización. Se espera su salida para principios del año 2018, puede encontrase más información en la página oficial (Wi-Fi Alliance, 2018).

2.5 Mikrotik

Mikrotik es una compañía cuya sede está ubicada en Latvian, un país de Europa. Fue fundado en 1996 con el objetivo de desarrollar *routers* y sistemas *wireless* ISP. Se dedica principalmente a la venta de equipos de hardware de red y *routers* que son denominados *routerboards* y *switches* conocidos por el software que los administra, *RouterOS* y *SwOS* (Mikrotik, 2018).

```
[admin@MikroTik] > ip route
[admin@MikroTik] ip route> print
Flags: X - disabled, I - invalid, D - dynamic, J - rejected,
C - connect, S - static, r - rip, o - ospf, b - bgp
    #    DST-ADDRESS        G GATEWAY         DISTANCE INTERFACE
    0  S 0.0.0.0/0          r 192.168.2.1     1        WAN
    1 DC 192.168.124.0/24   r 0.0.0.0         0        LAN
    2 DC 192.168.2.0/24     r 0.0.0.0         0        WAN
    3 DC 192.168.0.0/24     r 0.0.0.0         0        LAN

[admin@MikroTik] ip route>
```

Figura 2.7: Terminal Mikrotik, comando /ip route print

Fuente: (Mikrotik, 2018)

Durante el año 2002 la compañía decidió participar en el mercado de hardware lanzando el *RouterBoard*, el cual lo convertiría en el proveedor más famoso por las características únicas que lo diferenciaban de la competencia, un software operable y equipos de hardware adaptables (Saputra, 2013).

2.5.1 Terminal Console

La terminal es usada para acceder a la configuración del *router* Mikrotik y administrarla a través de instrucciones de texto llamados comandos. Ésta terminal es también usada para escribir scripts que se ejecutarán de manera interna en el equipo sin la necesidad de supervisión.

La estructura de comandos es similar al Unix Shell (ver Figura 2.7). Los comandos se encuentran organizados en grupos de manera jerárquica y por niveles (Mikrotik, 2018). La terminal permite tener el control total del dispositivo, obteniendo y modificando las tablas de datos con la información de la red que se administra.

2.5.2 Application Programmable Interface – API

Permite a los usuarios crear soluciones de software a medida que puede comunicarse con el sistema operativo RouterOS de Mikrotik para recoger información, ajustar configuraciones y administrar el equipo *router* de manera externa (Troncoso & Cruz, 2018).

El API sigue la sintaxis de la Interfaz de línea de comando (CLI). El objetivo principal es crear herramientas de configuración traducidas o personalizadas que puedan facilitar el uso de los equipos Mikrotik (Mikrotik Wiki, 2018).

a) API Words

La comunicación con el *router* se completa por el envío de sentencias que devuelven uno o más resultados. Las sentencias son una secuencia de palabras, estas pueden contener referencias a atributos específicos que son evaluadas y ejecutadas.

```
/login

 !done
=ret=ebddd18303a54111e2dea05a92ab46b4

/login
=name=admin
=response=001ea726ed53ae38520c8334f82d44c9f2

 !done
```

Figura 2.8: Sentencias API login

Fuente: (Mikrotik Wiki, 2018)La ejecución

Algunos comandos tienen atributos especiales que no están disponibles a través del uso directo del CLI.

```
/ip/address/add
=address=192.168.88.1/24
=interface=ether1
```

Figura 2.9: Comandos CLI Mikrotik

Fuente: (Mikrotik Wiki, 2018)

b) API Libraries

El manejo del API haciendo uso de *Words* de manera directa resulta complejo y aumenta cuando se desea usar *queries* que contienen muchos atributos. Para un manejo más eficiente del API de Mikrotik, la comunidad desarrolló varias librerías escritas en distintos lenguajes de programación. Entre la larga lista de lenguajes que permiten interactuar con el API, se encuentran: PHP, Delphi, Swift, C, C++, C#, Flash Actionscript 3, Ruby On Rails, VB .NET, Java, NodeJS, Python 3, RUST y GO.

Cada una de las librerías se encuentra documentada para que los desarrolladores interesados puedan consultar sus características y limitaciones, además se encuentran ejemplos sencillos que fácilmente pueden ser extendidos para alcanzar mayores resultados.

```
var api = require('mikronode');

var device = new api('192.168.0.1');
device.connect().then(([login])=>login('admin','password')).then(function(conn) {

   var chan=conn.openChannel();

   chan.write('/ip/address/add',{'interface':'ether1','address':'192.168.1.1'});
   chan.on('trap',function(data) {
       console.log('Error setting IP: '+data);
   });
   chan.on('done',function(data) {
       console.log('IP Set.');
   });
   chan.close();
   conn.close();
});
```

Figura 2.10: Asignación IP a ether1 con API NodeJS

Fuente: (Trakassure, 2018)

El ejemplo mostrado en la Figura 2.10 muestra la asignación de IP 192.168.1.1 al ether1 con una librería desarrollada para *NodeJS* utilizando el lenguaje *Javascript*.

2.6 PIN

El Número de Identificación Personal o PIN tiene aplicaciones bastas en el campo de la telefonía móvil y banca, que usa el identificador para realizar transacciones en cajeros automáticos.

Figura 2.11: Tarjeta SIM 4G con código PIN y PUK

Fuente: (Orange, 2018)

Sirve como herramienta de validación para usuarios en redes y sistemas. Su finalidad consiste en que sólo la persona beneficiaria conozca el PIN que le provee acceso al sistema (Techopedia, 2018).

La longitud de este código inicialmente fue de 4 dígitos aplicado a la telefonía móvil, actualmente se extiende a 8 aunque no existe una regla definida para su implementación.

2.7 Función Hash

Una función *hash* suele ser referido como función resumen, tiene como entrada un grupo de elementos normalmente cadenas que son convertidas en cadenas de longitud fija. Condensa la información sin proveer información acerca del contenido del material de entrada (Ministry of Justice and Security, 2018).

Son usados ampliamente para proteger la integridad de datos como por ejemplo firmas digitales, herramientas vinculadas a la autenticación y control de acceso entre muchos.

2.7.1 MD5

Es un algoritmo desarrollado por el profesor del MIT Ronald Rivest en el año 1992, su uso es extendido para la comprobación de integridad de archivos descargados.

Este algoritmo de reducción criptográfico se representa con un número de 32 símbolos hexadecimales.

2.8 Token de Seguridad

Los *token* son claves criptográficas que pueden ser portadas en un dispositivo electrónico entregado a los usuarios para completar procesos de autenticación.

Entre los variados tipos de token, en la presente investigación se hará referencia a los generadores de contraseña dinámicas conocidos como OTP *(One Time Password).*

2.8.1 One Time Password OTP

Son contraseñas que pueden ser utilizadas una sola vez y durante un corto espacio de tiempo, normalmente algunos segundos o minutos una vez el *token* ha sido generado.

Debido a su corto tiempo de vida puede o no ser obtenido a través de una función criptográfica, pero si debe ser generado en tiempo real por un dispositivo de hardware o software que se encuentre en posesión del usuario. Su uso forma parte del grupo de autenticación multi-factor (Vasco, 2018).

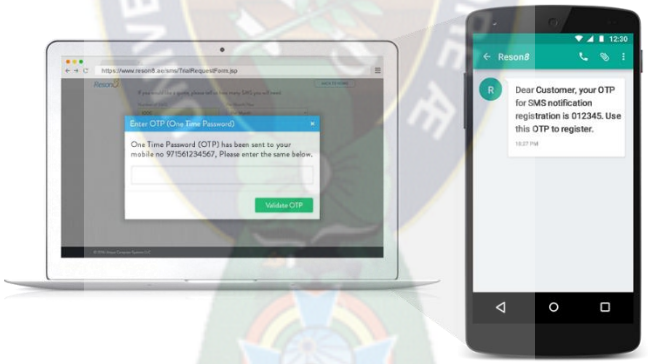


Figura 2.12: Token OTP sms de autenticación

Fuente: (Unique Computer System LLC, 2018)

2.9 Planificación de Procesos

La planificación de procesos ayuda a que no exista una saturación de cálculos y procesamiento que puedan afectar el rendimiento de un sistema.

2.9.1 First-In, First-out

Aunque el termino se usa ampliamente en estructura de datos, contabilidad y teoría de colas que no sólo se encuentran en el campo de sistemas, la definición de FIFO (First-In, First-Out) se aplica al procesamiento de información. Su implementación utiliza arreglos o vectores y su

significado es “Primero en entrar, primero en salir” (Tanenbaum, 2009). Otra de las definiciones que se usa ampliamente como sinónimo es el de FCFS (First Come, First Served) cuya traducción es: “primero en llegar, primero en ser atendido.”

2.10 MBSE Ingeniería de Sistemas Basada en Modelos

Model-Based System Engineering o MBSE tienen como objetivo formalizar la práctica del desarrollo de sistemas por medio del uso de modelos. Provee un mecanismo para impulsar la ingeniería de sistemas sin incrementar los costos (Hart, 2015).

Se hará una descripción definiendo qué es un modelo según la MBSE y posteriormente describiremos una de sus metodologías o método de modelado, uno de sus lenguajes y una de las herramientas de modelado.

2.10.1 Modelo

La terminología según la MBSE define un modelo como:

- Una simplificada versión de un concepto, fenómeno, relación, estructura o sistema.
- Una representación gráfica, matemática o física.
- Una abstracción de la realidad que elimina componentes innecesarios.

2.10.2 Metodología de Modelado OOSEM

Object-Oriented System Engineering Method o OOSEM, contiene un conjunto de actividades que capturan y comprenden el diseño de sistemas complejos. Mejora la integración entre sistemas, ya sea software o hardware, las pruebas relacionadas al sistema y otras disciplinas de ingeniería.

Uno de los objetivos más grandes es facilitar el rehúso de componentes y elementos del sistema en distintos niveles. Su uso se extiende a campos como la defensa, energía renovable, agricultura, comunicaciones, transporte y computación basada en la nube (INCOSE, 2018).

2.10.3 Características Principales

El método OOSEM contiene algunas características que facilitan su aplicación al diseño de cualquier tipo de sistema:

- Aprovecha los conceptos orientados a objetos y otras técnicas de modelado para ayudar a diseñar sistemas flexibles y extensibles, que puedan adaptarse a la evolución de la tecnología y los requerimientos cambiantes.
- Pretende facilitar la integración con el desarrollo de software orientado a objetos juntamente con el desarrollo de hardware y procedimientos de prueba.

2.10.4 Actividades OOSEM

Las actividades de este método son: análisis de necesidades, definición de requerimientos de sistema, definición de arquitectura lógica, síntesis de arquitecturas asignadas, optimizar y evaluar alternativas y por último validar y verificar el sistema (Friedenthal, Moore, & Steiner, 2015).

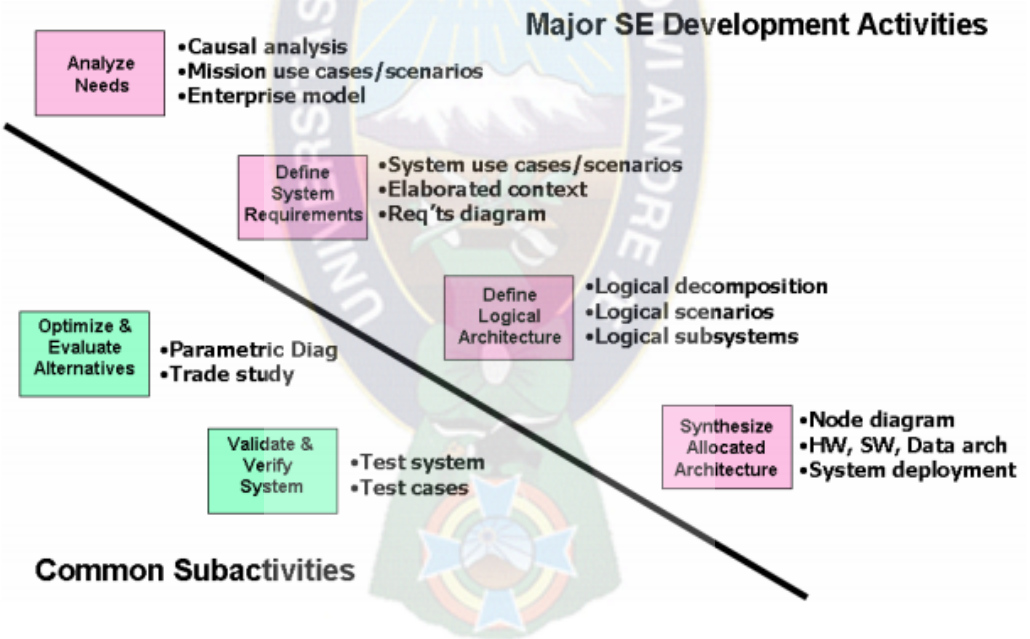


Figura 2.13: Actividades OOSEM

Fuente: (OMG, 2018)

Las actividades como conjunto se pueden ejecutar iterativamente y recursivamente para desarrollar sistemas de sistemas (Pearce & Hause, 2012).

a) Análisis de Necesidades de la parte Interesada

Esta actividad captura el sistema y la empresa como es, el resultado de su análisis es usado para desarrollar el cómo será la empresa y la misión de requerimientos asociada. Los requerimientos son especificados en términos de los objetivos, medidas de efectividad y casos de uso de alto nivel. Los casos de uso y los escenarios capturan la funcionalidad de la empresa.

b) Definición de Requerimientos de Sistema

Esta actividad está destinada a especificar los requerimientos del sistema que apoya la misión de requerimientos. Los casos de uso a nivel de sistema, así como los escenarios reflejan cómo se usa el sistema en la empresa.

