EVALUACIÓN DE LA SEGURIDAD DE LA RED INALÁMBRICA DEL CANTÓN MILITAR DE POPAYÁN

YEIMY CAROLINA RODRÍGUEZ RODRÍGUEZ
JORGE LUIS MUÑOZ PABÓN

Tesis de Maestría en Telecomunicaciones

Director:
SILER AMADOR DONADO
Magister

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Telecomunicaciones
Grupo de I+D GNTT
Popayán, 2020

EVALUACIÓN DE LA SEGURIDAD DE LA RED INALÁMBRICA DEL CANTÓN MILITAR DE POPAYÁN

YEIMY CAROLINA RODRÍGUEZ RODRÍGUEZ
JORGE LUIS MUÑOZ PABÓN

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Telecomunicaciones
Grupo de I+D GNTT
MAESTRÍA EN TELECOMUNICACIONES
Popayán, Cauca
2020

EVALUACIÓN DE LA SEGURIDAD DE LA RED INALÁMBRICA DEL CANTÓN MILITAR DE POPAYÁN

YEIMY CAROLINA RODRÍGUEZ RODRÍGUEZ
JORGE LUIS MUÑOZ PABÓN

Trabajo de grado para optar al título de:

MAGISTER EN TELECOMUNICACIONES

Director:
Mag. SILER AMADOR DONADO

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Telecomunicaciones
Grupo de I+D GNTT
MAESTRÍA EN TELECOMUNICACIONES
Popayán, Cauca
2020

Resumen Estructurado

El Cantón Militar de Popayán posee una red inalámbrica de área local distribuida mediante puntos de acceso inalámbricos para ofrecer el servicio de Internet a los usuarios del Ejército Nacional de Colombia, pero no realiza un diagnóstico para evaluar si un intruso puede acceder a la red inalámbrica con dispositivos no autorizados y afectar la integridad de los datos confidenciales del Ejército, además de evaluar la pertinencia de las políticas actuales sobre seguridad inalámbrica.

Para gestionar esta vulnerabilidad se plantearon como objetivos evaluar la seguridad de la red inalámbrica del Cantón Militar, buscando determinar la metodología adecuada para realizar la evaluación, aplicar la metodología de evaluación seleccionada y analizar el nivel de seguridad encontrado en la red inalámbrica. Para evaluar la seguridad de la red inalámbrica se aplicó el Manual de metodología de pruebas de seguridad de código abierto OSSTMM.

Dentro de los resultados obtenidos con las pruebas de penetración se logró evaluar la seguridad de la red inalámbrica, se obtuvo el mapa de infraestructura inalámbrica, la dirección física del punto de acceso inalámbrico de la Tercera División, las credenciales de autenticación en la red inalámbrica del Cantón Militar y el escaneo de activos y puertos lógicos de terminales. Las pruebas permitieron identificar riesgos en seguridad de la información militar mediante diferentes posibilidades que tiene un intruso malicioso de realizar un ataque informático para explotar vulnerabilidades de la red inalámbrica del Ejército.

Como recomendaciones para incrementar la seguridad de la red inalámbrica se plantearon la segmentación del direccionamiento de red, establecimiento de segmentos de red virtuales también por divisiones del Ejército, implementación de un sistema de detección de intrusos inalámbrico, un sistema de prevención de intrusiones inalámbrico, un controlador de red inalámbrica, un sistema de autenticación inalámbrico, un sistema de acceso inalámbrico en malla y el aislamiento de la infraestructura de red inalámbrica.

Finalmente como conclusiones se obtuvo que el nivel de seguridad de la red inalámbrica del Cantón Militar de Popayán es bajo, por cuanto no cumple con las recomendaciones de buenas prácticas para realizar la gestión apropiada de las vulnerabilidades de la red inalámbrica, con información confidencial de alta importancia, para minimizar el riesgo de un posible ataque informático por un intruso malicioso e incrementar el nivel de seguridad de la información militar del Ejército Nacional de Colombia.

Palabras Clave: *Red inalámbrica, Seguridad de la información, Análisis de vulnerabilidades, Pruebas de penetración, Metodologías de pruebas de penetración.*

Structured Abstract

The Canton Militar of Popayán has a wireless local area network distributed through wireless access points to offer Internet service to users of the Colombian National Army, but does not perform a diagnosis to assess whether an intruder can access the wireless network with unauthorized devices and affect the integrity of confidential Army data, in addition to assessing the relevance of current wireless security policies.

To manage this vulnerability, the objectives were to evaluate the security of the wireless network of the Military Canton, seeking to determine the appropriate methodology to perform the evaluation, apply the selected evaluation methodology and analyze the level of security found in the wireless network. To evaluate the security of the wireless network, the OSSTMM Open Source Security Test Methodology Manual was applied.

Among the results obtained with the penetration tests, the security of the wireless network was assessed, the wireless infrastructure map was obtained, the physical address of the Third Division's wireless access point, the authentication credentials in the wireless network of the Canton Militar and the scanning of assets and logical ports of terminals. The tests allowed to identify risks in security of the military information by means of different possibilities that a malicious intruder has to carry out a computer attack to exploit vulnerabilities of the Army's wireless network.

As recommendations to increase the security of the wireless network, the segmentation of the network addressing, establishment of virtual network segments also by Army divisions, implementation of a wireless intruder detection system, a wireless intrusion prevention system, a wireless network controller, a wireless authentication system, a wireless mesh access system and the isolation of the wireless network infrastructure.

Finally, as conclusions, it was obtained that the security level of the wireless network of the Canton Militar of Popayán is low, since it does not comply with the recommendations of good practices to perform the appropriate management of the vulnerabilities of the wireless network, with confidential high information importance, to minimize the risk of a possible computer attack by a malicious intruder and increase the level of security of the military information of the National Army of Colombia.

Keywords: *Wireless network, Information security, Vulnerability analysis, Penetration tests, Pentest Methodology.*

Contenido

Lista de Figuras

Lista de Tablas

Lista de Anexos

Lista de Símbolos


Celular


Computador portátil


Conmutador capa 2


Conmutador capa 3


Controlador inalámbrico WLAN


Dispositivo de seguridad IDS|IPS|Firewall


Dispositivo inalámbrico


Enrutador


Impresora


Nube | Internet


Portal acceso inalámbrico malla


Punto de acceso inalámbrico


Punto acceso inalámbrico malla


Sensor IDS


Servidor SAN|NAS RADIUS


Tablet

Teléfono IP


Terminal de datos

Lista de Siglas

IDS	Intrusion Detection System
IPS	Intrusion Prevention System
OSSTMM	Open Source Security Testing Methodology Manual
PTF	Penetration Testing Framework
RAV	Risk Assessment Values
WLAN	Wireless Local Area Network

Glosario

Amenaza: Cualquier elemento o acción que explote una vulnerabilidad presente en un sistema para atentar contra la seguridad de la información.

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Intruso: Persona maliciosa que ataca vulnerabilidades de sistemas informáticos o redes de datos, tomando control sin autorización mediante técnicas de penetración internas o remotas.

Prueba de Penetración: Conjunto de metodologías y técnicas que permiten identificar vulnerabilidades en seguridad de los sistemas informáticos.

Riesgo: Combinación de la probabilidad de ocurrencia de un determinado hecho y sus consecuencias. Materialización de una amenaza que explota una vulnerabilidad de un sistema informático, la información o sus recursos de gestión.

Seguridad de la información: Preservación de confidencialidad, integridad y disponibilidad de la información; además de otras propiedades como autenticidad, trazabilidad, no repudio y fiabilidad.

Vulnerabilidad: Debilidad o fallo presente en un sistema de información que puede ser explotada por un atacante para poner en riesgo la seguridad de la información comprometiendo su disponibilidad, confidencialidad e integridad.

1. Introducción

En el Cantón Militar de Popayán se encuentra implementada una red inalámbrica de área local distribuida mediante puntos de acceso inalámbrico de infraestructura con sus respectivas políticas de seguridad, para ofrecer el servicio de Internet a los usuarios del ejército, con una notable cantidad de accesos a ella, mediante una amplia variedad de dispositivos móviles conjunto con computadores portátiles. El canal para el acceso a Internet llega a la sede del cantón mediante fibra óptica desde el proveedor de servicios de Internet contratado.

El Cantón Militar se encuentra ubicado en la Carrera 15 con Calle 11 Norte en el barrio Machángara, Popayán, y se encuentra conformado por siete divisiones militares: Batallón de Infantería 7 General José Hilario López, Batallón ASPC 29, Vigésima Novena Brigada, Tercera División, Brigada Móvil, CENAC Y Batallón de Aviación. A continuación se puede apreciar una imagen satelital de la sede del Cantón Militar de la ciudad de Popayán.

Figura 1. Cantón Militar de Popayán

Como en toda institución donde se tiene implementada una red inalámbrica, se contrata con diferentes proveedores de soluciones de seguridad para la protección de los datos como antivirus y servidores o dispositivos de escaneo que buscan impedir el acceso a usuarios y/o dispositivos no autorizados en la red, pero actualmente no se realiza un diagnóstico en tiempo real para saber si un intruso puede acceder a la red inalámbrica y comprobar si efectivamente las soluciones de seguridad implementadas están logrando impedir el acceso de intrusos mediante dispositivos para ataques a redes inalámbricas.

La infraestructura de red inalámbrica del Cantón Militar de Popayán posee una vulnerabilidad en este sentido, debido a que no cuenta con un plan de pruebas para evaluar si un intruso puede penetrar en la red con dispositivos no autorizados en las políticas de seguridad del Ejército Nacional de Colombia. Se hace entonces indispensable poder conocer si un ataque de intrusión a la misma puede llegar a afectar la autenticidad, confiabilidad e integridad de la información militar confidencial del ejército y sus plataformas de operación institucional, porque al evaluar la seguridad de la red, se permitiría la toma de decisiones sobre las políticas de seguridad actuales de la red inalámbrica.

Además, esta evaluación debe ser periódica, no puede realizarse una primera vez y confiar en que la red ya es segura porque en este tema jamás se llega al 100% de seguridad, entonces el Cantón Militar de Popayán tiene la necesidad de contar con un procedimiento para realizar estas pruebas de manera permanente sobre la red inalámbrica. Al no existir dicho procedimiento que permita realizar esta evaluación, se implementó una metodología de pruebas de seguridad informática que permite evaluar la seguridad en cuanto al acceso de dispositivos no autorizados a la red inalámbrica.

Las pruebas de seguridad informática consisten en un tipo de auditoría externa orientada a ganar acceso en los sistemas de información, y realizadas con la finalidad de buscar fallas de seguridad con técnicas y procedimientos similares a los de un hacker, pero con autorización previa de las autoridades competentes del Cantón Militar y ejecutados de forma ética. Estas pruebas permitieron demostrar que las medidas de seguridad de la red inalámbrica no han sido diseñadas e implementadas de forma correcta.

También permitieron demostrar y concientizar que existe un verdadero y real peligro para la institución, dado que en ocasiones la seguridad es subestimada en la toma de decisiones estratégicas y operacionales de las instituciones, planteándose un cambio de actitud mediante la demostración de un ataque inocuo con resultados medibles en tiempo real que evidencian riesgos para la información confidencial y operativa del Ejercito.

2. Descripción de la red inalámbrica del Cantón Militar

2.1. Infraestructura de red de datos

La infraestructura de la red de datos del Cantón Militar de Popayán se conforma básicamente por un enlace troncal de red, compuesto por un enrutador de frontera en el borde de la red para direccionamiento del tráfico en Internet, un dispositivo de seguridad para el control del tráfico de datos entrante y saliente en Internet, un conmutador principal multicapa como núcleo central del flujo de datos, conmutadores de distribución de capa dos para las redes de área local de las

diferentes divisiones del Cantón Militar, puntos de acceso inalámbrico para el acceso a Internet de los usuarios en cada una de las unidades militares y servidores en el área de servidores del área de almacenamiento con aplicativos e información confidencial militar del Ejército.

A continuación, se presenta el diagrama con el esquema general de la infraestructura de red de datos completa del Cantón Militar de Popayán con las siete unidades militares que lo componen: Batallón de Infantería 7 General José Hilario López, Batallón ASPC 29, Vigésima Novena Brigada, Tercera División, Brigada Móvil, CENAC Y Batallón de Aviación. En ella se puede apreciar la distribución de los equipos de interconexión que componen la infraestructura de red inalámbrica para el acceso al servicio de Internet en el Ejército por cada contingente del Cantón.

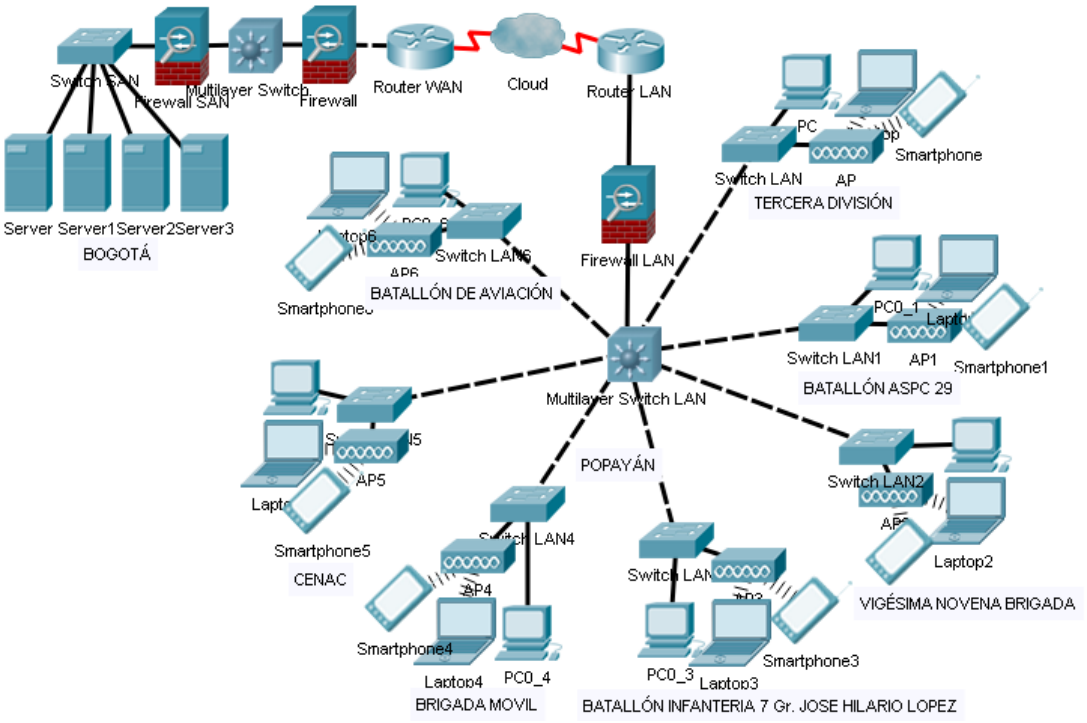


Figura 2. Infraestructura de red de datos del Cantón Militar de Popayán

El siguiente esquema resume la infraestructura de red de datos presentada anteriormente con una sola división del Cantón Militar, para visualizar y comprender mejor el funcionamiento lógico de la distribución de la infraestructura de red inalámbrica que provee el servicio de Internet a los usuarios del Ejército. Se puede observar que existe una distribución en estrella con un núcleo central que distribuye los segmentos de red de área local por cada división del Ejército conjunto con un punto de acceso inalámbrico para la distribución de la red inalámbrica por cada una de las unidades que componen la sede del Cantón Militar de Popayán.

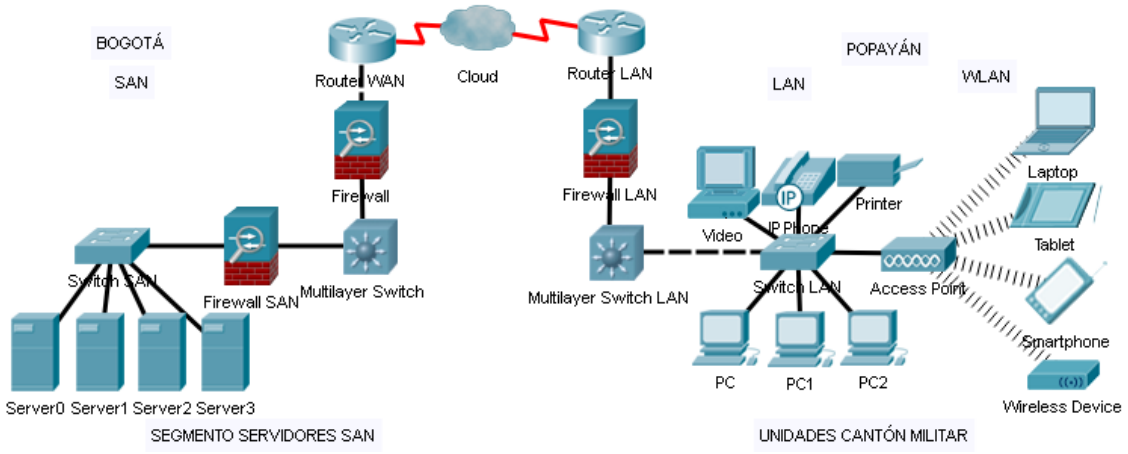


Figura 3. Esquema infraestructura de red de datos del Cantón Militar de Popayán

2.2. Infraestructura de red inalámbrica

El siguiente es el diagrama de la infraestructura de red inalámbrica en donde se aprecia la distribución de los puntos de acceso inalámbrico que proveen el servicio de Internet a los usuarios del Ejército, sin incluir los dispositivos que componen los segmentos de red de área local de cada unidad del Cantón Militar de Popayán.

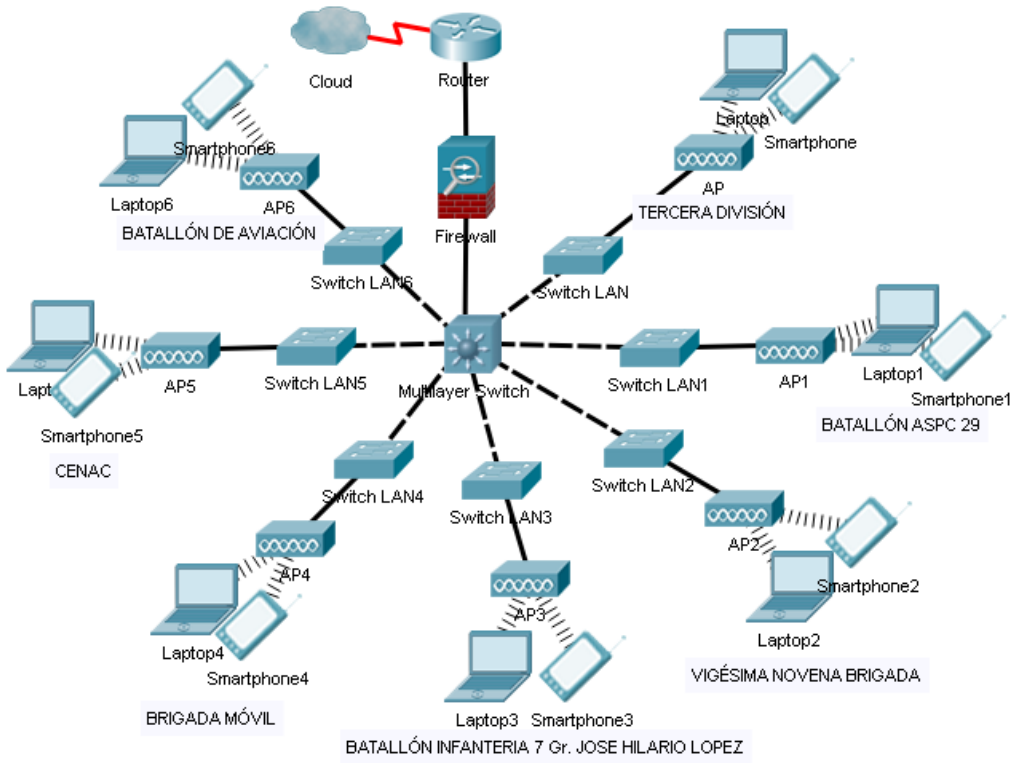


Figura 4. Infraestructura de red inalámbrica del Cantón Militar de Popayán

El direccionamiento de los puntos de acceso inalámbrico que componen la infraestructura de red inalámbrica del Cantón Militar de Popayán que distribuye el

servicio de Internet hacia las diferentes unidades militares del Ejército se puede apreciar en la tabla siguiente.

En la tabla se puede observar la configuración del enrutador de frontera de la red como puerta de enlace predeterminada para cada punto de acceso inalámbrico, así como de servidor de traducción de nombres de dominio DNS.

Tabla 1. Direccionamiento de los puntos de acceso de la red inalámbrica del Cantón Militar

Parámetro	Configuración
Dirección IP puerto WLAN	172.23.66.194
Dirección IP puerto WAN	172.23.0.10
Máscara de red	255.255.255.0
Puerta de enlace predeterminada	172.23.0.1
Servidor DNS	172.23.0.1

El direccionamiento de red que los puntos de acceso inalámbricos le configuran mediante el servicio de configuración dinámica DHCP a los computadores, teléfonos celulares, tabletas y demás terminales y dispositivos de red inalámbricos de los usuarios del Ejército al conectarse a la red inalámbrica del Cantón Militar, se puede apreciar en la tabla contigua.

Tabla 2. Direccionamiento automático de terminales de la red inalámbrica del Cantón Militar

Parámetro	Configuración
Dirección IP	172.23.66.1 - 172.23.66.254
Máscara de red	255.255.255.0
Puerta de enlace predeterminada	172.23.66.194
Servidor DNS 1	172.23.66.194
Servidor DNS 2	172.23.66.194

Finalmente, el direccionamiento de la infraestructura de red inalámbrica que provee el servicio de Internet a los usuarios del Ejército se puede apreciar en la siguiente gráfica, en donde se observa el direccionamiento de red de cada dispositivo que la compone, tanto de interconexión como terminal de datos. En ella se obviaron tanto los dispositivos de los segmentos de red de área local, como los conmutadores de distribución, enfocándose netamente en la distribución y el funcionamiento lógico de la red inalámbrica del Cantón Militar de Popayán para su mejor comprensión y análisis.

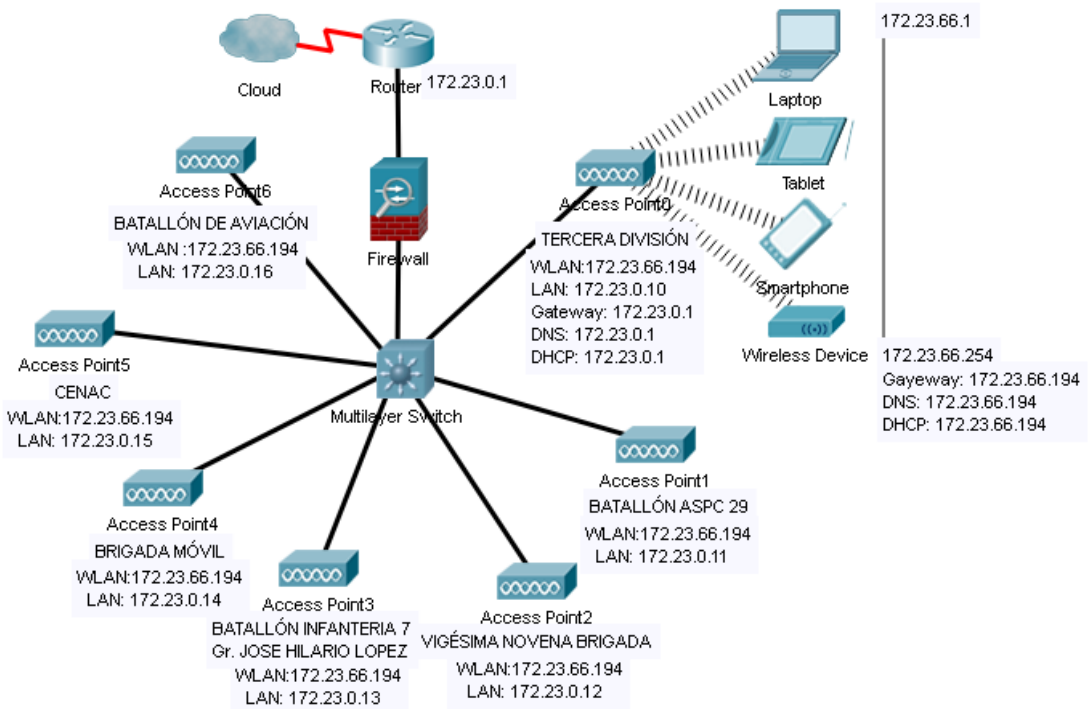


Figura 5. Direccionamiento de la red inalámbrica del Cantón Militar de Popayán

3. Metodología de pruebas de penetración

La seguridad informática es fundamental para el Cantón Militar de Popayán, ya que la pérdida o el robo de datos confidenciales de sus políticas de operación militar es un riesgo que se puede considerar de seguridad nacional y por ende se deben realizar todos los esfuerzos necesarios en materia informática para que este hecho no llegue a presentarse.

El objetivo de la evaluación de la seguridad informática es la preservación de la confidencialidad, la integridad y la autenticidad de los sistemas de información, y con las pruebas de seguridad se realizó una auditoría informática que permitió detectar y proponer soluciones para las vulnerabilidades presentes en cuanto al acceso a la red inalámbrica de la Tercera División. Este proceso también permitió capacitar al equipo de Tecnologías de la Información del contingente de la Tercera División encargado del área de sistemas en el Cantón Militar, debido a que al participar del proceso el equipo pudo entender, detectar y finalmente, trazar las bases para elaborar un plan de acción que posibilite resolver las vulnerabilidades informáticas con base en los informes y reportes de resultados que la implementación de la metodología entregó.

Para ello se planteó el uso de una metodología, que consiste principalmente en un conjunto de procedimientos, métodos y prácticas que se implementaron durante la ejecución del proceso de auditoría en seguridad de la información en la

infraestructura de red inalámbrica de la institución militar. Este proceso permitió evaluar el nivel de seguridad de las tecnologías de la información y redes de datos, ante posibles ataques, mediante procedimientos que permitieron identificar las vulnerabilidades y los problemas de seguridad existentes, utilizando las mismas herramientas y técnicas que utilizan los atacantes y/o intrusos, pero con procedimientos éticos de intrusión, logrando esquivar o anular características de seguridad de los componentes del sistema militar, con el propósito de incrementar su nivel de seguridad.

Básicamente entonces la metodología de pruebas de penetración en seguridad informática implementada en la infraestructura de red inalámbrica de datos consideró en su ruta de trabajo los pasos descritos a continuación:

- Definir la infraestructura informática a evaluar.
- Identificar las vulnerabilidades con una evaluación interna y una evaluación externa.
- Determinar el impacto de cada vulnerabilidad detectada durante la evaluación.
- Documentar los detalles de las vulnerabilidades identificadas y resultados de la evaluación una vez terminado el proceso de pruebas.
- Proponer soluciones de seguridad para gestionar las vulnerabilidades informáticas detectadas durante la evaluación.
- Plantear una futura la evaluación interna y externa para verificar que las soluciones de seguridad implementadas en la arquitectura sean efectivas, posterior a la implementación de las soluciones propuestas.

3.1. Comparación de las metodologías abiertas

Existen diferentes metodologías abiertas que determinan los requerimientos de las evaluaciones que se realizan en seguridad informática. La metodología plantea la ejecución de diferentes tipos de pruebas de penetración paso a paso para poder evaluar con mucha precisión la seguridad del sistema. Entre las metodologías abiertas reconocidas se encuentran las mencionadas a continuación.

- **OSSTMM:** Open Source Security Testing Methodology Manual.
- **OWASP:** Open Web Application Security Project.
- **ISSAF:** Information Systems Security Assessment Framework.
- **NIST:** The National Institute of Standards and Technology - Technical Guide to Information Security Testing and Assessment.
- **PTES:** Penetration Testing Execution Standard.
- **PTF:** Penetration Testing Framework.

Para la escogencia de la metodología adecuada para evaluar la seguridad de la red inalámbrica del Cantón Militar de Popayán, se realizó una comparación entre las

diferentes metodologías abiertas y su pertinencia con el proyecto, en donde se analizó cuales poseen un capítulo para redes inalámbricas y su idoneidad con los objetivos propuestos en este proyecto de grado, acordes con las necesidades en seguridad de la información de una institución militar tan importante como el Ejército Nacional de Colombia. A continuación, se presenta una breve descripción de cada una de las metodologías propuestas.

3.1.1. Metodología OSSTMM - Open Source Security Testing Methodology Manual

El manual de metodología de pruebas de seguridad de código abierto es un estándar para auditorías de seguridad que permite evaluar la seguridad operacional de un sistema de información. Es una metodología para probar la seguridad operativa de ubicaciones físicas, interacciones humanas y sus formas de comunicación tales como inalámbricas, cableadas, analógicas y digitales. Esta metodología permite una profunda comprensión de la interconexión de los usuarios, los procesos, los sistemas y el software, posibilitando valorar el nivel de seguridad del sistema, para que los controles se equilibren perfectamente con las interacciones de los usuarios en el sistema informático e incluye un marco de trabajo que describe las fases que se deben realizar para la ejecución de la auditoría.

OSSTMM, desarrollado por ISECOM[1], es un estándar internacional de pruebas de penetración para la evaluación de la seguridad en sistemas informáticos. Básicamente en su proceso de implementación se recolecta información de usuarios y activos de la red objetivo, se determinan canales de comunicación e interacción con los activos de red a evaluar, como seguridad física, entorno humano, información de red, medios de comunicación y políticas de seguridad, se identifican y clasifican activos objetivo y se determina la orientación para evaluar y auditar cada segmento o activo de red de datos objetivo. Esta metodología es flexible y evalúa los controles de acceso, procesos de seguridad, controles de información, localizaciones físicas, protección de perímetros, nivel de conciencia en seguridad, nivel de confianza y control de protección de fraude. La metodología analiza los resultados de las pruebas y permite la evaluación del nivel de seguridad de la red de datos. Los capítulos la componen esta metodología son: (Metodología OSSTMM, 2010).

Tabla 3. Capítulos metodología OSSTMM

Capítulo	Contenido
1	Lo que debe saber (seguridad, controles, objetivos, limitaciones, seguridad actual, cumplimiento)
2	Qué debe hacer (definición de la prueba de seguridad, alcance, proceso de prueba de seguridad operacional, manejo de errores)
3	Análisis de seguridad
4	Métricas de seguridad operacional
5	Análisis de confianza

[1] ISECOM: Institute for Security and Open Methologies. Instituto de seguridad y metodologías abiertas.

6	Flujo de trabajo
7	Pruebas de seguridad humana
8	Pruebas de seguridad física
9	Pruebas de seguridad inalámbrica
10	Pruebas de seguridad de telecomunicaciones
11	Pruebas de seguridad de redes de datos
12	Cumplimiento
13	Reportando con la STAR
14	Lo que obtienes (La defensa Möbius)
15	Licencia de metodología abierta

De esta metodología se destaca el capítulo 9 sobre Pruebas de seguridad inalámbrica, el cual es el tema central de este proyecto, y plantea un proceso muy completo para la evaluación de una red inalámbrica de datos que se ajusta completamente a las necesidades sobre la evaluación de la seguridad de la infraestructura de red inalámbrica que se requiere en el Cantón Militar de Popayán, dado que plantea un enfoque administrativo con ámbito muy completo de vulnerabilidades a evaluar desde el aspecto conceptual, combinándolo con múltiples pruebas de penetración que evalúan una red inalámbrica desde múltiples perspectivas de posibles atacantes e intrusos, siendo la metodología más completa para una institución militar como el Ejército Nacional cuya información es altamente confidencial y su seguridad es de alta importancia y criticidad. Este capítulo está compuesto por los siguientes temas:

Tabla 4. Capítulo 9 metodología OSSTMM pruebas de seguridad inalámbrica

Capítulo 9. Pruebas de seguridad inalámbrica				
N°	**Subcapítulo**		**N°**	**Subcapítulo**
9.1	Revisión de la postura		9.10	Validación de la propiedad
9.2	Logística		9.11	Revisión de la segregación
9.3	Verificación de detección activa		9.12	Verificación de la exposición
9.4	Auditoria de visibilidad		9.13	Exploración de inteligencia competitiva
9.5	Verificación de acceso		9.14	Verificación de cuarentena
9.6	Verificación de confianza		9.15	Auditoria de privilegios
9.7	Verificación de controles		9.16	Validación de la supervivencia
9.8	Verificación del proceso		9.17	Revisión de registros y alertas
9.9	Verificación de la configuración			

Dentro de los beneficios que se obtienen con la implementación de la metodología OSSTMM para la evaluación del nivel de seguridad de la información en la red inalámbrica del Cantón Militar de Popayán se encuentran la reducción de casos de falsos positivos y falsos negativos en las pruebas de penetración; adaptabilidad del marco de referencia a diferentes esquemas de evaluación de seguridad como pruebas de penetración o análisis de vulnerabilidades; profundidad en el alcance de

la evaluación en seguridad informática con resultados confiables, consistentes y cuantificables; actualización permanente de la metodología con nuevas tendencias de seguridad, normativas y enfoques éticos; compatibilidad del proceso de auditoria con las regulaciones de la industria, políticas institucionales y la legislación en materia; reconocimiento del nivel actual de seguridad de la información basado en seguridad operativa, limitaciones y pérdida de control; y posibilidad de certificación en auditoría del personal de gestión de sistemas del Ejército Nacional como Experto en seguridad inalámbrica OSSTMM (OWSE[2]).

3.1.2. Metodología OWASP - Open Web Application Security Project

El proyecto de seguridad de aplicaciones web abiertas es una comunidad centrada en mejorar la seguridad del software de aplicación. La metodología OWASP clasifica los riesgos de seguridad de una aplicación web identificando los principales riesgos de ataque informático, las vulnerabilidades en seguridad de la información y la relación de su impacto en la institución. Al evaluar la aplicación, cada riesgo identificado evidencia una vulnerabilidad ante un ataque informático, proporcionando instrucciones específicas sobre cómo gestionarla. Sus pruebas específicamente son: (Metodología OWASP, 2014)

Tabla 5. Capítulos metodología OWASP

Pruebas de seguridad de aplicaciones web				
N°	**Capítulo**		**N°**	**Capítulo**
1	Pruebas de configuración y gestión de la implementación		6	Pruebas de validación de entrada
2	Pruebas de gestión de identidad		7	Prueba de manejo de errores
3	Pruebas de autenticación		8	Pruebas de criptografía débil
4	Pruebas de autorización		9	Pruebas de lógica de negocios
5	Pruebas de gestión de sesión		10	Pruebas del lado del cliente

Los beneficios que se obtienen con la implementación de la metodología OWASP son la prueba de aplicaciones web con base en riesgos de seguridad para evitar ataques informáticos y vulnerabilidades comunes, disponibilidad de herramientas para evaluación de seguridad informática con pruebas desarrolladas por la comunidad OWASP, evaluación específica de cada tecnología para pruebas de seguridad en infraestructura web, ejecución de pruebas de seguridad en el desarrollo de la aplicación para que sea robusta y segura, y la compatibilidad de la evaluación de riesgos en seguridad informática que realiza la metodología con otros estándares de evaluación de seguridad de aplicaciones web.

Sin embargo, esta metodología no se ajusta a los requerimientos de este proyecto, por cuanto no posee un capítulo para evaluación de seguridad de redes inalámbricas, su objetivo se centra netamente en pruebas de seguridad para

[2] OWSE: OSSTMM Wireless Security Expert, certificado acreditado por el Instituto de Seguridad y Metodologías Abiertas (ISECOM).

aplicaciones web. Además, el tratamiento de la gestión del proceso no satisface las necesidades de una institución militar, por ejemplo, no se mencionan aspectos organizativos como definición del alcance de las pruebas, la suscripción de contratos de confidencialidad entre las partes o el planteamiento de procesos administrativos de planificación, seguimiento y control de vulnerabilidades. Por estas razones, la metodología OWASP se descartó como opción para ser la implementada en este proyecto de grado.

3.1.3. Metodología NIST - The National Institute of Standards and Technology - Technical Guide to Information Security Testing and Assessment

La guía técnica para evaluaciones y pruebas de seguridad de la información tiene como propósito ayudar a las instituciones en la planificación y ejecución de pruebas técnicas de seguridad de la información, analizar resultados y desarrollar estrategias de mitigación de vulnerabilidades. Proporciona recomendaciones prácticas para diseñar, implementar y mantener los procesos y procedimientos de pruebas técnicas de seguridad de la información, con múltiples propósitos como encontrar vulnerabilidades en un sistema o red de datos, o verificar el cumplimiento de una política de seguridad u otros requerimientos. Esta metodología no pretende presentar un programa completo de pruebas y exámenes de seguridad de la información, sino más bien una descripción general de los elementos clave de las pruebas y exámenes técnicas de seguridad, con énfasis en técnicas específicas, beneficios, limitaciones y recomendaciones para su uso.

Esta metodología incluye la ejecución de pruebas de penetración por fases donde se realiza el escaneo y recopilación de información de la infraestructura de red de datos y el descubrimiento de vulnerabilidades informáticas, se identifica el alcance de la prueba de penetración con las normas, objetivos y condiciones técnicas e institucionales, se comprueban las vulnerabilidades previamente identificadas y se genera un reporte con los problemas de seguridad encontrados. Esta metodología se compone de los siguientes capítulos: (Metodología NIST, 2008)

Tabla 6. Capítulos metodología NIST

Número	Capítulo
1	Introducción
2	Pruebas de seguridad y descripción general del examen
3	Técnicas de revisión
4	Identificación de objetivos y técnicas de análisis
5	Técnicas de validación de vulnerabilidad objetivo
6	Planificación de la evaluación de seguridad
7	Ejecución de la evaluación de seguridad
8	Actividades posteriores a la prueba

De esta metodología se destaca el capítulo 4 sobre Identificación de objetivos y técnicas de análisis, el cual contiene el subcapítulo 4.4. Escaneo Inalámbrico, que es el tema de este proyecto, y aunque plantea el proceso para la evaluación de una red inalámbrica de datos, con metodología y herramientas, este no se ajusta a las necesidades sobre la evaluación de la seguridad de la red inalámbrica del Cantón Militar de Popayán, dado que se encuentra basado en el esquema básico de pruebas de penetración Planeación-Ejecución-Evaluación-Reporte, y se ajustaría a una prueba de penetración a una red inalámbrica de una institución donde la información no se crítica y la seguridad no sea un factor crítico dentro de las políticas de la empresa, dado que tal vez un ataque informático no genere grandes repercusiones para su operación. Caso contrario es el del Cantón Militar debido a la obvia importancia y criticidad de la información militar del Ejército y los riesgos que puede conllevar un ataque que deteriore dicha información, o sea capturada por un atacante o intruso malicioso. Este capítulo y subcapítulo está compuesto por los siguientes temas:

Tabla 7. Capítulo 4 metodología NIST identificación de objetivos y técnicas de análisis

Capítulo 4 - identificación de objetivos y técnicas de análisis	
Número	**Subcapítulo**
4.1	Descubrimiento de red
4.2	Puertos de red e identificación de servicios
4.3	Escaneo de vulnerabilidades
4.4	Escaneo Inalámbrico
4.4.1	Escaneo Inalámbrico pasivo
4.4.2	Escaneo inalámbrico activo
4.4.3	Seguimiento de la ubicación de dispositivos inalámbricos
4.4.4	Escaneo Bluetooth
4.5	Resumen

3.1.4. Marco ISSAF - Information Systems Security Assessment Framework

El Marco de evaluación de seguridad de sistemas de información es un framework[3] que permite realizar un análisis detallado de todos los posibles aspectos que afectan la seguridad de un sistema de información, catalogados desde aspectos generales como conceptos básicos de administración de proyectos de pruebas de seguridad, hasta técnicas como la ejecución de pruebas de inyección de código SQL[4] o estrategias de desencriptación de contraseñas. Es un marco de referencia de código abierto para pruebas de penetración que ofrece integridad, precisión y eficiencia para evaluar la seguridad de red de una institución tan importante como la militar. Este marco se enfoca en pruebas técnicas para evaluaciones de seguridad, y

[3] Framework: Marco o entorno de trabajo. "Un framework es un conjunto de clases que incorpora un diseño abstracto para soluciones a familias de problemas relacionados" (Johnsonand Foote, 1988).

[4] SQL: Structured Query Language. Lenguaje de consulta estructurada para gestión de bases de datos.

pruebas de gestión administrativa para implementación de buenas prácticas en la red. El marco de evaluación incluye actividades operativas, evaluaciones de seguridad y análisis de vulnerabilidades completos mediante el uso de diferentes tecnologías y procesos con herramientas de pruebas actualizadas y mejoras en gestión administrativa. También se puede alinear con cualquier otra metodología de pruebas similar. Esta metodología se compone de los siguientes capítulos: (Marco ISSAF, 2006)

Tabla 8. Capítulos marco ISSAF

Número	Capítulo
A	Metodología de pruebas de penetración
B	Metodología de pruebas de penetración, fase II explicada
C	Manipulación de tasas de detección falsas - seguridad de red
D	Pruebas de seguridad de contraseñas
E	Evaluación de la seguridad en conmutadores
F	Evaluación de la seguridad en enrutadores
G	Evaluación de la seguridad en firewalls
H	Evaluación de la seguridad del sistema de detección de intrusiones
I	Evaluación de seguridad en VPN
J	Evaluación de seguridad del sistema antivirus y estrategia de gestión
K	Seguridad de red de área de almacenamiento (SAN)
L	Evaluación de seguridad WLAN
M	Seguridad de usuario de Internet
N	Seguridad de AS 400
O	Seguridad de Lotus notes – Seguridad de host
P	Evaluación de la seguridad del sistema Unix/Linux
Q	Evaluación de la seguridad del sistema Windows
R	Evaluación de la seguridad de la red Novell
S	Evaluación de seguridad del servidor web - Seguridad de aplicación
T	Evaluación de seguridad de aplicaciones web
U	Evaluación de seguridad de aplicaciones web - Inyecciones de SQL
V	Auditoría de código fuente
W	Auditoría binaria
X	Lista de evaluación de seguridad de aplicaciones - Seguridad bases de datos
Y	Evaluación de seguridad de base de datos

De este marco de pruebas se destaca el capítulo *L - Evaluación de seguridad WLAN*, el cual es el tema central de este proyecto, y plantea un proceso muy completo para la evaluación de una red inalámbrica de datos, con metodología y herramientas que se ajustan a las necesidades sobre evaluación de la seguridad de la red inalámbrica del Cantón Militar de Popayán, dado que se enfoca en el aspecto técnico de las pruebas de penetración, complementando muy bien los tipos de metodologías administrativas. Este capítulo está compuesto por los siguientes temas:

Tabla 9. Capítulo L marco ISSAF evaluación de seguridad WLAN

Capítulo L - Evaluación de seguridad WLAN	
Número	**Subcapítulo**
L.1	Mapa de la metodología de evaluación de la seguridad WLAN
L.2	Fundación edificio
L.3	Tipos de amenazas
L.4	Metodología
L.5	Uso de herramientas
L.6	Equipos
L.7	Descripción de software
L.8	Contaminantes globales
L.9	Más lecturas

Este marco ofrece como beneficio una auditoría completa para evaluar el nivel de seguridad de una red de datos, sistema o aplicación, así como la evaluación de controles de gestión contra vulnerabilidades críticas para garantizar la seguridad de la información, teniendo en cuenta múltiples enfoques como la evaluación de riesgos y controles de infraestructura de red de datos, evaluación de la gestión administrativa, buenas prácticas y de políticas de seguridad. Esta metodología puede centrarse en tecnologías específicas, permitiendo identificar riesgos y vulnerabilidades existentes incluso por segmentos de red garantizando la integridad de la información en toda la red de datos.

3.1.5. Marco PTES - Penetration Testing Execution Standard

El estándar de ejecución de pruebas de penetración plantea una prueba de penetración desde la comunicación inicial, el razonamiento detrás de una prueba de penetración y la recopilación de la información hasta las fases de modelado de amenazas donde se obtiene una mejor comprensión de la red evaluada, a través de la investigación, explotación y post explotación de las vulnerabilidades. Posee una guía técnica sobre cómo ejecutar una prueba de penetración actual. El marco está compuesto por siete fases de pruebas de penetración y puede utilizarse para realizar una prueba de penetración efectiva en cualquier entorno. Las siguientes son las principales secciones definidas por el estándar como la base para la ejecución de las pruebas de penetración: (Metodología PTES, 2012)

Tabla 10. Capítulos marco PTES

Número	Capítulo
1	Interacciones previas al compromiso
2	Recopilación de la información
3	Modelado de amenazas
4	Análisis de vulnerabilidad
5	Explotación
6	Post explotación
7	Informes

Básicamente las fases de este marco consisten en:

- Interacciones previas al compromiso: Se define el alcance de las pruebas de penetración.
- Recolección de información: Se recopila información sobre la red objetivo como información en línea o mediante ataques de ingeniería social.
- Modelado de amenazas: Se analizan planes de contingencia, equipo técnico, infraestructura de red y herramientas para seguridad de red.
- Análisis de vulnerabilidades: Se definen métodos de ataque y se identifican usuarios y activos de red.
- Explotación: Se ejecutan las herramientas de pruebas para comprometer el sistema y obtener acceso.
- Post explotación: Se obtiene acceso al sistema para atacar vulnerabilidades identificadas y se introduce código malicioso en terminales objetivo.
- Informes: Se analiza los resultados para evaluar el estado de la seguridad de la información en la red de datos.

Sin embargo, este marco de pruebas no se ajusta a los requerimientos de este proyecto por cuanto no posee un capítulo exclusivo para evaluación de seguridad de redes inalámbricas, la evaluación inalámbrica está distribuida por toda la metodología que incluye también la evaluación de infraestructura cableada, por ende, esta metodología se descartó como opción para ser implementada en este proyecto, dado que su alcance se limita a la red inalámbrica únicamente. A continuación, se presentan los apartes de la metodología que incluyen pruebas y apartados sobre la red inalámbrica, en donde se aprecia que están distribuidos por todos los capítulos de la metodología, precisando implementarla toda.

Tabla 11. Capítulos marco PTES relacionados con redes inalámbricas

Número	**Capítulo**		**Número**	**Capítulo**
1	Tools Required		3.1.4	Passive Testing
1.2	Radio Frequency Tools		3.1.4.2	Wireshark
1.2.1	Frequency Counter		3.2	Vulnerability Validation
1.2.2	Frequency Scanner		4	Exploitation
1.2.3	Spectrum Analyzer		4.2	Customized Exploitation
1.2.4	802.11 USB adapter		4.2.4	Sniffing
1.2.5	External Antennas		4.3	RF Access
2	Intelligence Gathering		4.3.1	Unencrypted Wireless LAN
2.4	Covert gathering		4.3.2	Attacking the Access Point
2.4.1	On-location gathering		4.3.3	Cracking Passwords
2.4.1.5	RF / Wireless Frequency scanning		4.3.3.1	WPA-PSK/ WPA2-PSK
2.4.2	Frequency Usage		4.3.3.2	WPA/WPA2-Enterprise
2.4.3	Equipment Identification		4.3.4	Attacks
2.4.3.1	Airmon-ng		4.3.4.1	LEAP
2.4.3.2	Airodump-ng		4.3.4.2	802.1X

2.4.3.3	Kismet-Newcore		4.3.4.3	PEAP
2.4.3.4	inSSIDer		4.3.4.4	EAP-Fast
3	Vulnerability Analysis		4.3.4.5	WEP/WPA/WPA2
3.1	Vulnerability Testing		4.3.4.6	Aircrack-ng
3.1.2	Automated Tools		4.4	Attacking the User
3.1.2.7	Core IMPACT		4.4.4	Personalized Rogue AP
3.1.2.7.2	Core IMPACT WiFi		4.7	Pillaging
3.1.2.7.7	Core WiFi		4.7.7	Wifi

Este marco ofrece como beneficios el ser un marco de auditoria muy completo para pruebas de penetración que cubre todo el alcance de seguridad de red, con tareas requeridas para probar con precisión la seguridad de un entorno de red de datos. Incluye diferentes tipos de tecnologías, es fácil de interpretar e implementar, y puede adaptarse a diferentes objetivos de pruebas de penetración, no obstante, no es el marco que mejor se adapta a los objetivos y alcance propuestos en este proyecto de grado que se enfocan únicamente en redes inalámbricas.

3.1.6. Marco PTF - Penetration Testing Framework

El marco de pruebas de penetración proporciona a los analistas de vulnerabilidades y ejecutores de pruebas de penetración, una lista muy completa para instalación de múltiples herramientas que permiten una evaluación profunda y un análisis detallado del estado de seguridad de un sistema de información. En este marco se propone la implementación de diversas herramientas para pruebas de penetración inalámbrica, organizadas de manera coherente con el Estándar de ejecución de pruebas de penetración (PTES). Este marco simplifica la instalación y el empaquetado, creando un marco de pruebas de penetración completo. Adicionalmente, se puede reconfigurar y agregar herramientas de acuerdo con los requerimientos de cada escaneo, utilizando incluso repositorios desarrollados internamente como parte de este marco. Sus temas principales son: (Marco PTF, 2014).

Tabla 12. Capítulos marco PTF

Marco PTF				
N°	**Capítulo**		**N°**	**Capítulo**
1	Visita previa a la inspección – plantilla		10	Pruebas específicas de Citrix
2	Huella de red (Reconocimiento)		11	Red troncal
3	Descubrimiento y sondeo		12	Penetración
4	Enumeración		13	Pruebas específicas del servidor
5	Crackeo de contraseñas		14	Seguridad VoIP
6	Evaluación de vulnerabilidades		15	Penetración inalámbrica
7	Auditoría AS 400		16	Seguridad física
8	Pruebas específicas de Bluetooth		17	Informe final
9	Pruebas específicas de Cisco			

De este marco de pruebas de penetración se destaca el capítulo sobre Penetración Inalámbrica, el cual contiene diferentes herramientas para el escaneo de una infraestructura de red inalámbrica, planteado una metodología y herramientas que se ajustan a las necesidades sobre la evaluación de la seguridad de la red inalámbrica del Cantón Militar de Popayán, dado que enfoca pruebas de penetración desde diferentes perspectivas acorde con dispositivos y servicios disponibles para los usuarios del Ejército. Este capítulo está compuesto por los siguientes temas:

Tabla 13. Capítulo 15 marco PTF penetración inalámbrica

Capítulo 15 - Penetración inalámbrica	
Categoría	**Subcapítulo**
Evaluación inalámbrica	Kit de herramientas inalámbricas
	Descubrimiento inalámbrico
	Captura de paquetes
	Herramientas de ataque EAP
	Herramientas de ataque LEAP
	Herramientas de ataque de contraseña WEP/WPA
	Software de generación de cuadros
	Software de mapeo
	Herramientas de conversión de formato de archivo
	Herramientas IDS
Descubrimiento de WLAN	WLAN sin cifrar
	WLAN encriptada WLAN
	WLAN / WPA2 cifrado WLAN
	WLAN encriptada LEAP
	WLAN 802.1x
	Recursos
Seguridad física	Seguridad física inalámbrica

3.1.7. Análisis comparativo de las metodologías de pruebas de penetración

Para determinar la metodología de pruebas de seguridad de servicios informáticos a implementar en la red inalámbrica del Cantón Militar de Popayán, se realizó una comparación entre las metodologías abiertas de pruebas de penetración para auditoría de una infraestructura de red inalámbrica más comunes, el resultado se consignó en la tabla relacionada a continuación, teniendo en cuenta principalmente la correlación y pertinencia de cada metodología con una evaluación para una red inalámbrica y el cumplimiento de los objetivos planteados en este proyecto.

Tabla 14. Comparación entre metodologías abiertas para evaluación de redes inalámbricas

Metodología | Marco	Enfoque Redes Inalámbricas			Cumple	
	Si	No	Descripción	Si	No
OSSTMM	X		Capítulo 9. Pruebas de seguridad inalámbrica	X	
OWASP		X	No posee un capítulo o enfoque para redes inalámbricas, solo seguridad de aplicaciones		X
ISSAF	X		Capítulo L. Evaluación de seguridad WLAN	X	
NIST - TGISTA	X		Capítulo 4. Identificación de objetivos y técnicas de análisis, subcapítulo 4.4. Escaneo inalámbrico	X	
PTES	X		No tiene un capítulo solo para redes inalámbricas, viene integrado en toda la metodología que incluye también infraestructura cableada		X
PTF	X		Capitulo Penetración Inalámbrica	X	

Ahora, para poder establecer una escala de valoración que permita la selección de la metodología adecuada, se identificaron los principales riesgos, vulnerabilidades y amenazas de ataques informáticos frecuentes en seguridad de redes inalámbricas, permitiendo posteriormente asignar una valoración cuantitativa a cada metodología, dependiendo de su grado de gestión ante el riesgo descrito en cuanto a seguridad de infraestructura de redes inalámbricas. Esta escala se estableció con base en el marco de seguridad contenido en la Norma Técnica Colombiana ISO 27001, la cual proporciona asesoría y orientación sobre las mejores prácticas de evaluación de objetivos de control y controles como parte del proceso del sistema de gestión de seguridad de la información para una infraestructura de red de datos. A continuación se presenta la síntesis de la clasificación de vulnerabilidades, amenazas y riesgos de la Norma Técnica Colombiana ISO 27001. La descripción detallada de la clasificación se puede apreciar en la tabla contenida en el *ANEXO C. Escala de valoración de metodologías de pruebas de penetración bajo definición de riesgos de la norma NTC-ISO 27001* de este documento.

Tabla 15. Norma Técnica Colombiana ISO 27001

Norma Técnica Colombiana ISO 27001	
Sección	**Vulnerabilidades, Amenazas y Riesgos**
1	Política de seguridad
2	Organización de la seguridad de la información
3	Gestión de activos
4	Seguridad de los recursos humanos
5	Seguridad física y del entorno
6	Gestión de comunicaciones y operaciones
7	Control de acceso
8	Adquisición, desarrollo y mantenimiento de sistemas de información
9	Gestión de los incidentes de la seguridad de la información
10	Gestión de la continuidad del negocio
11	Cumplimiento

Una vez identificadas vulnerabilidades, amenazas y riesgos informáticos, se establece la escala para realizar la valoración cuantitativa de las metodologías de pruebas de penetración abiertas, teniendo en cuenta el enfoque sobre seguridad en redes inalámbricas de este proyecto. Para ello se estableció una escala de valoración de gestión de vulnerabilidades, amenazas y riesgos en seguridad de redes inalámbricas, la cual se consigna en la siguiente tabla.

Tabla 16. Escala de valoración de gestión de vulnerabilidades, amenazas y riesgos inalámbricos

Calificación	Parámetro
0	No ofrece descripción ni enfoque de gestión de la vulnerabilidad, amenaza o riesgo, ni se describe la prueba de penetración
1	Se describe la vulnerabilidad, amenaza o riesgo, pero no describe su enfoque de gestión ni se describe la prueba de penetración
2	Se describe la vulnerabilidad, amenaza o riesgo y su enfoque de gestión, pero no describe la prueba de penetración
2	Se describe la vulnerabilidad, amenaza o riesgo y la prueba de penetración, pero no describe su enfoque de gestión
3	Se describe la vulnerabilidad, amenaza o riesgo, su enfoque de gestión y la prueba de penetración

Posteriormente se realizó la valoración de cada metodología de acuerdo con la cobertura de la vulnerabilidad, amenaza o riesgo descrito en la clasificación de riesgos de la Norma Técnica Colombiana ISO 27001. Los resultados detallados de la aplicación de la escala de valoración se pueden apreciar en la tabla contenida en este documento, en el *ANEXO C. Escala de valoración de metodologías de pruebas de penetración bajo definición de riesgos de la norma NTC-ISO 27001*. La síntesis de los resultados obtenidos en la aplicación de la escala de valoración de las metodologías de pruebas de penetración se consigna en la siguiente tabla.

Tabla 17. Valoración de las metodologías de pruebas de penetración

Riesgo | Amenaza | Vulnerabilidad		Metodología | Marco					
		OSSTMM	OWASAP	ISAAF	NIST	PTES	PTF
1	Política de seguridad	6	6	5	6	5	1
2	Organización de la seguridad de la información	33	24	9	31	12	5
3	Gestión de activos	15	3	9	14	5	3
4	Seguridad de los recursos humanos	24	10	0	23	0	0
5	Seguridad física y del entorno	27	12	10	21	11	4
6	Gestión de comunicaciones y operaciones	86	70	28	81	30	22
7	Control de acceso	72	69	65	69	65	65
8	Adquisición, desarrollo y mantenimiento de sistemas de información	41	48	33	38	34	33

9	Gestión de incidentes de seguridad de la información	15	14	4	11	6	4
10	Gestión de la continuidad del negocio	14	12	1	13	1	1
11	Cumplimiento	29	26	12	28	14	12
Valoración Metodologías		**362**	**291**	**176**	**335**	**183**	**150**
Porcentaje de Compatibilidad		**91%**	**73%**	**44%**	**84%**	**46%**	**38%**

Para poder apreciar mejor los resultados se puede observar el siguiente gráfico con el resultado de la valoración de las metodologías abiertas de pruebas de penetración contrastadas, en donde se observa que la metodología OSSTMM es la más adecuada para la ejecución de los objetivos planteados en este proyecto con una valoración del 91% de cobertura.

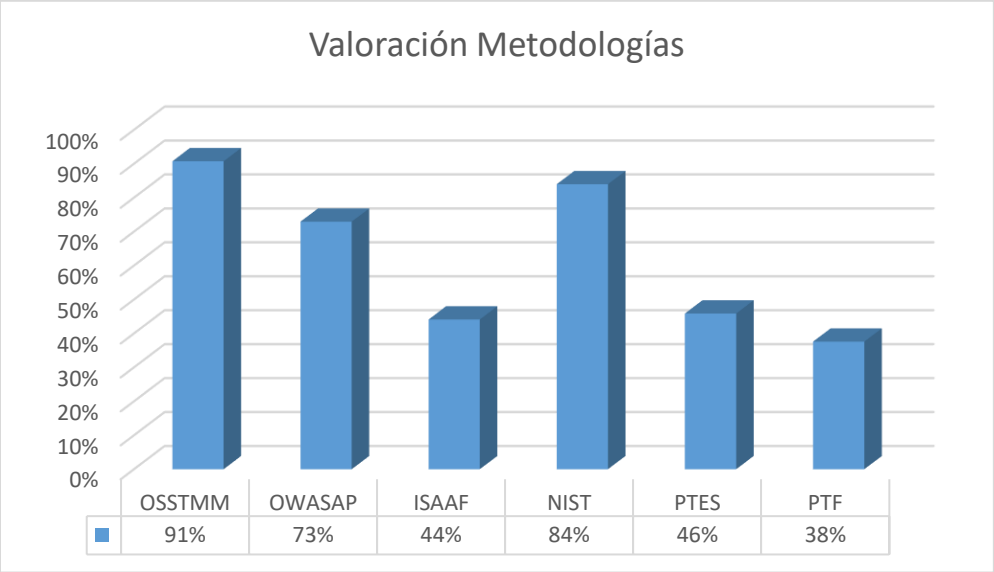


Figura 6. Valoración de las metodologías abiertas según la norma ISO 27001

En el siguiente gráfico se observa mejor la cobertura de los temas valorados por cada metodología de pruebas de penetración contrastada, en donde se puede apreciar que la metodología OSSTMM es la metodología que mejor abarca los riesgos, vulnerabilidades y amenazas en seguridad de la información enmarcados en la norma técnica colombiana ISO 27001, siendo la mejor opción para realizar la evaluación del nivel de seguridad de la red inalámbrica en el Cantón Militar de Popayán.

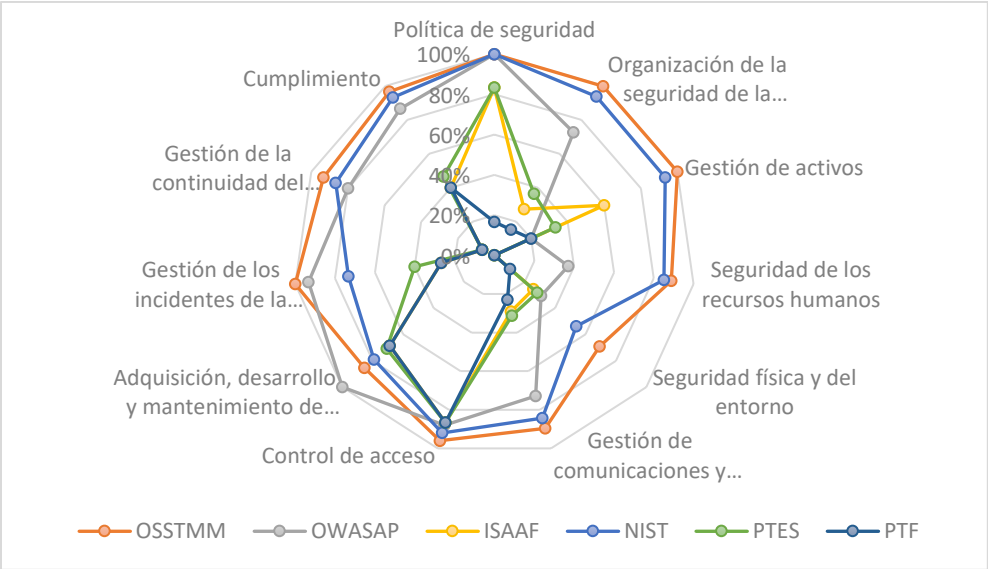


Figura 7. Riesgos norma ISO 27001 vs Metodologías abiertas de pruebas de penetración

Se escogió finalmente la metodología *OSSTMM - Manual de metodología de pruebas de seguridad de código abierto* en su tercera versión para para el diseño del plan de trabajo principal por su enfoque completo de gestión en seguridad de la información para la infraestructura de red inalámbrica del Cantón Militar de Popayán acorde con los objetivos de seguridad del Ejercito Nacional de Colombia, y se implementó en conjunto con el enfoque de pruebas de penetración planteadas en el marco *PTF - Marco de prueba de penetración versión 0.59*.

3.2. Planeación de la metodología de pruebas de penetración

Para que las pruebas de penetración fueran efectivas en su objetivo de identificar vulnerabilidades, se plantearon acorde con la arquitectura de seguridad existente en la infraestructura de red inalámbrica y las posibles vulnerabilidades a detectar de acuerdo con el tipo de información que se maneja en la institución militar. De igual manera, se estableció un marco común de trabajo para la ejecución de las pruebas de penetración, donde la metodología cubrió las tres fases de este tipo de proyectos.

3.2.1. Pre-ejecución

En esta fase se definieron los roles y responsabilidades de los participantes en las pruebas de penetración, los tipos de pruebas de penetración a ejecutar, la definición del entorno de red inalámbrica a ser evaluado, la documentación a ser provista como gráficos de red y diagramas de flujo, las políticas de la prueba de penetración como alcance y objetivos para su ejecución, canales de comunicación y acciones cuando se identificasen datos sensibles del Ejército, coordinación, aprobaciones y responsabilidades en el entorno de red del Cantón Militar, y los criterios para establecer la finalización de la prueba si se compromete el sistema, se inhabilita un control de seguridad o se obtienen datos militares confidenciales.

3.2.2. Ejecución

En esta fase se realizó el análisis de vulnerabilidades, se ejecutaron las pruebas de penetración en la infraestructura de red inalámbrica del Cantón Militar de Popayán, se realizó la revisión de los controles de segmentación de la red inalámbrica, se obtuvo el reporte de acceso a datos confidenciales del Ejército y se ejecutaron escaneos adicionales después de la evaluación del sistema en búsqueda de vulnerabilidades no detectadas.

3.2.3. Post-ejecución

En esta fase se definieron las mejores prácticas para plantear una posible solución de las vulnerabilidades identificadas en la red inalámbrica y se recomendó realizar nuevamente la ejecución programada de las pruebas de penetración, posterior a la ejecución de la implementación de las correcciones, para validar que el riesgo haya sido gestionado satisfactoriamente. Igualmente se realizó la eliminación de cuentas y/o software utilizado en las pruebas de penetración.

4. Aplicación de la metodología OSSTMM - Manual de metodología de pruebas de seguridad de código abierto

Dentro de la metodología OSSTMM se encuentra contenido el capítulo 9 que se enfoca específicamente en las pruebas para determinar el nivel de seguridad de una red inalámbrica. Este capítulo se centra básicamente en clasificaciones de seguridad del espectro, electrónica, de señales y emanaciones. Su objetivo principal es consistente con los objetivos planteados en este proyecto de grado para evaluar la seguridad de la información en la infraestructura de red inalámbrica del Cantón Militar de Popayán, el cual es el auditar la seguridad del espectro acorde con la clasificación de seguridad que incluye la seguridad electrónica, seguridad de señales, y seguridad de emanaciones en una red inalámbrica. (Metodología OSSTMM, 2010)

Tabla 18. Clasificación de seguridad del espectro

Clasificación	Sigla	Descripción
Seguridad del espectro	SPECSEC	Clasificación de seguridad
Seguridad electrónica	ELSEC	Medidas para denegar acceso no autorizado a información derivada de intercepción y análisis de radiaciones electromagnéticas de comunicaciones no autorizadas
Seguridad de señales	SIGSEC	Medidas para proteger las comunicaciones inalámbricas de acceso no autorizado y atasco
Seguridad de emanaciones	EMSEC	Medidas para prevenir emanaciones de dispositivos que, si son interceptadas y analizadas, revelaría información transmitida, recibida, manejada o procesada por equipos de sistemas de información

Se busca facilitar y proteger la interacción del analista que realiza el escaneo dentro del rango de proximidad de los objetivos de las pruebas de seguridad, que en este canal son pruebas de barrera física y lógica, así como la medición de brechas según el estándar de seguridad requerido y descrito en la política de la institución, regulaciones de la industria o legislación regional, para asegurar que la recopilación de datos genere los resultados esperados a través de la correlación y el análisis correspondiente.

El proceso ejecutado para la implementación de la metodología OSSTMM es el siguiente.

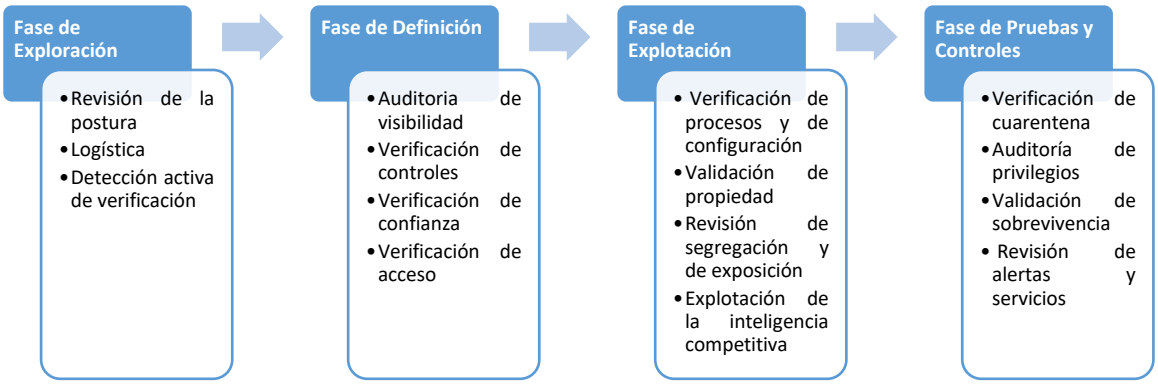


Figura 8. Metodología OSSTMM

4.1. Fase de Exploración

4.1.1. Revisión de la postura

Se presenta la revisión de la postura institucional que consiste en leyes, ética, políticas, reglamentos de la industria militar y la cultura política del Ejército en materia de seguridad de la información, las cuales influyen en la definición de los requisitos de seguridad y privacidad para la delimitación del alcance de la infraestructura de red inalámbrica del Cantón Militar de Popayán.

4.1.1.1. Política

El Ejército Nacional de la república de Colombia propende por brindar al personal de los diferentes Cantones Militares un servicio de Internet de alta disponibilidad, de tal manera que el flujo de datos a través de su infraestructura de red inalámbrica garantice autenticidad, confiablidad e integridad de la información militar en las comunicaciones bajo el marco legal jurídico vigente. Para ello ha estipulado las *Políticas de Uso Aceptable – PUA*, las cuales contienen las normas, políticas y estándares establecidos para el uso de activos informáticos de las Fuerzas Militares de Colombia, buscando garantizar la seguridad de la información y el uso responsable de los dispositivos de su infraestructura de red de datos. (Solicitud Servicios Informátivos Usuarios, 2018)

Las Políticas de Uso Aceptable del Ejército Nacional de Colombia bajo las cuales se rige el Cantón Militar de Popayán se relacionan en la tabla siguiente.

Tabla 19. Políticas De Uso Aceptable - PUA

Políticas de Uso Aceptable - PUA	
El uso aceptable de los activos informáticos de las Fuerzas Militares, implica la aceptación implícita por parte de los usuarios de estos, de las normas, políticas y estándares establecidos para garantizar la seguridad informática y el uso de los mismos, así como de los compromisos y responsabilidades adquiridas. Los siguientes se consideran actos no autorizados o de obligatorio cumplimiento para el uso de los activos informáticos de las Fuerzas Militares y están expresamente prohibidos así	
1	El intento o violación de los controles de seguridad establecidos para la protección de los activos informáticos de las FF.MM.
2	Realizar cualquier actividad que pudiera comprometer la seguridad de cualquier activo informático de las FF.MM.
3	El uso sin autorización de los activos informáticos de las Fuerzas Militares.
4	El uso no autorizado o impropio de la conexión al sistema.
5	Intentar evadir o violar la seguridad o autenticación de usuario de cualquier host, red o cuenta.
6	El uso indebido de las contraseñas, firmas digitales o dispositivos de autenticación.
7	Está prohibido a cualquier usuario acceder a servicios informáticos utilizando cuentas o medios de autenticación de otros usuarios. Aún con la autorización expresa del usuario propietario de la misma.
8	El almacenamiento, instalación, configuración o uso de software ilegal o no autorizado o de datos no autorizados en los activos informáticos de las FF.MM.
9	Está prohibido el uso, distribución y ejecución de software o código malicioso que cause daño, hostigamiento, molestias a personas, daño o alteración de información o traumatismos en la continuidad de los servicios informáticos o vulnere la seguridad de los sistemas.
10	El hurto, robo, sustracción o uso no autorizado de: datos, información, materiales, equipos y otros elementos pertenecientes a los activos informáticos de las FF.MM.
12	Está prohibido retirar de las instalaciones de las Fuerzas Militares o áreas bajo su administración o control, cualquier activo informático sin previa autorización.
13	El acceso, modificación o alteración no autorizada de componentes, datos o información de los activos informáticos de las FF.MM.
14	El uso de medios electrónicos, medios de almacenamiento, software, hardware, datos o información en medios digitales provenientes de fuentes no certificadas o de terceros sin la previa revisión o autorización del Administrador del Sistema y/o Oficial de Seguridad Informática.
15	El servicio de Internet puede ser utilizado solamente con fines autorizados y legales. Se prohíbe toda transmisión, difusión, distribución o almacenamiento de cualquier material –digital o impreso- en violación de cualquier ley o regulación aplicable. Esto incluye, sin limitación alguna, todo material protegido por los derechos de autor, marcas, secretos comerciales u otros derechos de prioridad intelectual usados sin

	la debida autorización, y todo material obsceno o pornográfico, difamatorio o que constituya una amenaza legal.
16	En el uso del correo electrónico, está prohibido: El Spam, el Troll, Mailbombing, reenvió o transmisión de mensajes de carácter no oficial ó la suscripción a otro usuario a una lista de correo sin su permiso.
17	Realizar por Internet, o a través de los activos informáticos, cualquier actividad que pudiera potencialmente traer desprestigio a las Fuerzas Militares de Colombia.
18	Los mensajes contenidos en los correos electrónicos no pueden ser contrarios a las disposiciones del orden público, la moral, las buenas costumbres nacionales e internacionales y los usos y costumbres aplicables en Internet y el respeto de los derechos de terceras personas.
19	Está prohibido el almacenamiento y reproducción de aplicaciones, programas, archivos de audio que no estén relacionados con las actividades propias de las funciones que cumple la dependencia o el usuario.
20	El usuario está de acuerdo en aceptar responsabilidad por todas las actividades realizadas con los activos informáticos bajo su responsabilidad y custodia o desde las cuentas asignadas para su acceso a los servicios informáticos de las Fuerzas Militares.
21	Está prohibido el intento o el hecho de agregar, remover o modificar información identificadora o de contenido en la red, que engañe o confunda al sistema o al usuario destinatario o suplante a otro usuario utilizando su información identificadora.
22	Las cuentas de red de las Fuerzas Militares operan con recursos compartidos. Está prohibido el uso abusivo de estos recursos por parte de un usuario en una forma tal que afecte negativamente el rendimiento de la misma.

4.1.1.2. Legislación

En Colombia, la intrusión no autorizada en sistemas informáticos es una actividad que se encuentra enmarcada dentro de las prohibiciones expresas consignadas en las leyes sancionadas para establecer las penas sobre delitos informáticos. Por esta razón, se deben establecer previamente todas las reglas, compromisos y responsabilidades entre las personas que ejecutan la prueba de penetración y la institución en la cual se realizan las pruebas de penetración correspondientes, estableciendo en el caso de la ejecución de este proyecto de grado, un acuerdo de aceptación y confidencialidad entre las partes que avala la ejecución del ataque a los sistemas de información del Ejército Nacional de Colombia, bajo un marco jurídico legal y ético, y por ende no se presente ninguna violación de la legislación en materia.

La normatividad que sanciona los delitos informáticos se encuentra tipificada bajo el marco de la ley 1273 de 2009, por medio de la cual se modifica el Código Penal, creando un nuevo bien jurídico tutelado - denominado "*de la protección de la información y de los datos*", que se enfoca en preservar integralmente los sistemas

que utilicen las tecnologías de la información y las comunicaciones[5]. Esta ley está compuesta por diez artículos que exponen la normatividad vigente sobre el tipo de hechos que pueden ser considerados como un delito informático en Colombia y cuáles son las circunstancias de agravación punitiva relacionadas. Esta ley está compuesta por los siguientes artículos:

Tabla 20. Ley 1273 de 2009 Protección de la información y de los datos

Artículo	Descripción
Capítulo I	*De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos*
269A	Acceso abusivo a un sistema informático
269B	Obstaculización ilegítima de sistema informático o red de telecomunicación
269C	Interceptación de datos informáticos
269D	Uso de software malicioso
269E	Violación de datos personales
269F	Suplantación de sitios web para capturar datos personales
269G	Acceso abusivo a un sistema informático
Capítulo II	*De los atentados informáticos y otras infracciones*
269H	Circunstancias de agravación punitiva
269I	Hurto por medios informáticos y semejantes
269J	Transferencia no consentida de activos

De igual manera, el gobierno nacional sancionó la ley estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales, definiendo como *dato personal "Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables"* y *tratamiento* como "*Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión*", estableciendo los principios para el tratamiento de datos personales y datos sensibles[6]. Esta ley se compone básicamente de los siguientes títulos:

Tabla 21. Ley 1581 de 2012 Disposiciones generales para la protección de datos personales

Titulo	Descripción
I	Objeto, ámbito de aplicación y definiciones
II	Principios rectores
III	Categorías especiales de datos
IV	Derechos y condiciones de legalidad para el tratamiento de datos
V	Procedimientos
VI	Deberes de los responsables del tratamiento y encargados del tratamiento

[5] Ley 1273 de 2009. Protección de la información y de los datos. Senado de la república. 05 de enero de 2009. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html.

[6] Ley 1581 de 2012. Disposiciones generales para la protección de datos personales. Senado de la república. 17 de octubre de 2012. http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html.

VII	De los mecanismos de vigilancia y sanción
Capítulo I	*De la autoridad de protección de datos*
Capítulo II	*Procedimiento y sanciones*
Capítulo III	*Del registro nacional de bases de datos*
VIII	Transferencia de datos a terceros países

Adicionalmente, se publica el documento CONPES 3854 el 11 de abril de 2016, por el cual se establece la Política nacional de seguridad digital. El enfoque de la política de ciberseguridad y ciberdefensa se concentra en contrarrestar el incremento de las amenazas cibernéticas bajo los objetivos de defensa del país; y lucha contra el cibercrímen en las instituciones del estado, estableciendo un marco institucional claro en torno a la seguridad digital y creando las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital, mediante mecanismos de participación activa y permanente, la adecuación del marco legal y regulatorio de la materia y la capacitación para comportamientos responsables en el entorno digital. Igualmente fortalece la defensa y seguridad nacional en el entorno digital, a nivel nacional y trasnacional, con un enfoque de gestión de riesgos, además de generar mecanismos permanentes para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional, con un enfoque estratégico[7].

Se tuvo en cuenta entonces entre las partes la anterior normativa descrita, para la planeación de los acuerdos de operación previos al ataque informático y durante la ejecución de las pruebas de penetración éticas a la infraestructura de red inalámbrica del Cantón Militar de Popayán, propendiendo por la protección de la información militar confidencial bajo el marco de la legislación mencionada en todo el proceso y garantizando la seguridad de los datos e información almacenada y gestionada por los sistemas de información del Ejército nacional en el Cantón Militar de Popayán.

4.1.1.3. Cultura

La cultura organizacional en la red inalámbrica se enfoca principalmente en el ámbito de la seguridad y conocimiento de la privacidad de la información, capacitación y disponibilidad del personal requerido, jerarquía organizacional, uso de la mesa de ayuda y requisitos para reportar problemas de seguridad en la red de datos.

Realizando un análisis bajo el contexto planteado, se encontró que no existe una cultura organizacional apropiada en el ámbito de la seguridad y conciencia de la

[7] CONPES 3854 de 2016. Política nacional de seguridad digital. CONPES 3854 del 11 de abril de 2016. Departamento Nacional de Planeación. https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf.

privacidad de información confidencial tan importante como la militar, no hay políticas institucionales que propendan la capacitación y disponibilidad del personal requerido en los diferentes batallones para gestionar adecuadamente la red de datos, no existe en el Ejército una jerarquía organizativa con responsabilidades definidas de acuerdo a perfiles adecuados para resolver las necesidades de administración, gestión y repulsión de un ataque informático, tampoco se cuenta con servicio de asistencia remota en caso de un ataque informático, intrusión en la red inalámbrica o perdida de información importante, no existen reportes sobre el uso de la infraestructura de red de datos o sobre un ataque o intruso informático, ni tampoco requisitos para reportar problemas de seguridad por parte de los usuarios en la red inalámbrica del Cantón Militar de Popayán, por cuanto no se capacita con cursos, diplomados o estudios superiores al personal que administra la infraestructura de red de datos, a pesar de la importancia de una institución que siempre se encuentra en un alto riesgo de ataques informáticos como lo es el Ejército Nacional de Colombia.

4.1.1.4. Edad

Consiste en la revisión de la antigüedad de los sistemas, software, firmware y aplicaciones de servicio requeridos para la operación de la red inalámbrica en el Cantón Militar de Popayán. Esta revisión es importante por cuanto sistemas operativos o firmware muy antiguo pueden generar vulnerabilidades ya identificadas por marca o fabricante que pueden ser explotadas por un intruso en un eventual ataque informático.

Se puede apreciar en la tabla siguiente que la antigüedad de los sistemas operativos, software de terminales y firmware de dispositivos de red no se encuentra dentro de un rango ideal de antigüedad para la operación de una institución militar, debido a que no han sido actualizados recientemente por parte del personal encargado del Ejército y por lo tanto existe una vulnerabilidad latente en este aspecto.

Tabla 22. Antigüedad del software en la red de datos del Cantón Militar de Popayán

Ítem	Descripción	Antigüedad
Sistemas Operativos	Estaciones de trabajo desactualizadas y con versiones antiguas de Windows	10 años
Firmware de Dispositivos de Red	Firmware desactualizado del punto de acceso inalámbrico de la Tercera División	4 años
Software Ofimática	Estaciones de trabajo con Microsoft Office 2010	9 años
Aplicaciones de Servicio Militar	Todas actualizadas a su última versión	1 año

Además, se encontró que no se están aplicando las actualizaciones de software respectivas y necesarias, tanto de los sistemas operativos de las terminales que

acceden a la red inalámbrica como de las aplicaciones ofimáticas instaladas en las terminales de la red de datos. Los sistemas operativos se encuentran desactualizados, sin parches de seguridad instalados e incluso, en algunos casos con la licencia vencida, siendo esta una vulnerabilidad importante a gestionar.

Para que esta vulnerabilidad sea gestionada se sugirió que cada seis meses se hiciera una revisión de software para que se mantuviese actualizados los sistemas operativos en su versión estable más reciente, que se instalen todos los parches de seguridad disponibles por la marca fabricante del sistema operativo de las terminales, que se compren las licencias de Windows vencidas, que se mantenga actualizado el firmware de los dispositivos de acceso e interconexión de red y que se actualicen las aplicaciones ofimáticas a su versión más reciente.

4.1.1.5. Artefactos frágiles

Consiste en la revisión de cualquier sistema, software y aplicaciones de servicio institucional que pudieran requerir un cuidado especial debido a su alto uso por parte del personal del Ejército, inestabilidades o una alta tasa de cambio de información militar.

Dentro de los resultados encontrados en la revisión se obtuvo que los puntos de acceso inalámbrico se pueden considerar como dispositivos que requieren un cuidado especial debido a que son el punto principal de flujo de información militar en la infraestructura de red inalámbrica, encontrándose que su uso lógico y acceso físico no se encuentran restringidos, por ende, son vulnerables a un posible ataque informático de un intruso interno en una división militar.

En cuanto a la información del Ejército y aplicaciones de software institucionales, se debe disponer una atención especial sobre los servidores que componen el segmento de red para el área de almacenamiento de la información del Ejército Nacional de Colombia, debido a la importancia y criticidad de la información militar confidencial que almacenan a través de sus aplicaciones de operación institucional.

Estas aplicaciones oficiales generan información importante para el Ejército Nacional, no solo en los entornos de operación de combate militar en cumplimiento con su objeto institucional, sino también en entornos cotidianos y rutinarios de operación corporativa como institución pública del estado de la república de Colombia como por ejemplo información contable y financiera o de recursos humanos. Estos servidores no cuentan con dispositivos de seguridad especializada para redes de datos sensibles que permitan monitorear y controlar posibles ataques de intrusos informáticos, siendo una vulnerabilidad importante que se deberá corregir en la división para garantizar la seguridad de la información militar corporativa.

Las principales aplicaciones de operación militar con ejecución en los servidores del área de almacenamiento de la infraestructura de red de datos del Ejército Nacional de Colombia se pueden apreciar en la siguiente gráfica.

Figura 9. Aplicaciones del Ejército Nacional en el Cantón Militar de Popayán

Las principales aplicaciones de operación militar del Ejército Nacional de la República de Colombia que se deben proteger ante posibles ataques informáticos a través de la infraestructura de red inalámbrica del Cantón Militar de Popayán se listan a continuación.

Tabla 23. Aplicaciones militares del Cantón Militar de Popayán

Aplicación	Descripción
SICOE	Sistema de Contratación del Ejército para licitación pública del Ejército Nacional de Colombia
SIGEWEB	Sistema de gestión de riesgos del Ejército Nacional de Colombia
Folio de vida digital	Sistema para los perfiles del personal del Ejército Nacional de Colombia
SIATH	Base de datos del Ejército Nacional de Colombia
SICOI	Sistema Control de Inspecciones
Estadísticas del Ejército	Sistema de gestión de datos y estadísticas del Ejército Nacional de Colombia

SILAE	Sistema de lecciones aprendidas del Ejército Nacional de Colombia
Balanced Scorecard	Sistema de cuadro de mando integral para definir y monitorear objetivos, estrategias y metas institucionales mediante indicadores de rendimiento
SIJUR	Sistema Jurídico del Ejército Nacional de Colombia
Pagos de Nómina	Sistema para el pago de la nómina de empleados contratados directamente por el Ejército Nacional
Acreedores Varios	Sistema para el pago de acreedores varios del Ejército Nacional de Colombia
Retenciones Militares	Sistema para ingresos y retenciones del Ejército Nacional de Colombia
Reintegros	Sistema de reintegros, ascensos y retiros del Ejército Nacional de Colombia
Prima de Orden Público	Sistema para prima o bonificación de orden público del personal uniformado activo de las Fuerzas Militares
Nómina Prestaciones Sociales	Sistema financiero para pago de nómina y prestaciones sociales del personal del Ejército Nacional de Colombia
Doceavas Partes	Sistema de liquidación de primas y vacaciones para retiros de personal del Ejército Nacional de Colombia
Exógena DIAN	Información exógena tributaria para declaración como persona jurídica para fiscalización de operaciones
Cobros Persuasivos	Sistema de cobros persuasivos de acreencias, créditos u obligaciones del Ejército Nacional de Colombia

4.1.2. Logística

A continuación, se expone la logística realizada para la preparación del entorno del canal de pruebas necesario para evitar falsos positivos y falsos negativos que puedan conducir a resultados de pruebas de penetración inexactos en la ejecución del ataque informático en la infraestructura de red inalámbrica del Cantón Militar de Popayán.

4.1.2.1. Equipo de comunicaciones

La evaluación del equipo de comunicaciones consiste en la realización de pruebas de equipos que puedan transmitir radiación electromagnética, como monitores LCD, teclados, impresoras y módems, que se pueden usar para interceptar los datos que se muestran en pantalla, digitados, impresos, o transmitidos. La explotación de esta vulnerabilidad informática se conoce como phreaking[8] de Van Eck.

Así una terminal no se encuentre conectada a Internet, es vulnerable a este tipo de ataque informático ante un intruso interno dado que existen varias formas de poder infectarla una vez se consigue acceso físico a ella para captar información indebidamente. Una forma eficiente de intrusión es la instalación en la terminal de

[8] Phreaking: Acción de penetrar un sistema de telecomunicaciones para obtener llamadas gratuitas.

un malware[9] que envíe los datos capturados a un teléfono celular para poder captar finalmente la información en remoto por el atacante, el cual, una vez instalado en la terminal, utiliza la propia tarjeta gráfica del equipo para emitir pequeñas señales electromagnéticas con el cable del monitor a modo de antena cada vez que se pulsa una tecla. Este sistema de ataque informático puede tener un alcance de unos ocho metros aproximadamente, suficiente para capturar una señal que contenga la contraseña de la red inalámbrica o un pequeño texto con información militar a una oficina contigua.

Esta prueba de penetración no fue ejecutada por cuanto requiere de la instalación del malware en la terminal atacada, hecho que viola las restricciones consagradas en la definición del alcance de las pruebas de penetración planteadas conjuntamente en el alcance de este proyecto, en donde no se autorizó por parte del Ejército Nacional, la instalación de programas de código malicioso en sus terminales de cómputo (*Ver ANEXO B*).