Los escenarios son modelados usando diagramas de actividad donde cada hilo representa el sistema, usuarios y sistemas externos. La base de datos de requerimientos se actualiza durante esta actividad. Puede incluirse un análisis de caja negra para observar cómo el sistema interactúa con otros sistemas.

c) Definición de Arquitectura Lógica

La actividad incluye descomponer y particionar el sistema en componentes lógicos que interactúan para satisfacer los requerimientos de sistema. Estos componentes lógicos capturan la funcionalidad del sistema.

d) Síntesis de Arquitectura Candidata Asignada

La arquitectura asignada describe relaciones entre componentes físicos incluyendo hardware, software, datos y procedimientos. Cada componente lógico se mapea primero en un nodo de sistema para notar como es distribuida la funcionalidad. El software, hardware, y arquitectura de datos son derivados basados en la relación de componentes.

e) Optimizar y Evaluar Alternativas

Se aplica a través de todas las otras actividades para optimizar la arquitectura candidata y conducir estudios de comercio para seleccionar la arquitectura preferida. Modelos paramétricos para ejecución de modelado, confiabilidad, disponibilidad, costo de ciclo de vida y otras especialidades concernientes a la ingeniería son usados para analizar y optimizar la arquitectura candidata. Esta actividad también incluye el monitoreo de medidas de desempeño técnico e identifica riesgos potenciales.

f) Validar y Verificar el Sistema

Intenta verificar que el diseño de sistema satisfaga sus requerimientos y validar que los requerimientos coincidan con las necesidades de la parte interesada. Se incluyen el desarrollo de verificación de planes, procedimientos y métodos. Además, el modelo del sistema operacional se puede integrar con un entorno de ejecución para admitir la validación temprana de los requisitos y la verificación del diseño. Es posible que sea necesario desarrollar y o modificar un sistema, aunque debe abordarse temprano para evitar impactos adversos más adelante como costos. Otras herramientas de validación son simulaciones por ordenador.

CAPÍTULO III

3 MARCO APLICATIVO

3.1 Análisis de Necesidades

Analizaremos la situación de la red corporativa en su situación actual, cuáles son los protocolos que usa, seguridad y además describiremos el medio y modo de autenticación.

3.1.1 Estado actual

Las redes corporativas implementan el protocolo de cifrado WPA2-Enterprise. Su uso viene acompañado de un servidor RADIUS que administra las credenciales. La Figura 3.1 muestra el esquema de este protocolo.

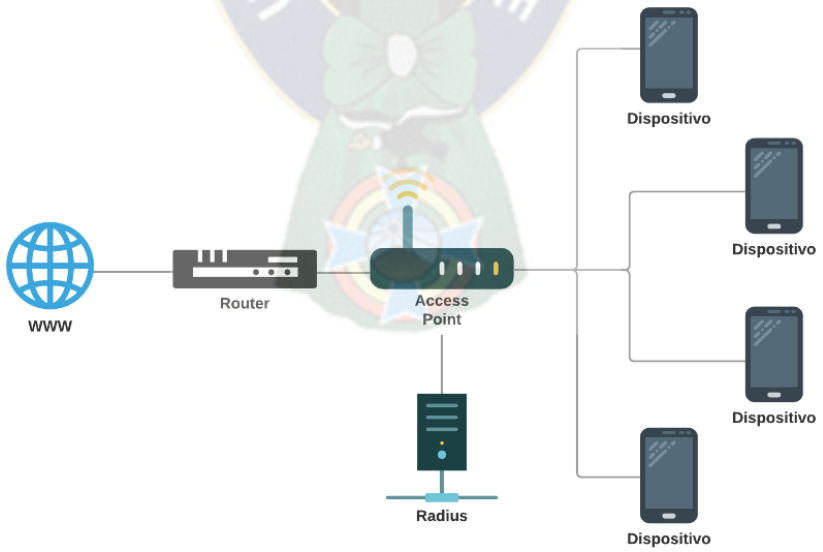


Figura 3.1: Servidor de autenticación Radius

Como se observa, el *Access Point* tiene una conexión con el servidor de autenticación, el modo de funcionamiento es el siguiente, los usuarios se conectan a la red, proveen las credenciales

que se les proporcionó previamente para el acceso, las credenciales son verificadas por el servidor de autenticación, en el caso de ser válidas, el servidor comunica al *Access Point* que el usuario puede hacer uso de la red y éste concede el acceso. En el caso contrario, las credenciales no son válidas, por lo que el servidor indicará al *Access Point* que el usuario no puede tener acceso a la red.

3.1.2 Acceso a la Red Wi-Fi

Para brindar acceso a la red Wi-Fi, el servidor extiende un portal de autenticación comúnmente llamado *Hotspot o* portal cautivo. Cada vez que el usuario se conecte a la red, se le pedirá que proporcione las credenciales de autenticación.

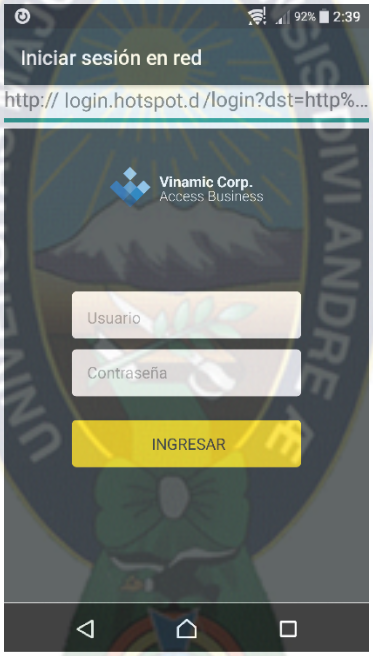


Figura 3.2: Portal de autenticación Hotspot

Las credenciales, como se mencionó en el capítulo dos, se encuentran compuestas por un usuario y una contraseña. Y son proporcionados por el administrador de red de la empresa, donde el usuario pasa previamente por un registro.

3.1.3 Proceso de Autenticación

Vamos a describir el proceso de autenticación en redes inalámbricas que utilizan el protocolo de cifrado WPA2-Enterprise.

La Figura 3.3 tiene dos procesos iniciales para la autenticación de usuarios, el primer proceso inicia cuando el usuario hace primer uso de la red, selecciona el SSID correspondiente en la

lista de conexiones Wi-Fi disponibles, ingresa al *Hotspot* y una vez dentro se escriben las credenciales compuestas por un nombre de usuario y una contraseña, el servidor verifica la información, si es correcta se permite el acceso a la red, de ser incorrecta se deniega el acceso y se re direcciona al portal, para que el usuario ingrese nuevamente la información.

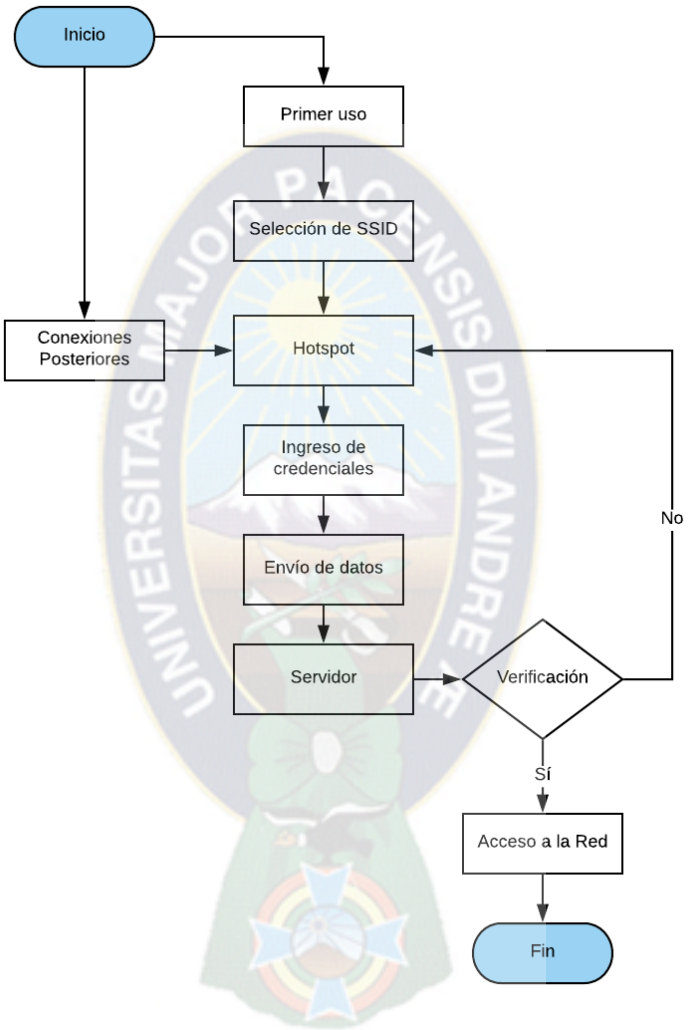


Figura 3.3: Diagrama de comportamiento de la situación actual

El segundo proceso sucede cuando el usuario se desconecta de la red. Los móviles y portátiles tienen una lista interna de redes a las cuales se tuvo acceso y existe una configuración que permite guardar las SSID. En este caso al volver a conectarse, el usuario no necesita seleccionar el SSID. Sólo debe ingresar al portal *Hotspot* para ingresar las credenciales y continuar con el procedimiento.

- **Nuevos Dispositivos**

  Las credenciales pueden ser usadas en cualquier dispositivo, pero sólo pueden ser utilizadas con un dispositivo a la vez. Por lo tanto, si el usuario quiere usar dos dispositivos al mismo tiempo con las mismas credenciales, el sistema no cubrirá esa necesidad.

  Para agregar un nuevo dispositivo, el usuario debe ponerse en contacto con el administrador de red para que pueda proporcionarle nuevas credenciales.

3.2 Definición de Requerimientos

En esta actividad se plantearán los requerimientos que se apoyan en el análisis realizado en la sección 3.1.

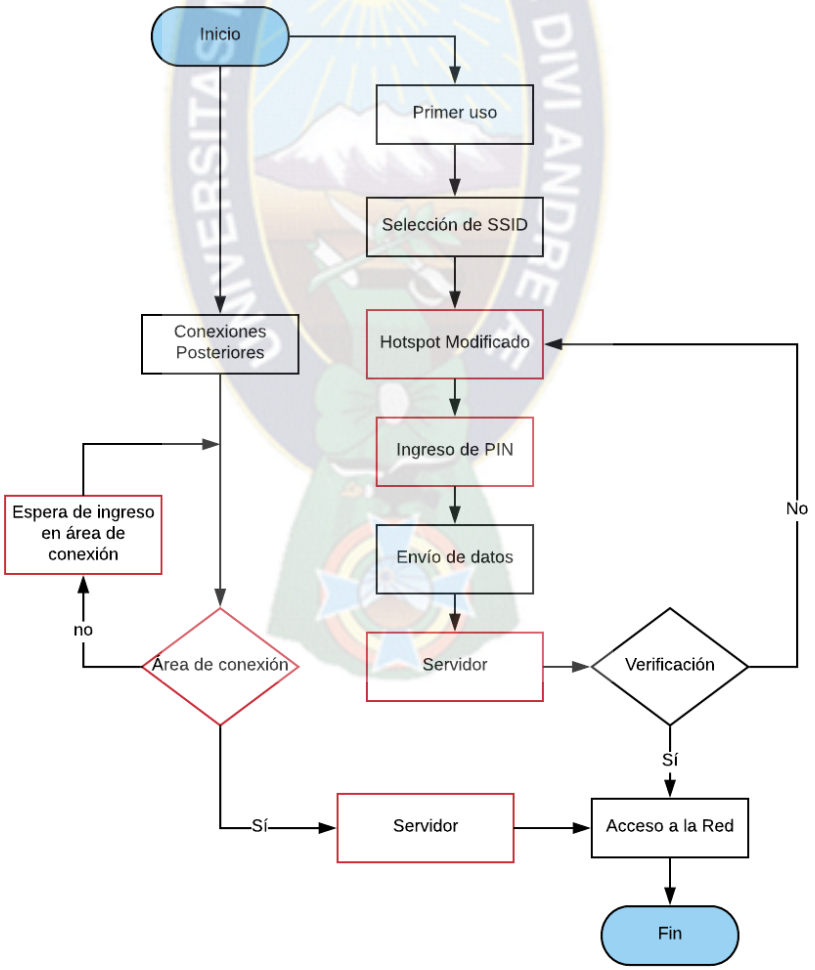


Figura 3.4: Diagrama de comportamiento del modelo propuesto

Se propone que el usuario realice el proceso de autenticación únicamente la primera vez. Para posteriores conexiones, se brindará el acceso de manera automática. En ambos casos, no deberá hacerse uso de ninguna credencial. El resultado será similar al protocolo WPA2-Personal donde sólo es necesario ingresar la clave durante la primera vez, sin embargo, mantendrá el protocolo de seguridad WPA2-Enterprise, donde cada usuario tiene una credencial de acceso distinta.