- Se restringen las pruebas de penetración informática únicamente a los puntos de acceso de la red inalámbrica del Cantón Militar de Popayán, no se autorizan pruebas de penetración contra las terminales, dispositivos de interconexión ni ningún otro activo de red diferente, por cuánto estás labores están restringidas y autorizadas únicamente al personal militar que labora en el área de seguridad informática en la institución, por protocolos de seguridad de contrainteligencia militar interna de la red del Ejército Nacional de Colombia.

4.1.2.2. Comunicaciones

En cuanto a las comunicaciones se realizó el análisis correspondiente para identificar los protocolos que se utilizan dentro del alcance de la red inalámbrica y los métodos de transmisión utilizados.

La comunicación de la red inalámbrica del Cantón Militar de Popayán se realiza mediante el protocolo Wi-Fi cuyo estándar es el IEEE 802.11n, en un medio de transmisión no guiado para cada una de las divisiones militares del Ejército Nacional. De igual manera, existen redes de viviendas aledañas al perímetro físico del Cantón Militar que se transmiten sobre el mismo protocolo, pero que no alcanzan a interferir con el alcance de la señal del punto de acceso inalámbrico de la Tercera División militar, objeto de este estudio.

[9] Malware: Software malicioso. Se refiere a cualquier tipo de software malicioso que trata de afectar un ordenador, teléfono celular u otro dispositivo informático.

4.1.2.3. Tiempo

La prueba para el marco de tiempo consiste en determinar los horarios de operación de los puntos de acceso inalámbrico para brindar el servicio de Internet a los usuarios del Ejército Nacional en el Cantón Militar de Popayán. Se encontró que están configurados para estar disponibles en operación 7/24 y no se realiza ningún control de tiempos muertos de trabajo en horarios no laborales, para así evitar que un intruso malicioso pueda tener acceso a la red inalámbrica para desplegar un ataque informático sobre la infraestructura de red de datos en horarios no laborales.

Se sugirió limitar el acceso a Internet a través de estos dispositivos en las áreas deshabitadas en los horarios no laborales, solo habilitar el acceso a este servicio durante la jornada de trabajo oficial mientras el personal del Ejercito se encuentre en las instalaciones militares.

Tampoco se hace diferencia, aislamiento o segmentación lógica en la infraestructura de red entre puntos de acceso inalámbrico exclusivos para el personal que labora en las divisiones militares con aplicaciones e información importante y confidencial que debe ser transmitida a los servidores del segmento de red de área de almacenamiento, y cuya contraseña de acceso es de alta importancia y por ende debe suministrarse únicamente al personal que realice la gestión de la red de datos; y puntos de acceso inalámbrico generales para visitantes, familiares y particulares, aislados del entorno de red que transmite la información confidencial en el Cantón Militar de Popayán y por ende el suministro de su clave de acceso no es un punto crítico dentro de las políticas de seguridad de la institución militar.

4.1.3. Verificación de detección activa

En esta etapa se realizó la determinación de los controles activos y pasivos para detectar la intrusión de un atacante malicioso en la infraestructura de red inalámbrica del Cantón Militar de Popayán y poder filtrarla o denegarla. Esta verificación debe ser realizada antes de la prueba para mitigar el riesgo de crear falsos positivos y negativos en los datos de resultados de la prueba, así como cambiar el estado de alarmas de monitoreo de personal o agentes guardianes.

Se pusieron en operación todos los controles activos y pasivos existentes por cuanto la idea es que se corrobore si existe la posibilidad de éxito de un ataque informático en la red inalámbrica del Cantón Militar aún con todas las defensas y escudos informáticos activos, por ende, en la planeación del ataque no se desactivo ningún mecanismo de seguridad que tuviese la infraestructura de red de datos del Ejército.

No obstante, en el análisis se encontró que no existen controles, dispositivos o mecanismos de control activos o pasivos que garanticen la seguridad en el servicio de red inalámbrica del Ejército Nacional en las diferentes divisiones militares, siendo una vulnerabilidad importante por gestionar. En la sección *Recomendaciones*

infraestructura de red inalámbrica de este documento se proponen controles de seguridad para la red inalámbrica del Cantón Militar de Popayán que gestionan esta vulnerabilidad.

4.1.3.1. Monitoreo de canales

El monitoreo de canales consiste en la comprobación de la existencia de controles para monitorear la intrusión o la manipulación de la señal de la red inalámbrica en un ataque informático.

Se encontró que no existen actualmente controles implementados para monitorear la intrusión o manipulación de la señal de la red inalámbrica ante un ataque informático en el Cantón Militar de Popayán.

Se sugirió la implementación de un sistema de detección de intrusos, el cual posee un método de autentificación seguro y tiene como características la prevención de ataques de negación de servicio, sistema de prevención de intrusiones, mensajes de registro en la red informática y negociación automática. Este sistema permite hacer el monitoreo de canales de la red inalámbrica de una manera óptima y eficiente con sensores detectores de intrusos por cada división militar. La descripción detallada de este sistema se muestra más adelante en este documento en la sección *Sistema de detección de intrusos inalámbrico*.

4.1.3.2. Moderación de canales

La moderación de canales consiste en la comprobación de la existencia de controles para bloquear las señales (interferencias) o avisar de actividades no autorizadas en la red inalámbrica.

Se encontró que no existen controles implementados para bloquear señales de atacantes e interferencias de señales de intrusos en la red inalámbrica del Cantón Militar de Popayán, ni que detecten o alerten de actividades no autorizadas, maliciosas o sospechosas en la infraestructura de la red inalámbrica y alertasen al personal del Ejercito correspondiente.

Como en el punto anterior, esta vulnerabilidad se gestiona con la implementación del sistema de detección de intrusos que también posee esta capacidad de detección y bloqueo de señales maliciosas mediante sus sensores detectores de intrusos y envío de mensajes de registro en la red inalámbrica, así como disposición en cuarentena de terminales o puntos de acceso sospechosos (Ver sección *Sistema de detección de intrusos inalámbrico*).

4.2. Fase de Definición

4.2.1. Auditoria de visibilidad

La auditoría de visibilidad consiste en la ejecución de pruebas de enumeración y verificación de la visibilidad de la señal de red inalámbrica al servicio del personal del Ejército y la posibilidad de interacción a través de todos los canales probables. Las pruebas de visibilidad ejecutadas se describen a continuación.

4.2.1.1. Interceptación

Se debe verificar si es posible una interceptación de la señal de la red inalámbrica por un intruso interno, identificando el control de acceso, la seguridad perimetral y la capacidad de interceptar o interferir con los canales inalámbricos de la institución militar.

Dentro de los resultados de la prueba se encontró que no es posible una interceptación de la señal para un intruso externo que quisiere acceder físicamente al área de cobertura de la red inalámbrica para ejecutar el ataque de red, debido a los estrictos controles que tiene el Cantón Militar para el ingreso a su sede física como cualquier otra institución de índole militar. Por ende, un intruso tendría que violar primero los diferentes controles biométricos de acceso al Batallón y además, la seguridad perimetral de los centinelas en turno de guardia de vigilancia para poder posteriormente ejecutar este tipo de ataque.

Ahora, suponiendo el escenario en que el intruso efectivamente logre violar los controles de acceso y la seguridad perimetral del Batallón, se encontró que si es posible realizar una interceptación o interferencia de la señal de la infraestructura de red inalámbrica del Cantón Militar de Popayán por un intruso informático.

Para ello se ejecutó la prueba de penetración *punto de acceso no autorizado* que consiste en un punto de acceso inalámbrico que se instala en la red de datos sin autorización de los administradores de la red, agregado por un atacante malicioso con acceso físico al área de cobertura de la señal de red inalámbrica. Este punto de acceso inalámbrico no autorizado puede ser configurado sin contraseña y permitir el acceso a la red de datos de personas no autorizadas por el Ejército, puede confundir a los usuarios para que se conecten a él, capturar el tráfico de datos y descifrar las credenciales de red o puede permitir ejecutar varios tipos de escaneos de vulnerabilidades, siendo posible incluso lograr acceso al segmento de red de área de almacenamiento con la información crítica confidencial militar del Ejército Nacional.

Esta prueba de penetración se ejecutó con el enrutador inalámbrico Nexxt Solutions Nébula en modo repetidor que permite propagar la señal de la red inalámbrica hacia nuevos usuarios no pertenecientes al Ejército Nacional, repitiendo la señal de red inalámbrica de la división militar pero con una nueva configuración de credenciales

de autenticación definida en este caso por el intruso malicioso que ejecutase el ataque a la red de datos. El esquema de la prueba ejecutada se presenta en la imagen a continuación.

Figura 10.Prueba de penetración interna punto de acceso no autorizado

El enrutador inalámbrico Nexxt Solutions Nébula utilizado en la prueba de penetración interna punto de acceso no autorizado ejecutada en la infraestructura de red inalámbrica del Cantón Militar de Popayán es el siguiente.

Figura 11. Enrutador inalámbrico Nexxt Solutions Nébula

Para realizar la gestión de esta vulnerabilidad se sugirió la implementación del sistema de detección de intrusos inalámbrico, el cual posee la capacidad de evitar la instalación de puntos de acceso inalámbrico maliciosos, monitoreando en tiempo real el espectro de radiofrecuencia de la señal de red mediante sus sensores detectores de intrusos, en busca de puntos de acceso no autorizados por cada división militar. Para ello, el sistema de detección de intrusos genera una lista de los puntos de acceso inalámbrico autorizados dentro de las políticas de seguridad de la red de datos, permitiendo identificar rápidamente un punto de acceso que no pertenezca a la infraestructura de red inalámbrica del Ejército. De esta manera se logra reducir la posibilidad que la señal sea interceptada desde el interior del perímetro físico del Cantón Militar de Popayán ante un eventual ataque informático de interceptación o interferencia de la señal inalámbrica (Ver sección *Sistema de detección de intrusos inalámbrico*).

Adicionalmente, se siguiere la implementación del sistema de prevención de intrusiones inalámbrico para monitorear cada segmento de red de datos en el Cantón Militar de Popayán, el cual detecta e identifica los dispositivos maliciosos que no pertenezcan a la infraestructura de red del Batallón de una manera bastante eficiente, permitiendo realizar gestión sobre el dispositivo malicioso detectado, como su disposición en cuarentena (Ver sección *Sistema de prevención de intrusiones inalámbrico*).

4.2.1.2. Detección pasiva de señales

Se debe realzar la detección de señal pasiva de señales de red inalámbrica, para la cual se debe:

a) Determinar qué frecuencias y señales pueden filtrarse dentro o fuera del área objetivo utilizando una antena direccional de alta ganancia y medios de detección pasivos como el análisis de frecuencias.
b) Crear un mapa de calor del alcance que muestre todas las fuentes de radiación, sus radios y fuerza.
c) Probar fuentes que interactúan sin autorización.
d) Recopilar información transmitida por estas fuentes.
e) Mapear todos los datos encontrados a los valores límite de emisión actualmente requeridos en la región para todas las radiaciones detectadas.

Los resultados de la ejecución de la prueba de detección pasiva de señales de red inalámbrica realizada en el Cantón Militar de Popayán, por cada uno de los ítems descritos anteriormente, se presentan a continuación.

a) Se realizó el estudio de las señales alcanzables dentro o fuera del área objetivo de la Tercera División del Cantón Militar de Popayán utilizando una antena direccional de alta ganancia y el análisis de frecuencias. Los resultados se presentan en las siguientes gráficas.

- *Interior*: En la siguiente gráfica se puede apreciar las señales de red inalámbrica que son alcanzables desde el interior del área objetivo de la prueba de penetración, la cual corresponde al área de acceso para usuarios al servicio de Internet del Ejército Nacional en la Tercera División del Cantón Militar de Popayán.

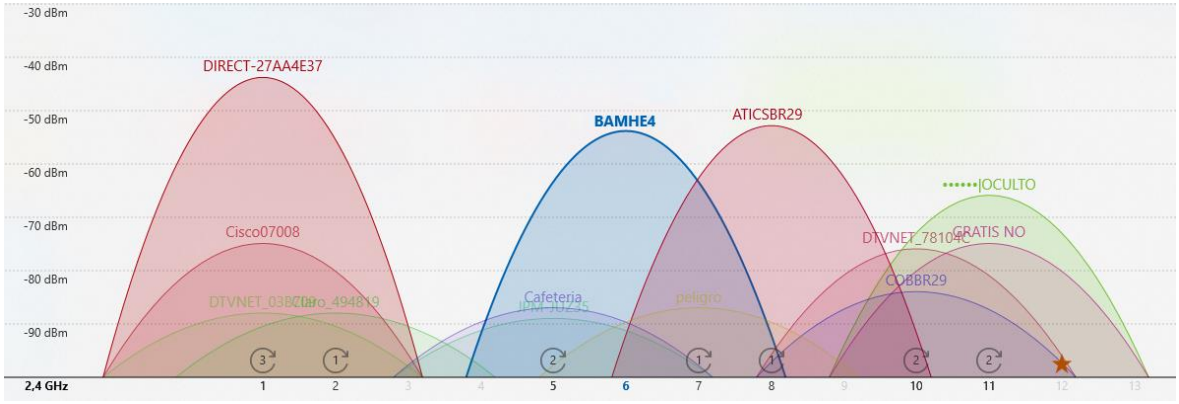


Figura 12. Redes alcanzables al interior de la Tercera División del Cantón Militar

De la gráfica se puede obtener el porcentaje de saturación de canales inalámbricos, para analizar si el canal seleccionado es el canal de operación ideal para que el punto de acceso de infraestructura pueda ofrecer el servicio de red inalámbrica en la Tercera División de Cantón Militar.

Tabla 24. Saturación de canales de red inalámbrica

Canal	N° Redes	% Saturación
1	3	23,1
2	1	7,7
3	0	0
4	0	0
5	2	15,4
6	**1**	**7,7**
7	1	7,7
8	1	7,7
9	0	0
10	2	15,4
11	2	15,4
Totales	**12**	**100**

En la tabla anterior se puede apreciar que en el canal 6, canal de operación el punto de acceso inalámbrico de la Tercera División del Cantón Militar de Popayán, no existen más redes inalámbricas, por lo tanto, su porcentaje de saturación, de 7,7% es apto para brindar un buen servicio de Internet a los usuarios del Ejército Nacional.

- *Exterior*: En esta gráfica se pueden apreciar las señales de red inalámbrica alcanzables desde fuera del área objetivo de la prueba de penetración en el Cantón Militar de Popayán. La descripción en detalle de esta prueba se presenta más adelante en la sección *4.3.5.2 Perfilado* en este documento.

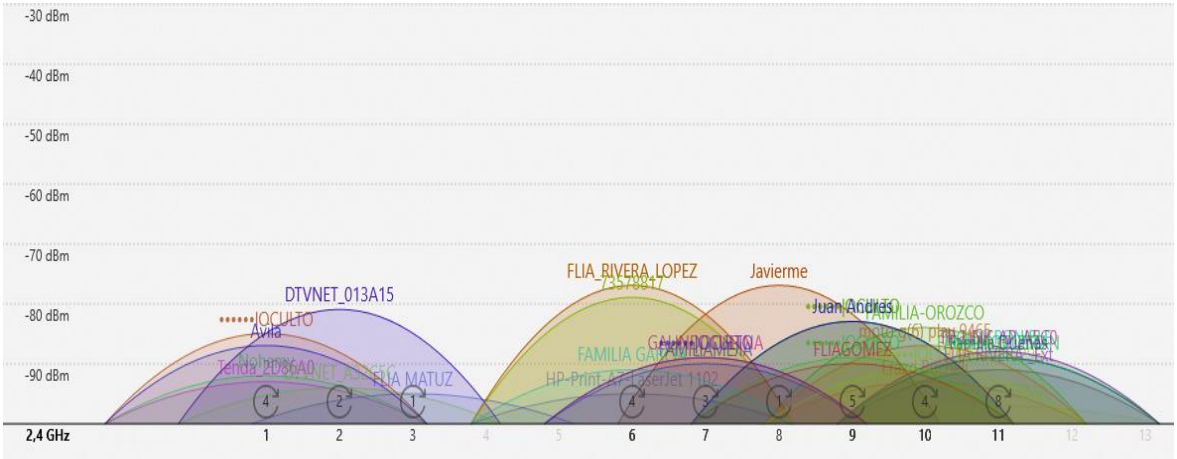


Figura 13. Redes alcanzables desde el exterior del Cantón Militar de Popayán

b) Se creó el mapa de calor del alcance que permite evidenciar la fuente de radiación, radio y fuerza del punto de acceso inalámbrico de la Tercera División del Cantón Militar de Popayán. El resultado se puede apreciar en la siguiente imagen

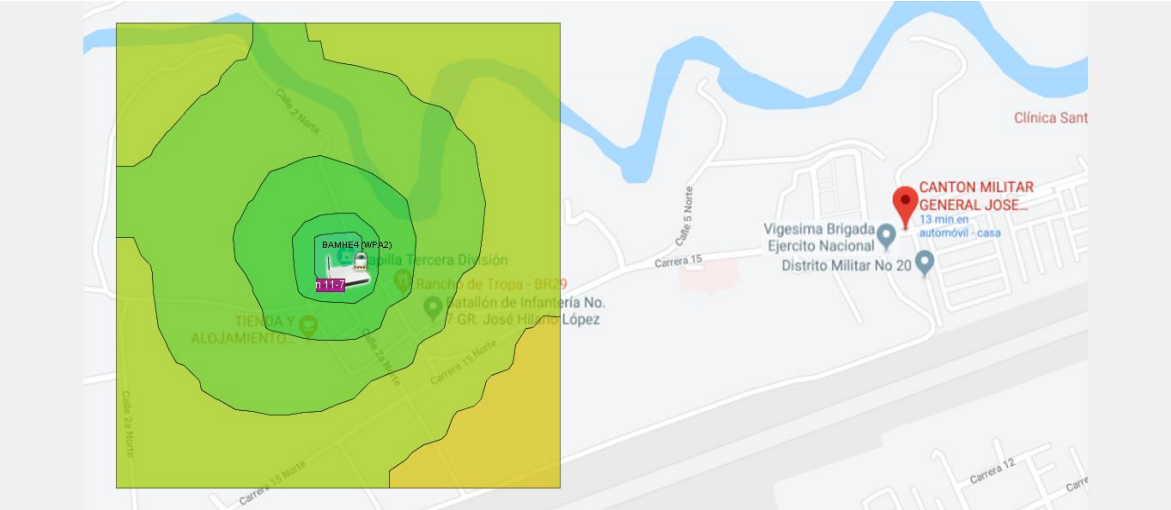


Figura 14. Mapa de calor punto de acceso inalámbrico Tercera División Cantón Militar

c) Se realizó la prueba de fuentes que interactúan sin autorización, encontrándose que existe en la división militar, un punto de acceso inalámbrico de infraestructura indebido marca *Tenda*, configurado para ampliar la cobertura de la señal de red inalámbrica en la cafetería del batallón, que no pertenece a la infraestructura de red de datos de la Tercera División del Cantón Militar de Popayán, siendo una vulnerabilidad latente por solucionar, dado que además este punto de acceso se encuentra sin contraseña de acceso a la interfaz de configuración administrativa y por ende cualquier usuario del personal del Ejército Nacional podría aprovecharla para realizar un ataque informático interno.

Los resultados de la prueba donde se analizó el punto de acceso inalámbrico indebido presente en la división militar para ampliación del servicio de Internet a los usuarios de la cafetería del Cantón Militar se pueden observar a continuación.

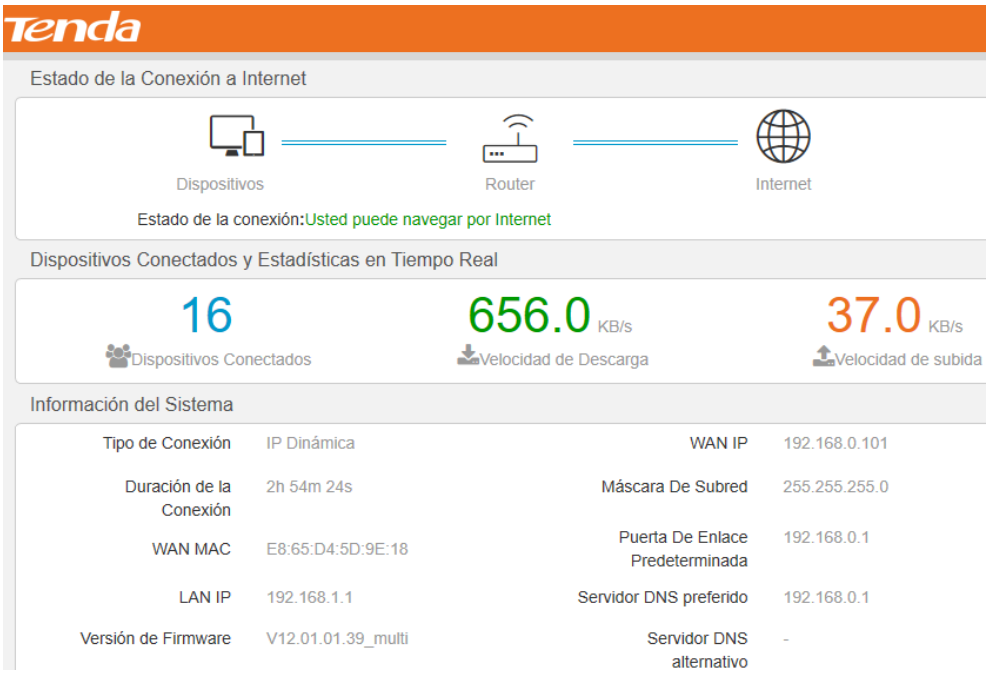


Figura 15. Punto de acceso inalámbrico de infraestructura indebido

En la imagen presentada a continuación se observa el nombre del punto de acceso inalámbrico: "*Cafeteria*" y su respectiva contraseña de acceso: "*Cafeteria9*", la cual no cumple claramente con los estándares mínimos de seguridad para una contraseña de acceso de un servicio en un entorno riesgoso como el de la institución militar, constituyendo una vulnerabilidad adicional al respecto.

De igual manera se puede detectar otra vulnerabilidad adicional, debido a que el punto de acceso inalámbrico indebido no tiene configurado un horario de servicio de operación, encontrándose disponible para un eventual ataque informático en horas no laborales del Ejército Nacional dentro del Cantón Militar de Popayán.

Figura 16. Configuración del punto de acceso inalámbrico no autorizado

En la imagen siguiente se pueden apreciar que se logró identificar los dispositivos y terminales de datos del personal del Ejército Nacional que están interactuando con este punto de acceso inalámbrico indebido en el preciso momento de ejecución del análisis en la Tercera División militar.

Este escenario constituye una amenaza informática crítica para la autenticidad, confiabilidad e integridad de la información militar transmitida por este punto de acceso inalámbrico, dado que este es un escenario muy riesgoso y constituye una vulnerabilidad importante que puede ser aprovechada por un intruso malicioso para lanzar un ataque informático contra la infraestructura de red de datos del Ejército Nacional desde el Cantón Militar de Popayán.

Figura 17. Dispositivos conectados al punto de acceso inalámbrico indebido

d) Se recopiló información transmitida por las fuentes no autorizadas detectadas en el Cantón Militar de Popayán. A continuación, se presentan los resultados de la prueba de penetración realizada donde se pueden observar parte de los datos capturados mediante la aplicación *Wireshark*. Cabe aclarar que no se muestra la información completa por cuanto trasgrede los límites establecidos en el alcance de las pruebas de penetración definidos en la sección *5.2.1 Alcance de las pruebas de penetración* de este documento.

En la siguiente gráfica se puede observar tráfico web interceptado dirigido al área de servidores de almacenamiento en la ciudad de Bogotá con las aplicaciones militares con información del Ejército Nacional de Colombia *www.ejercito.mil.co*, mediante el análisis de tráfico inalámbrico realizado con la aplicación Wireshark en la infraestructura de red inalámbrica de la Tercera División del Cantón Militar de Popayán.

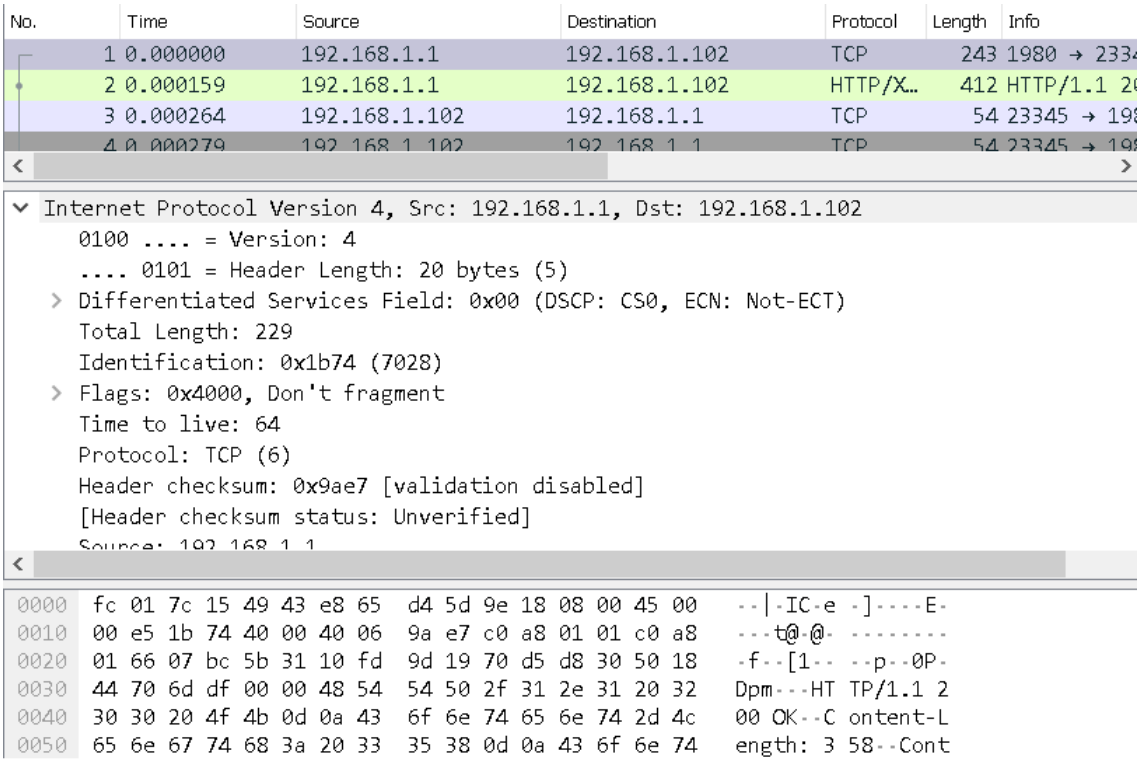


Figura 18. Análisis de tráfico de datos con la aplicación Wireshark

e) Se mapearon todos los datos encontrados referentes a los valores de emisión de la señal de red inalámbrica del punto de acceso de infraestructura de la Tercera División del Cantón Militar de Popayán, para identificar los valores del nivel de radiación de la señal que obtiene finalmente un usuario del Ejército Nacional en esta división militar.

Este mapeo se realizó con la aplicación *Wifi Analyzer* de código abierto de Android, la cual permite examinar las redes inalámbricas circundantes, medir su intensidad de señal, identificar canales saturados, identificar puntos de acceso cercanos, realizar gráficos de canales de señal, de intensidad de señal y estimar la distancia entre puntos de acceso. Los resultados del mapeo realizado con la aplicación *Wifi Analyzer* para mapear el nivel de señal de red inalámbrica del punto de acceso de infraestructura de la Tercera División del Cantón Militar de Popayán se observan en la siguiente gráfica. Los valores en la imagen se encuentran en decibeles dBm.

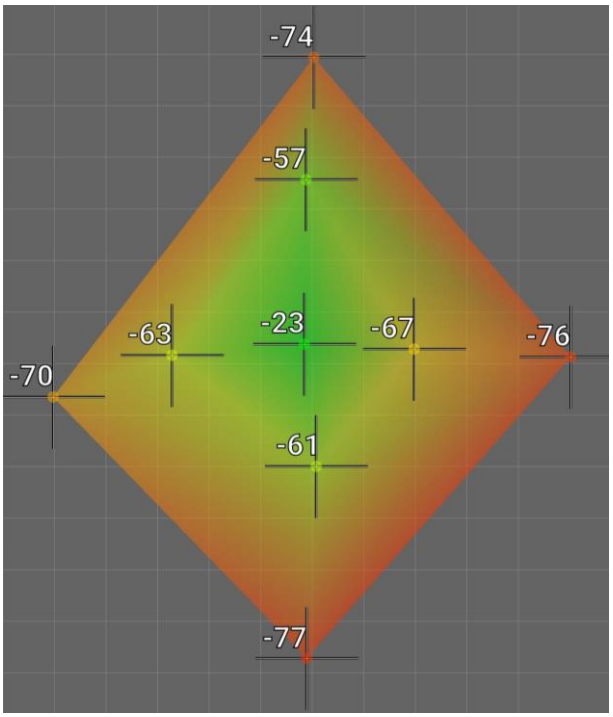


Figura 19. Mapeo de calor punto de acceso inalámbrico Tercera División Cantón Militar

4.2.1.3. Detección de señal activa

La detección de señal activa consiste en examinar qué frecuencias o señales de transmisión electromagnética desencadenan respuestas como la de RFID u otras fuentes inalámbricas interactivas. (Las etiquetas del identificador de radiofrecuencia están compuestas por un microcircuito integrado y una antena. La información se almacena en el circuito integrado y se transmite a través de la antena cuando es sondeada por la señal correcta).

Se realizó el escaneo de señales con la aplicación *NFC Tools* de Android, la cual permite detectar este tipo de señales emitidas por los microcircuitos de RFID, encontrándose que el punto de acceso inalámbrico de la Tercera División del Cantón Militar de Popayán no emite este tipo de señales y por ende no existe una vulnerabilidad latente en este aspecto.

4.2.2. Verificación de acceso

La verificación de acceso consiste en la ejecución de pruebas para la enumeración de puntos de acceso al personal del Ejército dentro del alcance de la red inalámbrica. Dado que el acceso al personal fuera del alcance de la red de datos es un escenario plenamente identificado para el robo de propiedades de información, la prueba se limita exclusivamente al ámbito de interacción de la red inalámbrica al interior de la institución militar para verificar que se protejan los derechos de privacidad de la información ante peticiones o intentos de acceso de cualquier usuario del Cantón Militar sin autorización o ante un eventual ataque de un intruso interno. Los resultados de la verificación de acceso se describen a continuación.

4.2.2.1. Evaluar el acceso administrativo a dispositivos inalámbricos

El punto de acceso inalámbrico de la Tercera División no cuenta con algún tipo de restricción de acceso a la interfaz de configuración administrativa de operación más allá de la interfaz de autenticación administrativa que trae el dispositivo por defecto de su marca fabricante y por ende son asequibles desde cualquier navegador de una terminal que se encuentre en las instalaciones del Cantón Militar, bien sea personal del Ejército o cualquier visitante en las instalaciones militares con acceso a la red inalámbrica de datos que pueda requerir el servicio de Internet, o que se encuentre realizando alguna acción administrativa de configuración y mantenimiento en los dispositivos de la red de datos. Este escenario puede representar una vulnerabilidad principalmente si se dejan las credenciales de autenticación que trae el dispositivos por defecto debido a que las claves de autenticación son ya reconocidas dependiendo de su marca fabricante.

Se encontró como resultado que si se realizó el cambio de las credenciales de autenticación por defecto del punto de acceso inalámbrico de la Tercera División, pero se recomendó deshabilitar el acceso a la interfaz de configuración administrativa desde cualquier terminal, restringiéndola únicamente desde las terminales que opera el personal de sistemas de la división militar para limitar el rango de alcance de un ataque de un intruso informático que quiera intentar acceder administrativamente a los puntos de acceso inalámbrico.

4.2.2.2. Evaluar la configuración de dispositivos inalámbricos

Dentro de la configuración de dispositivos de interconexión de red se debe probar utilizando antenas direccionales y de alta ganancia, que los dispositivos inalámbricos estén trabajando con la configuración de potencia más baja posible para mantener una operación suficiente que mantenga las transmisiones dentro de los límites seguros del Cantón Militar de Popayán.

Se encontró que los dispositivos de interconexión de red inalámbrica como puntos de acceso no se encuentran configurados con la transmisión de potencia más baja posible, se encuentran configurados por defecto con la potencia más alta que posee el dispositivo, encontrándose una vulnerabilidad en este aspecto.

Se sugirió que los puntos de acceso inalámbrico se configuren con la potencia mínima de transmisión para evitar que se puedan realizar interferencias de la señal de la red inalámbrica desde el exterior del perímetro físico del Cantón Militar de Popayán.

4.2.2.3. Evaluar la configuración, la autenticación y el cifrado de redes inalámbricas

Dentro de la configuración de los dispositivos de interconexión inalámbricos se debe verificar que se haya cambiado el identificador de conjunto de servicios (SSID)

predeterminado de los puntos de acceso inalámbricos de la infraestructura de red inalámbrica del Cantón Militar de Popayán.

Realizando la respectiva revisión se comprobó que efectivamente si se realizó el cambio del identificador de conjunto de servicios predeterminado de los puntos de acceso inalámbricos, el nombre del conjunto de servicios detectado en la ejecución de la prueba en la Tercera división de la red inalámbrica del Cantón Militar es BAMHE4.

Es importante revisar que este cambio se haya hecho efectivo dado que dejarle a la red inalámbrica el nombre predeterminado por el fabricante del dispositivo podría permitir a un posible atacante identificar el tipo de punto de acceso inalámbrico y posiblemente explotar cualquier vulnerabilidad conocida de la marca fabricante.

4.2.2.4. Autenticación

A continuación se enumeran y se presentan los resultados de las pruebas de deficiencias en los métodos de autenticación y autorización en la infraestructura de red inalámbrica del Cantón Militar de Popayán.

1. Contraseñas débiles: Después de realizar la inspección en la infraestructura de red inalámbrica de la Tercera División militar, la primera observación que se encuentra es la debilidad de la contraseña de autenticación a la red, la cual es *jkxw9759*. Se puede determinar fácilmente que esa contraseña no cumple con las especificaciones de una contraseña de acceso segura, por el contrario, cumple con todas las características de una contraseña débil y fácil de adivinar por ataques comunes de fuerza bruta como un diccionario de contraseñas, probando cada contraseña en el diccionario para cada cuenta conocida hasta que sea capaz de iniciar sesión. Una contraseña segura debe combinar letras mayúsculas y minúsculas, conjunto con números y símbolos especiales. Igualmente debe tener una mayor cantidad de caracteres y para su fácil recordación se utiliza la nomenclatura de combinar letras con números que reemplazan las vocales de las palabras y así facilitar su mnemotecnia.

2. No se encontró el uso de contraseñas predeterminadas que denotaran una debilidad en la política de seguridad en ese aspecto, ni que fueren otra vulnerabilidad del sistema de información del Ejército.

3. No existen restricciones de autorización de navegación de usuarios o dispositivos en las políticas de seguridad en cuanto al acceso a la red inalámbrica del Cantón Militar.

Para gestionar esta vulnerabilidad se sugirió la implementación del servidor de acceso a la red con el servicio de usuario de marcación de autenticación remota RADIUS, el cual es un sistema con un protocolo de autenticación y autorización de usuarios para acceso a la red de datos contra el directorio activo del dominio del Ejército para personal que labora en la división militar o contra la base de datos SIATH para los usuarios generales del Ejército Nacional, mediante un portal cautivo de seguridad, en donde los usuarios se autentican con sus credenciales de acceso personales, nombre de usuario y contraseña, en el controlador de dominio o en la base de datos, para poder acceder al servicio de red inalámbrica. Si el usuario no pertenece al directorio activo o se encuentra registrado en la base de datos SIATH del Ejército Nacional de Colombia entonces se negará su acceso a la red inalámbrica del Cantón Militar de Popayán. La descripción detallada de este sistema se puede apreciar más adelante en este documento en la sección *Sistema de autenticación* .

4.2.2.5. Control de acceso

Se evaluaron los controles de acceso, la seguridad del perímetro del Cantón Militar y la capacidad de interceptar o interferir una comunicación, determinando el nivel de control de acceso físico a puntos de acceso inalámbricos y dispositivos de control (cerraduras con llave, lectores de tarjetas de identificación y cámaras de vigilancia) en las instalaciones militares.

Se encontró que no existen controles para el acceso físico a los puntos de acceso de la red inalámbrica distribuidos en las diferentes unidades del Cantón Militar, luego cualquier persona, civil o militar, puede acceder físicamente a ellos y ejecutar un ataque interno. De igual manera si un intruso malicioso intenta un ataque informático accediendo físicamente a los puntos de acceso inalámbrico tampoco queda registrado en las cámaras de vigilancia del Batallón debido a que estas cámaras se encuentran apuntando en su mayoría a las entradas de las diferentes unidades militares por ende no tienen alcance de captura en el video de la ubicación física de los puntos de acceso inalámbrico, encontrándose una vulnerabilidad latente en este aspecto.

Se sugirió la implementación de controles para restringir el acceso físico a los puntos de acceso de la red inalámbrica distribuidos en varios lugares geográficos dentro del campus del Cantón Militar, otorgando acceso únicamente al personal del Ejército encargado de la gestión de la red de datos para disminuir el riesgo de ataques internos.

Igualmente se sugirió la ampliación del lote de cámaras de vigilancia en los diferentes contingentes militares para cubrir todos los dispositivos de la infraestructura de red inalámbrica, o en caso de no disponer de los recursos

económicos necesarios, entonces como mínimo la reubicación de las cámaras de vigilancia actuales para que alcancen a enfocar si un intruso manipula físicamente un punto de acceso inalámbrico para ejecutar un ataque informático y quede registrado en video para su posterior identificación.

4.2.3. Verificación de confianza

La verificación de confianza consiste en la ejecución de pruebas de confianza entre el personal del Ejército con alcance a la red inalámbrica, donde la confianza se refiere al acceso a información o propiedad física, sin necesidad de identificación o autenticación. Los resultados de la verificación de confianza son los siguientes.

4.2.3.1. Tergiversación

La tergiversación consiste en probar y documentar el método de autenticación de los usuarios en la red inalámbrica.

En este aspecto se encontró que los usuarios de las diferentes divisiones del Ejército en el Cantón Militar de Popayán se autentican en la infraestructura de red inalámbrica mediante el uso de autenticación encriptada con el *protocolo de acceso protegido Wi-Fi 2 personal* (WPA2-personal) de clave pre-compartida, con una contraseña de 8 caracteres que utiliza el Estándar de cifrado avanzado (AES), así como también compatibilidad con el protocolo de código de autenticación de mensajes de encadenamiento de bloques de cifrado en modo contador.

Esta es una vulnerabilidad latente debido a que la clave pre-compartida puede ser conocida por un posible intruso informático debido a que es la misma clave para la autenticación de todos los usuarios de la red inalámbrica en el Cantón Militar.

Para gestionarla se debe utilizar en la red únicamente el protocolo de acceso protegido Wi-Fi 2 empresarial (WPA2-Enterprise) que transmite la información encriptada entre las terminales y los puntos de acceso inalámbrico mediante autenticación del usuario en el directorio activo o en la base de datos SIATH y por ende cada usuario del Ejército Nacional posee sus credenciales de acceso individuales. La descripción detallada de esta solución se presenta en la sección *Sistema de autenticación inalámbrico* de este documento.

4.2.3.2. Fraude

Para revisar si existe fraude se debe probar la profundidad de los requisitos para acceder a los dispositivos inalámbricos dentro del alcance con el uso de credenciales fraudulentas.

Se encontró que si es posible acceder a dispositivos inalámbricos dentro del alcance de la señal de red inalámbrica de la Tercera División del Cantón Militar de Popayán sin conocer las credenciales de autenticación de la red, siendo una vulnerabilidad

importante a gestionar para garantizar la seguridad de la información militar del Ejército Nacional de Colombia.

En primera instancia no fue posible lograr el acceso a la red inalámbrica con el uso de credenciales fraudulentas, se realizaron varias pruebas de penetración tratando de probar diferentes credenciales de autenticación pero no se tuvo éxito debido a que la red inalámbrica cuenta con un método aceptable de cifrado basado en el *Protocolo de acceso protegido Wifi 2* (WPA2) con el *Estándar de cifrado avanzado* (AES), el cual es un método de cifrado suficientemente seguro para acceso a redes inalámbricas públicas, pero se descubrió una vulnerabilidad importante por cuanto el punto de acceso inalámbrico de la Tercera División tiene activado el estándar de Configuración segura de Wi-Fi (WPS).

El estándar WPS es un mecanismo creado para facilitar la conexión de terminales con un punto de acceso inalámbrico a través de cuatro métodos de autenticación diferentes para el intercambio de credenciales de la red como lo son PIN, PBC, NFC y USB, pero que generan diferentes vulnerabilidades descritas a continuación:

- PIN (Personal Identification Number): Consiste en un Número de identificación personal PIN de ocho dígitos para autenticación en la red inalámbrica. La terminal envía el código numérico al punto de acceso inalámbrico y el punto de acceso le envía las credenciales para acceder a la red, existiendo una vulnerabilidad latente dado que este código PIN viene escrito en la parte inferior del punto de acceso o se puede averiguar en la página web de la marca fabricante, siendo fácil de obtener por un intruso malicioso.
- PBC (Push Button Configuration): La autenticación sucede cuando el usuario presiona un botón en el punto de acceso inalámbrico. Existe el riesgo que cualquier terminal maliciosa cercana pueda ganar el acceso a la red en el lapso de tiempo que ocurre entre la presión del botón en el punto de acceso y la entrega de las credenciales a la terminal.
- NFC (Near Field Communications): Consiste en el intercambio de credenciales a través de comunicación con tecnología NFC, basada en RFID, la cual permite comunicación sin hilos entre dispositivos cercanos. Para ello la terminal se debe situar junto al punto de acceso inalámbrico para autenticarse, lo cual genera una vulnerabilidad dado que cualquier usuario que tenga acceso físico al punto de acceso inalámbrico puede obtener credenciales de autenticación válidas.
- USB (Universal Serial Bus): Con este método, las credenciales de acceso se transfieren mediante un dispositivo de memoria flash desde el punto de acceso inalámbrico a la terminal con puerto USB. Existe la vulnerabilidad que el dispositivo USB caiga en manos de un intruso malicioso y pueda acceder a la red de datos para lanzar un ataque informático con credenciales de autenticación reales.

En términos generales existe una vulnerabilidad importante debido a que se encuentra presente un problema de seguridad que afecta a los dispositivos de acceso a red inalámbrica que tienen habilitada la función de *Configuración de seguridad rápida* (QSS) mediante el estándar WPS. Esta vulnerabilidad permite a un atacante informático obtener el código PIN o el acceso WPS y la clave pre-compartida del protocolo WPA2 usando ataques de fuerza bruta en un lapso corto de tiempo.

Se recomienda deshabilitar la función WPS en todos los puntos de acceso inalámbrico de la infraestructura de red de datos del Cantón Militar de Popayán como solución a esta vulnerabilidad debido a que el principal inconveniente que se genera con esta funcionalidad activa es que posibilita que un intruso malicioso no necesite un lapso de tiempo grande para averiguar el código PIN de ocho dígitos en un ataque informático, requiere un tiempo mucho menor que el lapso de tiempo necesario para descifrar la contraseña configurada con el protocolo WPA2. Para mantener la red inalámbrica segura se debe entonces inhabilitar la funcionalidad de conectarse mediante esta utilidad a los puntos de acceso inalámbrico, obligando a los usuarios del Ejército a introducir las credenciales de autenticación cada vez que deseen conectar una terminal a la red inalámbrica en las unidades del Cantón Militar de Popayán.

4.2.3.3. Abuso de recursos

Para estipular si existe abuso de recursos se debe examinar la profundidad de los requisitos para enviar información fuera del alcance de la red inalámbrica a una fuente conocida y de confianza, o dentro del alcance mismo a otro personal sin ningún tipo establecido de credenciales requeridas.

Se encontró que si es posible enviar información fuera del alcance de la señal de red inalámbrica de la institución generando un repetidor inalámbrico con antenas direccionales de alta ganancia desde el exterior del Batallón, dándole acceso a una fuente conocida y de confianza con las credenciales necesarias para autenticarse en la red de datos del Cantón Militar de Popayán sin necesidad de requisitos o permisos adicionales por parte del personal del Ejército, siendo una vulnerabilidad que puede desencadenar en un posible ataque informático desde el exterior del perímetro físico de la institución militar.

Para determinar la vulnerabilidad se ejecutó la prueba de penetración externa *Punto de acceso no autorizado* generando la repetición de la señal de red inalámbrica de la Tercera División, conectando una antena direccional de alta ganancia al enrutador inalámbrico Nexxt Solutions Nébula en modo repetidor para realizar una extensión de la red inalámbrica hacia el exterior del perímetro físico del Cantón Militar y poder

atacarla sin necesidad de ingresar presencialmente a la sede del Batallón (Ver *Figura 11. Enrutador inalámbrico Nexxt Solutions Nébula*).

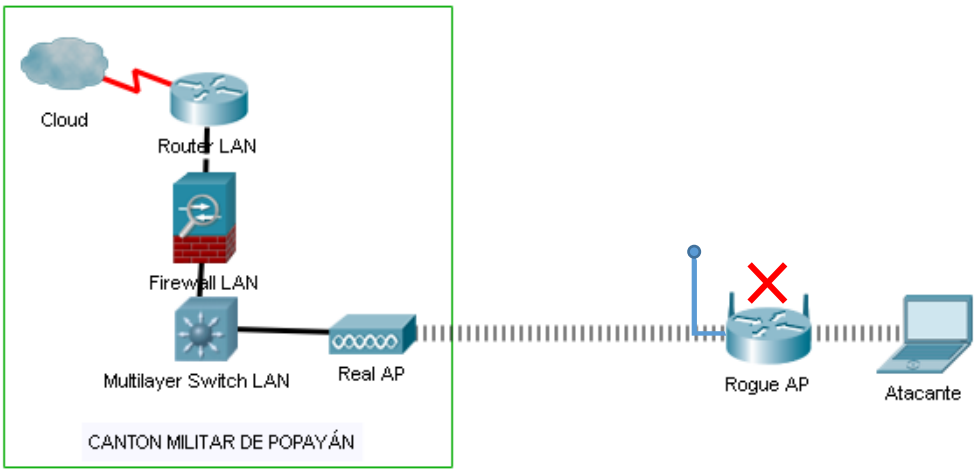


Figura 20. Prueba de penetración externa punto de acceso no autorizado

Con esta prueba de penetración externa se pudo comprobar que si existe una vulnerabilidad importante dado que si es posible autenticarse y navegar en la red inalámbrica de datos del Batallón si se conocen las credenciales de acceso desde el exterior del perímetro físico del Cantón Militar de Popayán. Esta vulnerabilidad se gestiona con la implementación del sistema de detección de intrusos inalámbrico, el cual posee la capacidad de proteger y no exponer la información confidencial institucional a través de puntos de acceso no autorizados y mal configurados, evitando que los usuarios del Ejército Nacional se conecten a puntos de acceso inalámbrico intrusos cercanos al perímetro físico de la institución pero que no están bajo el control del personal de gestión del sistema, protegiendo la información confidencial militar. La descripción detallada de este sistema se puede apreciar más adelante en la sección *Sistema de detección de intrusos inalámbrico* de este documento.

En la siguiente imagen se puede comprobar que se logró realizar la conexión del punto de acceso inalámbrico no autorizado en modo repetidor, con el punto de acceso inalámbrico de la Tercera Brigada del Cantón Militar de Popayán, y cualquier usuario puede conectarse a la red inalámbrica para navegar a través del punto de acceso no autorizado, incluso sin contraseña de autenticación.

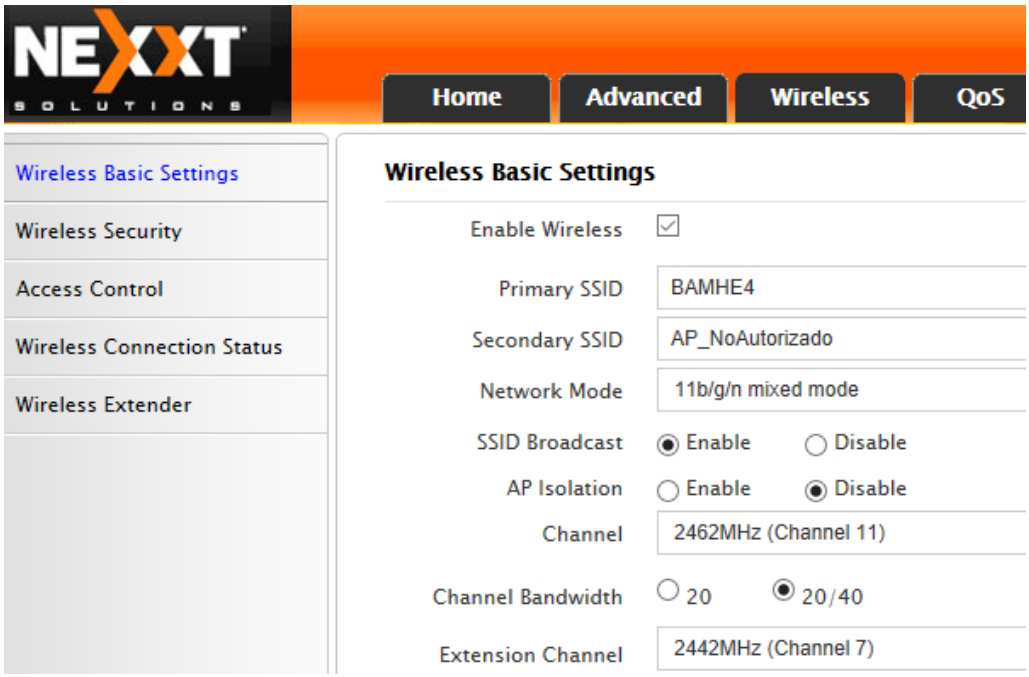


Figura 21. Prueba de penetración - Punto de acceso no autorizado

4.2.3.4. Confianza ciega

La prueba de confianza ciega consiste en probar una conexión que se realice a un receptor falso o comprometido y analizar sus resultados.

Para la ejecución de la prueba de confianza ciega en la red inalámbrica del Cantón Militar de Popayán se realizó la prueba de penetración *punto de acceso no autorizado*, que consistió en generar una conexión con un punto de acceso como extensor de señal marca Nexxt Solutions en modo repetidor que permitió generar un enlace con la repetición de la señal del Batallón, lo cual sería el escenario buscado por un intruso malicioso para poder navegar a través de la red inalámbrica sin necesidad de autenticación y poder atacar la información confidencial militar o lanzar un ataque de negación de servicios (Ver *Figura 11. Enrutador inalámbrico Nexxt Solutions Nébula*).

Se sugirió, al igual que en el punto anterior, la implementación del sistema de detección de intrusos para gestionar esta vulnerabilidad, dado que posee la capacidad de evitar falsos positivos evitando consumo de tiempo en conexiones fallidas a puntos de acceso inalámbrico que no pertenezcan al Cantón Militar de Popayán. Este sistema detecta un punto de acceso inalámbrico no autorizado, informando incluso si el punto de acceso descubierto está en su propia red o en una red cercana de un posible intruso malicioso. De esta manera se incrementa el nivel de protección de la información confidencial de la institución mediante el uso de técnicas de clasificación automática, los dispositivos internos se clasifican como seguros, los dispositivos externos se clasifican e ignoran con precisión, mientras

que los dispositivos que representan una posible amenaza para la red de datos se bloquean de forma inmediata (Ver sección *Sistema de detección de intrusos inalámbrico*).

4.2.4. Verificación de controles

Consiste en el desarrollo de pruebas para enumerar los tipos de controles de pérdida de datos utilizados en la infraestructura de red del Cantón Militar para proteger la información confidencial del Ejército.

4.2.4.1. No repudio

Se debe revisar el uso o las deficiencias de los demonios y sistemas para identificar y registrar correctamente acceso o interacciones a la propiedad para obtener evidencia específica para cuestionar el repudio, y documentar la profundidad de la interacción registrada y del proceso de identificación.

Se encontró que no existen sistemas en el Batallón que permitan identificar y registrar accesos o interacciones de posibles atacantes informáticos con la red inalámbrica. Esta vulnerabilidad también se puede gestionar con la implementación del sistema de detección de intrusos inalámbrico, el cual posee los demonios y detectores requeridos para identificar y registrar correctamente cualquier tipo de acceso o interacciones de posibles intrusos maliciosos ante un ataque informático a la infraestructura de red inalámbrica del Cantón Militar de Popayán, ejecutando los análisis correspondientes que determinan automáticamente el no repudio de la información, dada su capacidad de identificar la identidad del emisor de los datos, certificando que provengan de una fuente confiable dentro de la red inalámbrica de la unidad militar. De igual manera, el sistema entrega los respectivos informes que permiten documentar la profundidad de la interacción registrada y del proceso de identificación realizado. (Ver sección *Sistema de detección de intrusos inalámbrico*).

4.2.4.2. Confidencialidad

Para propender por la confidencialidad de la información se debe verificar el uso de equipos para amortiguar las señales de transmisión electromagnética en el exterior de la empresa y los controles establecidos para asegurar o cifrar las transmisiones inalámbricas.

Se encontró que no existe en la infraestructura de red del Cantón Militar, equipos para amortiguar las señales de transmisión electromagnética hacía el exterior de la institución militar, siendo una vulnerabilidad importante por gestionar, dado que un intruso malicioso puede intentar un ataque informático para obtener acceso a la red desde el exterior del perímetro físico, como se comprobó que es posible con la prueba de penetración ejecutada en la sección *4.2.3.3 Abuso de recursos* de este documento.

Por otra parte, aunque no existen controles adicionales establecidos para asegurar o cifrar las transmisiones de datos militares confidenciales en la red inalámbrica, si se encuentra configurado el *Estándar de cifrado avanzado* (AES) en los puntos de acceso inalámbrico, el cual es un estándar de cifrado seguro y confiable que traen los puntos de acceso suficiente para garantizar la confidencialidad en el acceso de usuarios del Ejército Nacional.

Adicionalmente, los puntos de acceso inalámbricos del Cantón Militar de Popayán poseen la capacidad de generar redes privadas virtuales (VPN) lo cual garantiza aún más la confidencialidad del intercambio de datos, en caso de necesitarse acceder o transmitir información de alta importancia militar.

4.2.4.3. Privacidad

Para propender por la privacidad de la información se debe determinar el nivel de controles de acceso físico a los puntos de acceso y dispositivos que los controlan como cerraduras con llave, lectores de tarjetas de identificación y cámaras de vigilancia.

En la revisión se encontró que no existen controles de acceso físico a los puntos de acceso inalámbrico en las diferentes divisiones del Cantón Militar, no cuentan con cerraduras o contenedores con llave que impidan su manipulación por parte de un intruso interno. Tampoco quedan registrados en las cámaras de vigilancia de las unidades militares por cuanto estas cámaras se encuentran enfocando hacia las entradas de las diferentes unidades militares y la mayoría no tiene alcance de captura en el video de la ubicación física de los puntos de acceso inalámbrico, encontrándose una vulnerabilidad en este aspecto

En cuanto al nivel de los controles para el acceso a los dispositivos que componen el núcleo de la infraestructura de red inalámbrica en el Cantón Militar existe restricción de acceso físico para las personas civiles, pero no para el personal del Ejército, existiendo una vulnerabilidad debido a un posible ataque informático por parte de un intruso interno del personal del Ejército.

Se recomendó la ampliación del lote de cámaras de vigilancia en los diferentes contingentes militares para cubrir todos los dispositivos de la infraestructura de red inalámbrica, o la reubicación de las cámaras de vigilancia actuales para que alcancen a enfocar si un intruso manipula físicamente un punto de acceso inalámbrico. Además, se recomendó restringir el acceso físico a los dispositivos del núcleo de la red únicamente al personal del Ejército encargado de la gestión de la red de datos para disminuir el riesgo de ataques internos.

4.2.4.4. Integridad

Para propender por la integridad de la información se debe determinar que solo el personal del Ejército autorizado pueda acceder y modificar los datos de configuración de los dispositivos de la infraestructura de red inalámbrica, verificando que las contraseñas de acceso a la interfaz de administración de estos dispositivos utilicen el cifrado adecuado para garantizar la firma y la confidencialidad de las comunicaciones en una institución tan importante como la militar.

Se encontró que solo el personal del Ejército autorizado para realizar gestión en la red de datos posee las contraseñas de ingreso a la interfaz de configuración de los dispositivos de interconexión de la red inalámbrica, pero el nivel de seguridad de las contraseñas es muy débil, como por ejemplo en el caso particular del punto de acceso inalámbrico de la Tercera División cuya contraseña administrativa es "*Batallon2017*". Se realizó la sugerencia que se cambien estas contraseñas débiles por contraseñas con un mayor nivel de seguridad para evitar la facilidad de incluso un ataque de diccionario simple para el ingreso a la interfaz de administración de los dispositivos de red.

Para solventar esta vulnerabilidad se sugirió la implementación de un sistema de gestión de contraseñas como mecanismo de control de seguridad de las claves de acceso empleadas para autenticación en las interfaces de configuración de los dispositivos de interconexión de la infraestructura de red de datos del Cantón Militar de Popayán, el cual genera contraseñas aleatorias para ser configuradas en cada dispositivo y las almacenan de manera encriptada. El administrador del sistema simplemente se limita a saber la contraseña maestra para obtener acceso a las demás contraseñas almacenadas de cada dispositivo de red sin tener que memorizarlas.

Además de generar contraseñas aleatorias extensas combinando letras, números y símbolos especiales, las contraseñas generadas se almacenan cifradas usando la contraseña maestra del sistema, de tal forma que únicamente el administrador del sistema puede tener acceso a ellas, incrementando el nivel de seguridad de la información en la red de datos.

Otro beneficio que se obtiene con su implementación es que estos gestores de contraseñas se integran en el navegador web del terminal de administración para completar los formularios de autenticación de los portales web de configuración de los dispositivos de interconexión de red, de tal forma que el sistema recuerde y complete automáticamente el usuario y contraseña de ingreso de cada dispositivo sin necesidad de digitarla, convirtiéndose en una medida de defensa contra ataques de suplantación de identidad, ya que a diferencia de un ser humano, el sistema no se equivoca al distinguir entre dos páginas parecidas pero con diferente dominio, con lo que garantiza que la contraseña se introducirá únicamente en una página

legítima de un dispositivo de interconexión de la infraestructura de red de datos del Ejército. De esta manera, se posibilita configurar contraseñas con un alto nivel de seguridad y facilidad en su gestión.

4.3. Fase de Explotación

4.3.1. Verificación del proceso

La verificación del proceso consiste en la ejecución de pruebas para examinar el mantenimiento de la conciencia sobre seguridad funcional del personal en los procesos establecidos y la debida diligencia como se definió en la revisión de la postura.

4.3.1.1. Línea base

Se debe examinar y documentar la configuración de la línea base para asegurar que la postura de seguridad de una terminal de datos esté en línea con la política de seguridad de la institución militar.

Se realizó el análisis de la configuración de seguridad de la línea base de la terminal utilizada para la prueba de penetración debido a las restricciones definidas en el alcance de este proyecto sobre el no uso de las terminales de la infraestructura de red de datos del Ejército Nacional de Colombia explícito en el *ANEXO B. Definición del alcance de pruebas de penetración en la red inalámbrica del Cantón Militar de Popayán*. Este análisis se ejecutó mediante la aplicación Microsoft Baseline Security Analyzer, la cual permite evaluar las vulnerabilidades en seguridad de una terminal de datos con sistema operativo Microsoft Windows, buscando evitar los riesgos de un posible ataque informático hacia el sistema de información militar.

Como resultado de la ejecución de este análisis, se encontró que la postura de seguridad de la terminal evaluada utilizada para la prueba de penetración no cumple con las políticas de seguridad del Ejército Nacional para el uso de su red inalámbrica de datos debido a que se encontraron las siguientes vulnerabilidades administrativas.

Tabla 25. Postura de seguridad de línea base

Report Details for EJC_NACIONAL – BR29B1004 (2019-11-14 16:01:02)

Security assessment:
Severe Risk (One or more critical checks failed.)

Computer name:	EJC_NACIONAL\BR29B1004
IP address:	172.23.66.115
Security report name:	EJC_NACIONAL – BR29B1004 (14-11-2019 16-01)
WSUS server:	http://SVREJCWSUS:8530
Scan date:	14/11/2019 16:01
Scanned with MBSA version:	2.1.2112.0
Catalog synchronization date:	2019-11-12T04:11:01Z
Security update catalog:	Microsoft Update (offline), Windows Server Update Services

Security Update Scan Results

Score	Issue	Result
	Windows Security Updates	2 security updates are missing. 31 security updates are missing and not approved.
	Microsoft Lync Server and Microsoft Lync Security Updates	No security updates are missing.
	Office Communications Server And Office Communicator Security Updates	No security updates are missing.
	SQL Server Security Updates	No security updates are missing.
	Developer Tools, Runtimes, and Redistributables Security Updates	1 security updates are missing and not approved.
	Office Security Updates	4 security updates are missing and not approved.
	Silverlight Security Updates	2 security updates are missing and not approved.

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	Guest Account	The Guest account is not disabled on this computer.
	Local Account Password Test	Some user accounts (1 of 2) have blank or simple passwords, or could not be analyzed.
	Administrators	More than 2 Administrators were found on this computer.
	Password Expiration	Some user accounts (1 of 2) have non-expiring passwords.
	Automatic Updates	Automatic Updates are managed through Group Policy on this computer.
	Incomplete Updates	No incomplete software update installations were found.
	Windows Firewall	Windows Firewall is managed through Group Policy on this computer and the policy has exceptions configured. Windows Firewall is enabled and has exceptions configured. Windows Firewall is enabled on all network connections.
	File System	All hard drives (2) are using the NTFS file system.
	Autologon	Autologon is not configured on this computer.
	Restrict Anonymous	Computer is properly restricting anonymous access.

Additional System Information

Score	Issue	Result
	Auditing	Neither Logon Success nor Logon Failure auditing are enabled. Enable auditing and turn on auditing for specific events such as logon and logoff. Be sure to monitor your event log to watch for unauthorized access.

	Services	Some potentially unnecessary services are installed.	
		Service	**State**
		Servicio de publicación World Wide Web	Running
	Shares	6 share(s) are present on your computer.	
	Windows Version	Computer is running Microsoft Windows Uknown.	

Internet Information Services (IIS) Scan Results

Score	Issue	Result
	IIS Status	IIS is not running on this computer.

SQL Server Scan Results

Score	Issue	Result
	SQL Server/MSDE Status	SQL Server and/or MSDE is not installed on this computer.

Desktop Application Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	IE Zones	Internet Explorer zones have secure settings for all users.
	Macro Security	No supported Microsoft Office products are installed.

4.3.1.2. Blindaje adecuado

Se debe determinar que los dispositivos de la infraestructura de la red inalámbrica posean el respectivo blindaje adecuado para protegerlos de ataques informáticos por captura de señales electromagnéticas. Por ejemplo, revisar que los dispositivos de interconexión de red se encuentren ubicados en los armarios especialmente diseñados para protegerlos y bloquear interferencias electromagnéticas y se utilice paneles o pintura metálica para bloquear las señales inalámbricas parásitas.

Se encontró que los dispositivos de interconexión de red se encuentran debidamente ubicados en armarios especiales para telecomunicaciones con su respectivo blindaje electromagnético, pero no se utilizan paneles o pintura metálica en los cuartos donde se encuentran ubicados para bloquear las emisiones electromagnéticas, evitando que señales puedan ser capturadas por dispositivos de intrusos informáticos, para así reducir riesgos por afectación de la emisión de este tipo de señales electromagnéticas.

Se sugirió implementar paneles de blindaje o utilizar pintura metálica en los cuartos de telecomunicaciones para minimizar el impacto de un posible ataque informático a la red inalámbrica por la exposición a este tipo de radiación de señales.

4.3.1.3. Diligencia debida

Se debe mapear y verificar cualquier brecha entre la práctica y los requisitos según lo determinado en la revisión de la postura de seguridad a través de todos los canales inalámbricos.

El mapeo y verificación de la postura de línea base se realizó en contraste con las *Políticas de Uso Aceptable – PUA* del Ejército Nacional de Colombia las cuales contienen las normas, políticas y estándares establecidos para garantizar la seguridad informática y el uso responsable de los dispositivos de su infraestructura de red de datos. (Solicitud Servicios Informátivos Usuarios, 2018). Los resultados del mapeo realizado se relacionan en la siguiente tabla.

Tabla 26. Políticas De Uso Aceptable - PUA

Políticas de seguridad PUA		**Línea base de seguridad MBSA**	**Aplica**	**Cumple**	
				SI	**NO**
1	Intento o violación de controles de seguridad para protección de activos informáticos de las FF.MM.		NO	X	
2	Realizar actividades que comprometan la seguridad de los activos informáticos de las FF.MM.	- Actualizaciones automáticas: Las actualizaciones automáticas se administran a través de políticas de grupo. - Actualizaciones incompletas: No hay actualizaciones de software incompletas.	SI	X	
3	Uso sin autorización de activos informáticos de las FF.MM.		NO	X	
4	Uso no autorizado o impropio de la conexión al sistema.	- Cortafuegos de Windows: Se administra a través de la política de grupo, está habilitado en todas las conexiones de red y tiene excepciones configuradas.	SI	X	
5	Intentar evadir o violar la seguridad o autenticación de usuario de cualquier host, red o cuenta.	- Restricción de anónimos: La restricción de acceso anónimo es apropiada.	SI	X	
6	Uso indebido de contraseñas, firmas digitales o dispositivos de autenticación.	- Prueba contraseña usuario local: Algunas cuentas de usuario tienen contraseñas débiles o no tienen. - Expiración de contraseña: Cuentas de usuario con contraseñas que no expiran.	SI		X
7	Prohibido a cualquier usuario acceder a servicios informáticos con cuentas o medios de autenticación de otros usuarios. Aún con la autorización del usuario propietario de la misma.	- Administradores: Mas de 2 administradores fueron encontrados. - Cuenta de invitados: La cuenta de invitados no está deshabilitada. - Autologon: Autologon no está configurado.	SI		X
8	Almacenamiento, instalación, configuración o uso de software ilegal o no autorizado o de datos no autorizados en los activos informáticos de las FF.MM.	- Versión de Windows: Se está corriendo una versión de Windows desconocida. - Herramientas de desarrollo, tiempos de ejecución y actualizaciones de seguridad redistribuibles: Faltan actualizaciones de seguridad y no están aprobadas.	SI		X
9	Prohibido uso, distribución y ejecución de software o código malicioso que cause daño, hostigamiento, molestias a personas, daño o alteración de información o traumatismos en continuidad de servicios informáticos o vulnere seguridad de sistemas.	- Actualizaciones de seguridad de Microsoft Lync Server y Microsoft Lync, Actualizaciones de seguridad de Office Communications Server y Office Communicator, Actualizaciones de seguridad de SQL Server: No faltan actualizaciones de seguridad. - Estado MSDE: SQL Server no está instalado.	SI	X	

		- Seguridad Macro: No hay productos soportados de Microsoft Office instalados.			
10	El hurto, robo, sustracción o uso no autorizado de: datos, información, materiales, equipos y activos informáticos de las FF.MM.		NO	X	
12	Prohibido retirar de las instalaciones de las FF.MM. cualquier activo informático sin previa autorización.		NO	X	
13	Acceso, modificación o alteración no autorizada de componentes, datos o información de activos informáticos de las FF.MM.	- Autologon: Autologon no está configurado. - Estado IIS: IIS no se está ejecutando.	SI	X	
14	Uso de medios electrónicos, de almacenamiento, software, hardware, datos o información en medios digitales de fuentes no certificadas o de terceros sin revisión o autorización del Administrador del Sistema y/o Oficial de Seguridad Informática.	- Actualizaciones de seguridad de Windows, Actualizaciones de seguridad de Office, Actualizaciones de seguridad de Silverlight: Faltan actualizaciones de seguridad y no están aprobadas.	SI		X
15	Servicio de Internet con fines autorizados y legales. Se prohíbe transmisión, difusión, distribución o almacenamiento de material –digital o impreso- en violación de ley o regulación aplicable.	- Zonas IE: Las zonas de Internet Explorer tienen configuración segura para todos los usuarios.	SI	X	
16	Prohibido en correo electrónico: Spam, Troll, Mailbombing, reenvió o transmisión de mensajes no oficiales ó suscripción a usuarios en listas de correo sin permiso.		NO	X	
17	Realizar por Internet o activos informáticos, cualquier actividad que desprestigie las FF.MM. de Colombia.		NO	X	
18	Los mensajes en correos electrónicos no pueden ser contrarios al orden público, moral, buenas costumbres nacionales e internacionales, usos y costumbres aplicables en Internet y respeto de derechos de terceras personas.		NO	X	
19	Prohibido almacenamiento y reproducción de aplicaciones, programas, archivos de audio no relacionados con actividades de funciones de la dependencia o el usuario.	- Compartimientos: Se están realizando varios compartimientos	SI		X
20	El usuario acepta responsabilidad por actividades realizadas con activos informáticos bajo su responsabilidad y custodia o desde cuentas para acceso a servicios informáticos de las FF.MM.	- Auditoría: Ni la auditoría de Logon exitoso o fallido están habilitadas	SI		X
21	Prohibido agregar, remover o modificar información identificadora o de contenido en la red, que engañe al sistema, al destinatario o suplante otro usuario.	- Servicios: Algunos servicios potenciales innecesarios están instalados	SI		X
22	Las cuentas de red de las FF.MM. operan con recursos compartidos. Prohibido su uso abusivo que afecte su rendimiento.	- Sistema de archivos: Todos los discos duros están usando sistema de archivos NTFS.	SI	X	

4.3.1.4. Indemnización

Se deben identificar los objetivos y servicios que están protegidos contra el abuso o elusión de la póliza del empleado, están asegurados por robo o daños, o usan responsabilidad y descargos de responsabilidad. Verificar la legalidad y el lenguaje apropiado en los descargos de responsabilidad.

Se encontró que los dispositivos y servicios de la infraestructura de red inalámbrica de las diferentes divisiones del Cantón Militar de Popayán no están protegidos por ningún tipo de póliza contra el abuso, robo o daños de ningún tipo o causalidad, siendo esta una vulnerabilidad importante en cuanto al restablecimiento del servicio de la red nuevamente en caso de un hecho siniestro que deteriore o desaparezca los activos de red del Ejército.

Se sugirió la adquisición de una póliza de seguros contra ataques informáticos, daños físicos y robo, que cubra todos los dispositivos de interconexión de la infraestructura de red de datos del Cantón Militar de Popayán pertenecientes al Ejército Nacional de Colombia.

4.3.2. Verificación de la configuración

La verificación de la configuración consiste en ejecutar pruebas para examinar la capacidad de eludir o alterar la seguridad funcional de los activos que componen la infraestructura de red inalámbrica del Cantón Militar de Popayán. Los resultados de las pruebas ejecutadas se presentan a continuación.

4.3.2.1. Errores comunes de configuración

Para determinar si existen errores comunes de configuración se debe realizar un ataque de fuerza bruta contra los puntos de acceso inalámbrico para discernir la fortaleza de las contraseñas configuradas. Se debe verificar que las contraseñas contienen letras mayúsculas y minúsculas, números y caracteres especiales, y que el punto de acceso distinga entre mayúsculas y minúsculas, dado que, en caso contrario, se facilita para los atacantes realizar un ataque de fuerza bruta debido al rango menor de probables contraseñas.

Se realizó un ataque de fuerza bruta con la herramienta Fern Wifi Cracker de la distribución Kali Linux, en donde se logró obtener la contraseña de autenticación del punto de acceso inalámbrico de la Tercera División del Cantón Militar de Popayán. Los resultados del ataque realizado se pueden observar más adelante en la sección *5.3 Resultados de las pruebas de penetración*.

Para gestionar esta vulnerabilidad, se sugirió la implementación de un sistema de autorización de usuarios basado en un servidor de acceso a la red con el protocolo RADIUS para autenticación del acceso a la red inalámbrica contra el directorio activo del dominio o contra la base de datos SIATH del Ejército Nacional mediante un portal cautivo de seguridad, en donde los usuarios se autentican con sus credenciales de acceso personales, evitando tener que generar contraseñas complejas para los puntos de acceso inalámbrico. Estas contraseñas de acceso a los puntos inalámbricos pueden ser de un nivel de seguridad bajo y altamente divulgadas entre el personal de la Tercera División, dado que si el usuario no pertenece al directorio activo o se encuentra registrado en la base de datos SIATH del Ejército Nacional de Colombia entonces se negará su acceso a la red inalámbrica en el portal cautivo, así el usuario se haya autenticado con dicha contraseña en un punto de acceso de la red inalámbrica del Cantón Militar de Popayán. La descripción en detalle de este sistema se puede apreciar más adelante en la sección *Sistema de autenticación* .

En caso de no ser posible la implementación del sistema de autenticación de usuarios, se sugiere entonces cambiar la contraseña de acceso actual por una contraseña que combine letras mayúsculas y minúsculas, conjunto con números y caracteres especiales. Igualmente se sugirió el uso de una contraseña con mayor nivel de cifrado, es decir con mayor cantidad de caracteres especiales y para su fácil recordación se sugirió el uso de la nomenclatura de combinar letras con números que reemplazan las vocales de las palabras y así facilitar su mnemotecnia.

4.3.2.2. Controles de configuración

Se debe verificar los controles, incluida la configuración de la línea base de las terminales de datos, para validar las configuraciones de acuerdo con la política de seguridad del Ejército Nacional de la república de Colombia.

En la comprobación realizada en la Tercera División del Cantón Militar de Popayán se encontró que no existen controles ni procedimientos de verificación para identificar si la configuración de las terminales cumple con las políticas de seguridad del Ejército Nacional de Colombia para el uso de su servicio de red inalámbrica y la transmisión de información militar hacia su infraestructura de red de datos, existiendo una vulnerabilidad importante debido a que un posible sistema operativo Windows con falencias puede ser utilizado por un intruso malicioso para desplegar un ataque informático.

Para realizar gestión a esta vulnerabilidad se sugirió utilizar la aplicación Microsoft Baseline Security Analyzer, la cual permite identificar si una terminal con sistema operativo Microsoft Windows cumple con las condiciones mínimas de seguridad para poder autorizar su acceso a la red inalámbrica del Ejército Nacional sin comprometer la autenticidad, confiabilidad e integridad del sistema de información

militar como el análisis realizado en la sección *4.3.1 Verificación del proceso* de este documento.

4.3.2.3. Evaluar y probar el cableado y las emisiones

Se debe comprobar que todas las conexiones de cableado estructurado de la infraestructura de red inalámbrica que ingresen y salgan de las habitaciones blindadas estén hechas de fibra óptica, siempre que sea posible.

Se encontró que efectivamente todas las conexiones de cableado estructurado que llegan y salen de las habitaciones blindadas se realizaron con empalmes de fibra óptica y por ende no existe una vulnerabilidad electromagnética en este aspecto dado que la fibra óptica no es sensible a este tipo de interferencias al transportar señales de luz.

4.3.3. Validación de la propiedad

La validación de la propiedad consiste en pruebas para examinar la legalidad y propiedad física de la información compartida y disponible dentro del área de cobertura de la red de datos, o si puede existir información compartida de manera fraudulenta por el mismo personal del Ejército, lo cual puede ser ilegal o no ético por parte de la institución militar.

4.3.3.1. Compartir

Se debe verificar el grado en que las licencias individuales, privadas, falsificadas, reproducidas, no libres o de propiedad no abierta, se comparten entre el personal del Ejército, ya sea a través de procesos y programas compartidos, bibliotecas, y cachés personales o involuntariamente a través de la mala gestión de las licencias y recursos, o negligencia del Ejército.

Se encontró que no existe un adecuado sistema de monitoreo y control que permita evitar que se compartan este tipo de licencias, siendo posible su obtención por cualquier persona con acceso a la intranet mediante conexión a la red inalámbrica de la unidad militar, siendo esta una vulnerabilidad en materia legal y jurídica para la institución.

Para gestionar esta vulnerabilidad se deberá prohibir mediante políticas de seguridad en los dispositivos de control y monitoreo de la red, que se compartan archivos e información a través de la intranet del Cantón. Además, se sugiere la implementación de un sistema de almacenamiento de información basado en Microsoft Sharepoint Server, el cual es una plataforma basada en gestión de procesos y gestión de documentos licenciada.

Este sistema de gestión de información permite espacios de trabajo compartidos para almacenamiento, organización y compartimiento de información y documentos

institucionales de manera protegida, restringida y segura debido a su compatibilidad con autenticación mediante el directorio activo del dominio de la red de datos. También permite revisión de todos los archivos, nombres de archivo y longitudes dada su compatibilidad con una amplia gama de tipos y convenciones de nomenclatura, incluida la compatibilidad con los símbolos # y % como caracteres admitidos en los nombres de archivos y carpetas en bibliotecas de documentos, además de aumentar las restricciones de longitud de ruta del localizador de recursos uniforme. Por otra parte, incrementa el rendimiento de carga y descarga de archivos al tiempo que maximiza el uso del ancho de banda de la red. (Servidor archivos, 2018)

Del mismo modo permite la implementación de políticas de seguridad para el almacenamiento y transferencia de archivos en el servicio de gestión de información de la institución, para evitar que licencias individuales, privadas, falsificadas, reproducidas, no libres o de propiedad no abierta, se compartan en la institución militar. También permite generar copias de seguridad de la información contenida de fácil restauración para su disponibilidad inmediata en caso de perdida por un ataque informático

Este sistema permite cumplir las normas regulatorias y proteger los datos confidenciales y críticos de la institución ante posibles ataques informáticos lanzados desde la intranet de la unidad militar, dado que controla cuales usuarios tienen acceso a la información y advierte sobre cuales usuarios accedieron a información confidencial específica en particular. Al ofrecer configuración y administración para políticas reguladoras, proporciona cumplimiento y seguridad de datos mejorados, controlando el acceso a los datos privados de los usuarios, mediante gestión de autorizaciones y auditorías, con un modelo de seguridad que garantiza el cumplimiento de las políticas institucionales.

Adicionalmente protege contra malware[10], fuga de datos y otros riesgos bajo una metodología de garantía de seguridad que incluye modelado de amenazas, pruebas de penetración y prácticas de desarrollo centradas en seguridad, evitando acceso a contenido no autorizado y prevención de pérdida de datos, manejando múltiples tipos de información clasificada que permite buscar contenido confidencial en su centro de exhibición de documentos electrónicos, manteniendo el contenido organizado y permitiendo encontrar información en tiempo real. También permite establecer una política de seguridad propia con reglas personalizadas que solventen las necesidades de la institución en cuanto a prevención de tratamiento de datos. (Servidor archivos, 2018)

[10] Malware: Malicious software. Programa malicioso que trata de afectar un sistema de información o red de datos en un ataque informático.

Dentro de las posibilidades de licenciamiento para acceso de usuarios a la información institucional almacenada que ofrece Microsoft Sharepoint Server se encuentran los siguientes escenarios para acceso a la información. (Servidor archivos licenciamiento, 2017)

- *Intranet*: Intercambio de archivos entre usuarios internos de una institución dentro de una red corporativa segura. Solo a usuarios internos se les concede acceso a contenido, información o aplicaciones dentro del dispositivo de seguridad principal a través de la red de área local de la institución. Ningún otro usuario tiene acceso a la información institucional confidencial restringida.
- *Extranet*: Intercambio de archivos y colaboración entre usuarios y socios o afiliados externos dentro de una red corporativa segura. Una institución extiende el acceso dentro del dispositivo de seguridad principal a un número limitado de usuarios externos previamente identificados y autorizados, a contenido, información o aplicaciones restringidas de uso privativo institucional.
- *Internet*: Intercambio de archivos para sitios web de interés público y sitios de comercio electrónico sin restricción de usuarios. Los usuarios internos colocan contenido, información y aplicaciones institucionales no confidenciales a través de Internet con acceso a un grupo de usuarios internos y externos que accede de forma anónima al sitio, incluidos los empleados de la institución. No existen requisitos para usuarios internos en cuanto al acceso a contenido, información y aplicaciones disponibles públicamente a través de Internet.

4.3.3.2. Transceptores inalámbricos maliciosos

Para poder identificar transceptores inalámbricos maliciosos se debe realizar un inventario completo de todos los dispositivos de interconexión que componen la infraestructura de red inalámbrica del Cantón Militar, para así identificar cuando se conecten dispositivos desconocidos que no acceden regularmente a la red de datos y poder identificar posibles intrusos informáticos.

Se realizó entonces el respectivo inventario de los dispositivos de interconexión que conforman la infraestructura de red inalámbrica del Cantón Militar de Popayán mediante un escaneo de los activos que componen la red de datos de la unidad militar para su identificación y clasificación.

Se puede apreciar que la organización no tiene una adecuada política de seguridad para el uso de la tecnología inalámbrica teniendo en cuenta que es una institución militar con información de importancia crítica y confidencial, dado que se detectaron varios dispositivos que no pertenecen a los activos del Ejército Nacional de Colombia. El escaneo de activos ejecutado se puede apreciar en la sección *5.3.3 Escaneo de activos desde la infraestructura de red inalámbrica* más adelante en

este documento. Los dispositivos que componen la infraestructura de red de datos del Cantón Militar de Popayán desde el punto de vista del acceso al servicio de Internet desde la red inalámbrica se consignan en la siguiente tabla.

Tabla 27. Inventario de activos de red del Cantón Militar de Popayán

Dispositivo	Cantidad	Marca	Modelo	Configuración
Enrutador	1	HP	MSR3012 E	Gateway de frontera
Firewall	1	HP	S8010F	Seguridad perimetral
Conmutador troncal	1	3Com	S7902E	Core o núcleo troncal
Conmutador troncal	1	3Com	4500g capa3	Estándar ethernet
Conmutador distribución	7	HP	1920	Estándar ethernet
Punto de Acceso Inalámbrico	7	HP	425	Punto de acceso para usuarios
Teléfono IP	7	HP	3500	Estándar
Impresora	7	HP	Pro M281fdw	Impresora – Escáner

Finalmente, para poder identificar y gestionar transceptores inalámbricos maliciosos se sugirió la implementación de un sistema de detección de intrusos, el cual clasifica automáticamente los dispositivos detectados como maliciosos y los dispone en cuarentena, bloqueando de inmediato los dispositivos que representan una amenaza para la red de datos. Además, posee la opción de colocar en cuarentena tanto terminales infectados y/o sospechosos, como puntos de acceso inalámbrico que pudieren estar infectados o tratarse de un punto de acceso espía de algún intruso. Igualmente se sugiere la implementación de un sistema de prevención de intrusiones, el cual bloquea los dispositivos maliciosos detectados por cada segmento de red de datos tanto cableada como inalámbrica en el Cantón Militar de Popayán. El esquema de la solución planteada se puede apreciar más adelante en este documento en la sección *Sistema de detección de intrusos inalámbrico* y *Sistema de prevención de intrusiones inalámbrico*.

4.3.4. Revisión de la segregación

La revisión de la segregación consiste en la ejecución de pruebas para la realizar una apropiada separación de la propiedad de información privada o personal, de la propiedad de información institucional militar. Es una revisión de la privacidad en el almacenamiento, transmisión y control legal y ético de la propiedad de información privada del personal, socios y usuarios del Ejército.

Se encontró que la Tercera División del Cantón Militar de Popayán no cuenta con mecanismos o procedimientos para diferenciar y proteger los derechos de privacidad de la información militar del Ejército, por una parte, ni los derechos de privacidad del personal del Ejército en cuanto a la información de su vida privada por otro lado, dado que se permite el compartimiento de archivos en la intranet de la red de área local de la unidad militar.

Para gestionar esta vulnerabilidad se sugirió mediante políticas de seguridad, prohibir el compartimiento de cualquier tipo de archivos en la intranet de la unidad militar. Además, se sugiere la implementación de un sistema de almacenamiento de información basado en Microsoft Sharepoint Server para la información de la vida privada del personal del Ejército en la Tercera División. El esquema de solución propuesto se puede observar más adelante en este documento en la sección *4.3.3.1 Compartir*.

4.3.4.1. Mapeo de Contención de Privacidad

Para realizar el mapeo de contención de privacidad se deben mapear los guardianes de información privada dentro del alcance, qué información es almacenada, cómo y dónde se almacena la información, y sobre qué canales se comunica la información.

La información que se almacena en la institución se clasifica como de carácter militar, se almacena información sobre las operaciones militares, institucionales, jurídicas, financieras y administrativas del Ejército Nacional de Colombia. Esta información se almacena centralizada y custodiada en el segmento de red de área de almacenamiento ubicado en la ciudad de Bogotá y el acceso a la información se realiza mediante canales de comunicación privados contratados con el proveedor de servicios de internet del Ejército desde cada sede departamental.

4.3.4.2. Divulgación

Para la divulgación se debe examinar los tipos de divulgaciones de información privada en el espectro inalámbrico.

Se encontró que existe divulgación de múltiples tipos de información multimedia privada de los usuarios que se conectan a la intranet de datos a través de la infraestructura de red inalámbrica de la Tercera División del Cantón Militar de Popayán que infringe las políticas de seguridad en materia del Ejército Nacional, pero los resultados de esta revisión no se incluyen en este documento por cuanto viola las restricciones de no divulgación de información privada del personal del ejército expresadas en el alcance de este proyecto en la sección *5.2.1 Alcance de las pruebas de penetración*.

Para gestionar esta vulnerabilidad se sugirió, al igual que en la sección *4.3.4 Revisión de la segregación*, mediante políticas de seguridad, prohibir el compartimiento de cualquier tipo de archivos en la intranet de la unidad militar, así como la implementación de un sistema de almacenamiento de información basado en Microsoft Sharepoint Server para la información de la vida privada del personal del Ejército en la Tercera División. El esquema de solución propuesto se puede observar en este documento en la sección *4.3.3.1 Compartir*.

4.3.4.3. Limitaciones

En cuanto al análisis de limitaciones se debe identificar los tipos de puertas de enlace y alternativas de canal accesibles para personas con limitaciones físicas dentro de ese canal.

Se encontró que no existen puertas de enlace o algún tipo de alternativas de canal accesibles para que personas con limitaciones físicas puedan acceder al servicio de internet inalámbrico en la Tercera División del Cantón Militar de Popayán. Sin embargo, aunque sería importante contar con dispositivos que faciliten el acceso a personas con limitaciones físicas a manera de inclusión social, este hecho no representa una vulnerabilidad como tal para la seguridad de la red inalámbrica del Ejército Nacional en la unidad militar.

4.3.5. Verificación de la exposición

La verificación de la exposición consiste en la realización de pruebas para descubrir información que proporciona o lleva a un acceso autenticado o permite el acceso a ubicaciones múltiples dentro de la infraestructura de red inalámbrica del Cantón Militar con la misma autenticación. A continuación se presentan los resultados de las pruebas ejecutadas.