En la Figura 3.4 se observa el nuevo comportamiento del modelo propuesto donde se agrega el área de conexión como un bloque de decisión para tener acceso a la red. Se muestra algunas modificaciones en contraste con la Figura 3.3. Estas modificaciones colaborarán con la propuesta de autenticación automática.

3.2.1 Hotspot Modificado

El *Hotspot* o portal de acceso sólo recibirá un parámetro de entrada, es decir que el portal que opera como formulario enviará al servidor únicamente un valor para ser verificado durante la primera vez.

3.2.2 PIN

Los usuarios utilizarán un código PIN para el acceso durante la primera vez, al igual que un nombre de usuario este no debe repetirse. El administrador de red será el que decida cuál será el identificador único y su longitud. Este puede resultar ser una cadena formada entre números y letras, números únicamente o letras.

3.2.3 Área de conexión

El área de conexión será un espacio circunferencial dentro del cual los usuarios pueden acceder a la red, al ingresar serán autenticados. Cuando los usuarios salgan del área de conexión el acceso a la red les será denegado, es decir, al salir serán desautenticados. Para definirla se utilizará la intensidad de señal que el *Access Point* proporciona y será medida en dBm como se ilustra en la Figura 3.5.

3.2.4 Servidor

El servidor será el encargado de monitorear el estado del *Access Point* en un intervalo de tiempo recurrente, y este será el que detectará de manera automática el ingreso de usuarios dentro del área de conexión. El servidor utilizará una base de datos que contiene la información de los

usuarios y PIN's de acceso, posteriormente guardará la información de sus credenciales de acceso por dispositivo al hacer uso de sus direcciones MAC.

Figura 3.5: Área de conexión y comportamiento

3.3 Definición de la Arquitectura Lógica

Describiremos los componentes del modelo a fin de observar los bloques que interactúan entre sí para realizar la autenticación automática.

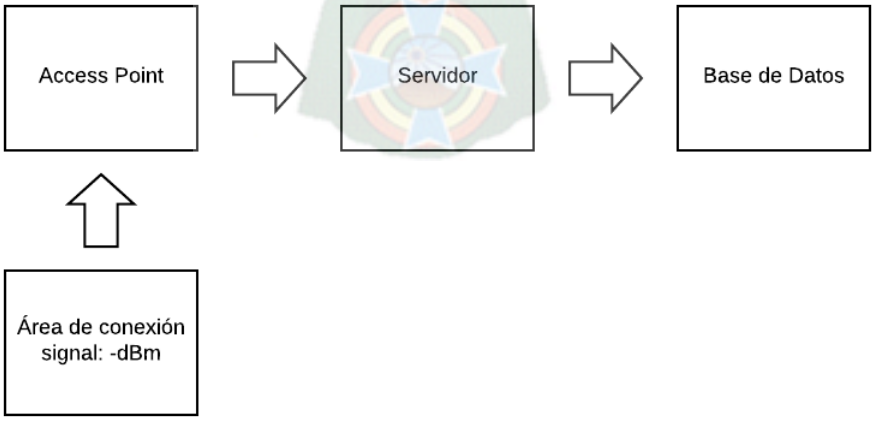


Figura 3.6: Diagrama de bloques, componentes lógicos

En la Figura 3.6 se puede observar una representación lógica de la ilustración realizada en la Figura 3.5, donde el *Access Point* se señala en color rojo y es el que controla el área de conexión. Su relación es uno a uno debido a que un *Access Point* sólo puede administrar un área de conexión. Aunque el servidor no se encuentra representado en la Figura 3.5 este se encargará de monitorear el *Access Point* y guarda una relación de dependencia ya que a través del mismo se hacen las lecturas de señal entre otras acciones como acceso de dispositivos y las bajas respectivamente.

Por último, se tiene la base de datos donde se guarda la información que se recopilará acerca de los dispositivos, las operaciones con la base de datos incluyen altas, bajas y consultas de dispositivos por su dirección física.

3.4 Síntesis de Arquitectura Candidata Asignada

En el desarrollo de la actividad se describirán las relaciones y comportamiento entre los componentes descritos en la sección 3.3 y para facilitar una mejor comprensión el proceso de análisis será dividido en tres procesos principales.

Se identificarán además los estados de los dispositivos, acciones de usuario y acciones de sistema dentro del modelo.

3.4.1 Proceso de Autenticación

Existen tres casos donde el proceso de autenticación toma lugar: el primer uso, conexiones posteriores y cuando se desea brindar acceso a la red a nuevos dispositivos.

a) Primero Uso

Durante el primer uso, dentro del área de conexión el usuario deberá ingresar el PIN en el portal *Hotspot,* el servidor procesará la información realizando una búsqueda en la base de datos. Al encontrar una coincidencia generará las credenciales. Tanto el usuario como la contraseña contenidas dentro de la credencial serán cadenas de una longitud de 32 símbolos hexadecimales proporcionadas por el uso del algoritmo de codificación MD5. Por otra parte, se salvará la información de la dirección física del dispositivo MAC, para que en futuras conexiones las credenciales se recuperen sin hacer uso del PIN, sino directamente por el uso de la dirección física. Estas credenciales y la dirección MAC se guardarán en la base de datos trazando una relación con la coincidencia encontrada anteriormente.

Terminado el procedimiento, el servidor cargará la información de las credenciales generadas al *Access Point* para completar el proceso de autenticación y brindar al usuario el acceso a la red.

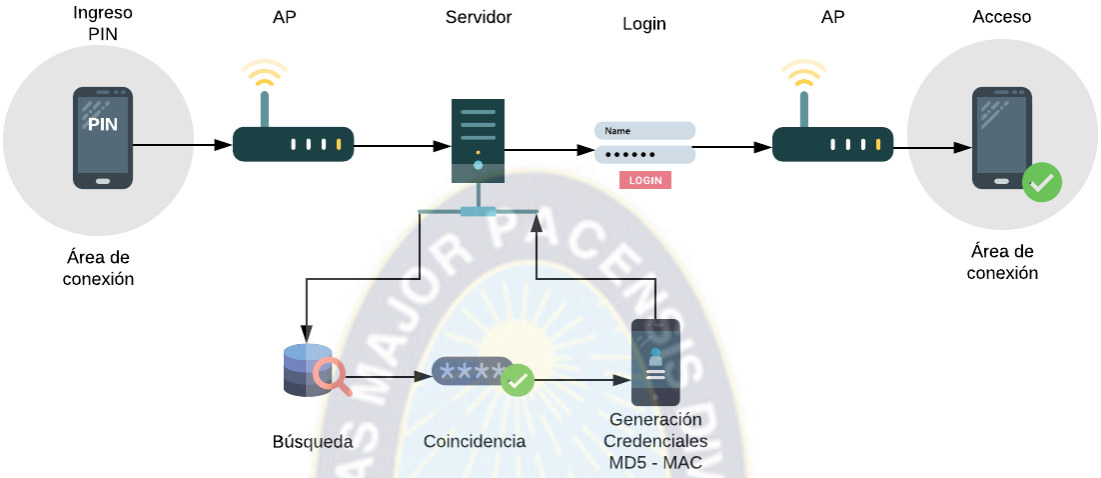


Figura 3.7: Diagrama de primero uso del modelo propuesto

b) Conexiones Posteriores

Durante las siguientes conexiones, el usuario no debe ingresar ningún PIN. Sólo deberá encontrarse dentro del área de conexión, así el servidor identificará el dispositivo por la dirección física MAC, buscará las credenciales correspondientes en la base de datos y cargará la información de las credenciales al *Access Point* para brindar el acceso a la red.

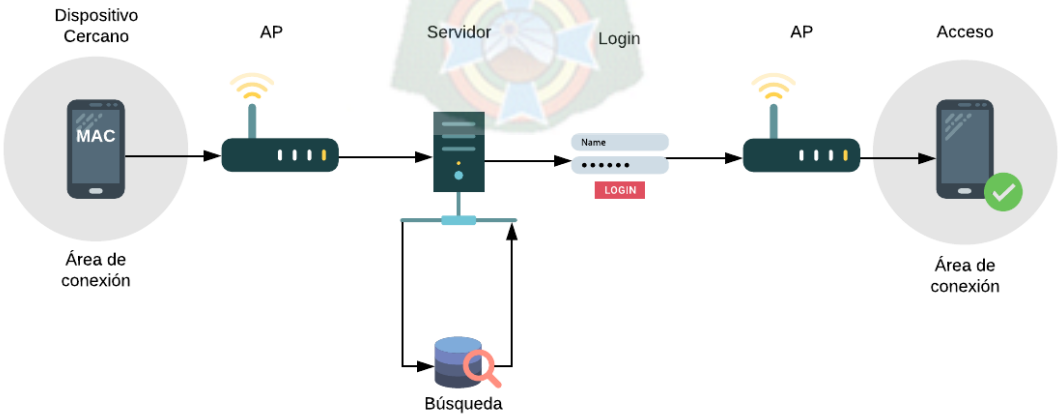


Figura 3.8: Diagrama de conexiones posteriores del modelo propuesto

c) Nuevos Dispositivos

Para agregar nuevos dispositivos el usuario hará uso de un *token*, este será generado desde cualquiera de los dispositivos que el usuario ya tenga agregado.

En el nuevo dispositivo, el usuario deberá ingresar el *token*. El servidor se encargará de generar las credenciales correspondientes como en el caso de primer uso. La diferencia con el caso de primer uso radica en la definición de este código. El *token* sólo podrá ser usado por un intervalo de tiempo corto, que en muchos casos son minutos.

Uno de los valores a tomar en cuenta será el número de dispositivos que puede tener un usuario dentro del a red. Dependerá del administrador de red establecer el número.

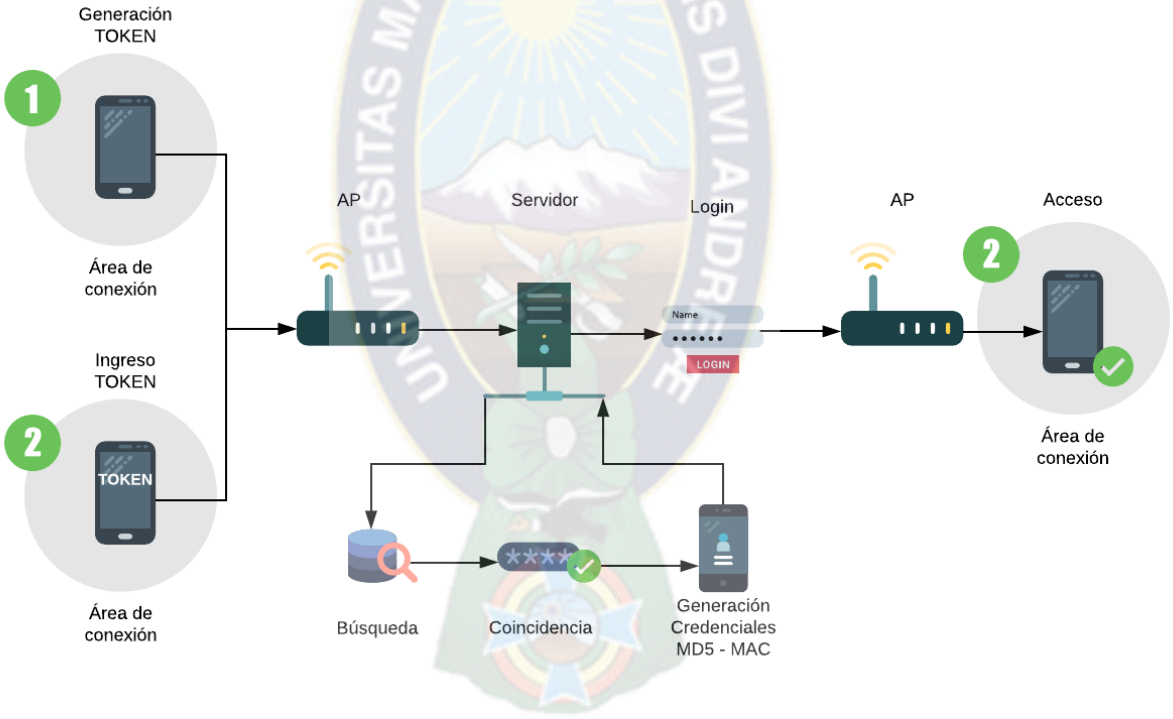


Figura 3.9: Diagrama de acceso de nuevos dispositivo con el uso de Tokens

Un aspecto importante es que ambos dispositivos deben encontrarse dentro del área de conexión, tanto para producir el *token* como para ingresarlo y producir las credenciales respectivas.

3.4.2 Identificación de Estados de dispositivos

A continuación, se describirá los estados posibles de los dispositivos dentro del modelo:

Tabla 3.1: Estados de los dispositivos conectados

Área	Estado	Acción
Dentro	Activo	Sin Acción
Dentro	Inactivo	Autenticación
Fuera	Activo	Desautenticación
Fuera	Inactivo	Sin Acción

3.4.3 Identificación de Acciones del Usuario

La siguiente tabla describe las acciones del usuario dentro del modelo:

Tabla 3.2: Acciones del usuario dentro del modelo

Acción	Descripción
Ingreso y envío de PIN	El usuario escribe su PIN de usuario para agrega el primer dispositivo.
Obtención de *Token*	El usuario obtiene un *Token* desde cualquier dispositivo que ya tenga agregado.
Ingreso y envío de *Token*	El usuario ingresa el *Token* para agregar un nuevo dispositivo.

3.4.4 Identificación de Acciones del Sistema

Describiremos las acciones que se ejecutarán según el estado del dispositivo descrito en el punto 3.4.2 y las acciones del usuario descrito en el punto 3.4.3.

a) Generación de credenciales

Esta acción realizará una escritura en la base de datos con la cual el servidor realiza una comunicación.

El disparador de esta acción será el ingreso del PIN que el usuario posee, sin olvidar que el dispositivo debe encontrarse dentro del área de conexión.

El primer paso será la búsqueda del PIN en la base de datos. Para la cual únicamente debe encontrarse una coincidencia. Seguidamente se hará una escritura en la base de datos, los campos serán: usuario y contraseña. Además, se salvará la información de la dirección física del dispositivo en un tercer campo.

Tanto el usuario y la contraseña pasarán por un proceso de codificación antes de ser almacenados en la base de datos. Sin importar el tamaño de la cadena que se vaya a introducir, el algoritmo MD5 extenderá la longitud a 32 caracteres, que sería muy difícil de recordar para los usuarios, pero muy útil contra ataques de diccionarios, por ejemplo.

Aunque el algoritmo ya ha sufrido ataques por colisión como se indica en el apartado 2.7.1 se prefiere su uso en el modelo debido al tiempo de obtención del *hash* de salida, recordando que los resultados *hash* de otros algoritmos como la variante SHA son más difíciles de romper, pero así también tienen un costo mayor durante el procesamiento de cadenas de entrada.

Tabla 3.3: Ejemplo de campos de credencial a almacenar en la base de datos

Usuario	1b9fc01e98389d29c1506fe944b07d16
Contraseña	457d171a987226c13b3ec72dfcd35ae
Mac-address	B4-4E-2C-FC-EB-FE

Los tres campos deberán ser instanciados en la base de datos como cadenas de texto *varchar*.

b) Búsqueda de dispositivos

Esta acción usará el intervalo de búsqueda de dispositivos introducido anteriormente (ver pág. 45) donde se menciona que será recurrente. Una vez iniciado el servidor ingresará en un ciclo. En cada ciclo realizará la búsqueda de dispositivos consultando el *Access Point* a través del uso de comandos proporcionados por el API de *Mikrotik* según el lenguaje de programación que se haya seleccionado.

Una vez enviados los comandos de la consulta al *Access Point* este responderá con una lista de todos los dispositivos conectados a la misma SSID.

La información de la lista será separada por grupos: dispositivos inactivos y dispositivos activos. Para esto realizaremos otra consulta al *Access Point* para ver que dispositivos están activos verificando los ítems de la segunda lista con la primera, así se obtendrá la lista de todos los dispositivos inactivos. El trabajo en ambas listas se describirá en los puntos c) y d) respectivamente.

c) Autenticación

Para completar la autenticación revisaremos la lista de dispositivos inactivos. Nuevamente se separará la información en dos grupos: dispositivos registrados y dispositivos no registrados.

Para obtener la lista de usuarios registrados se realizará una consulta a la base de datos. La consulta deberá recuperar la información de: la dirección física MAC, usuario y contraseña. Se buscará la dirección física MAC de cada dispositivo de la lista de inactivos, en la consulta.

Haremos referencia a esta lista resultante como: usuarios inactivos registrados.

En este punto, se comenzará a recorrer la lista ítem por ítem, verificando que el dispositivo se encuentre dentro del área de conexión. De no encontrarse dentro del área de conexión no habrá acción alguna y se pasará al siguiente ítem. En caso de cumplir con el requisito se realizará una escritura en el *Access Point* del usuario y contraseña correspondiente.

Al final de cada procedimiento se ingresará un comando para que el dispositivo se autentique.

Durante las consultas al *Access Point* no se devuelve la lista de dispositivos con hora y fecha de conexión al SSID. Pero se debe mencionar que la lista si se encuentra organizada de manera cronológica.

Para el tratamiento de información se utilizará el concepto de *First In, First out* o primero en entrar, primero en salir. Para prevenir cualquier inconveniente, los dispositivos que se hayan unido a la red primero serán los primeros en autenticarse.

d) Desautenticación

Como proceso inverso, se tomará la lista de dispositivos activos. Se comenzará a recorrer ítem por ítem verificando si estos se encuentran fuera del área de conexión. Si se encuentran dentro no se realizará acción alguna, se pasará directamente al siguiente ítem.

En el caso de encontrarse fuera, se hará una escritura en el *Access Point*, borrando el usuario y la contraseña que como resultado tendrá la desautenticación del dispositivo.

No es necesario que la desautenticación siga un orden como el *First In, First out*, pero puede incluirse de ser necesario.

En la Figura 3.10 se muestra un resumen realizado a través del uso de diagramas de ven, donde se observa que para autenticar un dispositivo será necesario que esté inactivo, se encuentre

dentro del área de conexión y además se encuentre registrado, haciendo referencia a la generación de sus credenciales.

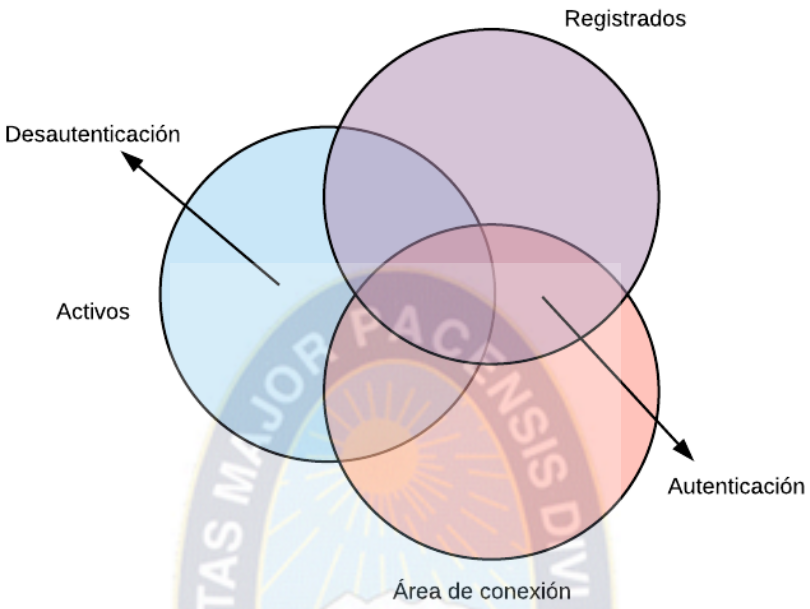


Figura 3.10: Diagrama de Venn, autenticación y desautenticación

Para desautenticar un dispositivo sólo es necesario que el dispositivo se encuentre fuera del área de conexión y esté activo.

e) Generación de Token

Desde uno de los dispositivos que el usuario tenga agregado, se podrá ejecutar esta acción en el sistema.

Una vez ejecutado, el sistema generará de manera aleatoria un código de longitud definida por el administrador de red. Este código en particular sólo aparecerá en el dispositivo desde el cual se hizo la llamada a la acción.

El código será guardado en la base de datos con dos campos: *token* y dirección física MAC. La dirección física hará referencia al dispositivo al cual se envía el *token* y el cual inicia la acción.

Tabla 3.4: Ejemplo de campos token a almacenar en la base de datos

Token	78546
Mac-address	B4-4E-2C-FC-EB-FE

El intervalo de tiempo de duración del *token* será de minutos y dentro de ese intervalo el usuario deberá introducirlo en el otro dispositivo. Para la destrucción del *token* se utilizará una función que hará una cuenta regresiva del intervalo de duración, al finalizar se iniciará un proceso de escritura en la base de datos para eliminar el token. Otra acción que destruirá el *token* será su uso, una vez utilizado el *token* también será eliminado.

f) Generación de Credenciales por Token

Dentro del intervalo de duración, una vez ingresado el *token,* el sistema realizará un proceso de acciones similar al descrito en el apartado a), realizará primero una búsqueda del *token* en la base de datos. Encontrará la única coincidencia y comenzará el proceso de escritura de usuario, contraseña y dirección física del nuevo dispositivo.

Los campos de usuario y contraseña tendrán una longitud de 32 caracteres resultado del uso del algoritmo MD5.

3.5 Optimización

Como indica la documentación este proceso se implementa a través de todas las actividades a fin de optimizar la arquitectura candidata. Dado que la investigación es un modelo propuesto no se seleccionará una arquitectura preferida según indica la actividad en la metodología. Utilizaremos esta sección para describir algunos aspectos que podría afectar el desempeño del modelo.

3.5.1 Identificación de Variables de Tiempo de Respuesta

Entre el ingreso dentro del área de conexión y la autenticación automática, existe un intervalo de tiempo necesario para las asignaciones IP, lecturas de intensidad de señal y el intervalo de búsqueda de nuevos dispositivos que se encuentra relacionado con los dos valores anteriores.

a) Tiempo Asignación IP

Una vez que el usuario selecciona un SSID o nombre de red al cual desea conectarse, el *Access Point* que usa un DHCP server asigna una dirección IP al dispositivo. El tiempo de asignación varía de entre dispositivos debido a que el DHCP también envía la información de configuración de acceso a la red, mostraremos un ejemplo a continuación.

Tabla 3.5: Tiempo de asignación IP

Modelo	Asignación IP (seg)
Xperia C2304	7.565
Xperia F3313	3.657

En la Tabla 3.5 se muestra dos valores de ejemplo. Los dispositivos son de la misma marca y distinto modelo. Se observa que los tiempos de asignación varían entre dispositivos, así el hardware juega un papel importante.

b) Tiempo de Lectura de Cambio de Posición

Es importante analizar este valor ya que las redes inalámbricas se implementan para el uso de dispositivos móviles. Quiere decir que el dispositivo constantemente estará cambiando de posición.

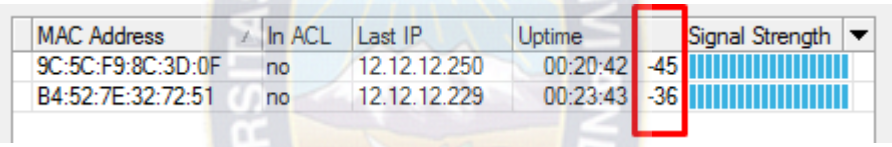


Figura 3.11: Lectura de señal por dispositivos en el Access Point

Los valores enmarcados en rojo en la Figura 3.11 muestran la intensidad de señal de cada dispositivo conectado al *Access Point.* Estos valores se actualizan cada vez que el dispositivo cambia de posición. Pero no se actualizan en tiempo real, la velocidad de actualización dependerá del hardware de cada dispositivo. La siguiente tabla muestra el tiempo en el cual el *Access Point* tarda en reconocer la nueva posición del dispositivo.

Tabla 3.6: Tiempo de actualización de intensidad de señal

Modelo	Actualización (seg)
Xperia C2304	10.282
Xperia F3313	5.923

c) Intervalo de Búsqueda Dispositivos

Cada vez que un dispositivo ingrese en el área de conexión el servidor debe autenticarlo y si el dispositivo sale del área, el servidor debe desautenticarlo. El monitoreo se realizará por

intervalos de tiempo recurrentes. Para definir este intervalo de tiempo se debe incluir la información de tiempo de asignación IP y el tiempo de lectura de cambio de posición.

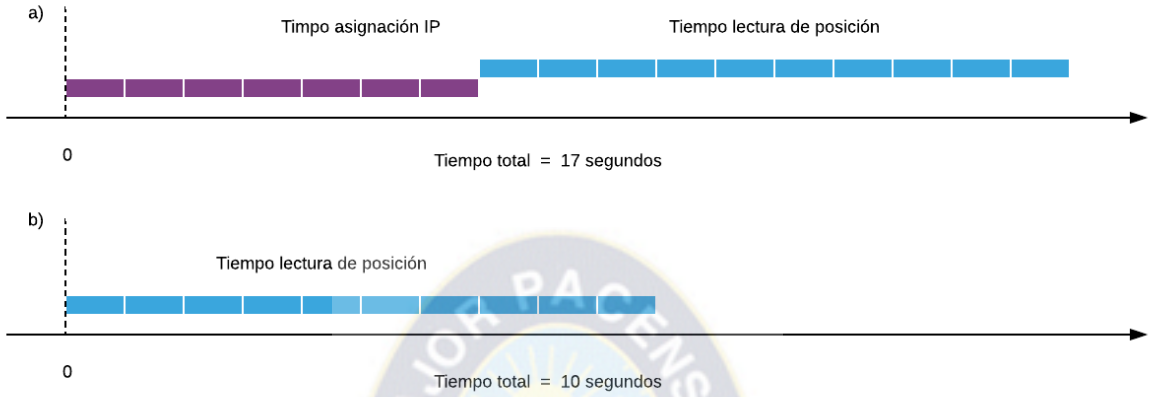


Figura 3.12: Casos de tiempo total de lectura

Antes de definir el intervalo final, debemos analizar los casos mostrados en la Figura 3.12. El caso a) toma en cuenta el tiempo de asignación de IP y el tiempo de lectura de posición. Este caso sucede cuando el usuario ingresa por primera vez al área de conexión o cuando definitivamente se aleja al punto donde la señal del *Access Point* no lo alcanza y vuelve a ingresar en la red.