4.3.5.1. Mapeo de la exposición

Se debe mapear la información del personal del Ejército con respecto a la institución, como los cuadros de organización, títulos de personal militar clave en la gestión de la red inalámbrica, descripciones de puestos de trabajo, números de teléfono personales y laborales, números de teléfono fijo y móvil, tarjetas de presentación, documentos compartidos, hojas de vida, afiliaciones organizativas, direcciones de correo electrónico públicas y privadas, inicios de sesión, esquemas de inicio de sesión, contraseñas, métodos de copia de seguridad, aseguradores o cualquier otra información organizacional declarada implícitamente como confidencial en las regulaciones y políticas de seguridad del Cantón Militar de Popayán.

La relación del personal del Ejército que realiza la gestión de la infraestructura de red inalámbrica en la Tercera División del Cantón Militar de Popayán es la siguiente:

Tabla 28. Personal de gestión de red en la Tercera División del Cantón Militar de Popayán

Nombre	Yeimi Carolina Rodríguez
Cargo	B6-Comunicaciones C5
Celular	3502479042
Email	yeimy.rodriguez@ejercito.mil.co

4.3.5.2. Perfilado

Para el perfilado se debe examinar con el uso de una antena direccional y de alta ganancia, si las señales inalámbricas del dispositivo de acceso se extienden más allá de las paredes o la propiedad objetivo dentro de las unidades del Cantón Militar.

Para el análisis de perfilado de la red inalámbrica se utilizó la antena *Tenda U6*, la cual es una antena direccional de 6dBi de alta ganancia con velocidad de transmisión/recepción de 300Mbps que posee el modo monitor de redes Wifi. La antena se utilizó para monitorear la señal de red inalámbrica desde el exterior del perímetro físico del Cantón Militar de Popayán como análisis de vulnerabilidad externa en la infraestructura de red inalámbrica se observa a continuación.

Figura 22. Antena Tenda U6 de alta ganancia

Para ello, se realizó un estudio de red externo mediante una terminal con la antena direccional de alta ganancia, que incrementó su capacidad de alcanzar señales de red inalámbrica distantes, encontrándose que fue posible autenticarse en la red del Batallón desde el exterior de su perímetro físico con las credenciales de acceso identificadas, siendo este un posible escenario para un ataque informático por parte de un intruso malicioso externo. El esquema del análisis de vulnerabilidad externo ejecutado se puede apreciar en la siguiente gráfica.

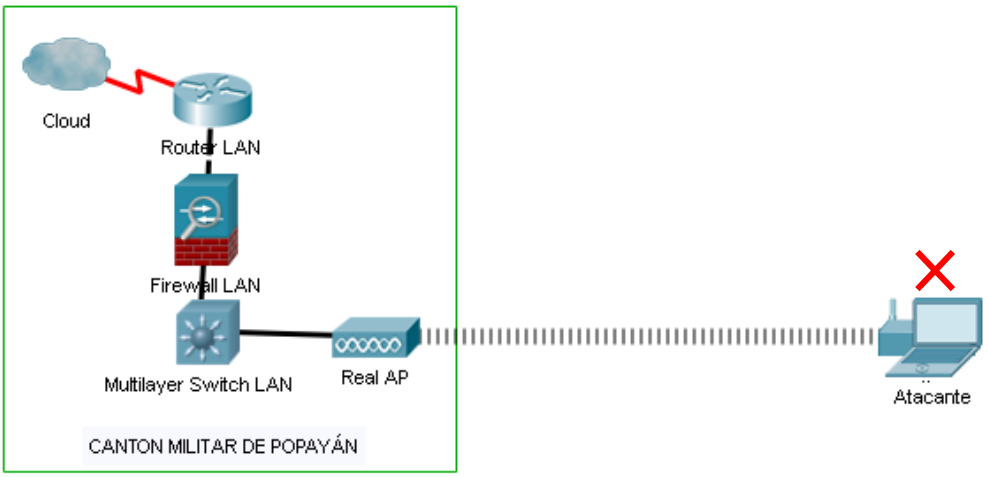


Figura 23. Prueba de penetración externa intruso informático

Con la ejecución de este análisis de vulnerabilidad se encontró que las señales de radiofrecuencia que transmiten la información militar a través de los puntos de acceso de la infraestructura de red inalámbrica si se extienden más allá de la planta física de las unidades del Cantón Militar de Popayán, debido a que la potencia de transmisión de señal de los puntos de acceso inalámbrico se encuentra configurada para su potencia de transmisión máxima. De esta manera, se comprueba que si es posible enviar información a otro personal o intruso informático externo sin ningún tipo de credenciales adicionales, evidenciando que existe una vulnerabilidad en la red inalámbrica del Batallón en este aspecto. Para la ejecución de este análisis se utilizó la aplicación *WiFi Analyzer* de Windows, el cual es un analizador de redes inalámbricas útil para identificar problemas de conexión inalámbrica, así como encontrar el mejor canal o ubicación para puntos de acceso inalámbrico.

Los resultados obtenidos en la ejecución del análisis externo realizado en la infraestructura de red inalámbrica del Cantón Militar de Popayán, para comprobación de la posibilidad de acceso remoto a las señales de red inalámbrica alcanzables desde el exterior del perímetro físico por parte de un intruso malicioso, se presentan en la siguiente gráfica. En ella se observan las direcciones físicas MAC de algunos de los puntos de acceso inalámbrico del Cantón Militar, las cuales son necesarias para poder ejecutar un posible ataque de penetración como la prueba de punto de acceso no autorizado.

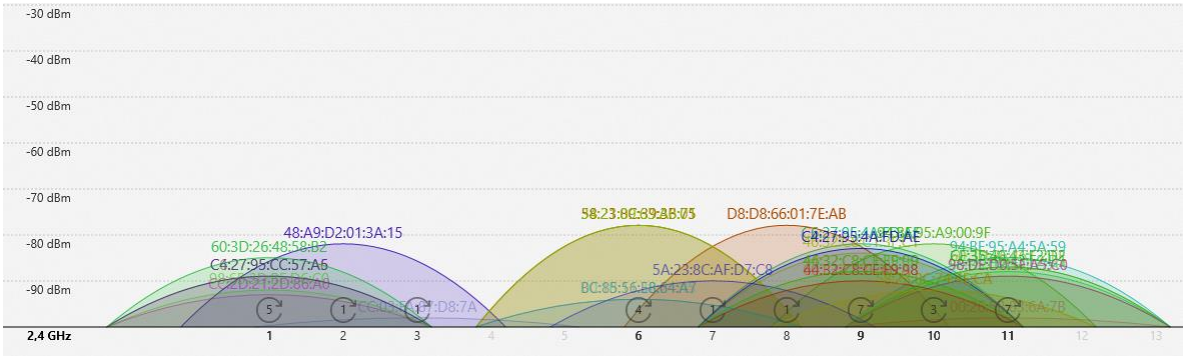


Figura 24. Análisis externo de frecuencias de red inalámbrica

También se utilizó la aplicación Vistumbler, la cual es un escáner de redes inalámbricas para Windows que permite mapear y visualizar con mayor profundidad los puntos de acceso inalámbrico que le rodean en función de los datos inalámbricos y GPS recopilados.

Los resultados obtenidos con la ejecución de esta aplicación se observan en la siguiente gráfica, en donde se pueden apreciar datos completos de los puntos de acceso inalámbrico del Ejército Nacional alcanzables desde el exterior del perímetro físico del Cantón Militar, tales como el tipo de autenticación o la casa fabricante del dispositivo para buscar vulnerabilidades de marca reconocidas.

#	Mac Address	SSID	Signal	High ...	RSSI	High RSSI	Channel	Authentication	Encryption	Network Type	Manufacturer	Radio Type	Last Updated
1	0C:CB:85:D5:FA:8C	moto g(6) play 9465	0%	56%	-100 dBm	-71 dBm	10	WPA2-Personal	CCMP	Infrastructure	Unknown	802.11n	29-10-2019 10:22:11.1...
2	58:23:8C:39:3B:75	FLIA_RIVERA_LOPEZ	70%	70%	-81 dBm	-74 dBm	6	WPA2-Personal	CCMP	Infrastructure	Technicolor CH U...	802.11n	29-10-2019 10:23:09.8...
3	82:2A:A8:01:9F:AF	CASINO2018	47%	56%	-82 dBm	-79 dBm	6	WPA2-Personal	CCMP	Infrastructure	Unknown	802.11n	29-10-2019 10:23:09.8...
4	60:E3:27:3E:A0:A8	TP-LINK_A0A8	0%	7%	-100 dBm	-88 dBm	9	WPA2-Personal	CCMP	Infrastructure	TP-LINK TECHNO...	802.11n	29-10-2019 10:21:48.5...
5	46:32:C8:C1:3F:C1		47%	60%	-82 dBm	-82 dBm	9	WPA2-Personal	CCMP	Infrastructure	Unknown	802.11n	29-10-2019 10:23:09.8...
6	C6:27:95:4A:FD:AF		60%	60%	-84 dBm	-78 dBm	9	WPA2-Personal	CCMP	Infrastructure	Unknown	802.11n	29-10-2019 10:23:09.8...
7	CE:35:40:3D:1A:0A		0%	5%	-100 dBm	-90 dBm	1	WPA2-Personal	CCMP	Infrastructure	Unknown	802.11n	29-10-2019 10:21:30.2...
8	34:21:09:63:A6:01	73578817	64%	64%	-70 dBm	-70 dBm	6	WPA2-Personal	CCMP	Infrastructure	Jensen Scandinav...	802.11n	29-10-2019 10:23:09.8...
9	C4:27:95:4A:FD:AE	Juan Andres	56%	60%	-79 dBm	-78 dBm	9	WPA2-Personal	CCMP	Infrastructure	Technicolor CH U...	802.11n	29-10-2019 10:23:09.8...
10	48:A9:D2:01:3A:15	DTVNET_013A15	56%	60%	-79 dBm	-78 dBm	2	WPA2-Personal	CCMP	Infrastructure	Wistron Neweb Co...	802.11n	29-10-2019 10:23:09.8...
11	30:B5:C2:3A:69:A4	Almacend290	0%	47%	-100 dBm	-84 dBm	11	WPA2-Personal	CCMP	Infrastructure	TP-LINK TECHNO...	802.11n	29-10-2019 10:23:03.7...
12	98:DE:D0:5F:A5:C0	TP-LINK_AP_A5C0	46%	56%	-84 dBm	-82 dBm	11	WPA2-Personal	CCMP	Infrastructure	TP-LINK TECHNO...	802.11n	29-10-2019 10:23:07.7...
13	BC:85:56:E8:64:A7	HP-Print-A7-LaserJet 1102	0%	46%	-100 dBm	-84 dBm	6	Open	None	Infrastructure	Hon Hai Precision ...	802.11g	29-10-2019 10:22:51.5...
14	0C:8C:24:65:CE:6B	Olivito	0%	6%	-100 dBm	-89 dBm	6	WPA2-Personal	CCMP	Infrastructure	Unknown	802.11g	29-10-2019 10:21:46.4...
15	C4:27:95:CC:57:A5	Avila	46%	46%	-84 dBm	-81 dBm	1	WPA2-Personal	CCMP	Infrastructure	Technicolor CH U...	802.11n	29-10-2019 10:23:09.8...
16	60:3D:26:48:58:B2	Nohemy	47%	47%	-82 dBm	-81 dBm	1	WPA2-Personal	CCMP	Infrastructure	Technicolor CH U...	802.11n	29-10-2019 10:23:09.8...
17	D8:D8:66:01:7E:AB	Javierme	70%	70%	-78 dBm	-73 dBm	8	WPA2-Personal	CCMP	Infrastructure	SHENZHEN TOZ...	802.11n	29-10-2019 10:23:09.8...
18	CE:35:40:43:F2:D2		47%	56%	-78 dBm	-74 dBm	11	WPA2-Personal	CCMP	Infrastructure	Unknown	802.11n	29-10-2019 10:23:09.8...
19	C6:27:95:CC:57:A6		0%	46%	-100 dBm	-84 dBm	1	WPA2-Personal	CCMP	Infrastructure	Unknown	802.11n	29-10-2019 10:22:18.2...
20	CC:03:FA:87:D8:7A	FLIA MATUZ	47%	56%	-84 dBm	-82 dBm	3	WPA2-Personal	CCMP	Infrastructure	Technicolor CH U...	802.11n	29-10-2019 10:23:09.8...
21	CC:35:40:43:F2:D1	FAMILIA_GUZMAN	47%	60%	-75 dBm	-75 dBm	11	WPA2-Personal	CCMP	Infrastructure	Technicolor CH U...	802.11n	29-10-2019 10:23:09.8...
22	94:BF:95:A9:00:9F	FAMILIA-OROZCO	0%	60%	-100 dBm	-75 dBm	10	WPA2-Personal	CCMP	Infrastructure	Shenzhen Coship ...	802.11n	29-10-2019 10:22:55.5...
23	98:6B:3D:BE:D6:C0	ARRIS-D6C2	0%	4%	-100 dBm	-93 dBm	1	WPA2-Personal	CCMP	Infrastructure	ARRIS Group, Inc.	802.11n	29-10-2019 10:21:32.2...
24	5A:23:8C:74:4E:CB		0%	46%	-100 dBm	-84 dBm	10	WPA2-Personal	CCMP	Infrastructure	Unknown	802.11n	29-10-2019 10:22:05.2...
25	58:23:8C:74:4E:CA	Erazo Bucheli	0%	46%	-100 dBm	-84 dBm	10	WPA2-Personal	CCMP	Infrastructure	Technicolor CH U...	802.11n	29-10-2019 10:22:49.4...
26	BC:CA:B5:57:61:F0	GALINDOOSPINA	0%	47%	-100 dBm	-84 dBm	7	WPA2-Personal	CCMP	Infrastructure	ARRIS Group, Inc.	802.11n	29-10-2019 10:23:01.6...
27	1C:49:7B:A3:2C:5A	DTVNET_A32C5C	0%	46%	-100 dBm	-84 dBm	2	WPA2-Personal	CCMP	Infrastructure	Gemtek Technolo...	802.11n	29-10-2019 10:22:49.4...
28	94:BF:95:F5:A1:89	Claro123	0%	6%	-100 dBm	-89 dBm	11	WPA2-Personal	CCMP	Infrastructure	Shenzhen Coship ...	802.11n	29-10-2019 10:21:30.2...
29	60:3D:26:46:C2:FE	ESCOLEDEZMA	46%	47%	-82 dBm	-82 dBm	11	WPA2-Personal	CCMP	Infrastructure	Technicolor CH U...	802.11n	29-10-2019 10:23:09.8...
30	94:BF:95:A4:5A:59	NO DISPONIBLE	0%	9%	-100 dBm	-83 dBm	11	WPA2-Personal	CCMP	Infrastructure	Shenzhen Coship ...	802.11n	29-10-2019 10:21:48.5...
31	20:10:7A:0E:6D:AF	ESPERANZA	47%	60%	-78 dBm	-78 dBm	6	WPA2-Personal	CCMP	Infrastructure	Gemtek Technolo...	802.11n	29-10-2019 10:23:09.8...
32	CC:35:40:3D:1A:09	RUEDA	0%	46%	-100 dBm	-84 dBm	1	WPA2-Personal	CCMP	Infrastructure	Technicolor CH U...	802.11n	29-10-2019 10:22:14.2...
33	CC:2D:21:2D:86:A0	Tenda_2D86A0	0%	46%	-100 dBm	-84 dBm	1	WPA2-Personal	CCMP	Infrastructure	Tenda Technolog...	802.11n	29-10-2019 10:22:59.6...
34	BC:3E:07:C6:79:C8	COMANDO	0%	7%	-100 dBm	-87 dBm	1	WPA2-Personal	CCMP	Infrastructure	Unknown	802.11n	29-10-2019 10:21:46.4...
35	B0:89:00:99:05:7A	paola gutierrez	0%	2%	-100 dBm	-97 dBm	1	WPA2-Personal	CCMP	Infrastructure	HUAWEI TECHN...	802.11n	29-10-2019 10:19:50.8...
36	5A:23:8C:AF:D7:C8		0%	7%	-100 dBm	-87 dBm	7	WPA2-Personal	CCMP	Infrastructure	Unknown	802.11n	29-10-2019 10:21:30.2...
37	58:23:8C:AF:D7:C7	FAMILIAMEJIA	0%	7%	-100 dBm	-86 dBm	7	WPA2-Personal	CCMP	Infrastructure	Technicolor CH U...	802.11n	29-10-2019 10:21:30.2...
38	B0:BE:76:04:23:69	FLIA RIVERA _Ext	47%	56%	-82 dBm	-82 dBm	11	WPA2-Personal	CCMP	Infrastructure	Unknown	802.11n	29-10-2019 10:23:37.8...
39	44:32:C8:CE:E9:98	FLIAGOMEZ	46%	56%	-84 dBm	-82 dBm	9	WPA2-Personal	CCMP	Infrastructure	Technicolor CH U...	802.11n	29-10-2019 10:23:37.8...
40	00:1D:D6:50:A1:60	Familia Duenas	0%	56%	-100 dBm	-82 dBm	11	WPA2-Personal	CCMP	Infrastructure	ARRIS Group, Inc.	802.11n	29-10-2019 10:23:26.0...
41	46:32:C8:CE:E9:99		0%	60%	-100 dBm	-84 dBm	9	WPA2-Personal	CCMP	Infrastructure	Unknown	802.11n	29-10-2019 10:23:03.7...
42	34:21:09:63:A6:09	73578817	0%	5%	-100 dBm	-91 dBm	6	WPA2-Personal	CCMP	Infrastructure	Jensen Scandinav...	802.11n	29-10-2019 10:20:42.8...
43	60:02:B4:FE:A0:07	DTVNET_FEA007	0%	5%	-100 dBm	-91 dBm	2	WPA2-Personal	CCMP	Infrastructure	Wistron Neweb Co...	802.11n	29-10-2019 10:21:34.3...
44	00:1B:11:3B:21:45	FAMILIA GARCIA	0%	46%	-100 dBm	-84 dBm	6	WPA2-Personal	TKIP	Infrastructure	D-Link Corporation	802.11g	29-10-2019 10:22:53.5...
45	CE:35:40:D1:C7:18		0%	3%	-100 dBm	-94 dBm	6	WPA2-Personal	CCMP	Infrastructure	Unknown	802.11n	29-10-2019 10:21:16.8...
46	CC:03:FA:C7:92:E2	LUCHO	0%	46%	-100 dBm	-84 dBm	7	WPA2-Personal	CCMP	Infrastructure	Technicolor CH U...	802.11n	29-10-2019 10:22:55.5...
47	BC:30:7D:F1:7F:E8	DTVNET_F17FE8	0%	5%	-100 dBm	-90 dBm	1	WPA2-Personal	CCMP	Infrastructure	Wistron Neweb Co...	802.11n	29-10-2019 10:21:42.4...
48	24:92:0E:7D:51:4A	Bp8C-SnVhbiBBbmRyZ...	0%	81%	-100 dBm	-58 dBm	6	Open	None	Infrastructure	Samsung Electroni...	802.11n	29-10-2019 10:23:13.8...
49	00:26:5B:83:6A:7B	Juancho	0%	5%	-100 dBm	-92 dBm	11	WPA-Personal	TKIP	Infrastructure	Hitron Technologi...	802.11g	29-10-2019 10:21:30.2...
50	10:C2:5A:28:9E:7B	LOPEZ	0%	46%	-100 dBm	-84 dBm	9	WPA2-Personal	CCMP	Infrastructure	Technicolor CH U...	802.11n	29-10-2019 10:22:14.2...
51	CE:03:FA:C7:92:E3		0%	46%	-100 dBm	-84 dBm	7	WPA2-Personal	CCMP	Infrastructure	Unknown	802.11n	29-10-2019 10:23:07.7...
52	CC:35:40:D1:C7:17	FLIA IBARRA	0%	5%	-100 dBm	-93 dBm	6	WPA2-Personal	CCMP	Infrastructure	Technicolor CH U...	802.11n	29-10-2019 10:21:34.3...
53	CE:35:40:B0:25:20		0%	5%	-100 dBm	-91 dBm	11	WPA2-Personal	CCMP	Infrastructure	Unknown	802.11n	29-10-2019 10:21:19.9...
54	10:C2:5A:37:93:02	CAPO	0%	4%	-100 dBm	-95 dBm	6	WPA2-Personal	CCMP	Infrastructure	Technicolor CH U...	802.11n	29-10-2019 10:21:19.9...
55	94:87:7C:5A:FF:90	JESSICAALEJANDRA	0%	46%	-100 dBm	-84 dBm	9	WPA2-Personal	CCMP	Infrastructure	ARRIS Group, Inc.	802.11n	29-10-2019 10:23:30.1...
56	D0:FC:CC:C8:C3:07	SAMSUNG J7 SILVIA c...	56%	56%	-78 dBm	-78 dBm	6	WPA2-Personal	CCMP	Infrastructure	Samsung Electroni...	802.11n	29-10-2019 10:23:37.8...
57	CC:35:40:B0:25:2F	familia AC	0%	3%	-100 dBm	-94 dBm	11	WPA2-Personal	CCMP	Infrastructure	Technicolor CH U...	802.11n	29-10-2019 10:21:19.9...
58	94:44:52:F3:F2:14	Alejandra	0%	6%	-100 dBm	-89 dBm	11	WPA2-Personal	CCMP	Infrastructure	Belkin Internationa...	802.11n	29-10-2019 10:21:23.0...
59	34:21:09:62:EC:59	ANGELAMARTINEZ1	0%	1%	-100 dBm	-98 dBm	6	WPA2-Personal	CCMP	Infrastructure	Jensen Scandinav...	802.11n	29-10-2019 10:21:28.0...
60	44:32:C8:C1:3F:C0	defensascia	60%	60%	-79 dBm	-75 dBm	9	WPA2-Personal	CCMP	Infrastructure	Technicolor CH U...	802.11n	29-10-2019 10:23:37.8...
61	D8:D8:66:19:35:4B	DTVNET_19354B	0%	56%	-100 dBm	-78 dBm	6	WPA2-Personal	CCMP	Infrastructure	SHENZHEN TOZ...	802.11n	29-10-2019 10:23:28.0...
62	D8:D8:66:08:18:E9	Danis/Mattias	0%	46%	-100 dBm	-84 dBm	1	WPA2-Personal	CCMP	Infrastructure	SHENZHEN TOZ...	802.11n	29-10-2019 10:22:59.6...
63	D8:D8:66:0A:C7:A0	DTVNET_0AC7A0	0%	46%	-100 dBm	-84 dBm	1	WPA2-Personal	CCMP	Infrastructure	SHENZHEN TOZ...	802.11n	29-10-2019 10:23:09.8...

Figura 25. Análisis de red inalámbrica del Cantón Militar de Popayán con Vistumbler

Para gestionar esta vulnerabilidad se sugirió que se redujera la potencia de transmisión de los puntos de acceso de la red inalámbrica por su configuración de potencia de transmisión mínima, generalmente de un 25% de la potencia total del dispositivo, suficiente para la cobertura interna del servicio y disminuyendo la posibilidad que la señal de la red inalámbrica sea alcanzada e interceptada desde el exterior del perímetro físico del Cantón Militar en un eventual ataque informático.

Adicionalmente, también se gestiona con la implementación del sistema de detección de intrusos inalámbrico, el cual posee la capacidad de proteger la información confidencial institucional de no exponerse a través de puntos de acceso no autorizados y mal configurados, y controlar el acceso de usuarios evitando que se conecten a puntos de acceso inalámbrico incorrectos, como aquellos que están cerca del perímetro físico de la institución pero que no están bajo el control del

personal de gestión de la infraestructura de red de datos , protegiendo la información confidencial militar. La descripción detallada de este sistema se muestra más adelante en este documento en la sección *Sistema de detección de intrusos inalámbrico*.

4.3.6. Exploración de inteligencia competitiva

La exploración de inteligencia competitiva consiste en la ejecución de pruebas de propiedades de eliminación que pueden ser analizadas como inteligencia de negocios. Mientras la inteligencia competitiva como campo esté relacionada con el marketing, el proceso incluye cualquier forma de recopilación de inteligencia competitiva, incluido, entre otros, el espionaje económico e industrial. Sus resultados se presentan a continuación.

4.3.6.1. Molienda de negocios

En este paso se debe mapear los objetivos dentro del alcance del análisis activo y pasivo de las emanaciones de información: qué información es almacenada, cómo y dónde se almacena la información, y cómo se comunica la información.

La información que se almacena es de carácter militar, de seguridad nacional, confidencial, restringida y clasificada, la cual se almacena en servidores ubicados en el segmento de red de área de almacenamiento del Ejército Nacional de Colombia ubicado en la ciudad de Bogotá, y se comunica mediante canales de datos privados contratados con diferentes proveedores de servicios de Internet en cada ciudad del país donde opere un Cantón Militar.

Mas sin embargo, el escaneo activo o pasivo de servidores del segmento de red de área de almacenamiento no se realiza por cuanto viola las restricciones expresadas en el alcance de este proyecto en la sección *5.2.1 Alcance de las pruebas de penetración*, más adelante en este documento, en donde se expresa que.

- Se restringen las pruebas de penetración informática únicamente a los puntos de acceso de la red inalámbrica del Cantón Militar de Popayán, no se autorizan pruebas de penetración contra las terminales, dispositivos de interconexión ni ningún otro activo de red diferente, por cuánto estás labores están restringidas y autorizadas únicamente al personal militar que labora en el área de seguridad informática en la institución, por protocolos de seguridad de contrainteligencia militar interna de la red del Ejército Nacional de Colombia.
- Las pruebas de seguridad serán ejecutadas únicamente en el Cantón Militar de Popayán - Tercera División como fue autorizado, no podrán realizarse desde ninguna otra unidad militar.

- Se debe suspender inmediatamente las pruebas de penetración si se logra acceder al área de almacenamiento SAN con los servidores que contienen información militar confidencial y de acceso restringido en la ciudad de Bogotá.

4.3.6.2. Entorno de negocios

Para identificar el entorno de negocios se deben explorar los detalles comerciales, como alianzas, socios, principales clientes, proveedores, distribuidores, inversores, relaciones comerciales, producción, desarrollo, información de productos, planificación, acciones y comercio, y cualquier información comercial o propiedad en particular declarada implícitamente como confidencial en las normas y políticas.

En este aspecto se encontró que en la red inalámbrica de la Tercera división del Cantón Militar de Popayán no existen políticas de seguridad con enfoques comerciales que tengan en cuenta parámetros de seguridad adicionales o especiales para información relacionada con alianzas, socios, clientes, proveedores, distribuidores, inversores, relaciones comerciales, producción, desarrollo, información de productos, planificación, acciones y comercio, o cualquier información comercial.

Por otra parte, este análisis no se realiza en profundidad por cuanto viola las restricciones expresadas en el alcance de este proyecto en la sección *5.2.1 Alcance de las pruebas de penetración*, en donde se enmarca que.

- Se debe suspender inmediatamente las pruebas de penetración si se logra acceder al área de almacenamiento SAN con los servidores que contienen información militar confidencial y de acceso restringido en la ciudad de Bogotá.

4.3.6.3. Entorno organizacional

Examinar y documentar los tipos de revelaciones de propiedad comercial de los guardianes en operaciones, procesos, jerarquías, informes financieros, oportunidades de inversión, fusiones, adquisiciones, canal, inversiones, mantenimiento de canales, políticas sociales internas, insatisfacción y cambio de personal, tasa, tiempos de vacaciones primarios, contrataciones, despidos y cualquier propiedad organizativa en particular declarada implícitamente como confidencial en las normas y políticas.

En este aspecto se encontró que en la red inalámbrica de la Tercera división del Cantón Militar de Popayán no existen implementadas políticas de seguridad con enfoques comerciales que tengan en cuenta parámetros de seguridad adicionales o especiales para información relacionada con revelaciones de propiedad comercial de los guardianes en operaciones, procesos, jerarquías, informes financieros,

oportunidades de inversión, fusiones, adquisiciones, canal, inversiones, mantenimiento de canales, políticas sociales internas, insatisfacción y cambio de personal, tasa, tiempos de vacaciones primarios, contrataciones, despidos y cualquier propiedad organizativa en particular.

Pero, de igual manera que los puntos predecesores, este análisis no se realiza en profundidad por cuanto también se violan las restricciones expresadas en el alcance de este proyecto en la sección *5.2.1 Alcance de las pruebas de penetración*, por las mismas razones ya expresadas anteriormente en esta misma sección.

4.4. Fase de Pruebas y Controles

4.4.1. Verificación de cuarentena

La verificación de cuarentena consiste en la determinación y medición del uso efectivo de la cuarentena para todos los accesos hacia y desde la infraestructura de red inalámbrica del Cantón Militar de Popayán. L os resultados de la verificación se observan a continuación.

4.4.1.1. Identificación del proceso de contención

El proceso de contención consiste en identificar los métodos y procesos de cuarentena en todos los canales para contactos agresivos y hostiles que se detecten en la infraestructura de red inalámbrica.

Se encontró que no existe ningún procedimiento o dispositivo que permita aislar en cuarentena las terminales detectadas como infectadas con malware o que presenten un comportamiento hostil al ser de un posible intruso malicioso que pueda intentar lanzar algún ataque informático en la red.

Esta vulnerabilidad también se gestiona con la implementación del sistema de detección de intrusos inalámbrico, el cual posee la opción de colocar en cuarentena tanto terminales infectados y/o sospechosos, como puntos de acceso inalámbrico que pudieren estar infectados o tratarse de un punto de acceso espía de algún intruso, para su revisión. Además, mediante el uso de técnicas de clasificación automática, los dispositivos detectados como maliciosos se clasifican y disponen en cuarentena con precisión, mientras que los que representan una amenaza para la red de datos se bloquean de inmediato, incrementando la protección de la infraestructura de red inalámbrica del Cantón Militar de Popayán en tiempo real (Ver sección *Sistema de detección de intrusos inalámbrico*).

4.4.1.2. Niveles de contención

Para determinar los niveles de contención se debe verificar el estado de contención, el tiempo y todos los canales donde las interacciones tienen métodos de

cuarentena, asegurándose que los métodos estén dentro de los límites y el contexto legal.

Se encontró, al igual que en el punto anterior, que no existe ningún procedimiento o dispositivo que permita verificar el estado de contención, el tiempo y los canales con métodos de cuarentena. A esta vulnerabilidad también se le realiza gestión con la implementación del sistema de detección de intrusos en cuanto a la disposición en cuarentena de dispositivos y puntos de acceso inalámbrico sospechosos para su revisión y monitoreo en el tiempo por cada uno de los canales o segmentos de red de datos existente por cada división del Ejército en el Cantón Militar de Popayán (Ver sección *Sistema de detección de intrusos inalámbrico*).

Adicionalmente se refuerza su gestión con la implementación del sistema de prevención de intrusiones inalámbrico propuesto, el cual realiza un control y monitoreo minucioso del tráfico de datos por cada segmento de red que llega a cada división del Ejército Nacional, incluida la inalámbrica, detectando en un mayor nivel posibles intrusos y dispositivos maliciosos en un ataque de red y alertando al sistema de detección de intrusos para su disposición en cuarentena. (Ver sección *Sistema de prevención de intrusiones inalámbrico*).

4.4.2. Auditoria de Privilegios

La auditoría de Privilegios consiste en la ejecución de pruebas donde las credenciales se suministran al usuario y se concede permiso para la ejecución de las pruebas con aquellas credenciales. Los resultados de la auditoría realizada fueron los siguientes.

4.4.2.1. Identificación

Se debe examinar y documentar el proceso para obtener la identificación a través de medios legítimos y fraudulentos en el canal de comunicación de la Tercera División del Cantón Militar de Popayán.

Para obtener la identificación en general, se debe acudir a la división de sistemas de cada brigada en donde el personal encargado de TI le hará al usuario el respectivo proceso de registro en el directorio activo del Ejército Nacional si fuere necesario, previa comprobación de sus credenciales militares, y posteriormente le entrega las claves de acceso a la red inalámbrica para utilizar el servicio de internet.

Existe una vulnerabilidad en este sentido dado que, al manejarse una única clave de red para todos los usuarios de cada unidad militar del Cantón, cualquier persona, usuario o intruso malicioso puede obtener la clave del servicio de red inalámbrica y por ende tener acceso a la infraestructura de red de datos del Ejército Nacional de manera fraudulenta.

Para realizar la gestión de esta vulnerabilidad se sugirió la implementación de un sistema de autenticación inalámbrico para que cada usuario se autentique desde el acceso a la red inalámbrica, contra el directorio activo del dominio de la institución o la base de datos del personal del Ejército Nacional de Colombia y por ende un intruso no pueda obtener la clave de acceso a la red inalámbrica de manera fraudulenta, tendría que forzosamente lograr su registro en el directorio activo de la institución. El esquema de solución planteado se expone en detalle más adelante en este documento, en la sección *Sistema de autenticación inalámbrico*.

4.4.2.2. Autorización

Se debe verificar el uso de la autorización fraudulenta en todos los canales para obtener privilegios similares a los de otro personal.

Se comprobó que no es posible obtener privilegios similares a los de otro personal con mayor jerarquía desde la red inalámbrica del Ejército Nacional, debido a que existe un directorio activo que controla los privilegios de cada usuario en cuanto al acceso a los servicios o sistemas de información en la red de datos. Con la autorización fraudulenta obtenida, bien sea por ingeniería social, o mediante ataques de fuerza bruta, solo se puede obtener acceso al servicio de Internet de la institución. No obstante, este escenario puede ser aprovechado por un intruso malicioso para capturar información en la intranet del Cantón Militar o lanzar un posible ataque informático contra el directorio activo del dominio de la institución en busca de acceso al segmento de red de área de almacenamiento con la información militar confidencial y restringida, por lo que se sugiere la implementación del sistema de autenticación propuesto en la sección *Sistema de autenticación inalámbrico*.

4.4.2.3. Escalada

La escalada consiste en la verificación y validación del acceso a la información mediante el uso de privilegios para obtener privilegios más altos.

Se logró comprobar igualmente que no es posible obtener privilegios más altos a través del uso u obtención de privilegios conseguidos mediante autorización fraudulenta desde la red inalámbrica del Ejército Nacional, debido a que existe un directorio activo que controla a cada usuario los privilegios de acceso a servicios o sistemas de información en la red de datos. Solo se puede obtener acceso al servicio de Internet de la institución, no se puede incrementar privilegios de usuario para acceder a los servidores del segmento de red de área de almacenamiento o a las interfaces de configuración de los dispositivos de la infraestructura de red y por ende no se detectó una vulnerabilidad en este aspecto.

4.4.2.4. Subyugación

La subyugación consiste en enumerar y probar las deficiencias de todos los canales para usar o habilitar los controles de pérdida no habilitados por defecto.

En la inspección realizada se logró identificar que no existen mecanismos para habilitar controles de perdida de información en canales ante un eventual ataque informático por parte de un intruso malicioso.

Existe una vulnerabilidad en este aspecto que se gestiona con la implementación en la red de datos del sistema de detección de intrusos inalámbrico y del sistema de prevención de intrusiones inalámbrico, los cuales poseen mecanismos automatizados para habilitar los controles de perdida de información en los canales para reducir el impacto de un eventual ataque informático. El esquema de solución propuesto con la implementación de estos sistemas se puede apreciar respectivamente en la sección *Sistema de detección de intrusos inalámbrico* y *Sistema de prevención de intrusiones inalámbrico* de este documento.

4.4.3. Validación de la supervivencia

La validación de la supervivencia consiste en determinar y medir la resistencia del objetivo dentro del alcance, a cambios excesivos u hostiles diseñado para causar fallas en el servicio de red inalámbrica.

4.4.3.1. Continuidad

Para establecer la continuidad se debe enumerar y probar las deficiencias del objetivo con respecto a los retrasos de acceso al servicio de red inalámbrica con tiempo de respuesta del personal de respaldo o medios automatizados para acceso alternativo.

En el análisis se encontró que el restablecimiento del acceso al servicio de red inalámbrica a través del personal de gestión de sistemas de la Tercera División del Cantón Militar de Popayán o a través de medios automatizados para acceso alternativo no es muy eficiente acorde con el carácter militar de la institución, se atiende por personal del Ejército en la oficina de sistema de cada unidad militar que no cuenta con la debida capacitación para gestionar este tipo de circunstancias, con tiempos de respuesta que dependen de su disponibilidad laboral, y además no existe un procedimiento de respaldo automatizado para reactivar el servicio de red inalámbrica en el Cantón Militar de Popayán en caso de caída del servicio por un posible ataque informático.

Para gestionar esta vulnerabilidad se sugirió adquirir puntos de acceso inalámbrico iguales en marca y modelo, a los puntos de acceso en producción actualmente en la infraestructura de red de datos y que el personal del Ejército lo configure previamente con exactamente la misma configuración de red inalámbrica de cada unidad del Cantón Militar de Popayán, para en caso de un ataque informático se puedan reemplazar inmediatamente y se pueda reestablecer el servicio de red inalámbrica en el menor tiempo posible.

Otra solución posible para gestionar esta vulnerabilidad es la implementación del sistema de acceso inalámbrico en malla que permite realizar balanceo de carga entre diferentes puntos de acceso interconectados en un sistema de distribución inalámbrico, logrando que, si un punto de acceso es atacado, el resto de los puntos de acceso pueda atender las peticiones de los usuarios del Ejército Nacional y no se suspenda el servicio de red inalámbrica en el Cantón Militar de Popayán. El esquema de solución del sistema de acceso inalámbrico en malla propuesto se puede apreciar más adelante en este documento, el a sección *Sistema de autenticación inalámbrico*.

4.4.3.2. Resiliencia

Para determinar la resiliencia se debe mapear el proceso de los guardianes que desconectan los canales debido a una falla o preocupación de seguridad detectado en un análisis de deficiencias con la regulación y políticas de seguridad pertinentes.

Se encontró que no existe un procedimiento actualmente mediante algún sistema que posibilite o alerte a guardianes que desconectan los canales debido a fallas o amenazas de seguridad detectadas por un posible ataque informático de un intruso malicioso en la red inalámbrica del Batallón Militar.

Se sugirió la implementación del sistema de detección de intrusos inalámbrico para solventar también esta vulnerabilidad, dado que se encuentra compuesto por un servidor de seguridad y sensores detectores de intrusos que escanean permanentemente el medio de transmisión de la red inalámbrica y proporciona prevención y alarmas de intrusiones contra actividades no autorizadas en la red, activando guardianes del sistema que desconectan los canales de acuerdo a las alertas generadas en el sistema, cumpliendo las políticas de seguridad del Ejército Nacional. La descripción detallada del sistema planteado se muestra más adelante en este documento en la sección *Sistema de detección de intrusos inalámbrico*.

4.4.4. Revisión de registro y alerta

La revisión de registro y alerta consiste en un análisis de deficiencias entre las actividades realizadas en las pruebas de penetración y la profundidad real de esas actividades según lo registrado o desde las percepciones de terceros tanto humanas como mecánicas. Los resultados obtenidos se observan a continuación.

4.4.4.1. Alarma

Para la generación de alarmas y alertas de amenazas se debe verificar el uso de un sistema de advertencia, registro o mensaje localizado o de alcance general para cada punto de acceso a través de cada canal donde el personal pudiere detectar una situación sospechosa de intentos de elusión, ingeniería social o actividad fraudulenta.

Se encontró que no existe en la red de datos, el uso de un sistema de advertencia, registro o mensaje localizado o de alcance general para cada punto de acceso a través de cada canal donde se informe que el personal del Ejército detectó una situación sospechosa de intentos de elusión, ingeniería social o actividad fraudulenta en la infraestructura de red inalámbrica del Cantón Militar de Popayán.

Esta esta vulnerabilidad también se soluciona con la implementación del sistema de detección de intrusos inalámbrico planteado anteriormente, debido a que posee un sistema centralizado de monitoreo y control compuesto por un servidor de seguridad y múltiples sensores detectores de intrusos con diferentes conjuntos de antenas que escanean continuamente las diferentes bandas de transmisión de la red inalámbrica y generan las alarmas y alertas de amenazas correspondientes cuando detectan intrusiones en la red inalámbrica de cualquier tipo de dispositivo con capacidad del conexión 802.11, alertando al personal de administración de la infraestructura tecnológica del Batallón sobre un posible ataque informático (Ver sección *Sistema de detección de intrusos inalámbrico*).

4.4.4.2. Almacenamiento y recuperación

Finalmente se debe documentar y verificar el acceso sin privilegios a información sobre alarmas, registros y almacenamiento de notificaciones de ubicaciones y propiedad de activos de red.

Se encontró que no existen controles para impedir el acceso sin privilegios a información sobre alarmas, registros y segmentos de almacenamiento de notificaciones de ubicaciones y propiedad de activos de la infraestructura de red de datos del Cantón Militar de Popayán.

La sugerencia de gestión de esta vulnerabilidad va conjunta en la implementación del sistema de detección de intrusos, el sistema de prevención de intrusiones más el controlador de red inalámbrica. El sistema de detección de intrusos inalámbrico posee un sistema centralizado de monitoreo y control que impide y/o bloquea el acceso de terminales y dispositivos a la red de datos o segmentos de red si detecta alarmas y alertas de amenazas sobre un posible intruso en la red inalámbrica (Ver sección *Sistema de detección de intrusos inalámbrico*). Como complemento, el sistema de prevención de intrusiones inalámbrico permite monitorear cada segmento de la red de datos para bloquear el acceso a canales o segmentos de red en riesgo, además de detectar, identificar y gestionar dispositivos maliciosos disponiéndolos en cuarentena (Ver sección *Sistema de prevención de intrusiones inalámbrico*). Adicionalmente, el controlador de red inalámbrica utiliza técnicas de clasificación y mitigación para bloquear el tráfico inalámbrico no autorizado (Ver sección *Controlador de red inalámbrica*).

5. Evaluación de vulnerabilidades y pruebas de penetración

La evaluación de vulnerabilidades y las pruebas de penetración son métodos que sirven para evaluar el nivel de seguridad de una red inalámbrica mediante pruebas de intrusión éticas que permiten identificar vulnerabilidades asociadas a los servicios informáticos inalámbricos de la institución militar desde la perspectiva de escenarios predefinidos como ataques de usuarios internos, usuarios externos, intrusos y atacantes maliciosos, con un conocimiento mínimo de los servicios e infraestructura de la red inalámbrica a evaluar.

La evaluación se inició con una etapa de exploración de los servicios informáticos ofrecidos en el Cantón Militar de Popayán, sus aplicaciones y la infraestructura tecnológica de la red inalámbrica existente. Este conjunto de pruebas consistió en un ataque con una primera etapa de análisis de vulnerabilidades donde se describe el marco general de trabajo conjunto con el diseño del plan de acción ejecutado, continuando con el descubrimiento, explotación y análisis de vulnerabilidades adicionales en la etapa de ejecución de las pruebas de penetración ejecutadas en múltiples escenarios en la red inalámbrica del Cantón Militar de Popayán, logrando identificar riesgos que pueden afectar la integridad y/o disponibilidad de la información.

La principal diferencia que existe entre un análisis de vulnerabilidades y una prueba de penetración radica en que las pruebas de penetración tienen un alcance más profundo que únicamente identificar vulnerabilidades, y van hacia el proceso de su explotación, escalar privilegios, y mantener el acceso en el sistema evaluado. Mientras que el análisis de vulnerabilidades proporciona una amplia visión de las fallas existentes en los sistemas, pero sin medir su impacto real para los sistemas informáticos en evaluación.

5.1. Evaluación de vulnerabilidades

Mediante una evaluación de vulnerabilidades informáticas se revisaron los controles de seguridad internos y externos de la infraestructura de red inalámbrica para identificar las amenazas que significan un alto riesgo para la información y servicios informáticos del Cantón Militar.