El caso b) ocurre cuando el usuario sale y entra del área de conexión, su configuración de red e IP aún continúan en el dispositivo, pero el usuario no tiene acceso a la red. Cuando el usuario ingrese nuevamente en el área de conexión el *Access Point* no necesitará asignarle una dirección IP.

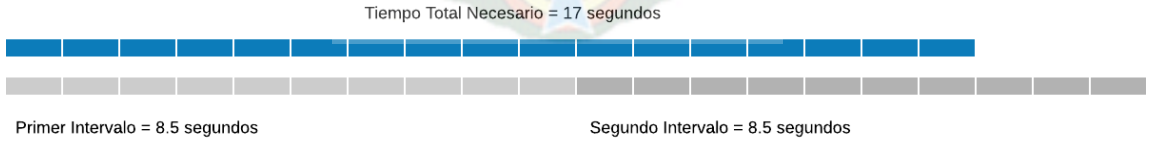


Figura 3.13: Intervalo recurrente resultante

Ahora analicemos el intervalo de búsqueda de dispositivos que resulta del análisis anterior. En la Figura 3.13 se muestra que el intervalo adecuado es 8.5 segundos, tomando en cuenta el caso a) de la Figura 3.12. El servidor revisará el *Access Point* cada 8.5 segundos para ver el estado de los dispositivos. Claramente se puede observar que, si el dispositivo no se autentica en el

primer intervalo, lo hará en el segundo. Si analizamos el caso b) de la Figura 3.12 el dispositivo se autenticará durante el primer intervalo.

Todo el análisis es resultado de analizar el dispositivo usado como ejemplo Xperia C2304 debido a su tiempo de respuesta más alto. Si ingresamos el dispositivo Xperia F3313 vemos que su tiempo total es menor que 8.5 segundos por lo que se autenticará durante el primer intervalo.

3.6 Validación y Verificación

Durante esta actividad, se procederá a verificar la funcionalidad del modelo propuesto de acuerdo a la actividad de optimización y evaluación, adicionalmente se realizó la corrección de defectos encontrados. Para validar y verificar el modelo se realizó la construcción de un prototipo construido de acuerdo a los requerimientos planteados en el modelo propuesto.

3.7 Prototipo

Para la prueba de hipótesis respectiva se desarrolló un prototipo que utiliza un servidor asíncrono con lenguaje de programación NodeJS. También hace uso de un *Access Point* de la marca Mikrotik como se especifica en el modelo de autenticación propuesto. Se implementó una base de datos no relacional MongoDB donde se almacena la información de PIN de acceso para cada usuario, así como la información relacionada a los *tokens* para agregar nuevos dispositivos.

3.7.1 Access Point

Se realizó las configuraciones necesarias para el acceso al API de Mikrotik para el control del dispositivo. Se activó el puerto de conexión y se añadió la información necesaria para el acceso por parte del servidor como el usuario y la contraseña. Además, se configuro el servidor DHCP para una adquisición de IP automática y se configuró la red inalámbrica utilizando los protocolos de seguridad WPA2-Enterprise como se indica en el modelo.

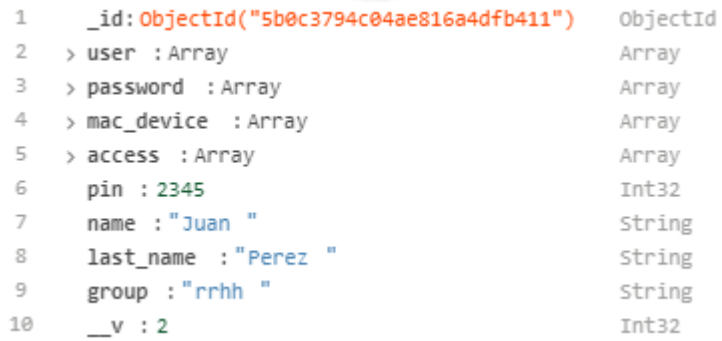


Figura 3.14: Visualización de datos con MongoDB Compass

3.7.2 Base de Datos

Como se mencionó anteriormente se hizo uso de una base de datos no relacional, donde se almacenan algunos campos requeridos además del PIN de usuario, ver Figura 3.14.

```
app.post('/access',function(req,res){
    console.log("\nPin ingresado: " + req.body.pin);
    console.log("Dispositivo: "+req.body.mac);
    Client.findOne({pin:req.body.pin}, function (error, client){
        if (error){
            console.log(error);
            res.redirect('http://login.wana.com/status');
        }
        else{
            if(client!=null){
                console.log("Usuario: " + client.name + " " + client.last_name);
                console.log('Dispositivos: '+client.mac_device.length);
                if(client.mac_device.length==0){
                    console.log('Enlazando dispositivo...');
                    mainDevice(client.id, req.body.mac, Client, req.body.ip, res);

                }else{
                    console.log('Ya tiene un dispositivo emparejado...');
                    res.redirect('http://login.wana.com/status');
                }
            }
            else{
                console.log('Usuario no encontrado...');
                res.redirect('http://login.wana.com/status');
            }
        }
    });
});
```

Figura 3.15: Fragmento de código del prototipo

3.7.3 Hotspot

Se modificó el *hotspot* para que responda a las necesidades del modelo incluyendo únicamente los campos de PIN y *Token*.

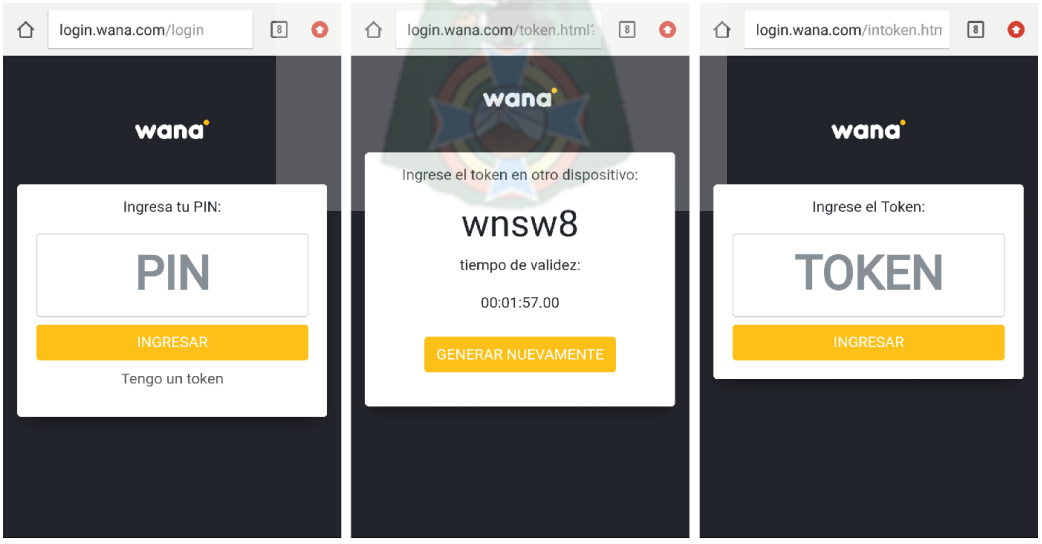


Figura 3.16: Hotpost, ingreso de PIN y Token

3.7.4 Servidor NodeJS

El servidor contiene el código necesario como se puede observar en la Fragmento de código del prototipoFigura 3.15 y se encuentra escrito en lenguaje *Javascript*, dentro del código se administra las credenciales para el acceso y control del *Access Point*, la conexión con la base de datos no relacional, entre otras configuraciones como los intervalos de búsqueda de dispositivos, configuraciones de área de conexión y funciones necesarias para producir el comportamiento especificado en el modelo.

3.8 Contraste de Hipótesis

Se considera la hipótesis planteada en el primer capítulo:

Un modelo de generación y autenticación automática de credenciales en redes inalámbricas Wi-Fi corporativas, basado en el control por áreas de conexión con Mikrotik, produce una ganancia del 45% en tiempo de autenticación sin afectar el nivel de seguridad.

Para comprobar la hipótesis se utilizará el método estadístico t-Pareada, que trabaja con dos muestras estadísticas, en la sección 3.8.1 se describirán las regiones respectivas a la prueba.

3.8.1 Prueba t-Pareada

La prueba t-Pareada posee dos regiones, una región de rechazo y una región de aceptación. Las representación de regiones puede observarse en la Figura 3.17.

La región de rechazo o región crítica formado por un conjunto de valores del estadístico nos lleva a rechazar la hipótesis nula H_0, la región de aceptación o región de No rechazo estará formado por el conjunto de valores de contraste que nos lleva a aceptar la hipótesis H_0.

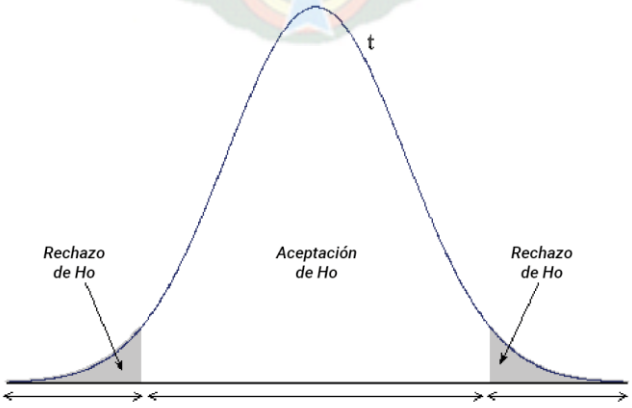


Figura 3.17: Región de rechazo y aceptación

3.8.2 Planteamiento de la Hipótesis Nula y Alternativa

A continuación, en la Tabla 3.7 se plantea la hipótesis nula (H_0), y la hipótesis alternativa (H_1) deacuerdo a la presente investigación.

Tabla 3.7: Hipótesis nula e hipótesis alternativa

Hipótesis	
H_0	El modelo de generación y autenticación de credenciales basado en el control por áreas de conexión NO produce una ganancia de tiempo.
H_1	El modelo de generación y autenticación de credenciales basado en el control por áreas de conexión produce una ganancia de tiempo.

3.9 Desarrollo experimental y recolección de datos

Para la recolección de datos se obtuvo la colaboración de la empresa AGADON S.R.L. que se dedica a desarrollar soluciones dentro del área de infraestructura de servicios tecnológicos como ser: infraestructura de comunicaciones, infraestructura de centro de datos, *networking* y TI, infraestructura de energía, seguridad electrónica y seguridad informática. La población para las pruebas respectivas serán los usuarios de la empresa con un tamaño de la muestra de 15 usuarios.

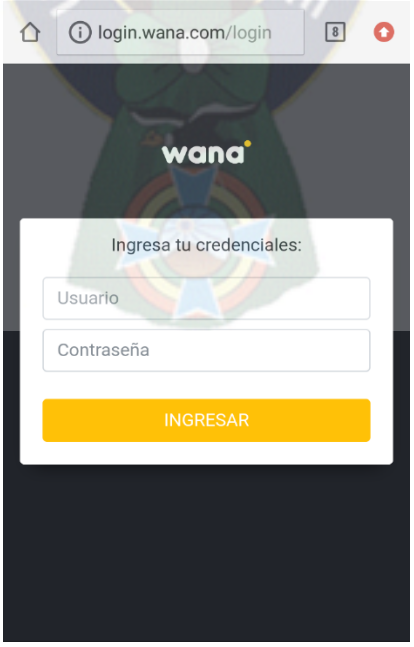


Figura 3.18: Autenticación por credenciales, primera recolección de datos

3.9.1 Procedimiento

Para las pruebas respectivas la población de estudio pasará por dos procedimientos de recolección de datos. El primer procedimiento se someterá a una autenticación común con el protocolo WPA2-Enterprise a través del uso de credenciales (ver Figura 3.18).

Posteriormente la misma población de estudio será sometida a la autenticación WPA2-Enterprise implementando las modificaciones basadas en el modelo propuesto.

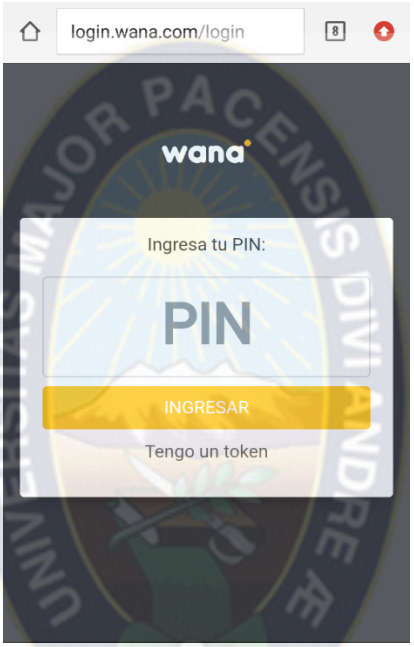


Figura 3.19: Autenticación con PIN de acceso, segunda recolección de datos

3.9.2 Tabla de datos

Los resultados de la recolección de datos de ambos procedimientos, autenticación común y autenticación basado en el modelo propuesto se muestran en la siguiente tabla:

Tabla 3.8: Tiempo de autenticación común y modelo propuesto

Usuario	Autenticación común (s)		Autenticación modelo propuesto (s)	
Nro	1ra Conexión	2da Conexión	1ra Conexión	2da Conexión
1	33.901	33.901	11.439	18.419
2	29.587	29.587	25.489	21.546
3	54.233	54.233	24.275	23.487
4	59.768	59.768	24.175	24.126
5	50.520	50.520	21.226	18.947
6	39.657	39.657	31.485	24.659
7	49.891	49.891	24.853	19.432

8	31.737	31.737	16.858	14.102
9	38.478	38.478	32.125	23.125
10	51.267	51.267	19.342	15.786
11	47.378	47.378	21.945	16.876
12	31.234	31.234	19.478	16.546
13	41.156	41.156	31.562	20.273
14	28.493	28.493	26.378	19.867
15	47.589	47.589	25.572	18.283

La Tabla 3.8 muestra la información obtenida acerca de los tiempos de primera conexión y segunda conexión. Para el tiempo de la segunda conexión en la autenticación común se decidió copiar el valor de la primera conexión debido a que es una acción que se repite y no existe modificación alguna.

3.9.3 Valores Para la Prueba

Para la prueba se tomarán en cuenta los valores de la segunda conexión en la autenticación común y la autenticación del modelo propuesto dado que reflejan en su mayor parte el comportamiento y procedimiento de autenticación.

3.10 Procedimiento de la Prueba t-Pareada

A continuación, se observa los cálculos realizados con la obtención de datos de la evaluación de tiempo de autenticación común y la autenticación basado en el modelo propuesto.

- **Prueba de Normalidad Chapiro Wilk**

  Nivel de significancia

  $$\alpha = 0.05$$

  Normalidad

  Prueba de normalidad Chapiro Wilk para muestras pequeñas (<30 individuos).

  Donde:

  $P - valor \geq \alpha, se\ acepta\ H_o =$ los datos provienen de una distribución normal.

  $P - valor < \alpha, se\ acepta\ H_1 =$ los datos NO provienen de una distribución normal.

  Valor para la prueba de normalidad Chapiro Wilk:

$$\alpha = 0{,}05$$

En la Figura 3.20 se puede observar la prueba de normalidad aplicada a la segunda conexión de la autenticación común. El valor obtenido para P es de 0,37.

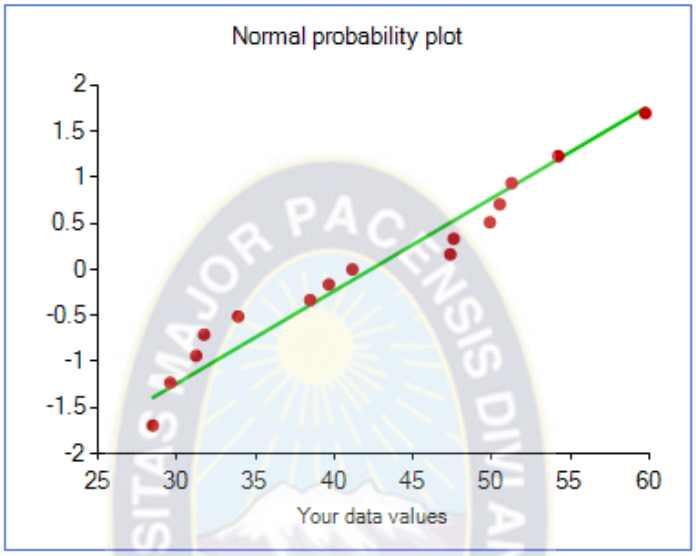


Figura 3.20: Normalidad de la segunda conexión en la autenticación común

En la Figura 3.21 se observa la prueba de normalidad aplicada a la segunda conexión de la autenticación basado en el modelo propuesto. Donde P tiene un valor de 0,783.

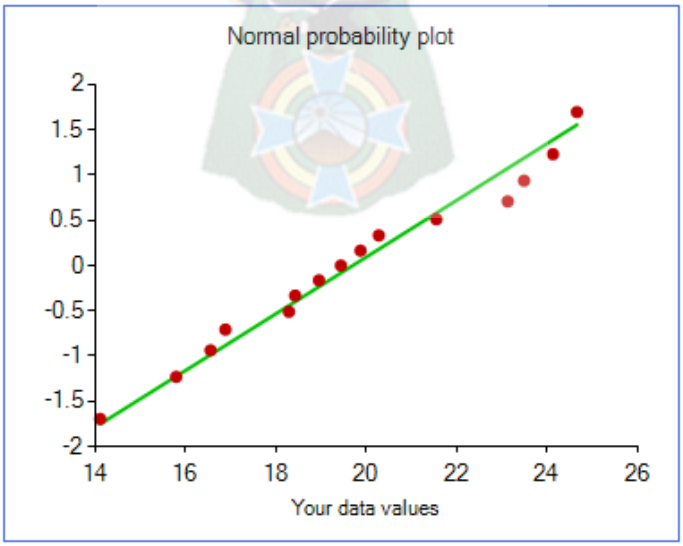


Figura 3.21: Normalidad de la segunda conexión en la autenticación propuesta

Conclusión

Tabla 3.9: Resultados P-valor prueba Chapiro Wilk

Normalidad		
P-valor (autenticación común) = 0,37	>	$\alpha = 0{,}05$
P-valor (autenticación propuesta) = 0,783	>	$\alpha = 0{,}05$

Los datos provienen de una distribución normal como se observa en la Tabla 3.9.

- **Cálculo t-Pareada**

La prueba presenta las siguientes fórmulas para el cálculo estadístico:

$n; tamaño\ de\ la\ muestra$

$x_i; tiempo\ 2da\ conexión\ antes\ del\ uso\ del\ prototipo.$

$x_j; tiempo\ 2da\ conexión\ después\ del\ uso\ del\ prototipo.$

$$t = \frac{\bar{d} - (\mu_2 - \mu_1)}{\frac{S_d}{\sqrt{n}}}\ ; t - pareada$$

$$\bar{d} = \frac{\sum d_i}{n}\ ; promedio\ de\ diferencias$$

$$S_d = \sqrt{\frac{\sum {d_i}^2 - n(\bar{d})^2}{n-1}}\ ; varianza\ de\ diferencias$$

Donde:

$$H_0 : \mu_2 = \mu_1$$
$$H_1 : \mu_2 \neq \mu_1$$

Valores de diferencia

Tabla 3.10: Valores iniciales y diferencia t-Pareada

Usuario	x_i	x_j	d_i	${d_i}^2$
1	33.901	18.419	15.482	239.692
2	29.587	21.546	8.041	64.658
3	54.233	23.487	30.746	945.317
4	59.768	24.126	35.642	1270.352
5	50.520	18.947	31.573	996.854

6	39.657	24.659	14.998	224.940
7	49.891	19.432	30.459	927.751
8	31.737	14.102	17.635	310.993
9	38.478	23.125	15.353	235.715
10	51.267	15.786	35.481	1258.901
11	47.378	16.876	30.502	930.372
12	31.234	16.546	14.688	215.737
13	41.156	20.273	20.883	436.100
14	28.493	19.867	8.626	74.408
15	47.589	18.283	29.306	858.842
Total	**634.889**	**295.474**	**339.415**	**8990.631**

Cálculo de los promedios

$$n = 15$$

$$\bar{d} = \frac{\sum d_i}{n}$$

$$\bar{d} = \frac{339.415}{15}$$

$$\bar{d} = 22.628$$

Cálculo de la varianza de diferencias

$$S_d = \sqrt{\frac{\sum {d_i}^2 - n(\bar{d})^2}{n-1}}$$

$$S_d = \sqrt{\frac{8990.631 - 15(22.628)^2}{15-1}}$$

$$S_d = 9.674$$

Cálculo de la estimación "t"

$$t = \frac{\bar{d} - (\mu_2 - \mu_1)}{\frac{S_d}{\sqrt{n}}}$$

Se dispone que no existe cambio alguno, tomando la hipótesis nula:

$$H_0 : \mu_2 = \mu_1$$

Por lo cual:

$$t = \frac{\bar{d} - 0}{\frac{S_d}{\sqrt{n}}}$$

Reemplazando los valores:

$$t = \frac{22.628 - 0}{\frac{9.674}{\sqrt{15}}}$$

$$t = 9.059$$

Nivel de confianza y grado de libertad

$$\alpha = 0.05\ ; 1 - 0.05 = 0.95\ Nivel\ de\ confianza$$

$$n = 15$$

Grados de libertad:

$$gl = n - 1$$

$$gl = 15 - 1 = 14$$

Tabla t-Student

Se buscan los siguientes valores en la tabla t-Student (ver Anexos)**:**

$$t_{(0,025;14)}$$

El valor correspondiente encontrado es:

$$t_{(0,025;14)} = 2.1448$$

Regla de decisión

$$Si\ t > t_{tab}; se\ rechaza\ H_0\ y\ se\ acepta\ H_1$$

$$Si\ t < t_{tab}; se\ acepta\ H_0\ y\ se\ rechaza\ H_1$$

En la Figura 3.22 se puede apreciar que el valor de t es mayor a t_{tab} y que el valor de t se encuentra dentro de la región de rechazo de H_0.

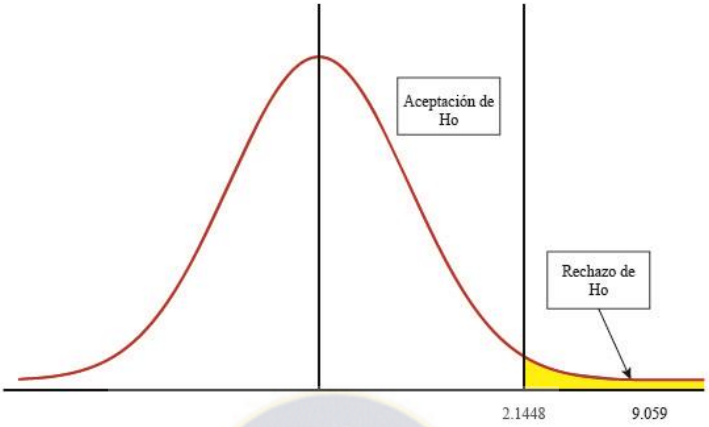


Figura 3.22: Gráfico de área de aceptación de la prueba t-Pareada

Porcentaje de ganancia

Deacuerdo a la fórmula de obtención de medias se tiene que:

$$\overline{x_i} = \frac{\sum x_i}{n}$$

$$\overline{x_i} = \frac{634.889}{15}$$

$$\overline{x_i} = 42.326$$

y

$$\overline{x_j} = \frac{\sum x_j}{n}$$

$$\overline{x_j} = \frac{295.474}{15}$$

$$\overline{x_j} = 19.698$$

Donde la diferencia es de:

$$\overline{x_i} - \overline{x_j} = 22.628$$

Que equivale a un 46,54% de ganancia de tiempo.

3.11 Análisis de Resultados

Como t es mayor a t_{tab} se acepta H_1 y se rechaza H_0 con un nivel de confianza del 95% y 14 grados de libertad.

Al aceptarse la hipótesis alternativa H_1 se prueba de manera formal que existe un cambio en el tiempo de autenticación. Pero este cambio como porcentaje de ganancia es del 46,54% el cual supera al 45% estimado en la hipótesis de la presente investigación.

Por lo tanto el modelo de generación y autenticación automática de credenciales en redes inalámbricas Wi-Fi corporativas, basado en el control por áreas de conexión con Mikrotik produce una ganancia del 45% en tiempos de autenticación sin afectar el nivel de seguridad.

CAPÍTULO IV

4 CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

Se produjo una ganancia del 46,54% en tiempo de autenticación en redes inalámbricas Wi-Fi corporativas a través del uso de áreas de conexión.

Existen valores que no se tomaron en cuenta en la presente investigación y que fácilmente pueden pasar desapercibidos, como ser la velocidad en la cual una persona se traslada de un lugar a otro. Se observó que este valor influye en el tiempo de autenticación, debido a que el tiempo de movimiento no es el mismo que el tiempo de autenticación al ingresar dentro del área de conexión.

Otro de los aspectos que influye en los resultados, es el perímetro del área de autenticación, el cual no es uniforme. Ocurre debido a los diferentes tipos, marcas y modelos de antenas que usan los dispositivos. En la Figura 4.1 se puede observar una representación de la variación.

En la etapa de pruebas los usuarios no realizan ninguna acción distinta al ingreso del PIN para acceder a la red inalámbrica. Logrando alcanzar la automatización durante el proceso de registro y generación de credenciales.

El PIN de acceso es de un solo uso, al realizar el uso del mismo se emparejó las credenciales generadas con el dispositivo donde se ingresó el PIN de acceso. La relación, credencial – dispositivo, es única, siendo así que otro dispositivo no puede acceder con las mismas credenciales, logrando así emparejar un único dispositivo a la credencial por medio del PIN durante el primer uso.