La evaluación de vulnerabilidades proporcionó una amplia visión de los riesgos y amenazas existentes en la red inalámbrica. A continuación, se presenta el proceso ejecutado.

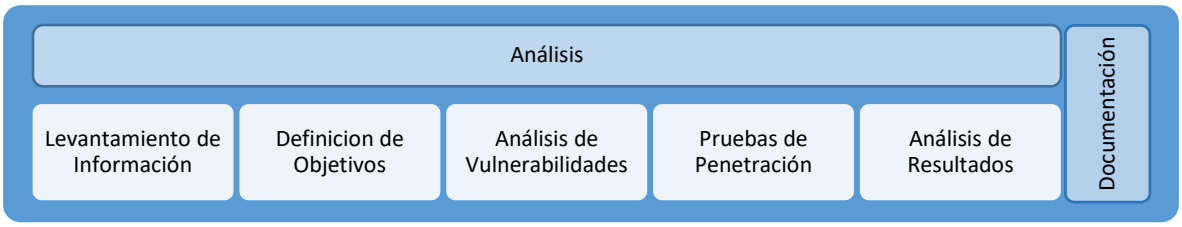


Figura 26. Proceso de evaluación de vulnerabilidades informáticas

5.1.1. Análisis de vulnerabilidades informáticas del Cantón Militar

Se realizó un análisis de vulnerabilidades informáticas a los dispositivos de la infraestructura de red inalámbrica de la institución militar con el fin de identificar vulnerabilidades, amenazas y riesgos en seguridad de la información de aplicaciones y servicios de red soportados. El análisis de vulnerabilidades informáticas permitió identificar, clasificar y reportar vulnerabilidades en la red de datos inalámbrica del Cantón Militar de Popayán que, si llegan a ser explotadas en un ataque informático, pueden comprometer la correcta operación del sistema informático y la corrupción o pérdida de la información crítica de la institución.

Dentro de los resultados se presentan los riesgos potenciales de vulnerabilidades conocidas y catalogadas que incluyen descripción e impacto sobre la institución, recomendaciones, soluciones y sugerencias sobre los problemas de seguridad encontrados. Una vez identificadas vulnerabilidades y amenazas informáticas, se deben determinar los riesgos correspondientes mediante el análisis de cada vulnerabilidad para determinar su probabilidad de ocurrencia e impacto en la infraestructura de red de datos. Para ello se considera, como se observa en la siguiente tabla, las variables probabilidad, impacto e importancia del riesgo.

Tabla 29. Escala de valoración de vulnerabilidades

Parámetro	Valor	Escala	Concepto
Probabilidad	3	Muy probable	Puede suceder una vez al año y ha sucedido anteriormente
	2	Probable	Ha sucedido una sola vez o puede suceder alguna vez
	1	Improbable	No ha sucedido antes pero puede suceder en circunstancias excepcionales
Impacto	3	Alto	Las consecuencias amenazarán objetivos y la estabilidad de la institución
	2	Medio	Las consecuencias generarán cambios significativos en la institución o sus operaciones
	1	Bajo	Las consecuencias pueden solucionarse con cambios y aplicación de políticas
Importancia	10	Alta	Factor muy importante para la institución
	5	Media	Factor de importancia media para la institución
	1	Baja	Factor no importante para la institución

Las vulnerabilidades deben entonces ser valoradas para poder determinar la importancia del riesgo en caso de llegar a ocurrir en la infraestructura de datos de la institución, los riesgos identificados se clasifican de acuerdo con la escala de valoración del riesgo que se muestra en la siguiente tabla.

Tabla 30. Escala de valoración de riesgos

Valoración	Riesgo	Color
0 – 10	Bajo	
11 – 30	Aceptable	
31 – 90	Alto	

Las redes inalámbricas pueden ser atacadas de diferentes maneras debido a que muchas redes inalámbricas se implementan con configuraciones predeterminadas o no cuentan con los dispositivos de seguridad necesarios, siendo posible acceder a ellas simplemente al estar dentro del alcance de la señal con un cliente configurado correctamente, lo cual constituye una vulnerabilidad para la red inalámbrica, pero si a ello se le añade la posibilidad de un eventual ataque en un escenario real con un intruso malicioso potencial real, entonces esta vulnerabilidad se convierte en una amenaza de red.

En la siguiente tabla se consignan las vulnerabilidades de redes inalámbricas más comunes potencialmente ejecutables en la infraestructura de red inalámbrica del Cantón Militar de Popayán.

Tabla 31. Vulnerabilidades de redes inalámbricas

N°	Vulnerabilidad	Descripción del ataque informático	Probabilidad	Impacto	Importancia	Nivel Riesgo
1	Suplantación Punto de Acceso	Simular un punto de acceso inalámbrico real para engañar usuarios y obtener información	2	3	10	60
2	Suplantación ARP	Crear un enlace con un dispositivo intruso para interceptar información	2	2	5	20
3	Negación del servicio	Saturar con peticiones la red inalámbrica para bloquearla mediante pedidos de disociación	3	1	10	30
4	Suplantación MAC	Clonar la dirección física de un usuario autorizado para acceder a la red inalámbrica	1	1	5	5
5	Escáner WLAN	Descubrir redes inalámbricas alcanzables para obtener información de puntos de acceso	2	1	1	2
6	Sniffing	Interceptar tráfico de una red inalámbrica con acceso	1	1	5	5

7	Wardriving	Recorrer una zona en auto para obtener ubicación e información de puntos de acceso inalámbrico	1	1	1	1

5.1.2. Referencia de vulnerabilidades de puertos PVR

La Referencia de vulnerabilidades de puertos PVR (Port Vulnerability Reference) es un listado de puertos lógicos de Internet con sus vulnerabilidades asociadas. Permite identificar y reconocer los diferentes ataques informáticos posibles ante la explotación de puertos lógicos abiertos en los dispositivos de acceso de la infraestructura inalámbrica del Cantón Militar de Popayán, por parte de un intruso malicioso.

Tabla 32. Referencia de vulnerabilidades de puertos PVR

N°	Puerto	Protocolo	Vulnerabilidad	Probabilidad	Impacto	Importancia	Nivel Riesgo
1	21	FTP	Posibilidad sniffer	1	1	1	1
2	22	SSH	Denegación Servicios Ataque Fuerza Bruta Punto de Acceso	2	2	1	4
3	23	Telnet	Ataque Fuerza Bruta Punto de Acceso	1	1	1	1
4	25	STMP	Denegación Servicios Ataque Fuerza Bruta Punto de Acceso Posibilidad sniffer	2	2	5	10
5	43	Ipswitch IMail (Prog)	Denegación Servicios Captura Información Punto de Acceso	3	1	5	15
6	53	DNS	Denegación Servicios	2	3	10	60
7	69	Trivial FTP	Denegación Servicios Punto de Acceso	1	1	1	1
8	80	HTTP	Captura Información	3	2	10	60
9	110	POP3	Denegación Servicios Captura Información Punto de Acceso Posibilidad sniffer	3	2	5	30
10	149	IMAP	Denegación Servicios Ataque Fuerza Bruta Punto de Acceso Captura Información	3	2	5	30
11	505	pbbser (Troyano)	Punto de Acceso Denegación Servicios	1	1	1	1
12	513	Rlogin	Punto de Acceso	1	1	1	1
13	555	Phase Zero (Troyano)	Posibilidad sniffer Punto de Acceso	2	2	10	40
14	1243	SubSeven (Troyano)	Punto de Acceso	2	1	5	10
15	2080	Qbik WinGate (Prog)	Punto de Acceso	2	1	5	10
16	2140	DeepThroat (Troyano)	Denegación Servicios	2	1	5	10

17	3150	DeepThroat (Troyano)	Punto de Acceso	2	1	5	10
18	3389	RDP Terminal Server	Punto de Acceso	1	1	1	1
19	5631	PCAnywhere32 (Prog)	Denegación Servicios	1	1	1	1
20	6000	X Server	Denegación Servicios	1	1	1	1
21	6549	APC PowerChute plus (Prog)	Posibilidad sniffer Punto de Acceso	1	1	1	1
22	6969	GateCrasher (Troyano)	Denegación Servicios	2	1	1	2
23	8080	HTTP	Punto de Acceso	3	2	10	60
24	8181	Ipswitch IMail (Prog)	Denegación Servicios Captura Información Punto de Acceso	2	1	1	2
25	8383	Ipswitch IMail (Prog)	Denegación Servicios	2	1	1	2
26	10067	Portal of Doom (Troyano)	Denegación Servicios	2	1	1	2
27	10167	Portal of Doom (Troyano)	Punto de Acceso	2	1	1	2
28	12345	NetBus (Troyano)	Punto de Acceso	2	1	5	10
29	14238	HotSync Manager (Prog)	Punto de Acceso	2	1	5	10
30	17300	kuang (Troyano)	Desborde de Buffer	2	1	1	2
31	20034	NetBus (Troyano)	Punto de Acceso	2	1	5	10
32	21554	GirlFriend (Troyano)	Punto de Acceso	2	1	1	2
33	23456	EvilFTP (Troyano)	Punto de Acceso	2	1	1	2
34	26092	QIB (Troyano)	Punto de Acceso	2	1	1	2
35	30100	NetSphere (Troyano)	Punto de Acceso	2	1	1	2
36	30102	NetSphere (Troyano)	Punto de Acceso	2	1	1	2
37	31337	Back Oriffice (Troyano)	Punto de Acceso	2	1	5	10
38	31457	Tetrinet (Prog)	Punto de Acceso	2	1	1	2
39	31785	Hack'a'Tack (Troyano)	Denegación Servicios	2	1	5	10
40	31789	Hack'a'Tack (Troyano)	Punto de Acceso	2	1	5	10
41	31791	Hack'a'Tack (Troyano)	Punto de Acceso	2	1	5	10
42	46256	ANTI-prym/h4g1s (Troyano)	Punto de Acceso	2	1	1	2

En el análisis se pudo identificar que la red inalámbrica del Cantón Militar cuenta con 49 vulnerabilidades por cada uno de los 7 puntos de acceso inalámbricos existentes en la red, por lo tanto se tiene un total de 343 vulnerabilidades, cifra importante dado que la mayoría de vulnerabilidades obedecen a la posibilidad de ejecución de código remoto arbitrario, comunicación con cifrado débil y servicios implementados con debilidades serias que afectan la confidencialidad y la integridad de la información y los activos informáticos.

5.2. Pruebas de penetración

Las pruebas de penetración ejecutadas consistieron principalmente en procedimientos aplicados para explotar vulnerabilidades que lograron esquivar o anular características de seguridad de los componentes de la red inalámbrica del Cantón Militar. Las pruebas de penetración son un proceso manual que incluyeron el uso de analizadores de vulnerabilidades y cuyo resultado es un informe completo y detallado sobre el estado de la seguridad de la red de datos evaluada.

Dentro de los resultados de la prueba de penetración ejecutada en la infraestructura de red inalámbrica del Cantón Militar de Popayán se obtuvo la descripción de cada vulnerabilidad identificada o problema potencial descubierto, incluyendo riesgos que dicha vulnerabilidad pudiere generar en la red inalámbrica de la división militar y los métodos en puede ser explotada por un posible intruso malicioso ante un eventual ataque informático.

5.2.1. Alcance de las pruebas de penetración

Se estableció el alcance de las pruebas de seguridad informática para la red inalámbrica del Cantón Militar, clasificadas por los tipos de riesgos de atacantes informáticos.

En conjunto con el personal encargado del área de sistemas de la Tercera División del Cantón Militar de Popayán se define el alcance de las pruebas de penetración a ejecutarse para evaluar el nivel de seguridad de la infraestructura de red inalámbrica y se consigna a continuación.

- Las pruebas de seguridad serán ejecutadas únicamente en el Cantón Militar de Popayán - Tercera División como fue autorizado, no podrán realizarse desde ninguna otra unidad militar.
- No se interrumpirá el servicio de red inalámbrica a los usuarios del Cantón Militar durante la ejecución de las pruebas de penetración, ni de ningún otro servicio informático.
- No se modificarán los parámetros de configuración de los dispositivos de la red inalámbrica del Cantón Militar ni de autenticación de los usuarios del Ejército para navegar en Internet.
- No se afectará ni se modificarán los parámetros de configuración de ningún dispositivo de toda la infraestructura de la red de datos del Ejército Nacional de Colombia.
- Se permite el uso de herramientas de hackeo informático ético que no violen las políticas de seguridad del Ejército Nacional de Colombia en cuanto al tratamiento de la información encontrada, la cual es considerada de orden clasificado y restringido, es decir, que no expongan públicamente ningún tipo de información o datos que pueda comprometer la seguridad de la información desde el Cantón Militar de Popayán.
- Se restringen las pruebas de penetración informática únicamente a los puntos de acceso de la red inalámbrica del Cantón Militar de Popayán, no se autorizan pruebas de penetración contra las terminales, dispositivos de interconexión ni ningún otro activo de red diferente, por cuánto estás labores están restringidas y autorizadas únicamente al personal militar que labora en el área de seguridad informática en la institución, por protocolos de seguridad

de contrainteligencia militar interna de la red del Ejército Nacional de Colombia.

- Se debe suspender inmediatamente las pruebas de penetración si se logra acceder al área de almacenamiento SAN con los servidores que contienen información militar confidencial y de acceso restringido en la ciudad de Bogotá.

5.2.1.1. Pruebas de penetración externa

Consiste en la evaluación externa del entorno de seguridad de la red inalámbrica desde la perspectiva de un atacante que ronda el perímetro externo del Cantón Militar de Popayán para acceder a la red inalámbrica, pero sin ingresar físicamente a la sede del Cantón.

5.2.1.2. Pruebas de penetración interna

Es la evaluación interna de la seguridad de la infraestructura de red inalámbrica del Cantón desde la perspectiva de posible personal del Ejército infiltrado o un intruso que ha conseguido obtener acceso desde el interior del Cantón Militar. Esta prueba cubre el perímetro interno de cualquier segmento de la red inalámbrica y permite identificar el riesgo de un ataque interno.

5.2.2. Definición de objetivos de las pruebas de penetración

En cuanto a los objetivos que se definieron para la prueba de penetración de la red inalámbrica del Cantón Militar de Popayán de acuerdo con el alcance pactado conjunto con el personal de sistemas del Ejército Nacional de Colombia, se plantearon los siguientes:

- Escaneo de la señal de red inalámbrica.
- Obtención de la dirección física del punto de acceso inalámbrico.
- Obtención de las credenciales de autenticación en la red inalámbrica.
- Escaneo de activos de la infraestructura inalámbrica de la Tercera División del Cantón Militar de Popayán.
- Escaneo de puertos en las terminales de la red inalámbrica para análisis de vulnerabilidades.

5.2.3. Clasificación de pruebas de penetración

Se ejecutaron básicamente tres tipos de pruebas de penetración para ataques éticos, que se pueden aplicar a un sistema informático para evaluar la seguridad de su red inalámbrica de datos.

- **Pruebas de penetración de caja negra:** En esta prueba se simuló desconocer cualquier tipo de información sobre la red inalámbrica del Cantón Militar, no se tuvo en cuenta ningún tipo de conocimiento o información previa sobre la red inalámbrica del Ejercito, simulando un ataque externo realizado por un intruso que intenta irrumpir en la red de datos vía inalámbrica y solo conoce la dirección de dominio del Ejército.

- **Pruebas de penetración de caja gris:** En esta prueba se tuvo en cuenta información parcial del entorno de red inalámbrica antes de iniciar la prueba. Se tuvo acceso a la red inalámbrica desde el interior del Cantón. Esta prueba entregó mejores resultados que la prueba de caja negra debido a que la información previamente suministrada evitó requerir más tiempo y recursos para su ejecución. Esta prueba simuló un ataque realizado por un miembro interno o intruso al interior del Cantón Militar.

- **Pruebas de penetración de caja blanca:** En esta prueba se tuvo en cuenta información completa sobre la infraestructura de red inalámbrica, ejecutándose con conocimiento en detalle sobre su diseño e implementación, con diagramas e información sobre el hardware y software antes de realizar la evaluación, y acceso interno a la red, acelerándose el proceso y obteniéndose resultados más precisos, dado que se enfocó la prueba contra dispositivos previamente identificados, evitando invertir tiempo en su reconocimiento. Esta prueba simuló una situación donde el atacante puede tener conocimiento completo de la infraestructura de red de datos interna de la institución militar.

5.2.4. Aplicación del Marco de pruebas de penetración PTF

Dentro de la metodología Penetration Testing Framework - PTF existe el capítulo *Penetración inalámbrica,* que trata de las pruebas de seguridad para infraestructura de red inalámbrica

Evaluación inalámbrica: La siguiente información describe el proceso que se ejecutó para realizar la evaluación de la seguridad de la red inalámbrica del Ejército, obteniendo una imagen clara y concisa del estado de la infraestructura de red inalámbrica del Cantón Militar de Popayán.

Tabla 33. Marco PTF – Marco de pruebas de penetración de redes inalámbricas

Marco PTF – Marco de pruebas de penetración		
Mapa del sitio	Mapa de RF	Cobertura de señal
	Mapa físico	Triangulación de puntos de acceso Imágenes de satélite
	Filtro MAC	Dirección MAC del punto de acceso

Mapa de red	Claves de cifrado	WPA/ PSK	AES	Clave acceso
		802.1x		
	Puntos de acceso	ESSID	ESSIDs de difusión	Redes inalámbricas con AP
		BSSIDs	Vendedor Canal Asociaciones Actividad AP rogue	Redes inalámbricas ad-hoc
	Clientes inalámbricos	Direcciones MAC	Vendedor	
		Tráfico interceptado	Cifrado	

5.3. Resultados de las pruebas de penetración

Se presentan los resultados de las pruebas de penetración ejecutadas en la infraestructura de red inalámbrica del Cantón Militar de Popayán que permitieron evaluar el nivel de seguridad de los sistemas de información militares, así como el esquema de acceso de usuarios del Ejército Nacional al servicio de red inalámbrica bajo el Marco de pruebas de penetración PTF.

5.3.1. Mapa del sitio

El mapa del sitio se compone del mapa de radiofrecuencia de la señal inalámbrica y el mapa físico de la infraestructura de red inalámbrica de la institución militar.

4.3.1.1 Mapa de Radiofrecuencias con direccionamiento MAC

El mapa de radiofrecuencia de la señal inalámbrica del Cantón Militar de Popayán se observa en la siguiente gráfica. En ella se puede apreciar el identificador básico del conjunto de servicios de cada red alcanzable desde la Tercera División, el cual es el primer objetivo a obtener por un intruso malicioso en un escaneo inalámbrico para un ataque informático a los puntos de acceso de infraestructura.

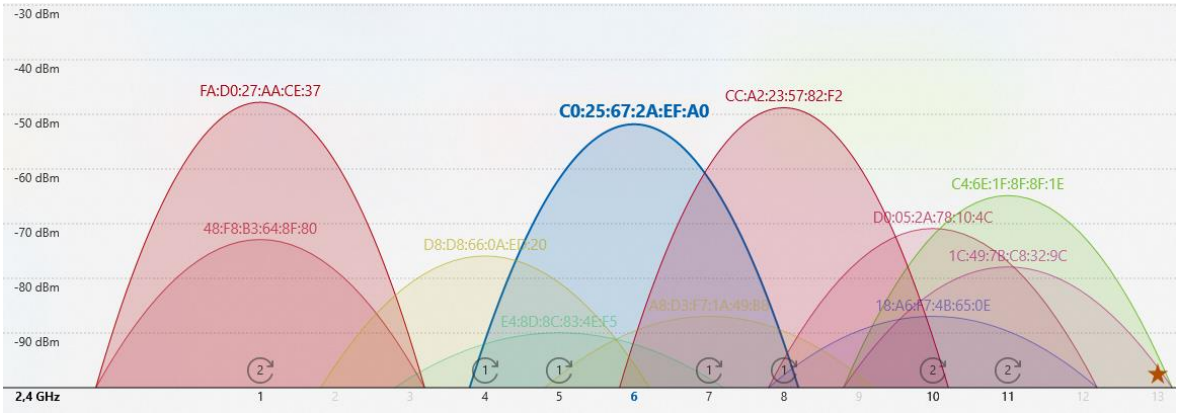


Figura 27. Mapa de radiofrecuencias de la red inalámbrica del Cantón Militar de Popayán

4.3.1.2 Mapa físico

Se presenta a continuación el mapa físico del Cantón Militar de Popayán con la triangulación de los puntos de acceso que componen la infraestructura de red inalámbrica representado mediante una imagen satelital.

Figura 28. Triangulación de puntos de acceso red inalámbrica del Cantón Militar de Popayán

5.3.2. Obtención de la contraseña del punto de acceso inalámbrico

Para realizar la prueba de penetración en la infraestructura de red inalámbrica del Cantón Militar de Popayán se utilizó una terminal con sistema operativo Kali-Linux versión 2.0, el cual posee diferentes herramientas para ataques inalámbricos. Kali Linux es una distribución Debian Linux especializada en ciberseguridad para pruebas de penetración y detección de vulnerabilidades en redes de datos.

Kali Linux es la versión actualizada y optimizada de la distribución BackTrack 5, la cual fuere bastante utilizada en ciberseguridad inalámbrica. Para iniciar el ataque de fuerza bruta a la red inalámbrica se debe elegir en el menú principal la opción "*Aplicaciones*", posteriormente se selecciona la opción "*Ataques Inalámbricos*" y luego se escoge la aplicación a utilizar. Para el desarrollo del ejercicio de captura de la contraseña de la red inalámbrica del Cantón Militar de Popayán se utilizó la aplicación *Fern Wifi Cracker*. Esta es una aplicación de auditoría seguridad inalámbrica capaz de descifrar y recuperar claves WEP, WPA y WPS de la red.

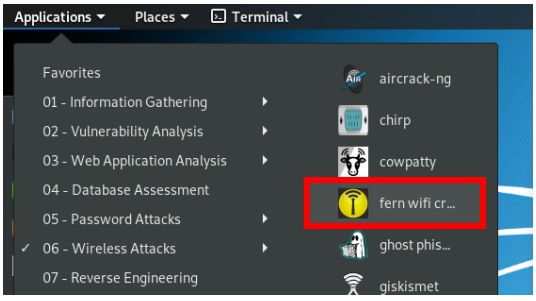


Figura 29. Aplicación Fern Wifi Cracker de Kali Linux

Primero se debe seleccionar la interfaz de red inalámbrica para realizar el ataque, como se muestra a continuación, en donde se escoge la interfaz *wlan0* correspondiente a la antena inalámbrica pero en modo monitor, para escanear el medio para detectar las redes inalámbricas disponibles, por ende es *wlan0mon*.

Figura 30. Selección de interfaz de red para ataque en Fern WiFi Cracker

Se activa la "*Búsqueda de puntos de acceso*" y se activan las opciones WIFI WEP o WPA como se observa a continuación, se selecciona en este caso WPA:

Figura 31. Escaneo e identificación de redes activo para ataque en Fern WiFi Cracker

Posteriormente se selecciona el nombre del conjunto de red inalámbrica de la Tercera División del Cantón Militar de Popayán, cuya denominación es **BAMHE4**, y la aplicación obtiene su direccionamiento MAC como se puede apreciar en la siguiente gráfica. De igual manera se selecciona la opción "*ataque regular*" la cual

corresponde a un ataque de diccionario por contraseña, se selecciona el archivo de diccionario que se utilizará para el ataque, en este caso se utilizó el diccionario *rockyou.txt*, y se procede a ejecutar el ataque de manera automática.

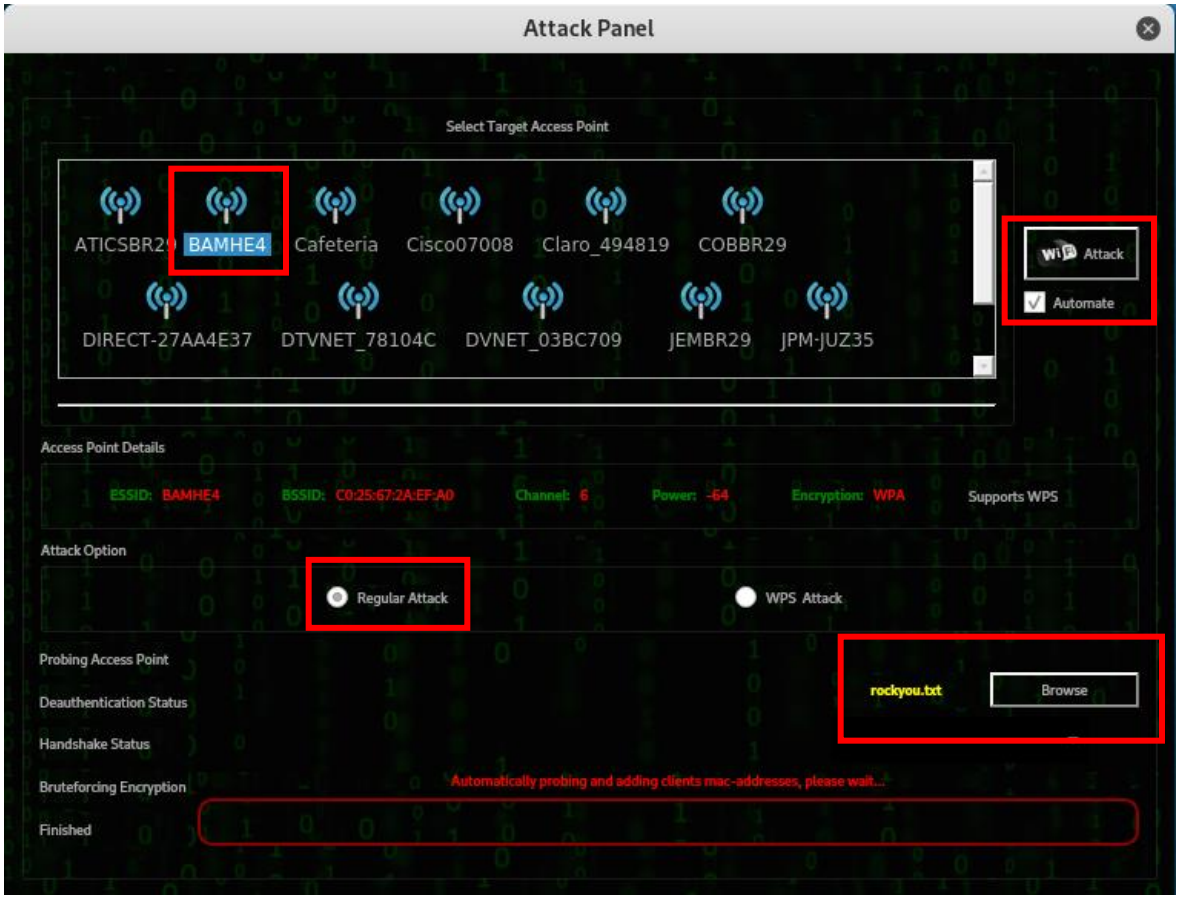


Figura 32. Red inalámbrica identificada en ataque Fern WiFi Cracker

El Ataque que realiza la aplicación *Fern Wifi Cracker* consiste en desautenticar una terminal de un cliente conectado a la red inalámbrica objetivo para forzarlo a autenticarse nuevamente y obligarlo a reenviar la contraseña de la red al punto de acceso inalámbrico, acto que es aprovechado por la aplicación para capturar el handshake[11] de la red inalámbrica y proceder a descifrar la contraseña de acceso a la red. La aplicación encontró un cliente para desautenticar en la red inalámbrica de la Tercera División del Cantón Militar como se observa en la siguiente imagen.

[11] Negociación entre cliente y punto de acceso inalámbrico para establecer conexión mediante una serie de parámetros, entre ellos la contraseña cifrada de la red inalámbrica.

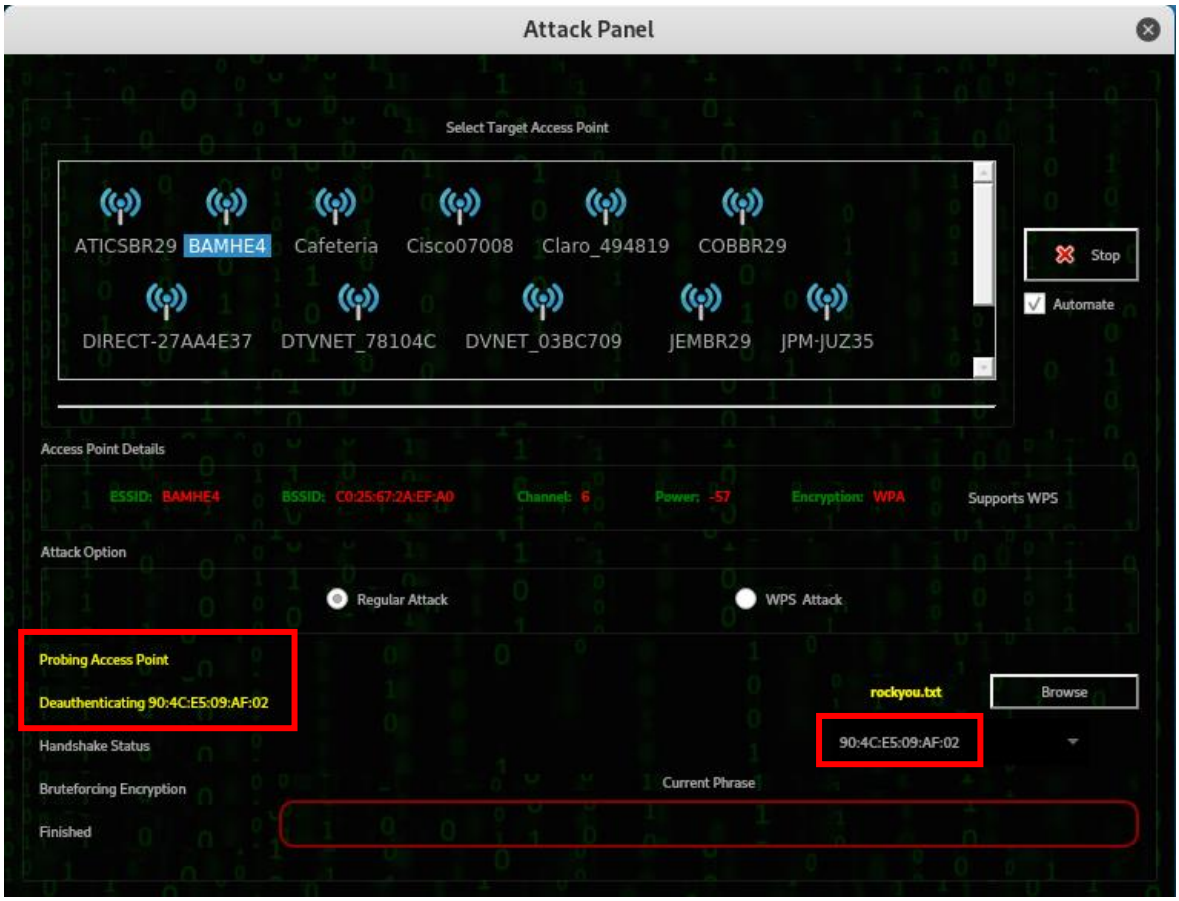


Figura 33. Desautenticación de terminal en ataque en Fern WiFi Cracker

Una vez que ocurre la reautenticación de la terminal del usuario, es decir, el reenvío de las credenciales de acceso de la terminal al punto de acceso, y la aplicación Fern WiFi Cracker captura el handshake de la red inalámbrica, comienza el ataque de diccionario para tratar de descifrar finalmente la contraseña de la red inalámbrica en texto plano como se puede observar en la siguiente imagen, para posibilitar un ataque informático por parte de un intruso malicioso.

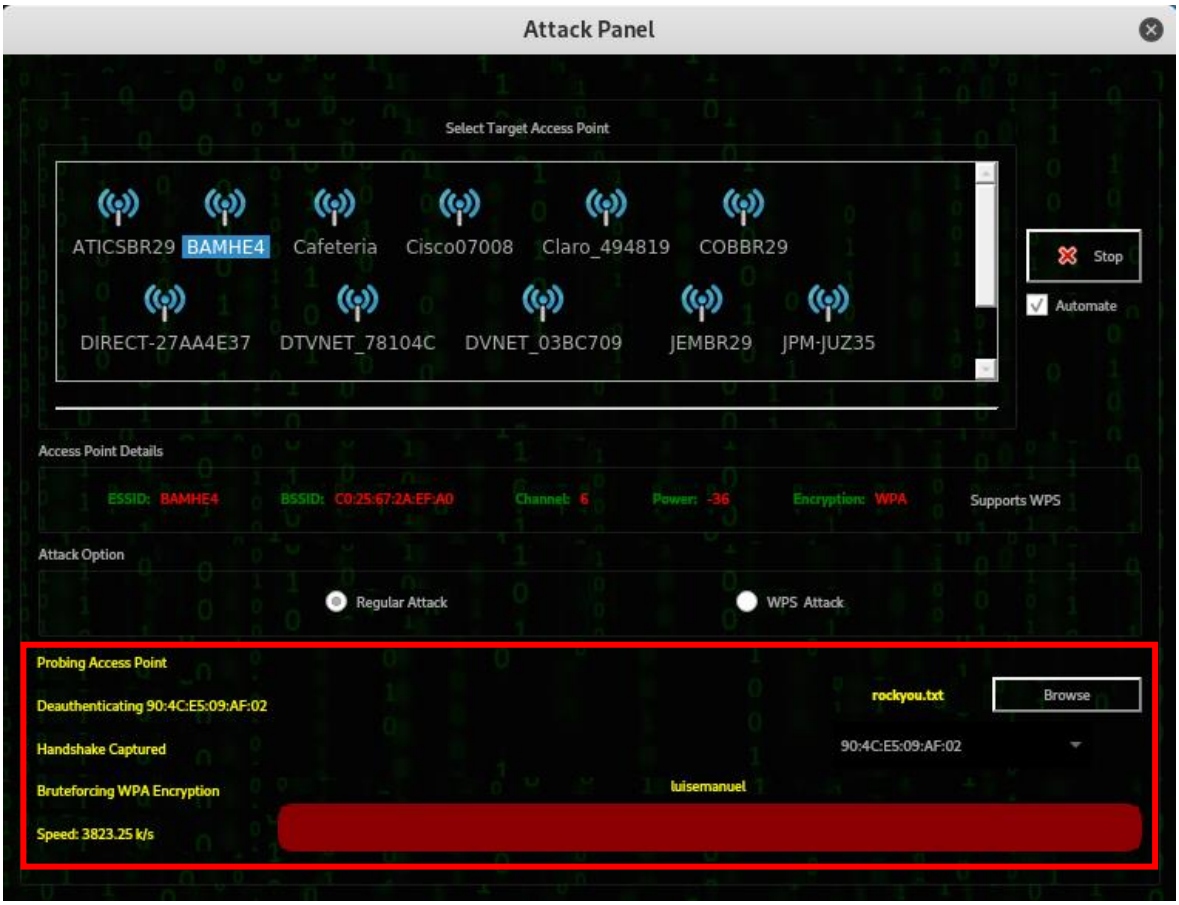


Figura 34. Descifrado del handshake de red en ataque Fern WiFi Cracker

Con el ataque de diccionario se logra finalmente la obtención de la contraseña WPA de la red inalámbrica con protocolo Wi-Fi del Cantón Militar de Popayán, la cual es ***jkxw9759*** como se puede apreciar en la gráfica mostrada a continuación.

Se puede observar que la contraseña no contiene letras mayúsculas y minúsculas combinadas, ni tampoco contiene caracteres especiales, solo contiene letras minúscula y números, además de ser bastante corta, solo tiene 8 caracteres. Obtener acceso no autorizado forzando la autenticación en puntos acceso inalámbrico que utilizan contraseñas que no combinan letras mayúsculas, minúsculas, caracteres especiales y números es más sencillo para un atacante, basta con realizar un ataque de fuerza bruta debido a las pocas probabilidades de contraseñas posibles, máxime si son tan cortas.

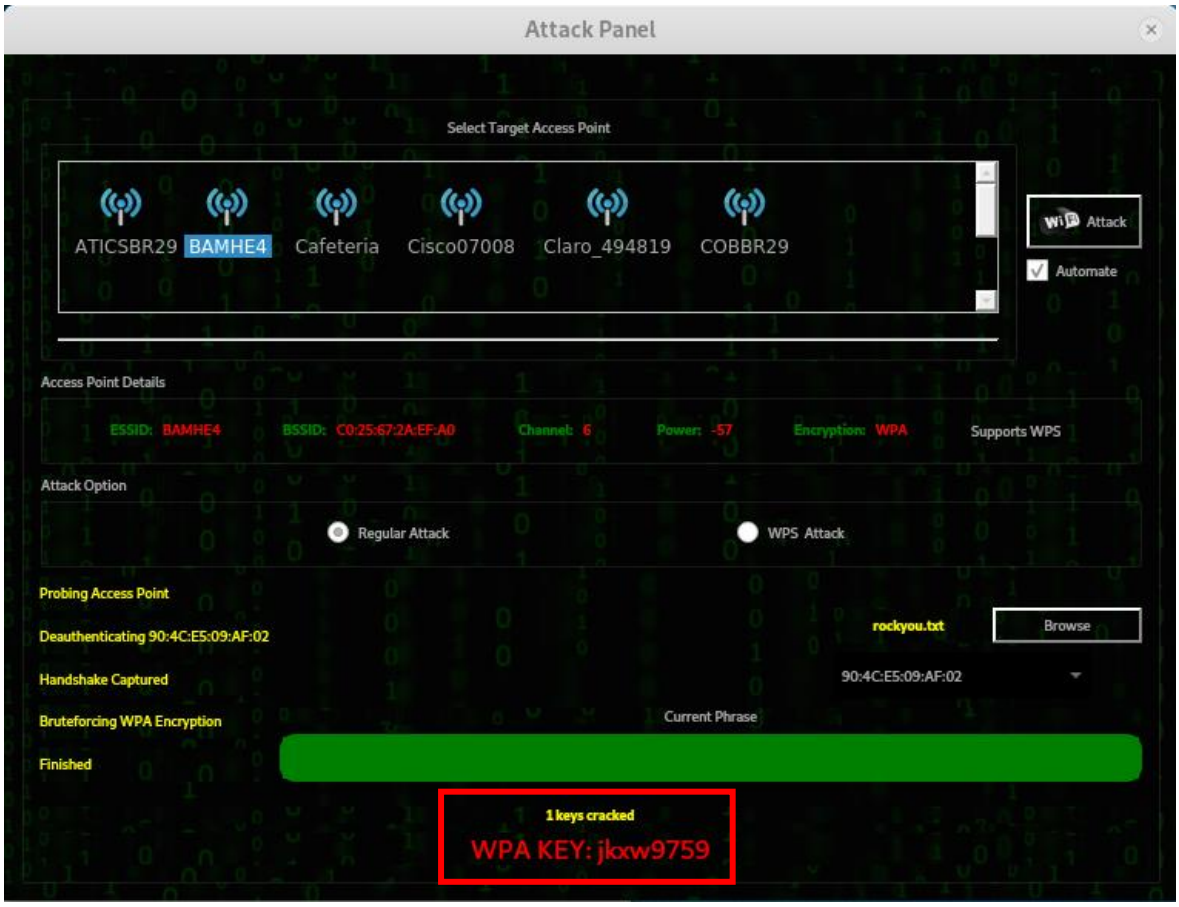


Figura 35. Contraseña descifrada en ataque Fern WiFi Cracker

5.3.3. Escaneo de activos desde la infraestructura de red inalámbrica

Una vez obtenida la contraseña de la red inalámbrica, se realizó el escaneo de activos desde la red inalámbrica de la Tercera División del Cantón Militar de Popayán, con el fin de identificar todos los elementos que componen la infraestructura de red de datos y poder detectar posibles vectores ante un eventual ataque informático que pudiere realizar un intruso malicioso que busque afectar la confidencialidad, integridad y disponibilidad de la información militar que transita a través de la red inalámbrica. De esta manera se posibilita recomendar medidas de gestión contra actividades maliciosas o de identificación y neutralización estratégica de intrusos internos o externos que pretendan atacar los sistemas de información militar mediante la explotación de las estructuras de comunicación militares, canales lógicos, señales, protocolos y herramientas de penetración, determinándose el curso de acción para su gestión.

Se realizó entonces el descubrimiento de los activos que componen la red de datos de las divisiones del Ejército, hecho que permite identificar rápidamente un posible intruso malicioso o un ataque de suplantación de identidad con un punto de acceso no autorizado y evitar un ataque informático mediante la exploración de la red inalámbrica con la aplicación *Netdiscover* de Kali Linux.