A través del uso del área de conexión se logró identificar los dispositivos, recuperar la información como ser la dirección física MAC, e ingresar la información en la base de datos. Al ser un proceso automatizado, durante el emparejamiento con la credencial se logró evitar errores de escritura.

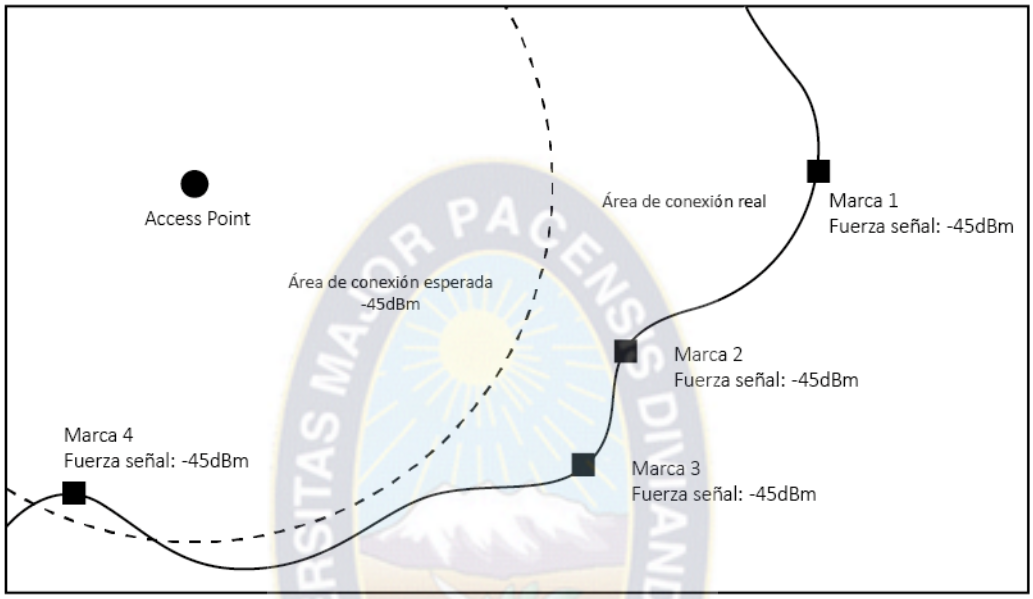


Figura 4.1: Variación del área de autenticación

Los usuarios no necesitaron ingresar ningún componente de la credencial, como ser usuario y contraseña, permitiendo esa automatización agregar el algoritmo de encriptación MD5 el cual logró incrementar la longitud promedio común de 8 a 32 caracteres.

Durante la etapa de pruebas, los usuarios podían trasladarse de un lugar a otro sin la necesidad de preocuparse por la autenticación una vez que la señal se perdía, logrando automatizar el proceso de autenticación por medio del reconocimiento de áreas de autenticación.

La configuración de área de conexión fue realizada en el servidor donde se instanciaba el valor en –dBm. La conexión del *Access Point* con el servidor permitió que este último pudiera hacer las lecturas respectivas logrando controlar el acceso a la red corporativa a través del uso de la intensidad de señal del *Access Point.*

El control de acceso a través del uso del área de conexión fue exitoso, denegando el servicio de acceso a la red a los dispositivos que se encontraban fuera, logrando limitar el uso de la red corporativa dentro de las instalaciones y área definida.

Cada vez que los usuarios realizaban el uso de los PIN's de acceso, la información como fecha y hora fue almacenada en la base de datos, logrando resguardarse la información de acceso.

4.2 Recomendaciones

Como base para investigaciones futuras en la misma línea de investigación, a continuación, se presentan algunas ideas:

- Para obtener un área de autenticación uniforme, se podría almacenar los valores de señal por dispositivo, para que con un algoritmo pueda acercar esos valores al área de autenticación deseada. Reduciendo de esta manera la variación entre áreas de autenticación esperada y la real.
- Se deben ajustar los parámetros como el intervalo de autenticación dentro del servidor deacuerdo a los tipos de dispositivos que se conectarán a la red y su tiempo de respuesta.
- Se puede realizar un estudio sobre un conjunto de nodos dentro de una red inalámbrica extendida, para autenticar dispositivos mientras estos se mueven y así lograr el *roaming* dentro de una red corporativa.

Por último, recordar que el proceso de autenticación en una red corporativa debe trabajar con protocolos de seguridad altos, pero sin descuidar la facilidad de acceso por parte de los usuarios, debido a que la productividad de una empresa está estrechamente relacionada al empleo del tiempo.

Con la evolución tecnológica, se debe tomar en cuenta, incluso las tendencias como BYOD (*Bring Your Own Device*) que cada día se vuelve más generalizado en las empresas; donde los usuarios deciden llevar sus propios dispositivos.

Es así que la generación de credenciales y autenticación, se convierte en un problema que requiere de nuevas soluciones, más requeridas en el área de las comunicaciones inalámbricas Wi-Fi, ya que hoy en día, la portabilidad juega un papel muy importante en la productividad de las empresas.

5 BIBLIOGRAFÍA

Bailey, D., Brainard, J., Juels, A., & Kaliski, B. (2006). *USA Patente nº US9137012B2.*

Ballmann, B. (2012). *Understanding Network Hacks.* Uster, Switzerland: Springer.

Banerji, S., & Singha, R. (2013). On IEEE 802.11: Wireless LAN Technology. *International Journal of Mobile Network Communication & Telematics (IJMNCT)* , 45-64.

Bartoli, A., Medvet, E., & Onesti, F. (2018). Evil twins and WPA2 Enterprise: A coming security disaster? *Computer & Security*, 1-11.

Bell, A. G. (1880). On the production and reproduction of sound by light. *Am J Sci*, 305-324.

Belton, L., Beaty, B., Morris, T., Rodgers, D., & Smith, L. (2012). *USA Patente nº US9088891B2.*

Ben Ayed, M. (2013). *USA Patente nº US8646060B1.*

Carballar, J. (2010). *Wi-Fi Lo que se necesita conocer.* Madrid: RC Libros.

Cárdenas, O., Molina, J., & Armijos, J. (2017). *Los dispositivos inalámbricos de red en el desarrollo académico.* Babahoyo, Ecuador: CIDEPRO.

Castro, R. (2005). Avanzando en la seguridad de las redes WIFI. *RedIRIS.*

Chaabouni, R. (Junio de 2006). *lasec.* Obtenido de lasec.epfl.ch: https://lasec.epfl.ch/pub/lasec/doc/cha06.pdf

Cheney, M. (2009). *Nikola Tesla. El genio al que le robaron la Luz.* US: Turner.

Churchman, C. W., Ackoff, R. L., & Arnoff, E. L. (1957). *Introduction to operations research.* England: Oxford.

Ciampa, M. (2013). *CWNA Guide to Wireless LANs, Thrid Edition.* Boston, MA: Course Technology, Cengage Learning.

Cisco. (2017). *Wireless LAN Design Guide - For high-density client environments in higher education.*

Cisco. (30 de Abril de 2018). Obtenido de https://www.cisco.com/c/dam/en/us/products/collateral/routers/rv180w-wireless-n-multifunction-vpn-router/data_sheet_c78-697399_es.pdf

Cisco. (30 de Abril de 2018). *Cisco Systems, Inc.* Obtenido de https://www.cisco.com/c/dam/global/es_mx/assets/ofertas/desconectadosanonimos/routing/pdfs/brochure_redes.pdf

COIT. (2004). *La situación de las Tecnologías WLAN basadas en el estándar IEEE 802.11 y sus variantes ("Wi-Fi").* Madrid: Colegio Oficial de Ingenieros de Telecomunicación.

Comer, D. E. (2015). *Computer Networks and Internets 6th Edition.* West Lafayette: Pearson.

Comunidad UBNT. (13 de Febrero de 2016). *forum-es.ubnt.com.* Obtenido de https://forum-es.ubnt.com/discussion/1281416/tabla-de-pontencia-wifi

Friedenthal, S., Moore, A., & Steiner, R. (2015). *A Practical Guide to SysML The Systems Modeling Language 3rd Edition.* Waltham, MA: ELSEVIER.

Gaddam, V., Ahmed, S., SHANMUGAM, S., & Rahman, M. (2011). *USA Patente nº US9037118B2.*

Giordano, F., Fox, W., & Horton, S. (2014). *A First Course in Mathematical Modeling Fifth Edition.* Boston, MA: Brooks/Cole, Cengage Learning.

Gonzales, D., Pérez, I., Marquéz, A., & Badillo, L. (2017). Análisis de vulnerabilidades en redes inalámbricas instaladas en diversos municipios del estado de Hidalgo. *Revista de Tecnología Informática*, 32-40.

Goode, H., & Machol, R. (1957). *Systems Engineering.* N.Y.: Mc Graw Hill.

Griffith, E. (02 de Octubre de 2002). *www.internetnews.com.* Obtenido de http://www.internetnews.com/wireless/article.php/1474361/WECA-becomes-Wi-Fi-Alliance.htm

Hart, L. (30 de Junio de 2015). *www.incose.org.* Obtenido de https://www.incose.org/docs/default-source/delaware-valley/mbse-overview-incose-30-july-2015.pdf

IEEE. (30 de Abril de 2018). *standards.ieee.org.* Obtenido de standards.ieee.org: http://standards.ieee.org/develop/regauth/tut/eui.pdf

INCOSE. (20 de 05 de 2018). *www.incose.org.* Obtenido de https://www.incose.org/docs/default-source/wgcharters/object-oriented-se-method.pdf?sfvrsn=6

Key Reinstallation Attacks. (30 de 04 de 2018). *www.krackattacks.com*. Obtenido de https://www.krackattacks.com/

Khan, A.-S. (2010). *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*. CRC Press.

Kiddle. (30 de Abril de 2018). *Kids Encyclopedia*. Obtenido de https://kids.kiddle.com/MAC_address

Lamberti, P. (2009). Las investigaciones de Heinrich Hertz Sobre las Ondas Electromagnéticas. *Revista APFA.*

Lawson, D., & Marion, G. (2008). *people.maths.bris.ac.uk.* Obtenido de https://people.maths.bris.ac.uk/~madjl/course_text.pdf

Lee, J.-S., Su, Y.-W., & Shen, C.-C. (2007). A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee, and Wi-Fi. *The 33rd Annual Conference of the IEEE Industrial Electronics Society (IECON)* . Taipei.

Linksys. (27 de 04 de 2018). *Linksys*. Obtenido de www.linksys.com: https://www.linksys.com/es/r/qu%C3%A9-es-un-extensor-de-red/qu%C3%A9-es-un-punto-de-acceso/

Márquez, J., Pardo, K., & Pizarro, S. (2001). Ethernet: Su origen, funcionamiento y rendimiento. *Ingeniería & Desarrollo. Universidad del Norte*, 22-34.

Mikrotik. (30 de Abril de 2018). Obtenido de https://mikrotik.com/product/RB2011UiAS-2HnD-IN

Mikrotik. (19 de Abril de 2018). *Mikrotik*. Obtenido de Mikrotik: https://mikrotik.com/aboutus

Mikrotik. (2 de Mayo de 2018). *www.mikrotik.com.* Obtenido de https://mikrotik.com/testdocs/ros/2.8/guide/console.php

Mikrotik Wiki. (2 de Mayo de 2018). *Mikrotik Wiki*. Obtenido de https://wiki.mikrotik.com/wiki/Manual:API

Ministry of Justice and Security. (Enero de 2018). *www.forensischinstituut.nl.* Obtenido de https://www.forensischinstituut.nl/binaries/nfi/documenten/publicaties/2018/02/13/vak bijlage-forensisch-gebruik-van-bestandskenmerken-en-bijbehorende-hashalgoritmen/Supplement-hashes-v2018_01a_English.pdf

Ochoa, V. A. (2010). Seguridad en Redes WLAN. *Electiva IV.* Bucaramanga.

OMG. (21 de Mayo de 2018). *Object Management Group, Inc.* Obtenido de http://www.omgwiki.org/MBSE/doku.php?id=mbse:incoseoosem

Onofre, E. (5 de Julio de 2013). *SlideShare.* Obtenido de https://es.slideshare.net/eduardo_onofre123/topologas-y-componentes-de-una-red-inalmbrica

Orange. (15 de Mayo de 2018). Obtenido de https://ayuda.orange.es/particulares/movil/sim-pin-puk/302-como-activar-la-nueva-tarjeta-sim-4g

Pannell, D. (30 de Abril de 2018). *IEEE802.* Obtenido de www.ieee802.org: http://www.ieee802.org/1/files/public/docs2014/New-pannell-MAC-Address-Issues-in-802dot1-1114-v1.pdf

Pathsolutions. (30 de Abril de 2018). *Pathsolutions, Inc.* Obtenido de https://www.pathsolutions.com/mac-addresses-not-a-cheesy-subject/

Pearce, P., & Hause, M. (2012). *www.omgsysml.org.* Obtenido de http://www.omgsysml.org/Pearce_Hause_ISO-15288_OOSEM_and_Model-Based_Submarine_Design_SETE_APCOSE_20121.pdf

Ruz, J., Riveros, B., & Varas, A. (2012). *Redes WPA/WPA2.* Valparaíso.