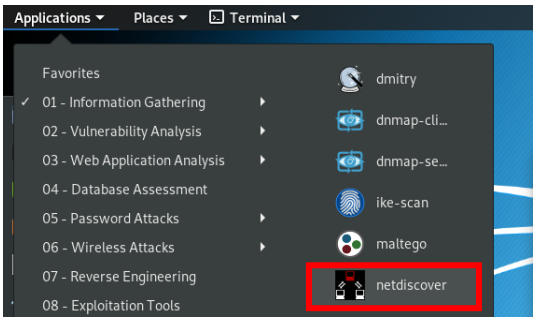


Figura 36. Aplicación Netdiscover de Kali Linux

La aplicación se ejecuta con el comando *netdiscover -r dir_IP_punto_acceso* como se puede apreciar en la siguiente imagen. Para este caso el comando es:

netdiscover -r 172.23.66.194

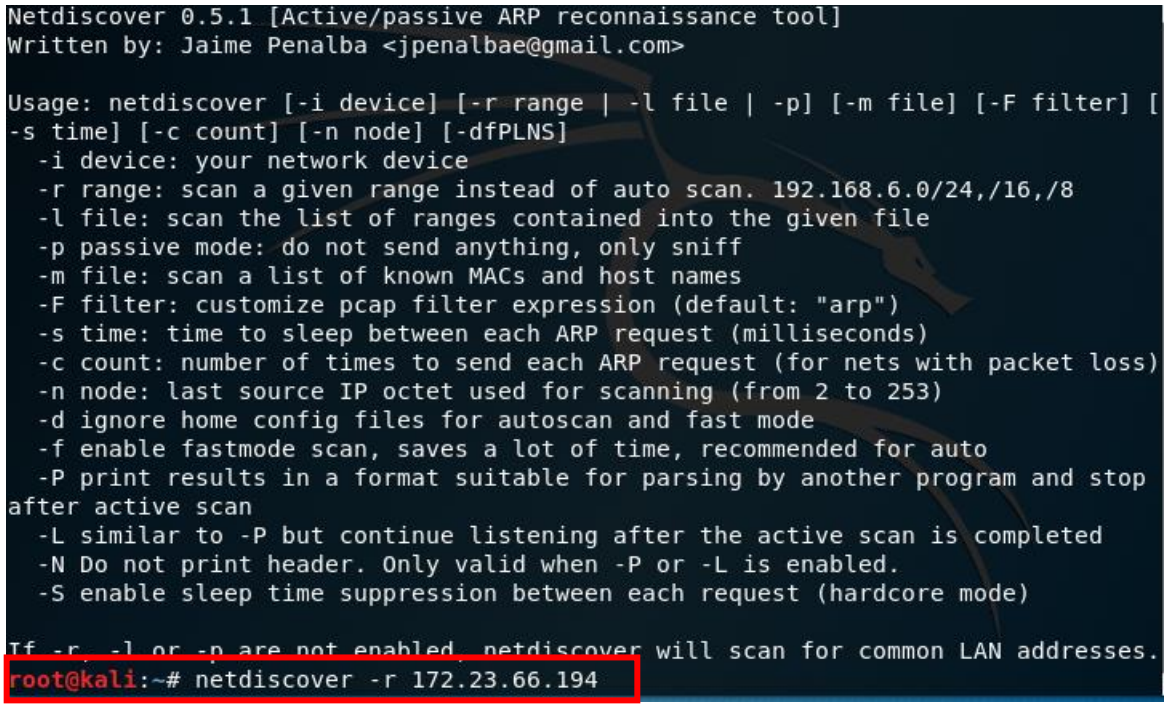
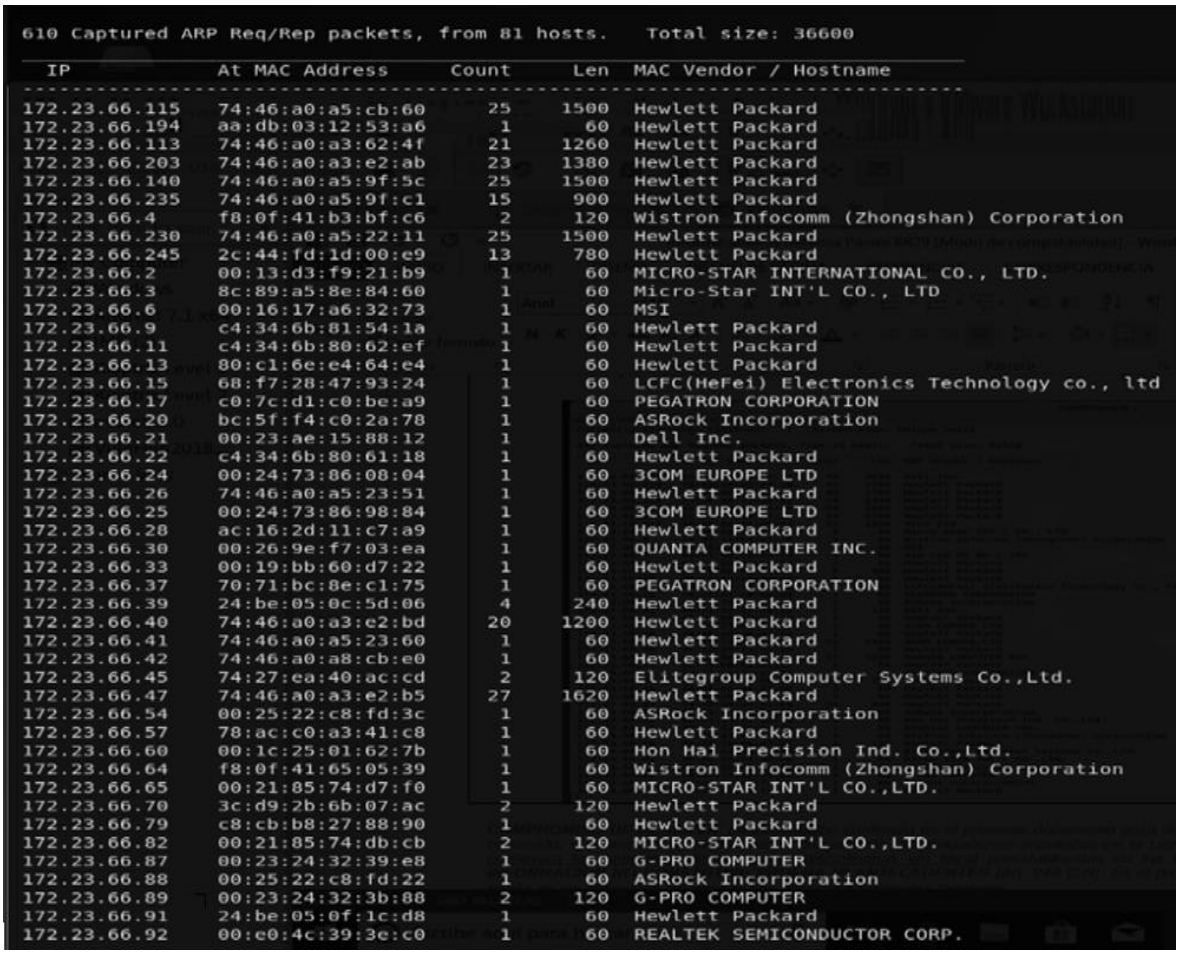


Figura 37. Comando de ejecución aplicación Netdiscover de Kali Linux

Como resultado del escaneo realizado en la red inalámbrica de la Tercer División del Cantón Militar de Popayán se detectaron 81 activos informáticos conectados a la red del Ejército Nacional de Colombia como se puede apreciar en la siguiente imagen.



610 Captured ARP Req/Rep packets, from 81 hosts. Total size: 36600

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
172.23.66.115	74:46:a0:a5:cb:60	25	1500	Hewlett Packard
172.23.66.194	aa:db:03:12:53:a6	1	60	Hewlett Packard
172.23.66.113	74:46:a0:a3:62:4f	21	1260	Hewlett Packard
172.23.66.203	74:46:a0:a3:e2:ab	23	1380	Hewlett Packard
172.23.66.140	74:46:a0:a5:9f:5c	25	1500	Hewlett Packard
172.23.66.235	74:46:a0:a5:9f:c1	15	900	Hewlett Packard
172.23.66.4	f8:0f:41:b3:bf:c6	2	120	Wistron Infocomm (Zhongshan) Corporation
172.23.66.230	74:46:a0:a5:22:11	25	1500	Hewlett Packard
172.23.66.245	2c:44:fd:1d:00:e9	13	780	Hewlett Packard
172.23.66.2	00:13:d3:f9:21:b9	1	60	MICRO-STAR INTERNATIONAL CO., LTD.
172.23.66.3	8c:89:a5:8e:84:60	1	60	Micro-Star INT'L CO., LTD
172.23.66.6	00:16:17:a6:32:73	1	60	MSI
172.23.66.9	c4:34:6b:81:54:1a	1	60	Hewlett Packard
172.23.66.11	c4:34:6b:80:62:ef	1	60	Hewlett Packard
172.23.66.13	80:c1:6e:e4:64:e4	1	60	Hewlett Packard
172.23.66.15	68:f7:28:47:93:24	1	60	LCFC(HeFei) Electronics Technology co., ltd
172.23.66.17	c0:7c:d1:c0:be:a9	1	60	PEGATRON CORPORATION
172.23.66.20	bc:5f:f4:c0:2a:78	1	60	ASRock Incorporation
172.23.66.21	00:23:ae:15:88:12	1	60	Dell Inc.
172.23.66.22	c4:34:6b:80:61:18	1	60	Hewlett Packard
172.23.66.24	00:24:73:86:08:04	1	60	3COM EUROPE LTD
172.23.66.26	74:46:a0:a5:23:51	1	60	Hewlett Packard
172.23.66.25	00:24:73:86:98:84	1	60	3COM EUROPE LTD
172.23.66.28	ac:16:2d:11:c7:a9	1	60	Hewlett Packard
172.23.66.30	00:26:9e:f7:03:ea	1	60	QUANTA COMPUTER INC.
172.23.66.33	00:19:bb:60:d7:22	1	60	Hewlett Packard
172.23.66.37	70:71:bc:8e:c1:75	1	60	PEGATRON CORPORATION
172.23.66.39	24:be:05:0c:5d:06	4	240	Hewlett Packard
172.23.66.40	74:46:a0:a3:e2:bd	20	1200	Hewlett Packard
172.23.66.41	74:46:a0:a5:23:60	1	60	Hewlett Packard
172.23.66.42	74:46:a0:a8:cb:e0	1	60	Hewlett Packard
172.23.66.45	74:27:ea:40:ac:cd	2	120	Elitegroup Computer Systems Co.,Ltd.
172.23.66.47	74:46:a0:a3:e2:b5	27	1620	Hewlett Packard
172.23.66.54	00:25:22:c8:fd:3c	1	60	ASRock Incorporation
172.23.66.57	78:ac:c0:a3:41:c8	1	60	Hewlett Packard
172.23.66.60	00:1c:25:01:62:7b	1	60	Hon Hai Precision Ind. Co.,Ltd.
172.23.66.64	f8:0f:41:65:05:39	1	60	Wistron Infocomm (Zhongshan) Corporation
172.23.66.65	00:21:85:74:d7:f0	1	60	MICRO-STAR INT'L CO.,LTD.
172.23.66.70	3c:d9:2b:6b:07:ac	2	120	Hewlett Packard
172.23.66.79	c8:cb:b8:27:88:90	1	60	Hewlett Packard
172.23.66.82	00:21:85:74:db:cb	2	120	MICRO-STAR INT'L CO.,LTD.
172.23.66.87	00:23:24:32:39:e8	1	60	G-PRO COMPUTER
172.23.66.88	00:25:22:c8:fd:22	1	60	ASRock Incorporation
172.23.66.89	00:23:24:32:3b:88	2	120	G-PRO COMPUTER
172.23.66.91	24:be:05:0f:1c:d8	1	60	Hewlett Packard
172.23.66.92	00:e0:4c:39:3e:c0	1	60	REALTEK SEMICONDUCTOR CORP.

Figura 38. Escaneo de activos de red del Cantón Militar de Popayán

En la gráfica anterior se puede apreciar que se detectaron algunos dispositivos conectados a la red pero que no pertenecen a los activos informáticos de la unidad militar del Ejército. Esta situación se presenta por un acceso autorizado indebido de dispositivos en la red, ya que existen varios usuarios que se encuentran en el Cantón Militar compartiendo la misma red inalámbrica que el personal operativo del Ejército, inclusive los edificios donde viven los familiares de los militares. Esto incrementa tanto la superficie de ataque como el rango de explotación que puede existir ante un eventual ataque por una intrusión interna debido a la exposición de la red al alcance de una mayor población atacante posible.

Se sugirió segmentar la red inalámbrica en segmentos de red virtuales VLANs, habilitando un segmento VLAN restringido solo para los familiares de los militares, que les permita navegar en Internet únicamente, pero que tenga máxima restricción en cuanto al acceso de la información militar confidencial del Cantón Militar. El esquema de solución propuesta se puede apreciar más adelante en este documento en la sección *Segmentos de red virtuales por brigadas del Ejército.*

5.3.4. Escaneo de puertos lógicos de terminales desde la red inalámbrica

Se realizó el escaneo de puertos lógicos abiertos de terminales desde la red inalámbrica del Cantón Militar de Popayán. Aunque tener puertos abiertos no necesariamente representa un riesgo o una amenaza en sí, es importante conocer cuales tienen demasiados puertos lógicos abiertos, para identificar cuales protocolos y/o aplicaciones innecesarias no deberían estar abiertos en las terminales y dispositivos de acceso e interconexión de red, y de esta manera poder analizar si existen vulnerabilidades o intrusiones en la red de datos a través de ellos.

Durante el escaneo de puertos lógicos ejecutado se detectaron diferentes terminales o elementos conectados a la red inalámbrica con múltiples puertos abiertos, los cuales, en la gráfica, son nodos representados con círculos de colores, de los cuales los nodos rojos tienen cada uno más de 6 puertos lógicos abiertos, los nodos amarillos de 3 a 6 puertos lógicos abiertos y los nodos verdes tienen 3 o menos puertos lógicos abiertos.

Tabla 34. Clasificación de puertos herramienta de escaneo Zenmap

Color círculo	Puertos abiertos	Color
Rojo	Más de 6	
Amarillo	3 a 6	
Verde	Menos de 3	

Para la ejecución del escaneo de puertos lógicos se utilizó la aplicación *Zenmap d*e Kali Linux, aplicación para descubrimiento y auditoría de seguridad en redes de datos que permite realizar inventario de la red y supervisión de servicios o terminales. Zenmap básicamente utiliza paquetes de datos sin procesar para identificar terminales conectadas en la red, qué servicios están ofreciendo estas terminales, qué sistemas operativos están ejecutando y qué tipo de dispositivos de seguridad están en uso.

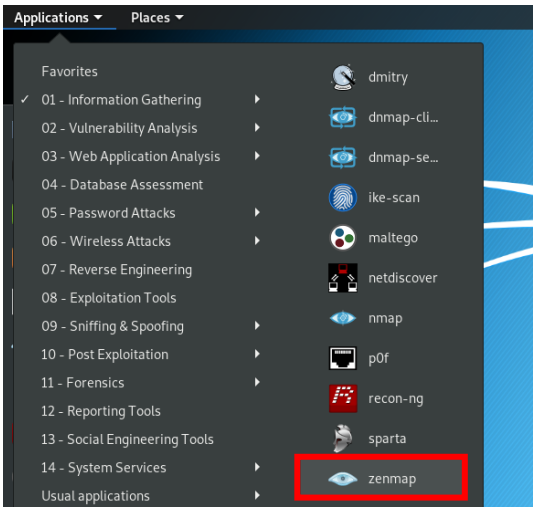


Figura 39. Aplicación Zenmap de Kali Linux

Para realizar el escaneo de puertos lógicos se debe ingresar el rango de direccionamiento de red objetivo, en este caso de la dirección 172.23.66.1 a la 172.23.66.254, y luego se procede a ejecutar el escaneo para detectar los puertos abiertos de cada terminal conectado a la red inalámbrica, como se observa en la gráfica siguiente.

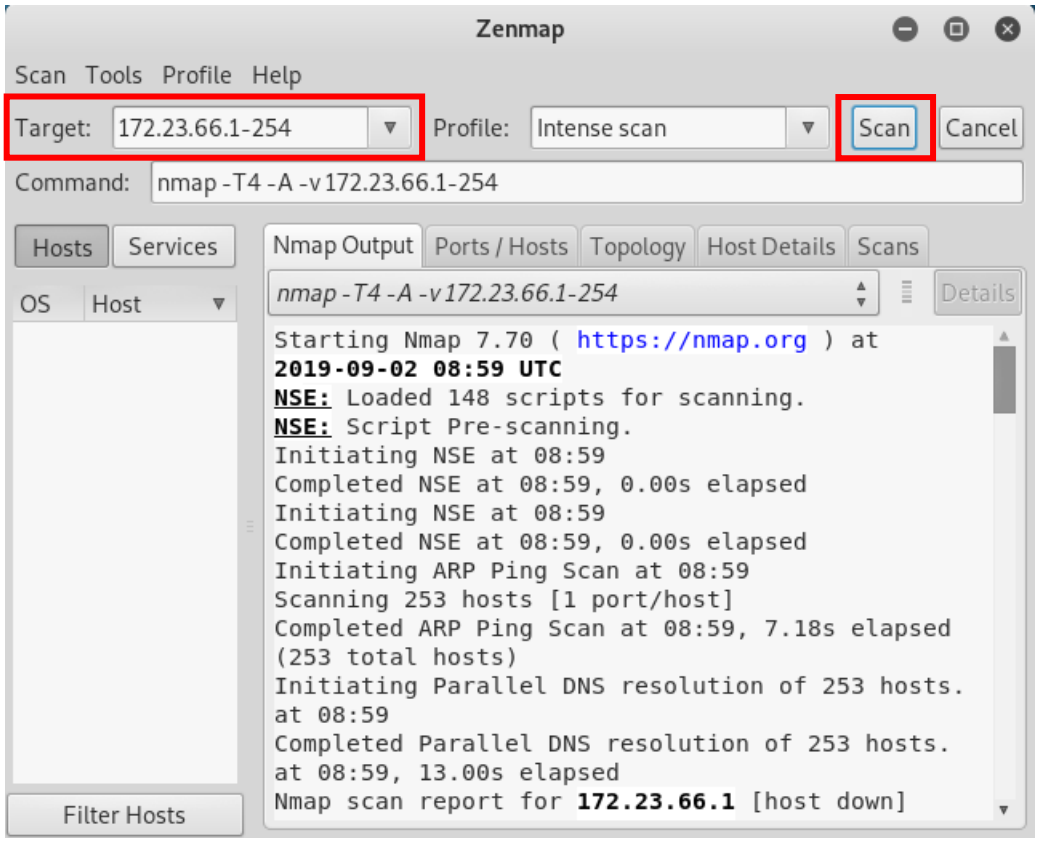


Figura 40. Escaneo de puertos con aplicación Zenmap

Los resultados del escaneo de puertos lógicos realizado en las terminales de usuarios del Ejército Nacional con acceso a la infraestructura de red inalámbrica de la Tercera División del Cantón Militar de Popayán se pueden apreciar en la siguiente gráfica.

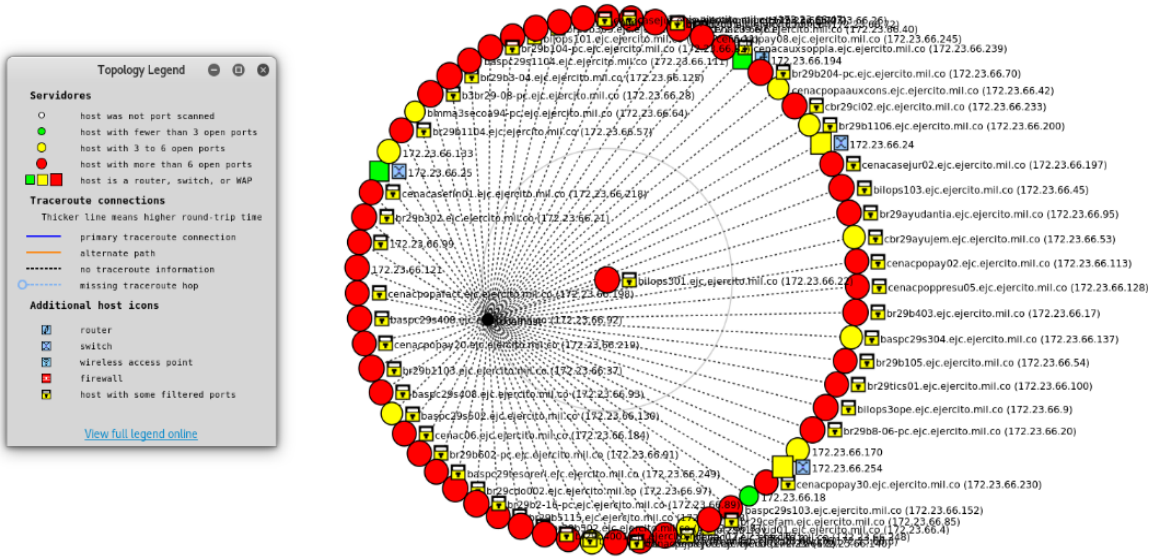


Figura 41. Escaneo de puertos lógicos con la aplicación Zenmap

En la gráfica de resultados se puede observar que casi todas las terminales conectadas a la red inalámbrica de la Tercera División del Cantón Militar de Popayán se encuentran en un nivel crítico de vulnerabilidad ante un eventual ataque informático por parte de un intruso malicioso, debido a que tienen más de 6puertos lógicos abiertos, incrementando la posibilidad de éxito del atacante al tener múltiples posibilidades para lograr el acceso no autorizado. Se detectaron 81 terminales o estaciones de trabajo de los cuales 66 son vulnerables a ataques remotos que pueden desencadenar un incidente de seguridad.

5.3.5. Interceptación de tráfico desde la red inalámbrica

Para realizar la interceptación de tráfico de información militar desde la red inalámbrica de la Tercera División del Cantón Militar de Popayán se utilizó la aplicación *Wireshark* de Kali Linux, la cual es un analizador de protocolos que permite capturar tráfico fluyente por una red de datos y analizar la información capturada por cada paquete.

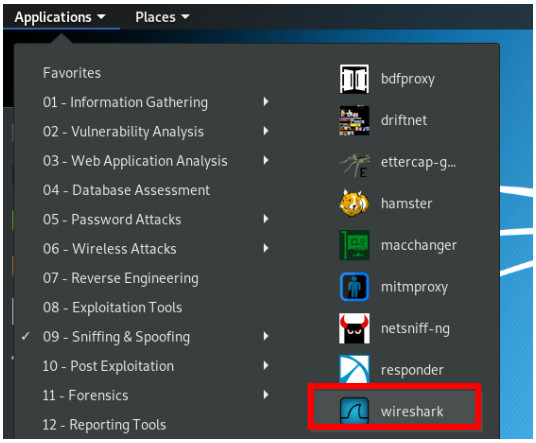


Figura 42. Aplicación Wireshark de Kali Linux

Para corroborar que se capturaron paquetes de datos con información dirigida y proveniente de los servidores militares, se realizó un ping a la dirección web del Ejército Nacional de Colombia *www.ejército.mil.co* como se puede apreciar en la siguiente gráfica, en donde la dirección de red de destino resuelta por el comando es la 45.183.247.140.

```
C:\Users\Home>ping www.ejercito.mil.co

Haciendo ping a ejercito.mil.co [45.183.247.140] con 32 bytes de datos:
Respuesta desde 45.183.247.140: bytes=32 tiempo=51ms TTL=52
Respuesta desde 45.183.247.140: bytes=32 tiempo=37ms TTL=52
Respuesta desde 45.183.247.140: bytes=32 tiempo=57ms TTL=52
Respuesta desde 45.183.247.140: bytes=32 tiempo=60ms TTL=52

Estadísticas de ping para 45.183.247.140:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 37ms, Máximo = 60ms, Media = 51ms
```

Figura 43. Dirección de red de los servidores militares

En la siguiente gráfica se presentan los resultados de la información capturada, en donde se puede observar que se logró interceptar datos enviados y recibidos de los servidores principales del Ejército Nacional de Colombia desde la Tercera División del Cantón Militar de Popayán.

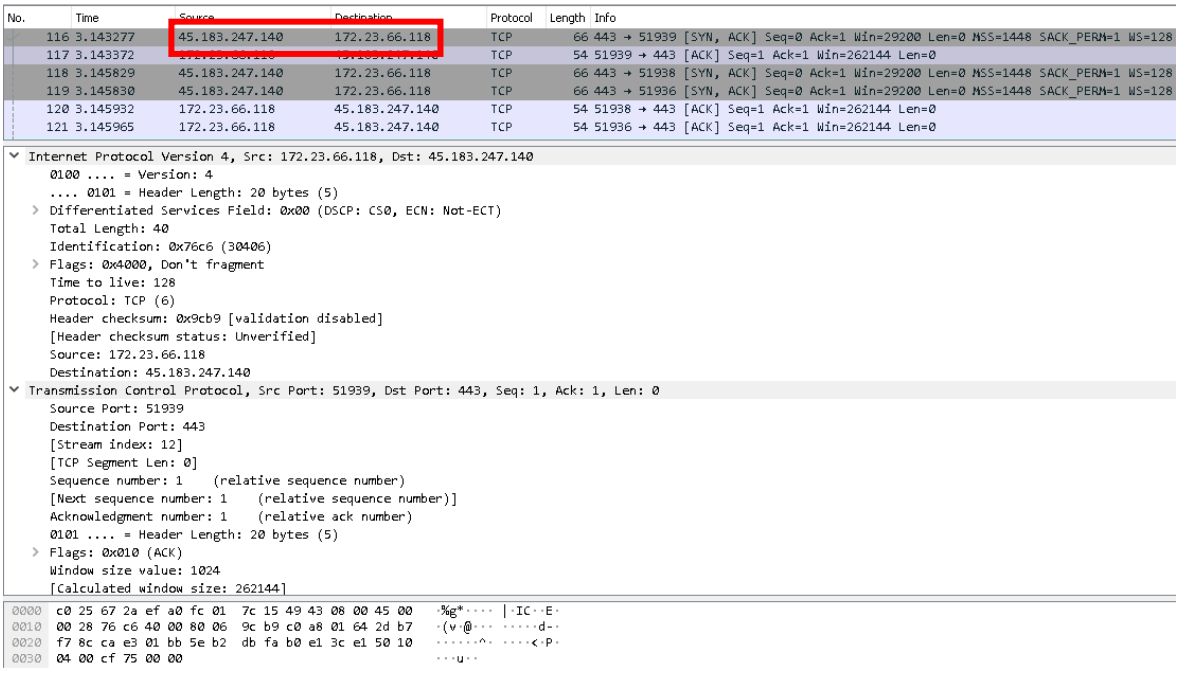


Figura 44. Tráfico interceptado por la aplicación Wireshark

5.4. Valoración de Evaluación de Riesgos – RAV

Una vez que se detecta y verifica un riesgo, la metodología OSSTMM lo clasifica dependiendo de las limitaciones y e incapacidad de los mecanismos de protección y control del sistema de información para gestionar adecuadamente la vulnerabilidad o amenaza asociada. Dicha clasificación de riesgos es la Valoración de Evaluación de Riesgos – RAV y consiste en una métrica de seguridad que permite evaluar el nivel de protección de un sistema de información ante posibles amenazas informáticas, estableciendo un valor cuantitativo para determinar el nivel de seguridad de la infraestructura de red de datos.

La metodología OSSTMM plantea una clasificación de riesgos informáticos categorizada mediante tres factores para calcular el valor RAV de un sistema de información. El primer factor es la seguridad operativa o porosidad, la cual se compone de la visibilidad, el acceso y la confianza. El segundo factor son los controles implementados para cada punto relacionado en la sección de seguridad operativa, agrupados en clase A, autenticación, indemnización, resiliencia, subyugación y continuidad, y clase B, no repudio, confidencialidad, privacidad, integridad y alarma. El tercer factor son las limitaciones, riesgos clasificados como vulnerabilidades, debilidades, preocupaciones, exposiciones y anomalías del sistema informático. La clasificación de la metodología OSSTMM para la obtención de la escala de Valoración de Evaluación de Riesgos - RAV de una infraestructura de red de datos se consigna en la siguiente tabla.

Tabla 35. Clasificaciones de riesgos

Clasificación	Descripción
SEGURIDAD OPERTIVA – OPSEC (Porosidad)	
Visibilidad	Oportunidad de un ataque informático. Todos los objetivos visibles se deben contabilizar, buscando evitar puntos ciegos a través de los cuales puedan perpetrarse ciberataques
Acceso	Oportunidad de interactuar con un objetivo. Todas las formas individuales de interactuar con un objetivo se deben contabilizar por separado, como cantidad de puntos de acceso interactivos o cada puerto de red abierto en un dispositivo
Confianza	Posibilidad de acceso no autenticado en sistemas confiables. El objetivo interactúa libre con otro objetivo en la red, como un servicio web puede conectarse a una base de datos sin necesidad que el usuario se autentique en el servidor de bases de datos
CONTROLES	
Clase A	
Autenticación	Son controles de identificación que solicitan la identidad del usuario, autentican que tiene derecho a la identidad solicitada y autoriza permisos de usuario de acuerdo a su identidad, como autenticación por contraseña, tarjeta de identificación, token o certificado, huella digital, patrón de iris o de ADN, o a través de listas blancas de cortafuegos o listas negras de antivirus

Indemnización	Todo tipo de documentos que contengan reglas y políticas para cubrir y garantizar su propia seguridad legal y jurídica, por ejemplo, contratos, términos y condiciones o seguros
Resiliencia	Si un componente falla, la seguridad continúa, por ejemplo, si el cortafuegos falla, no hay acceso en absoluto a la red de datos, manteniéndose la seguridad de la información
Subyugación	Forzar un procedimiento o proceso de una manera determinada, eliminando la posibilidad que el usuario interactúe de manera diferente, como el protocolo HTTPS obliga al uso de un protocolo seguro, o no continuar con el siguiente paso de un procedimiento hasta que las fases requeridas del paso anterior se completen
Continuidad	Si se produce un fallo en un dispositivo, el proceso, procedimiento o servicio continúa sin el riesgo de perderse por falta de controles de seguridad, por ejemplo, un balanceador de carga o un servidor redundante de nombre de dominio o de correo electrónico
Clase B	
No Repudio	Una parte no puede negar que estuvo involucrado en una interacción informática. Su identidad debe ser comprobable y la prueba sobre la interacción debe ser capturada y conservada, como una firma digital
Confidencialidad	El contenido de una interacción, datos e información se oculta para otras partes, por ejemplo, el cifrado o encriptado de datos
Privacidad	Enmascaramiento de la interacción para evitar ser detectado en el medio, por ejemplo, servidores proxy y balanceadores de carga que ocultan otros componentes y/o dispositivos
Integridad	Detección de cambios durante el tránsito de la información por el remitente o el receptor, por ejemplo, hashes criptográficos
Alarma	Reporte de eventos anormales al administrador del sistema, por ejemplo, el sistema de detección de intrusiones
LIMITACIONES	
Vulnerabilidad	Falla o error que niega el acceso a activos para usuarios o procesos autorizados, permite el acceso privilegiado a activos a usuarios o procesos no autorizados, o permite que usuarios o procesos no autorizados oculten activos o a ellos mismos dentro del alcance
Debilidad	Falla o error que interrumpe, reduce, abusa o anula específicamente los efectos de los cinco controles de interactividad: autenticación, indemnización, resistencia, subyugación y continuidad
Preocupación	Falla o error que interrumpe, reduce, abusa o anula los efectos del flujo o la ejecución de los cinco controles del proceso: no repudio, confidencialidad, privacidad, integridad y alarma
Exposición	Acción injustificable, falla o error que proporciona visibilidad directa o indirecta de objetivos o activos dentro del canal de alcance elegido
Anomalía	Cualquier elemento no identificable o desconocido que no ha sido controlado y que no puede contabilizarse en operaciones normales

En cuanto a la escala de valoración, su medición varía de 0 a 100, siendo 100 RAV el estado de seguridad ideal con un equilibrio óptimo entre las posibles interacciones con vulnerabilidades informáticas y los controles implementados en la red de datos para evitarlas. Cuando un RAV está por debajo de 100, el cálculo muestra qué controles son insuficientes, ausentes o necesarios de ser implementados en la red

de datos. Cuando un RAV es 100 y se agregan más controles, el RAV supera los 100, lo que significa que estos nuevos controles no son necesarios porque la red ya se encuentra en un nivel ideal de protección.

A continuación, se presentan los resultados del análisis realizado en la Tercera División del Cantón Militar de Popayán para la determinación del valor de evaluación de riesgos RAV de su infraestructura de red inalámbrica.

- El sistema es visible en 8 puntos diferentes por cada punto de acceso inalámbrico visible al usuario, por lo tanto, **visibilidad 1x8=8**.
- Los puntos de acceso inalámbrico responden con puertos abiertos en 80 /tcp y 443 /tcp. No hay respuesta en los demás puertos (TCP, UDP e ICMP), es decir, el sistema es accesible en 2 puertos por cada punto de acceso inalámbrico y en el Cantón Militar de Popayán se encuentran instalados 8 dispositivos, por lo tanto, **acceso 2x8=16**.
- En el puerto 443 /tcp escucha el protocolo HTTPS que proporciona cifrado de datos, detecta cuándo se modifica la negociación de claves y además impide el uso de protocolos de comunicación insegura. Por lo tanto, se cuenta como **confidencialidad x1**, **integridad x1** y **subyugación x1**.
- El protocolo SSLv2 tiene defectos plenamente reconocidos y se cuenta como limitación en la confidencialidad y la integridad. **Preocupación x2**.
- El sistema debe notificar al cliente acerca de los puertos cerrados. Estas notificaciones no se reciben y se filtran mediante el cortafuegos, por lo tanto, se incrementa 1x en autenticación para cada acceso protegido. **Autenticación x2**.
- Las claves con longitudes de 40 y 56 bits son descifrables y no deben utilizarse para proteger datos confidenciales, su cifrado es débil por cada punto de acceso existente lo que se cuenta como otra **preocupación 1x8**.
- Se encuentra configurado un servidor proxy y es posible la interacción con él, entonces se agrega **visibilidad x1** y **acceso x1**.
- Se cuenta con 3 documentos que firman los usuarios con las políticas de seguridad PUA para el uso de activos del Ejército Nacional, los cuales cubre los 7 puntos de acceso inalámbrico de infraestructura y el servidor proxy, por lo tanto, **indemnización 3x8=24**.
- En el análisis de vulnerabilidades se encontraron 7 posibles vulnerabilidades de redes inalámbricas x7, del análisis de referencia de vulnerabilidades de puertos PVR x42, por cada punto de acceso inalámbrico, por lo tanto, **vulnerabilidades 42+7=49x7=343**.
- En el escaneo de puertos lógicos abiertos en la red se detectaron 66 terminales con valoración crítica dada la cantidad de puertos abiertos atacables, por lo tanto, **exposiciones 1x66=66**.
- Se encontró un punto de acceso inalámbrico no perteneciente a los activos de red del Ejército Nacional, para la red de la cafetería del Cantón, por lo tanto, **anomalías x1**.

La evaluación obtenida con la aplicación de la escala de valoración de evaluación de riesgos RAV a la infraestructura de red inalámbrica de la Tercera División del Cantón Militar de Popayán se presenta en la tabla a continuación.

Tabla 36. Valoración de evaluación de riesgos RAV del Cantón Militar de Popayán

Attack Surface Security Metrics

OSSTMM version 3.0

OPSEC		
Visibility	9	
Access	17	
Trust	0	
Total (Porosity)	26	

CONTROLS		
Class A		Missing
Authentication	2	24
Indemnification	24	2
Resilience	0	26
Subjugation	1	25
Continuity	0	26
Total Class A	27	103

Class B		Missing
Non-Repudiation	0	26
Confidentiality	2	24
Privacy	1	25
Integrity	2	24
Alarm	0	26
Total Class B	5	125

		True Missing
All Controls Total	32	228
Whole Coverage	12,31%	87,69%

LIMITATIONS		Item Value	Total Value
Vulnerabilities	343	9,769231	3350,846154
Weaknesses	0	4,961538	0,000000
Concerns	10	5,807692	58,076923
Exposures	66	14,453846	953,953846
Anomalies	1	13,576923	13,576923
Total # Limitations	420		4376,4538

OPSEC	11,663184
True Controls	6,282567
Full Controls	6,282567
True Coverage A	20,77%
True Coverage B	3,85%
Total True Coverage	12,31%
Limitations	31,822273
Security Δ	-37,20
True Protection	62,80

Actual Security: 63,7766 ravs

Como se puede observar, el resultado de la valoración RAV del nivel de seguridad de la infraestructura de red inalámbrica de la Tercera División del Cantón Militar de Popayán es 63,7766 ravs. Este resultado es demasiado bajo para una institución tan importante y que maneja información tan crítica y confidencial como lo es una institución militar de carácter nacional como el Cantón Militar de Popayán, perteneciente al Ejército Nacional de la república de Colombia, siendo necesario la implementación de controles de seguridad para redes de datos que permitan incrementar el nivel de seguridad de la información militar accesible a través del servicio de red inalámbrica de las fuerzas militares en la ciudad de Popayán.

6. Recomendaciones y Conclusiones

6.1. Recomendaciones infraestructura de red inalámbrica

A continuación, se realizan recomendaciones para optimizar la seguridad de la información militar en la infraestructura de red inalámbrica que provee el servicio de Internet a los usuarios del Ejército en el Cantón Militar de Popayán.

- **Cambio del direccionamiento de red del Cantón Militar:** Existe una vulnerabilidad en cuanto a esquema de direccionamiento de red inalámbrica del Cantón Militar de Popayán debido a que los puntos de acceso inalámbricos mediante el servicio de configuración dinámica DHCP están entregando direcciones de red del esquema de direccionamiento interno de la infraestructura de red de datos a las terminales que acceden a la red inalámbrica. Este escenario puede ser aprovechado por un intruso malicioso para identificar el direccionamiento general de toda la red y lanzar un ataque informático hacía segmentos de red críticos o importantes. Para gestionar esta vulnerabilidad se sugiere cambiar el direccionamiento de red inalámbrica que se entrega a las terminales de los usuarios por el direccionamiento tradicional de la red privada 192.168.0.0. En la tabla siguiente se puede observar la configuración sugerida para el punto de acceso inalámbrico de la infraestructura de red inalámbrica de la Tercera División del Cantón Militar de Popayán.
-

Tabla 37. Esquema de direccionamiento de red propuesto

Parámetro	Configuración Actual	Configuración Propuesta
WLAN		
Dirección de red	172.23.66.1 - 172.23.66.254	192.168.0.2 - 192.168.0.254
Máscara de red	255.255.255.0	255.255.255.0
Puerta de enlace predeterminada	172.23.66.194	192.168.0.1
Servidor DNS 1	172.23.66.194	192.168.0.1
Servidor DNS 2	172.23.66.194	192.168.0.1

LAN		
Dirección de red	172.23.0.13	172.23.0.13
Máscara de red	255.255.255.0	255.255.255.0
Puerta de enlace predeterminada	172.23.0.1	172.23.0.1
Servidor DNS	172.23.0.1	172.23.0.1

El direccionamiento sugerido para la infraestructura de red inalámbrica se puede apreciar en la siguiente gráfica, en donde se obviaron tanto los dispositivos de los segmentos de red de área local, como los conmutadores de distribución, enfocándose únicamente en la distribución de la red inalámbrica del Cantón Militar de Popayán para mejor comprensión y análisis.

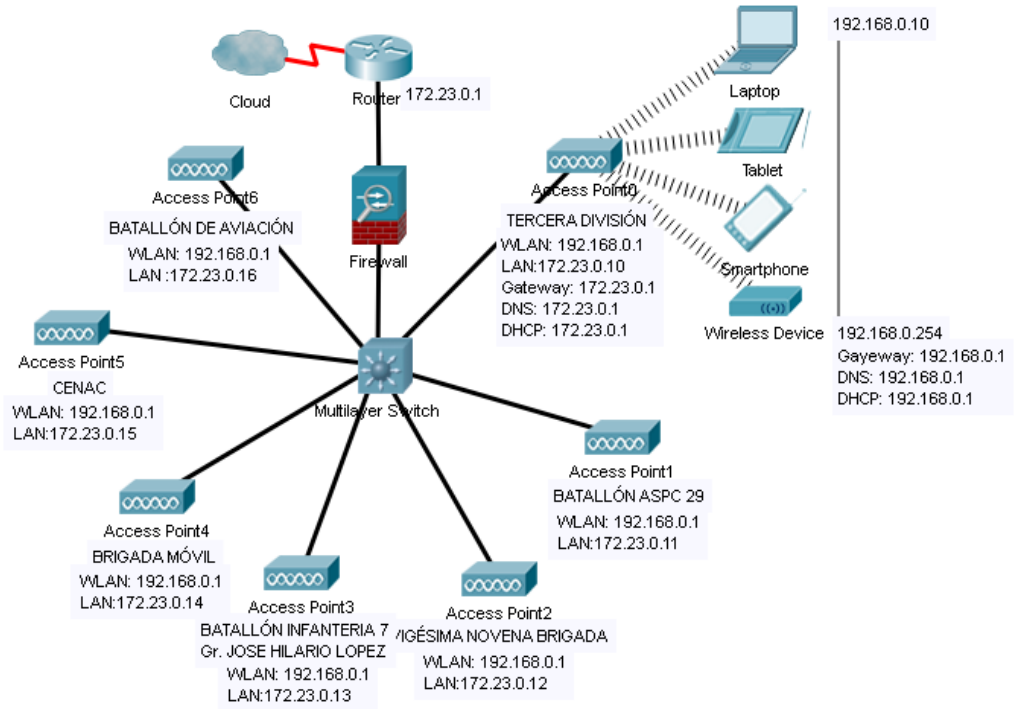


Figura 45. Esquema de direccionamiento de red propuesto

- **Segmentos de red virtuales por brigadas del Ejército:** La infraestructura de red de datos del Cantón Militar opera toda en el mismo segmento lógico de red, siendo una vulnerabilidad importante debido a que un intruso tiene un único segmento de penetración para lanzar un eventual ataque informático, hecho que facilita completamente su labor maliciosa. Para gestionar esta vulnerabilidad se recomienda la implementación de segmentos de red locales virtuales en la infraestructura de red inalámbrica por cada una de las unidades militares que conforman el Ejército en el Cantón Militar de Popayán, para segmentarla en redes lógicas independientes y reducir el riesgo ante un posible un ataque informático debido a que la red no tendría un único dominio

de difusión del ataque, impidiendo el alcance lógico al segmento de red con los servidores que poseen la información confidencial del Ejército desde una terminal con acceso a la red inalámbrica del Cantón Militar.

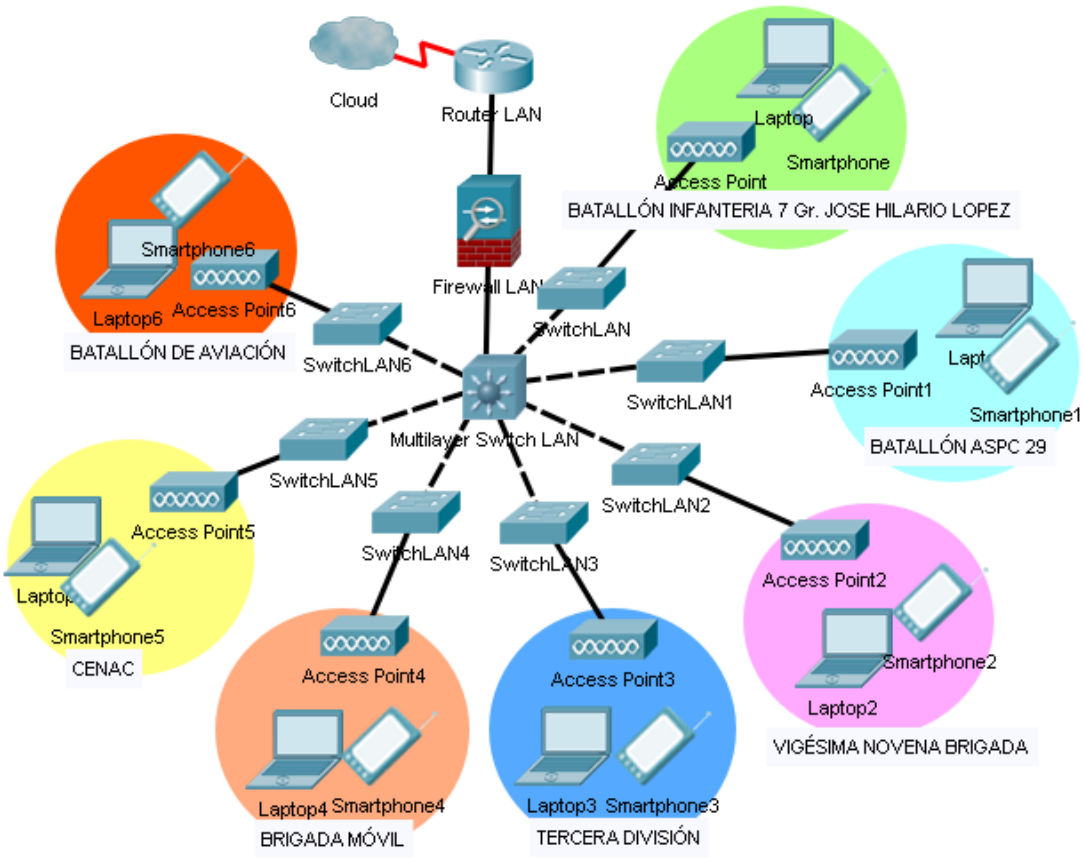


Figura 46. Segmentos de red virtuales por brigadas del Ejército

- **Sistema de detección de intrusos inalámbrico:** Para incrementar la seguridad en la infraestructura de red inalámbrica del Cantón Militar se propone la implementación de un sistema de detección de intrusos que permita realizar control de acceso y supervisión de la red inalámbrica en tiempo real. Este sistema se compone de un dispositivo de monitoreo y control, y sus respectivos sensores inalámbricos detectores de intrusos en cada segmento de red, que permiten detectar, identificar y gestionar intrusos maliciosos en la red inalámbrica, posibilitando tomar acciones de control sobre el atacante informático detectado. Este sistema detecta y previene amenazas inalámbricas con capacidades de seguimiento de ubicación basadas en políticas de seguridad, reduce alertas de falsos positivos y utiliza técnicas de clasificación y mitigación para bloquear tráfico inalámbrico no autorizado sin interrumpir el rendimiento de dispositivos autorizados. Además

proporciona protección contra puntos de acceso no autorizados, denegación de servicio y ataques de desencriptado. El sensor proporciona capacidades de detección y prevención señalando la ubicación física de dispositivos no autorizados, detecta y reduce amenazas mediante clasificación de puntos de acceso y dispositivos inalámbricos de usuarios. De igual manera brinda seguridad, incluso si se pierde la conectividad entre el sensor y el controlador, así como análisis forenses inteligentes. (IDS HPE, 2012).