Saputra, R. (21 de 05 de 2013). *Story of Technology*. Obtenido de http://lagilagiryan.blogspot.com/2013/05/mikrotik-history_21.html

Sari, R., Supiyandi, Utama, A., Muttaqin, M., & Ginting, R. (2017). A Review of IP and MAC Address Filtering in Wireless Network Security. *IJSRST* , 470-473.

Sharma, K., & Dhir, N. (2014). A Study of Wireless Networks: WLANs, WPANs, WMANs, and WWANs with Comparison. *International Journal of Computer Science and Information Technologies*, 7810-7813.

Soldo, I. (2013). Wi-Fi Parameter Measurements and Analysis. *Proceedings of the 9th International Conference, Measurement 2013*, 339-342.

Symantec. (30 de Abril de 2018). *www.symantec.com.* Obtenido de www.symantec.com: https://www.symantec.com/es/mx/security_response/glossary/define.jsp?letter=m&word=mac-address

Tanenbaum, A. (2009). *Ssitemas Operativos Modernos 3ra Edición.* México: Pearson Prentice Hall.

Techopedia. (15 de Mayo de 2018). *Techopedia Inc.* Obtenido de https://www.techopedia.com/definition/12128/personal-identification-number-pin

Trakassure. (2 de Mayo de 2018). *Github Inc.* Obtenido de Github: https://github.com/Trakkasure/mikronode

Troncoso, A., & Cruz, J. (2 de Mayo de 2018). *mum.mikrotik.com.* Obtenido de https://mum.mikrotik.com/presentations/UR17/presentation_4932_1510780314.pdf

Unique Computer System LLC. (15 de Mayo de 2018). *www.reson8.ae*. Obtenido de https://www.reson8.ae/sms/one-time-passwords.html

Vasco. (14 de Mayo de 2018). *Vasco Data Security International, Inc.* Obtenido de https://www.vasco.com/es-es/glossary/one-time-password.html

Wi-Fi Alliance. (Abril de 2003). *repository.mdp.ac.id.* Obtenido de http://repository.mdp.ac.id/ebook/library-ref-eng/ref-eng-3/physical/wireless/security/wp_8_WPA%20Security_4-29-03.pdf

Wi-Fi Alliance. (8 de Enero de 2018). *www.wi-fi.org*. Obtenido de https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-security-enhancements

ANEXOS

- **ANEXO A – ÁRBOL DE PROBLEMAS**

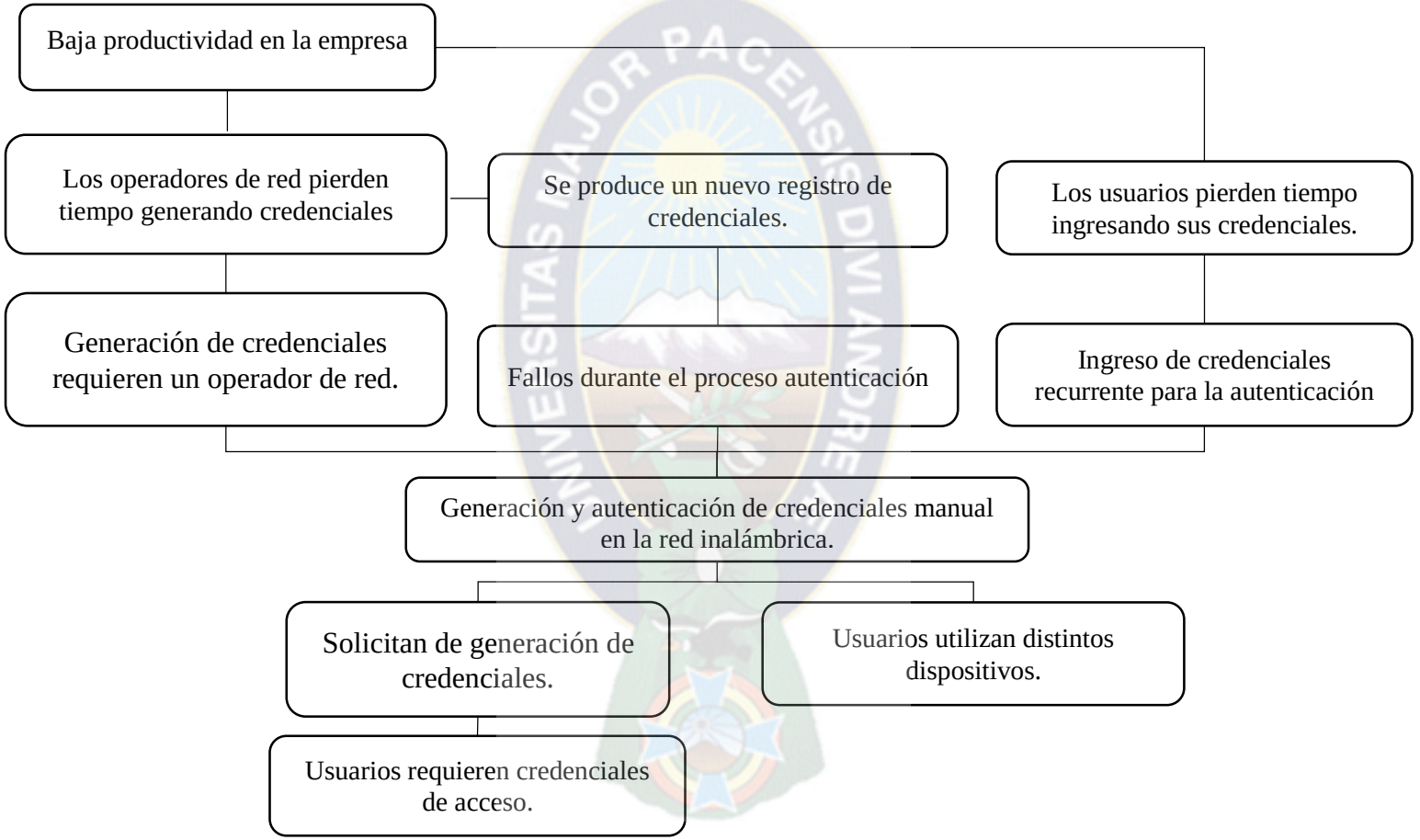


Figura 5.1: Árbol de Problemas

- **ANEXO B – ÁRBOL DE OBJETIVOS**

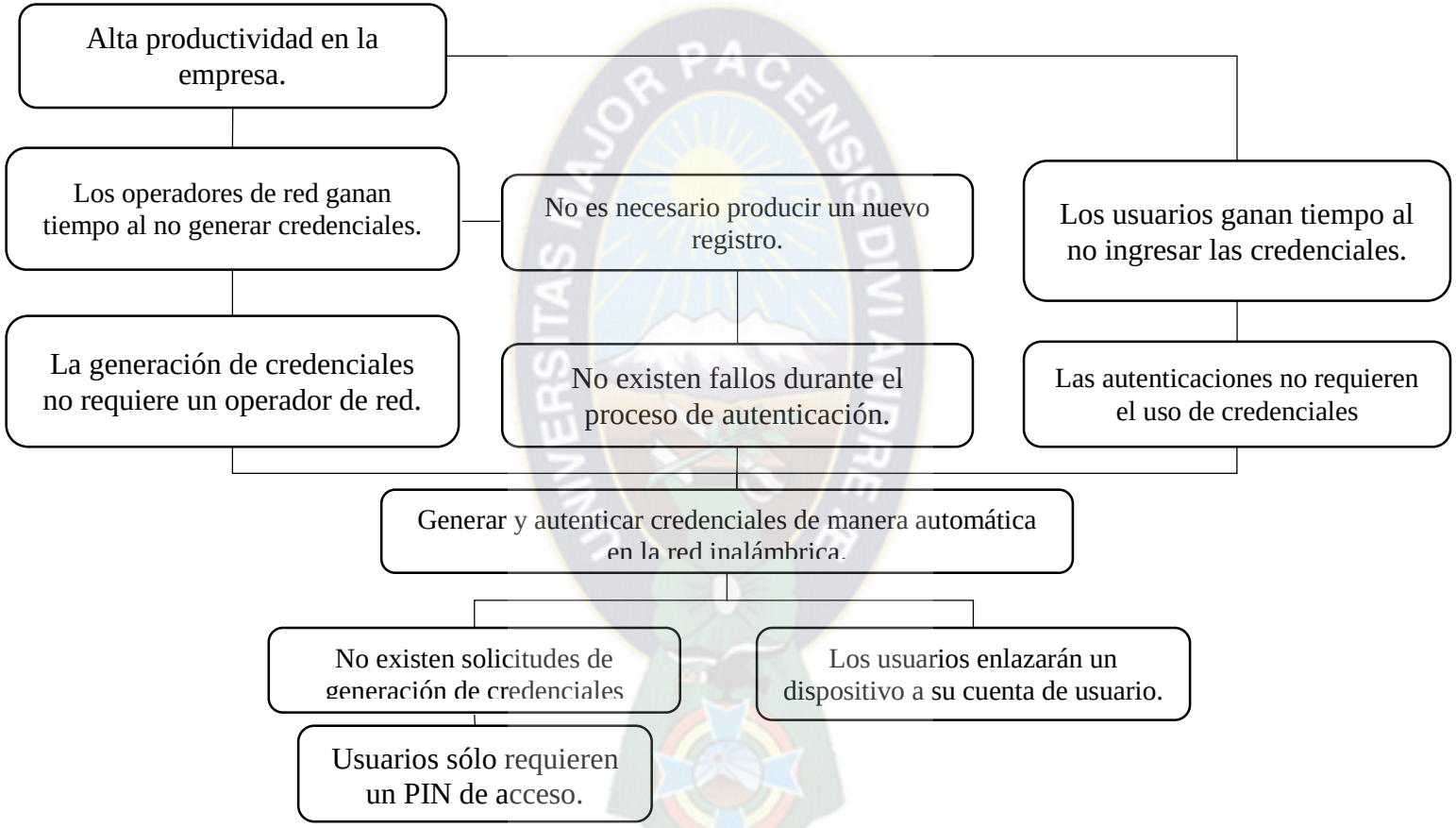
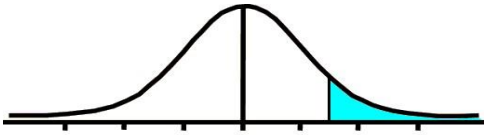


Figura 5.2: Árbol de Objetivos

- **ANEXO C – TABLA T-STUDENT**



Grados de libertad	0.25	0.1	0.05	0.025	0.01	0.005
1	1.0000	3.0777	6.3137	12.7062	31.8210	63.6559
2	0.8165	1.8856	2.9200	4.3027	6.9645	9.9250
3	0.7649	1.6377	2.3534	3.1824	4.5407	5.8408
4	0.7407	1.5332	2.1318	2.7765	3.7469	4.6041
5	0.7267	1.4759	2.0150	2.5706	3.3649	4.0321
6	0.7176	1.4398	1.9432	2.4469	3.1427	3.7074
7	0.7111	1.4149	1.8946	2.3646	2.9979	3.4995
8	0.7064	1.3968	1.8595	2.3060	2.8965	3.3554
9	0.7027	1.3830	1.8331	2.2622	2.8214	3.2498
10	0.6998	1.3722	1.8125	2.2281	2.7638	3.1693
11	0.6974	1.3634	1.7959	2.2010	2.7181	3.1058
12	0.6955	1.3562	1.7823	2.1788	2.6810	3.0545
13	0.6938	1.3502	1.7709	2.1604	2.6503	3.0123
14	0.6924	1.3450	1.7613	2.1448	2.6245	2.9768
15	0.6912	1.3406	1.7531	2.1315	2.6025	2.9467
16	0.6901	1.3368	1.7459	2.1199	2.5835	2.9208
17	0.6892	1.3334	1.7396	2.1098	2.5669	2.8982
18	0.6884	1.3304	1.7341	2.1009	2.5524	2.8784
19	0.6876	1.3277	1.7291	2.0930	2.5395	2.8609
20	0.6870	1.3253	1.7247	2.0860	2.5280	2.8453
21	0.6864	1.3232	1.7207	2.0796	2.5176	2.8314
22	0.6858	1.3212	1.7171	2.0739	2.5083	2.8188
23	0.6853	1.3195	1.7139	2.0687	2.4999	2.8073
24	0.6848	1.3178	1.7109	2.0639	2.4922	2.7970
25	0.6844	1.3163	1.7081	2.0595	2.4851	2.7874
26	0.6840	1.3150	1.7056	2.0555	2.4786	2.7787
27	0.6837	1.3137	1.7033	2.0518	2.4727	2.7707
28	0.6834	1.3125	1.7011	2.0484	2.4671	2.7633
29	0.6830	1.3114	1.6991	2.0452	2.4620	2.7564
30	0.6828	1.3104	1.6973	2.0423	2.4573	2.7500
31	0.6825	1.3095	1.6955	2.0395	2.4528	2.7440
32	0.6822	1.3086	1.6939	2.0369	2.4487	2.7385
33	0.6820	1.3077	1.6924	2.0345	2.4448	2.7333
34	0.6818	1.3070	1.6909	2.0322	2.4411	2.7284