- **Sistema de prevención de intrusiones inalámbrico:** Otro mecanismo propuesto para incrementar el nivel de seguridad en la infraestructura de red de datos es la implementación de un sistema de prevención de intrusiones inalámbrico que realice control y monitoreo sobre el tráfico de datos generado en cada segmento de red inalámbrica correspondiente a cada división del Cantón Militar de Popayán, para detectar posibles ataques informáticos de intrusos maliciosos en cada división y disponer de acciones de en tiempo real. Este sistema permitirá incrementar su nivel de seguridad y hacerla menos propensa a ataques informáticos de intrusos dada su compatibilidad en operación, monitoreo y control con el sistema de detección de intrusos inalámbricos planteado dado que realiza inspección de paquetes para proteger redes contra ataques informáticos, brinda protección en línea con seguridad de red proactiva, investiga amenazas con correlación de eventos de seguridad y vulnerabilidades, ofreciendo visibilidad de activos de red con aplicaciones críticas de la institución y gestionando riesgos en seguridad informática. (IPS HPE, 2015).

- **Controlador de red inalámbrica:** Para centralizar la administración de los puntos de acceso inalámbrico se sugiere la implementación de un controlador de red inalámbrica, dispositivo que permite monitoreo en tiempo real de todos los puntos de acceso inalámbrico, segmentación dinámica de la red inalámbrica mediante la aplicación de políticas de seguridad y configuración de segmentos virtuales de red inalámbrica, generando un primer control de usuarios, así como visibilidad y control de aplicaciones en uso. El controlador es un dispositivo de conmutación con capacidad para control de flujo, soporte para segmentos de red locales virtuales, monitoreo del protocolo de gestión de grupos de Internet, prevención contra ataque de negación de servicio, sistema de detección de intrusos, listas de control de acceso y calidad de servicio. Adicionalmente ofrece rastreadores de paquetes de red, defensa de admisión de punto final y bloqueo de direcciones físicas. De igual manera permite que dominios de servicios virtuales implementen políticas de seguridad por división o ubicación, autenticación basada en el protocolo de autenticación y autorización para aplicaciones de

acceso a la red RADIUS, aislamiento seguro de usuarios con servicios de punto de acceso virtual clasificando servicios específicos para grupos de usuarios, control de autenticación y acceso de usuarios únicamente en puntos de acceso predeterminados basados en ubicación, permitiendo controlar las ubicaciones donde un usuario puede acceder a la infraestructura de red inalámbrica. (Switch WLAN, 2015). El esquema de solución planteado se puede apreciar en la siguiente gráfica.

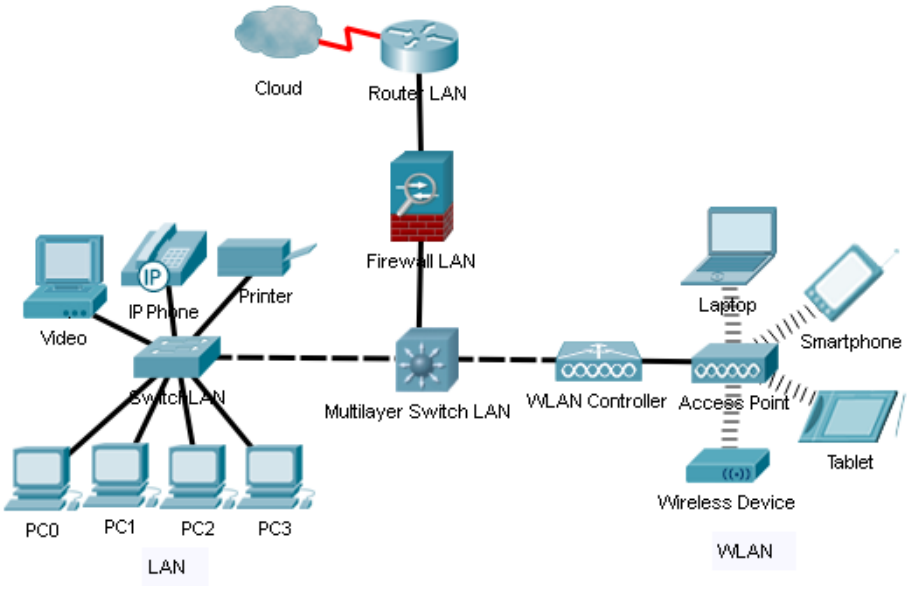


Figura 47. Esquema controlador de red inalámbrica

- **Sistema de autenticación inalámbrico:** Es un sistema con un protocolo de autenticación y autorización de usuarios para acceso a la red de datos contra el directorio activo o contra la base de datos SIATH del dominio de la institución mediante un portal cautivo de seguridad, en donde los usuarios deberán ingresar sus credenciales de acceso individuales, es decir su nombre de usuario y contraseña de autenticación en el controlador de dominio del Ejercito, para poder acceder a la red de datos inalámbrica. Básicamente consiste en un mecanismo de autenticación de usuarios en modo cliente-servidor para acceder a un recurso de red compartido. Para ello es necesario implementar un servidor de acceso a la red con el servicio de usuario de marcación de autenticación remota RADIUS, el cual es un protocolo que ofrece un mecanismo de seguridad y administración simplificada de credenciales de acceso a recursos de la red de datos. El esquema de funcionamiento del sistema de autenticación de usuarios que se propone implementar es el siguiente.

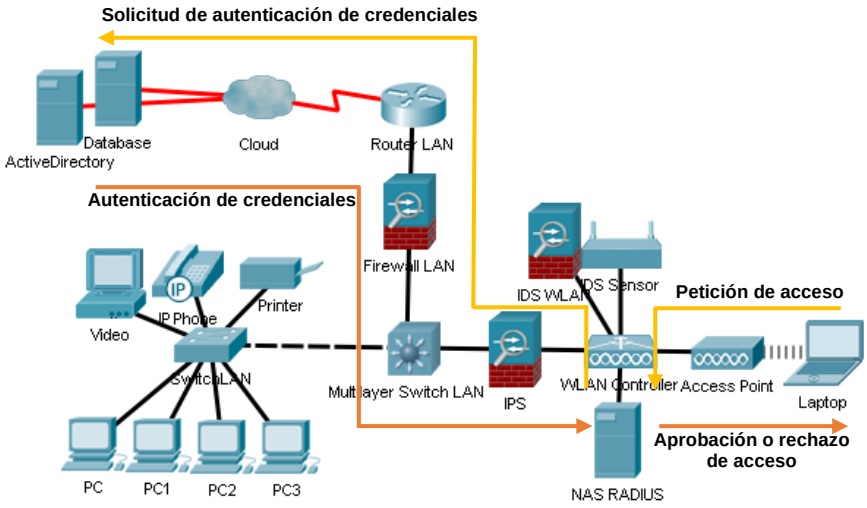


Figura 48. Funcionamiento del sistema de autenticación RADIUS

En caso de necesitarse autorizar acceso a personal no perteneciente al Ejercito Nacional de Colombia, como familiares, clientes, proveedores y demás usuarios externos, el sistema permite generar credenciales temporales para acceso limitado a la red inalámbrica con fecha límite, pierden su vigencia, y el servidor de acceso no autorizará nuevamente el uso de la red inalámbrica a este grupo de usuarios.

- **Sistema de acceso inalámbrico en malla:** Dentro de los diferentes ataques que pueden presentarse en la red inalámbrica, el servicio puede suspenderse debido a un bloqueo u hostigamiento del punto de acceso inalámbrico en un eventual ataque de negación de servicios, evidenciando una vulnerabilidad latente en cuanto a garantizar la disponibilidad del servicio de red inalámbrica para acceso a Internet de los usuarios del Ejército Nacional. Para gestionar esta vulnerabilidad se sugiere la implementación de un sistema de acceso inalámbrico en malla que consiste en la instalación de puntos de acceso inalámbrico adicionales interconectados entre si mediante un sistema de distribución inalámbrico, los cuales permiten realizar balanceo de cargas de red como sistema de acción ante fallos, si un punto de acceso es bloqueado en un ataque informático los usuarios pueden conectarse al servicio de red inalámbrica desde cualquier otro de los puntos de acceso disponibles en su unidad militar. Este sistema ofrece alta disponibilidad, estabilidad y óptimo rendimiento, gran cobertura, ancho de banda y tolerancia a fallos. También permite control de dispositivos conectados, canales en uso y configuración de políticas de seguridad (WDS HPE1, 2012).

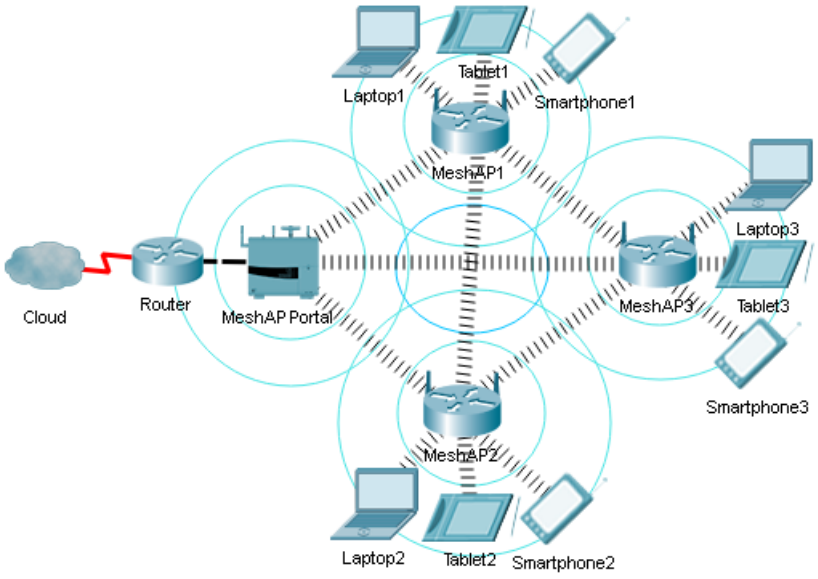


Figura 49. Esquema del sistema de acceso inalámbrico en malla

La solución de malla permite ampliar la cobertura de red inalámbrica para entornos interiores y exteriores, reconfigurándose automáticamente alrededor de rutas bloqueadas, proporcionando fiabilidad y redundancia dado que la red continúa funcionando si un punto de acceso deja de funcionar o falla una conexión. Los puntos de acceso de malla proporcionan cifrado y reenvío de tráfico, brindando conectividad con equilibrio de carga en la malla. También ofrece servicios de red confiables, gestión avanzada de tráfico y calidad de servicio para grupos de usuarios y rastreo de ubicación de equipos y usuarios de alto valor a través de la malla, reduciendo la posibilidad de robo en la institución (WDS HPE2, 2017).

- **Aislamiento Infraestructura de red inalámbrica:** Para incrementar el nivel de seguridad de la información se sugiere el aislamiento de la infraestructura de red inalámbrica, de la infraestructura de red interna del Cantón Militar de Popayán. De esta manera se puede aislar tanto física como lógicamente los segmentos de red de cada división del Batallón para garantizar el tráfico de información militar confidencial de los usuarios de la red inalámbrica que utilizan el servicio de Internet. En la siguiente gráfica se puede apreciar el esquema de la solución planteada para la red de datos del Cantón Militar.

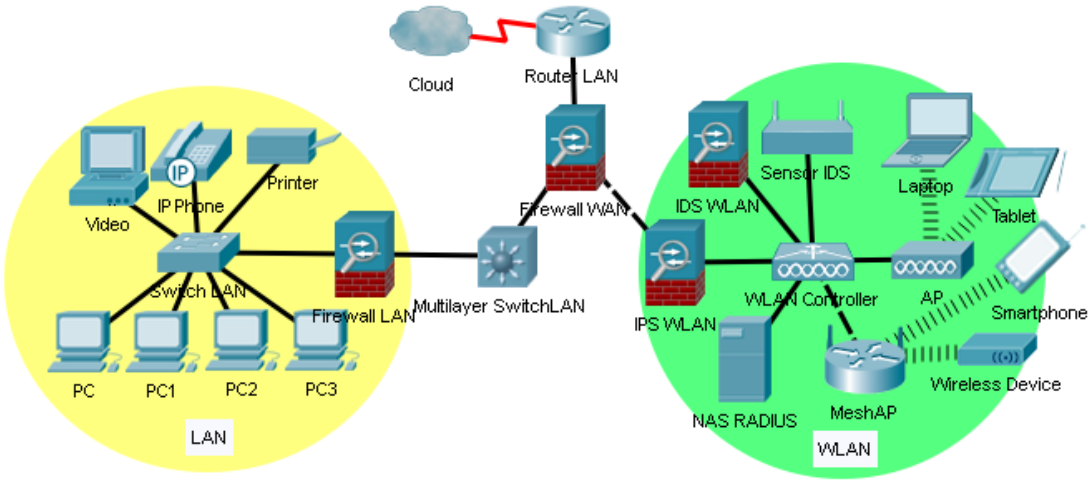


Figura 50. Esquema de infraestructura de red de datos propuesta

- **Propuesta de solución final:** Se sugiere aplicar de manera conjunta todas las recomendaciones planteadas en la infraestructura de red de datos para incrementar el nivel de seguridad de la información en la subestructura de red inalámbrica, el nuevo esquema de direccionamiento de red, la división en segmentos de red lógicos virtuales, el sistema de autenticación con portal cautivo, el controlador centralizado de red inalámbrica, conjunto con la implementación del sistema de detección de intrusos y el sistema de prevención de intrusiones en cada uno de los segmentos de red inalámbrica. Finalmente, la infraestructura de red de datos con todas las soluciones planteadas para incrementar el nivel de seguridad de la información del Ejército Nacional de Colombia en el Cantón Militar de Popayán quedaría como se observa en la siguiente gráfica.

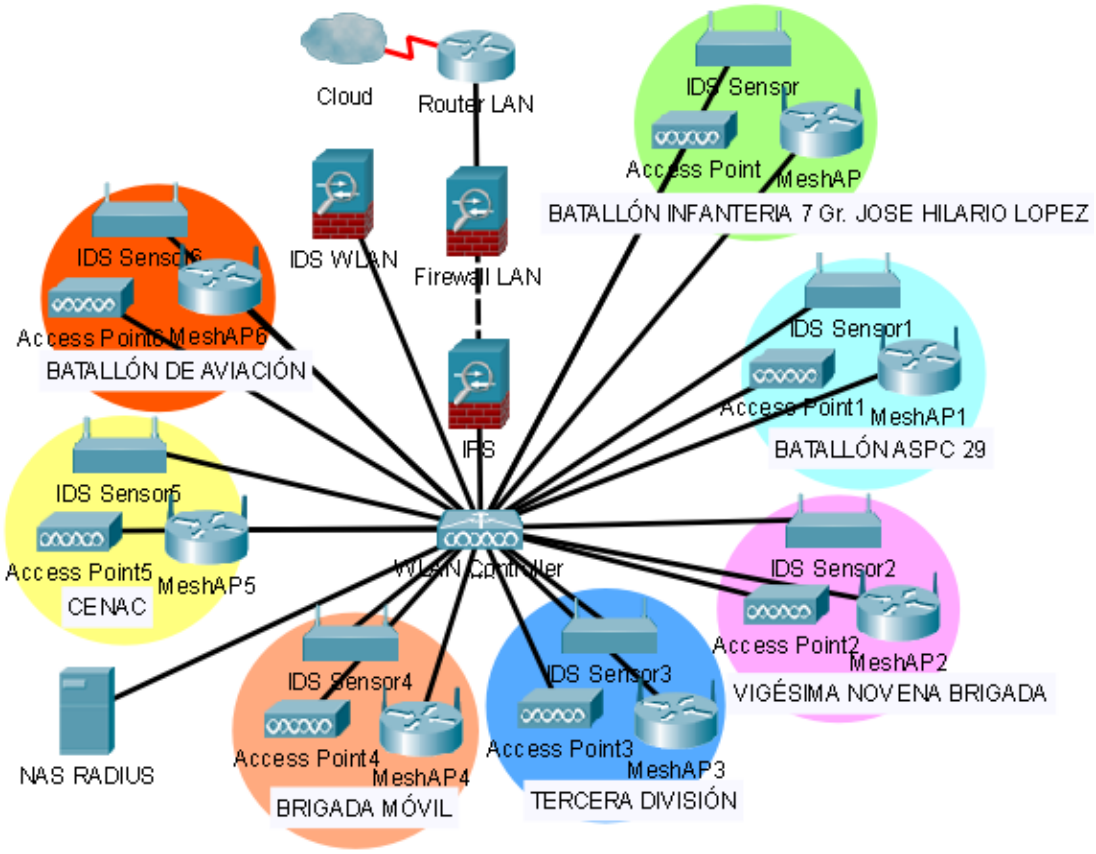


Figura 51. Infraestructura de red de datos propuesta

6.2. Recomendaciones de seguridad en la red inalámbrica

Para incrementar el nivel de seguridad de la red inalámbrica se sugiere adoptar las medidas necesarias para minimizar los riesgos ante la posibilidad de que ocurra un eventual ataque informático inalámbrico, de esta manera, se restringe el acceso a la información institucional militar por personas ajenas al Ejército Nacional de Colombia, evitándose la utilización de la red inalámbrica para fines maliciosos.

Dentro de las sugerencias para minimizar las vulnerabilidades de la red inalámbrica e incrementar el nivel de seguridad de la información en la infraestructura de red de datos del Cantón Militar de Popayán se plantean las siguientes.

- Llevar un registro de usuarios y direcciones de red que se asignan para navegar en la red inalámbrica del Cantón Militar de Popayán, para facilitar la solución de novedades informáticas, además de monitorizar el rango de direcciones libres ya que puede llegar a presentarse la inserción de equipos a la infraestructura de red inalámbrica en los rangos libres de direcciones de red sin autorización. De igual manera se posibilita conocer a que terminal, dispositivo de interconexión o servidor le fue asignada una determinada dirección de red y poder determinar el origen de un ataque de intrusión interno, minimizando la superficie de ataque a la red inalámbrica.

Tabla 38. Rango de direcciones de red sugerido por división del Cantón Militar

Parámetro	Configuración
Equipos de interconexión	192.168.0.1 - 192.168.0.20
Impresoras	192.168.0.21 - 192.168.0.30
Teléfonos IP	192.168.0.30 - 192.168.0.60
Terminales de red	192.168.0.60 - 192.168.0.254

- Restringir el acceso a la red de datos dado el contexto de seguridad de la institución militar, se sugiere que no se permita que usuarios no autorizados por el Ejército Nacional de Colombia accedan a la infraestructura de red inalámbrica del Cantón Militar de Popayán. Se sugiere restringir el acceso al dominio de la red de datos del Batallón filtrando las terminales y dispositivos que soliciten o brinden acceso a la red inalámbrica por su dirección de control de acceso a medios (MAC), manteniendo la confidencialidad de las credenciales de acceso y la integridad de la red inalámbrica.

- Deshabilitar el uso compartido de archivos en la intranet del Batallón como política de seguridad del Cantón Militar de Popayán. Para ello se recomienda crear un directorio dedicado para compartir información y restringir el acceso a todos los demás directorios, habilitando la protección con contraseña de cualquier archivo que se comparta en la red. Además, se sugiere la implementación de un sistema de gestión de información que permita espacios de trabajo compartidos para almacenamiento y organización de la información institucional militar de manera restringida con autenticación mediante el directorio activo del dominio de la red de datos, y con políticas de seguridad para el almacenamiento y transferencia de archivos, evitando que información individual, privada, falsa, reproducida, no libre o de propiedad no abierta sea compartida.

- Implementar sistemas de seguridad para detección y prevención de intrusos y ataques informáticos conjunto con un sistema de autenticaciones que permita reforzar y garantizar la seguridad de la información en las conexiones de red cuando los usuarios del Ejército Nacional accedan a la red inalámbrica del Cantón Militar de Popayán, además de permitir identificar ubicación de intrusos y tomar medidas de acción inmediata frente a un eventual ataque informático en tiempo real.

- Conectarse usando una red privada virtual (VPN) especialmente cuando se acceda al segmento de red de área de almacenamiento de información (SAN) desde Cantón Militar de Popayán. Las redes privadas virtuales permiten a los usuarios conectarse de forma segura a la red de datos cifrando las conexiones en los extremos de envío y recepción de la información, por ello se recomienda implementar redes privadas virtuales para usuarios que

acceden a la información militar crítica, estableciendo su inicio de sesión cada vez que se acceda mediante cualquiera de los puntos de acceso inalámbrico del Batallón. De esta manera la transmisión de los datos estará cifrada y encriptada, lo cual dificultaría mayormente la lectura de la información militar por un intruso en un ataque informático

- Realizar la gestión para que el personal del área de sistemas del Batallón pueda recibir las capacitaciones y formación necesaria para incrementar los conocimientos del personal del Ejército encargado de la administración de la infraestructura de redes de datos en la sede del Cantón Militar de Popayán.

6.3. Valoración de Evaluación de Riesgos con las recomendaciones

A continuación, se presentan los resultados de la valoración de evaluación de riesgos RAV de la infraestructura de red inalámbrica de la Tercera División del Cantón Militar de Popayán si se implementasen todas las sugerencias propuestas para incrementar el nivel de seguridad de la información en la prestación del servicio de internet inalámbrico a los usuarios del Ejército Nacional de Colombia. Los parámetros de la valoración de evaluación de riesgos RAVs adicionales con los controles implementados quedaría de la siguiente manera.

- Se sugiere desinstalar el punto de acceso inalámbrico indebido que se implementó para el prestar el servicio de internet a los usuarios del Ejército en la cafetería del Cantón Militar, y reemplazarlo por un punto de acceso inalámbrico oficial configurado y administrado correctamente desde el sistema central, por lo tanto, **no repudio x1**, **confidencialidad x1**, **privacidad x1** e **integridad x1**.
- Se sugirió cambiar el esquema de direccionamiento de red que entrega el protocolo de direccionamiento dinámico de host de cada punto de acceso inalámbrico a sus usuarios, por un esquema de direccionamiento de la red privada 192.168.0.0, por cada segmento de red inalámbrica de cada división militar, por lo tanto, **confidencialidad 1x7=7** y **privacidad 1x7=7**.
- Si se realiza el cambio sugerido del esquema de direccionamiento de red que entregan los puntos de acceso inalámbrico a sus usuarios por el esquema basado en el segmento de privada 192.168.0.0, también se oculta el esquema de direccionamiento interno del núcleo de la red de datos del Cantón Militar y del Ejército en general, por lo tanto, **confidencialidad x1** y **privacidad x1**.
- Se sugiere crear segmentos de red virtuales VLAN por cada segmento de red al que pertenece cada punto de acceso inalámbrico, la segmentación lógica de la red de datos incrementa el nivel de seguridad de la infraestructura informática por cada segmento de red inalámbrica de cada división militar,

por lo tanto, **no repudio 1x7=7**, **confidencialidad 1x7=7**, **privacidad 1x7=7** e **integridad 1x7=7**.

- Se sugiere implementar el sistema de detección de intrusos inalámbrico que ofrece controles de clase A, provee protección contra amenazas como puntos de acceso no autorizados, denegación de servicio y ataques de desencriptado, clasifica puntos de acceso y terminales, proporciona cobertura de seguridad, detección y prevención, incluso si se pierde conectividad entre el sensor y el control central, por cada segmento de red inalámbrica de cada división militar, por lo tanto, **autenticación 1x7=7**, **resiliencia 1x7=7** y **subyugación 1x7=7**.
- Igualmente, el sistema de detección de intrusos inalámbrico provee controles de clase B, ofrece monitoreo y control, sensores inalámbricos, detectores de intrusos, control sobre ataques a contenidos de tráfico, detecta y previene amenazas inalámbricas con capacidades de seguimiento de ubicación basadas en políticas de seguridad, reduce alertas de falsos positivos, y realiza clasificación y mitigación para bloquear tráfico inalámbrico no autorizado, por cada segmento de red inalámbrica de cada división militar, por lo tanto, **no repudio 1x7=7**, **confidencialidad 1x7=7**, **privacidad 1x7=7**, **integridad 1x7=7** y **alarma 1x7=7**.
- Se sugiere implementar el sistema de prevención de intrusiones inalámbrico que brinda controles de clase A, permite control y monitoreo de tráfico de paquetes datos en tiempo real, detección de ataques informáticos, control sobre dispositivos detectados, fiabilidad, redundancia, visibilidad, control, protección automatizada, gestión continua, precisión de filtrado de paquetes, no bloqueo de tráfico legítimo y protección de eventos de día cero, por lo tanto, **autenticación x1**, **resiliencia x1** y **subyugación x1**.
- Así mismo, el sistema de prevención de intrusiones inalámbrico provee controles de clase B, ofrece reconocimiento de aplicaciones y contenido, protección en línea en tiempo real, analiza amenazas con correlación de eventos de seguridad y vulnerabilidades, permite políticas de seguridad de red proactiva, visibilidad de activos de red con aplicaciones críticas, inspección de paquetes, gestiona riesgos en seguridad informática, recupera ancho de banda mal utilizado, minimiza cargas de tráfico y genera reporte de alarmas del sistema, por lo tanto, **no repudio x1**, **confidencialidad x1**, **privacidad x1**, **integridad x1** y **alarma x1**.
- Se sugiere la implementación del controlador de red inalámbrica que permite controles de clase A, como realizar control de flujo, prevención contra ataques de negación de servicio, soporte para servicios diferenciados, listas de control de acceso y calidad de servicio, por cada segmento de red inalámbrica de cada división militar, por lo tanto, **resiliencia 1x7=7** y **subyugación 1x7=7**.

- Así mismo, el controlador de red inalámbrica brinda controles de clase B, permite monitoreo de puntos de acceso, segmentación dinámica, aplicación de políticas de seguridad y configuración de segmentos virtuales con monitoreo de usuarios y aplicaciones, por cada segmento de red inalámbrica de cada división militar, por lo tanto, **confidencialidad 1x7=7**, **privacidad 1x7=7**, **integridad 1x7=7** y **alarma 1x7=7**.
- Se sugiere implementar un sistema de autenticación inalámbrico que ofrece controles tipo A y B, dado que permite autenticación y autorización de usuarios en modo cliente-servidor para acceso a la red de datos, con monitoreo de sesión y reporte de estadísticas, por cada segmento de red inalámbrica de cada división militar, por lo tanto, **autenticación 1x7=7**, **subyugación 1x7=7**, **no repudio 1x7=7**, **confidencialidad 1x7=7**, **privacidad 1x7=7** e **integridad 1x7=7**.
- Se sugiere la implementación de un sistema de acceso inalámbrico en malla con puntos de acceso inalámbrico adicionales interconectados mediante un sistema de distribución para balanceo de cargas de red como acción ante fallos, si un punto de acceso falla, lo reporta y los demás están disponibles, por cada segmento de red inalámbrica de cada división militar, por lo tanto, **resiliencia 1x7=7**, **continuidad 1x7=7** y **alarma 1x7=7**.
- Se sugiere aislar la infraestructura de red inalámbrica de la infraestructura de red interna de datos, aislando tanto física como lógicamente los segmentos de red de cada división militar para incrementar el nivel de seguridad de la información, por cada segmento de red inalámbrica de cada división militar, por lo tanto, **resiliencia 1x7=7** y **subyugación 1x7=7**.
- Igualmente el aislamiento de la infraestructura de red inalámbrica de la infraestructura de red interna de datos facilitaría las labores de identificación, enmascarado y ocultado de interacciones informáticas, así como la detección de cambios de tránsito de información en él núcleo de la red de datos, por lo tanto, **confidencialidad x1**, **privacidad x1** e **integridad x1**.

La valoración de evaluación de riesgos RAV que se obtendría finalmente en la infraestructura de red inalámbrica de la Tercera División del Cantón Militar de Popayán, si se acogen e implementan todas las sugerencias y recomendaciones de control propuestas en el desarrollo de este proyecto de grado para la prestación del servicio de red inalámbrica del Ejército Nacional de Colombia, quedaría como se puede apreciar en la tabla a continuación.

En dicha tabla se observa cual sería el resultado de realizar una segunda valoración a la infraestructura de red inalámbrica del Cantón Militar con la implementación de los controles propuestos, en donde se puede apreciar claramente un incremento significativo en la valoración de evaluación de riesgos que finalmente se obtendría

comparado con la valoración de la red inalámbrica actual sin los controles implementados, la cual fue de 63,7766 ravs.

Tabla 39. Valoración de evaluación de riesgos RAV con las soluciones propuestas

Attack Surface Security Metrics

OSSTMM version 3.0

OPSEC		
Visibility	9	
Access	17	
Trust	0	
Total (Porosity)	26	

CONTROLS		
Class A		Missing
Authentication	17	9
Indemnification	24	2
Resilience	29	0
Subjugation	30	0
Continuity	7	19
Total Class A	107	30

Class B		Missing
Non-Repudiation	23	3
Confidentiality	41	0
Privacy	40	0
Integrity	33	0
Alarm	22	4
Total Class B	159	7

		True Missing
All Controls Total	266	37
Whole Coverage	102,31%	14,23%

LIMITATIONS		Item Value	Total Value
Vulnerabilities	0	2,423077	0,000000
Weaknesses	0	2,153846	0,000000
Concerns	0	1,269231	0,000000
Exposures	0	0,142308	0,000000
Anomalies	0	0,000000	0,000000
Total # Limitations	0		0,0000

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

OPSEC 11,663184
True Controls 11,212449
Full Controls 11,730932
True Coverage A 76,92%
True Coverage B 94,62%
Total True Coverage 85,77%
Limitations 0,000000
Security Δ 0,07
True Protection 99,55

OSSTMM
www.osstmm.org
Open Source Security Testing Methodology Manual

Actual Security: 98,6995 Ravs

6.4. Conclusiones

A continuación se presentan las conclusiones de la ejecución de este proyecto basadas en los resultados obtenidos al realizar la implementación de la metodología de pruebas de penetración para evaluar el nivel de seguridad de la información en la infraestructura de red inalámbrica del Cantón Militar de Popayán, las cuales al

concretarse soportaron la solución o mejora de buenas prácticas de las vulnerabilidades detectadas y enmarcadas en los resultados de esta investigación, brindando herramientas para hacer la debida gestión en auditoría de red inalámbrica en el Batallón para la prevención de intrusos y ataques informáticos. Por tanto, la evaluación del nivel de seguridad de la infraestructura de red inalámbrica del Cantón Militar de Popayán para auditar las políticas de seguridad del servicio de red inalámbrica del Ejército Nacional de Colombia entrega las siguientes conclusiones.

- El nivel de seguridad de la información en la infraestructura de red inalámbrica del Cantón Militar de Popayán es bajo, 63,7766 ravs, por cuanto no cumple con ninguna de las recomendaciones de buenas prácticas debidas para realizar la gestión apropiada de la seguridad de la infraestructura de red inalámbrica de una institución con un contexto tan importante como el militar, en donde se custodia información de alto valor con clasificación restringida y confidencial de índole nacional, principalmente para la adecuada operación militar e institucional del Ejército Nacional, lo cual es sumamente importante en un país con un constante conflicto armado como lo es la República de Colombia.

- Al realizar la comparación de las metodologías para pruebas de penetración tales como OSSTMM, OWASP, ISSAF, NIST, PTES y PTF, se logró identificar diferentes buenas prácticas que deben implementarse en la infraestructura de la red de datos del Cantón Militar de Popayán para gestionar vulnerabilidades en la red inalámbrica que minimicen el riesgo de un posible ataque informático por un intruso malicioso e incrementen el nivel de seguridad de la información. Las metodologías contrastadas básicamente contienen una estructura para realizar pruebas de penetración que permiten detectar vulnerabilidades existentes en una red de datos, no obstante, cada metodología tiene un enfoque particular con diferentes perfiles de evaluación que dependen de diversos objetivos a auditar en la red. Sin embargo, todas las metodologías contienen una estructura general que consiste en la identificación del contexto de las pruebas de penetración, la definición del alcance de las pruebas, la inspección de la red objetivo en busca de vulnerabilidades, la explotación de las vulnerabilidades identificadas, la elaboración de un informe de resultados y las recomendaciones para la gestión de las vulnerabilidades. Además, las metodologías de código abierto constituyen un marco de referencia y no un estándar que obligue a un seguimiento estricto para su implementación, pueden incluso adaptarse según el objetivo u orientación deseada de las pruebas, siendo posible combinar los lineamientos propuestos por varias metodologías para definir una estructura propia de pruebas. Así mismo, no tienen preferencias por el uso de determinadas herramientas de pruebas dado que no tienen compromisos comerciales con ninguna marca fabricante.

- Del análisis de las diferentes metodologías comparadas, se encontró que OSSTMM es la metodología para pruebas de penetración más completa para gestión de redes inalámbricas debido a su enfoque administrativo, siendo la metodología que mejor abarca los riesgos, vulnerabilidades y amenazas enmarcados en la norma técnica colombiana ISO 27001 sobre *Técnicas de Seguridad* para sistemas de gestión de la seguridad de la información y por ende es la metodología que mejor se adapta para evaluar el nivel de seguridad de la infraestructura de red inalámbrica del Cantón Militar de Popayán. Además, OSSTMM presenta una clasificación de tipos de pruebas más completa, que permite abarcar un rango más amplio de aspectos, necesidades y requerimientos de la institución militar, que los parámetros cubiertos por las demás metodologías abiertas comparadas en este proyecto.

- Las pruebas de penetración permiten comprender los riesgos a los cuales se encuentra expuesta la información de una institución, evaluando cada uno de los activos en producción que hacen parte de la infraestructura de la red de datos sin limitarse exclusivamente a componentes tecnológicos, sino involucrando todos los activos que participan en los procesos operativos, administrativos y de gestión de la red como son el personal de sistemas del Ejército, las políticas de seguridad y los usuarios de la institución. Este enfoque permite identificar las diferentes posibilidades de ataque informático que tiene un intruso malicioso para explotar las vulnerabilidades presentes en la red de la institución y plantear acciones para su gestión desde diferentes puntos de vista. Como resultado se pudo sugerir ocho (8) buenas prácticas en cuanto al diseño de la infraestructura de red de datos del Cantón Militar de Popayán, agrupadas en tres aspectos fundamentales en la gestión de una red de datos: diseño, administración y seguridad, permitiendo mayor eficiencia y eficacia en el proceso de auditoría a la red inalámbrica en la institución militar.

- El acceso al servicio de red inalámbrica por parte de los usuarios del Ejército Nacional no se encuentra regulado o controlado por ningún sistema de monitoreo y control que permita hacer gestión a la red inalámbrica, desde cualquier terminal o dispositivo se puede realizar algún tipo de acceso no autorizado o incluso se puede extender el alcance de la señal de la red inalámbrica más allá del perímetro físico del Cantón Militar, posibilitando atacar los dispositivos de la infraestructura de red inalámbrica para acceder a la información confidencial militar consignada en el área de almacenamiento de información. Igualmente existe desconocimiento de normas y políticas de seguridad de la información por parte de los usuarios del Ejército Nacional de Colombia en el Cantón Militar de Popayán que acceden a la red inalámbrica.

- La segmentación del direccionamiento de la infraestructura de red de datos del Cantón Militar de Popayán no es óptima debido a que la asignación de direcciones de red para las terminales y dispositivos que se autentiquen en la red inalámbrica no tiene ningún tipo de orden u organización desde un enfoque administrativo, tampoco existe segmentación virtual de la red por unidades militares, por ende todos los terminales y dispositivos de acceso e interconexión se encuentran en un único dominio de red, dificultando la gestión de la red de datos y facilitando la labor de inteligencia en ingeniería social que debe hacer un intruso para ejecutar un ataque informático exitoso.

- Las diferentes herramientas informáticas ejecutadas en la metodología de pruebas de penetración permitieron identificar vulnerabilidades existentes en la infraestructura de red inalámbrica del Cantón Militar de Popayán y proponer con base en ellas, las respectivas mejoras correspondientes tanto de infraestructura de red inalámbrica como de buenas prácticas en gestión de redes de datos, como lo son el monitoreo de canales, segmentación de la red, administración de credenciales de acceso y tipo de encriptación, detección y prevención de intrusiones y gestión de políticas de seguridad, lo cual permitirá disminuir la posibilidad de un ataque informático por parte de un intruso malicioso e incrementará el nivel de seguridad de la información en la red de datos del Ejército Nacional de Colombia.

- Existe falta de personal capacitado en administración de redes de datos por parte del Ejército Nacional de Colombia. Se evidenció falta de entrenamiento en seguridad de la información en el personal que realiza la gestión de la infraestructura de red de datos a nivel general, hecho que facilitaría circunstancialmente la labor de un intruso en un eventual ataque informático a la red inalámbrica del Cantón Militar de Popayán. De igual manera, no existen los mecanismos necesarios para proteger la red inalámbrica del Cantón Militar en tiempo real ante un eventual ataque inalámbrico, siendo un riesgo importante, principalmente si el ataque se ejecuta de manera remota desde el exterior del perímetro físico del Cantón.

- Con las recomendaciones y sugerencias propuestas en el desarrollo de este proyecto, se lograría incrementar el nivel de seguridad de la infraestructura de red inalámbrica del Cantón Militar de Popayán a una valoración RAV de 98,6995 ravs, con esto se logra un incremento del 34,9% del nivel de seguridad de la información actual, por lo tanto se espera que sean implementadas todas las soluciones de gestión propuestas para mejorar el nivel de seguridad, integridad, autenticidad y confidencialidad de la información militar del Ejército Nacional de Colombia en la infraestructura de red inalámbrica del Cantón Militar de Popayán.

7. Bibliografía

IDS HPE. (2012). HP procurve rf manager an sensors. *Installation and getting started guide*(5998-3285). Hewlett packard enterprise. Obtenido de https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-c02566037

IPS HPE. (2015). HPE TippingPoint NX Platform. *Next generation intrusion prevention systems*(Rev 4). Hewlett packard enterprise. Obtenido de https://www.trendmicro.co.kr/cloud-content/us/pdfs/business/datasheets/ds_next_gen_intrusion_prevention_systems.pdf

ISO 27001. (2006). Tecnología de la información. Técnicas de seguridad. *Sistemas de gestión de la seguridad de la información (SGSI). Requisitos*(v1). ICONTEC. Obtenido de intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

Marco ISSAF. (2006). Information Systems Security Assessment Framework. *Penetration testing framework PTF*(0.2.1.B). OISSG, Open information system security group. Obtenido de http://www.oissg.org/issaf

Marco PTF. (2014). Penetration Testing Framework. *Vulnerability analysts and penetration testers starting resource*(0.59). Vulnerability assessment. Obtenido de http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html

Metodología NIST. (2008). Technical Guide to Information Security Testing and Assessment. *Recommendations of the National Institute of Standards and Technology*(SP 800-115). NIST, The National Institute of Standards and Technology. Obtenido de https://www.nist.gov/publications/technical-guide-information-security-testing-and-assessment

Metodología OSSTMM. (2010). Open Source Security Testing Methodology Manual. *Contemporary security testing and analysis*(v3). ISECOM, Institute for security and open methodologies. Obtenido de http://www.isecom.org/research/osstmm.html

Metodología OWASP. (2014). Open Web Application Security Project. *Testing Guide*(v4). The OWASP Foundation. Obtenido de https://www.owasp.org/index.php/OWASP_Testing_Guide_v3_Table_of_Contents

Metodología PTES. (2012). The Penetration Testing Execution Standard. *Technical Guidelines*(v288). PTES, The Penetration Testing Execution Standard. Obtenido de http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

Servidor archivos. (2018). SharePoint Server 2019. *Reviewer's Guide*(v.1). Microsoft Corporation. Obtenido de https://spdocs.blob.core.windows.net/preview/SharePoint%20Server%202019%20Reviewer%27s%20Guide.pdf

Servidor archivos licenciamiento. (2017). Servidor Microsoft SharePoint. *Commercial licensing brief*(v1). Microsoft Corporation. Obtenido de

https://download.microsoft.com/download/3/D/4/3D42BDC2-6725-4B29-B75A-A5B04179958B/Licensing_Microsoft_SharePoint_Server.pdf

Solicitud Servicios Informátivos Usuarios. (2018). Comando General Fuerzas Militares. *Departamento de Comunicaciones Formato FO-JEMPP-CEDE6-1034*(v.1). Ministerio de Defensa Nacional. Obtenido de Ejército Nacional de Colombia

Switch WLAN. (2015). Conmutador HPE LAN-WLAN unificada. *HPE 830 Unified Wired-WLAN Switch Series*(Rev. 9). Hewlett packard enterprise. Obtenido de https://andovercg.com/datasheets/hp-830-switch-series.pdf

WDS HPE1. (2012). HPE Aruba Networks AirMesh. *Outdoor MIMO Wireless Networks*(v1.0). Hewlett packard enterprise. Obtenido de https://www.slideshare.net/ArubaNetworks/outdoor-mimo-wireless-networks

WDS HPE2. (2017). HPE Aruba Networks AirMesh. *High-Performance Outdoor Connectivity with*(v2). Hewlett packard enterprise. Obtenido de http://rhowireless.com/aruba/docs/AirMeshSolutionBrochure.pdf

Anexos

ANEXO A. Autorización pruebas de penetración en la red inalámbrica del Cantón Militar de Popayán

Bogotá, D.C., 25 de Junio 2018.

Señor
RAFAEL LONDOÑO CARANTON
Subdirector de Estándares y Arquitectura de TI
Bogotá D.C.-

Asunto: Autorización Anteproyecto.

Respetuosamente me permito informar al señor Subdirector de Estándares y Arquitectura de TI, que el anteproyecto "Evaluación de la Seguridad de la Red Inalámbrica del Cantón Militar de Popayán", está autorizado para realizarse en el Cantón Militar de Popayán – Tercera División, por parte de la TE. YEIMY CAROLINA RODRIGUEZ RODRIGUEZ con CM. 38364916.

En atención a la presente solicitud para los fines y tramites que estime convenientes.

Cordialmente,

SP. DIEGO ANDRES VALENCIA HOLGUIN
Suboficial Comunicaciones Tercera División

Correo: diego.valencia@ejercito.mil.co
diegoholguinv1979@gmail.com
Celular: 3112870090.

Bogotá, D.C., 29 de Junio de 2018

Señor
RAFAEL LONDOÑO CARANTON
Subdirector de Estándares y Arquitectura de TI
Bogotá D.C.-

Asunto: Definición alcance pruebas de penetración proyecto

Respetuosamente me permito informar al señor Subdirector de Estándares y Arquitectura de TI, que el presente documento se establece para definir el alcance de las pruebas de seguridad autorizadas para ejecutarse en el Cantón Militar de Popayán - Tercera División en el desarrollo del proyecto "Evaluación de la seguridad de la red inalámbrica del Cantón Militar de Popayán" por parte de la TE. YEIMY CAROLINA RODRIGUEZ RODRIGUEZ con CM 38364916.

La definición del alcance de las pruebas de penetración a ejecutarse en la red inalámbrica del Cantón Militar de Popayán - Tercera División es la siguiente:

- Las pruebas de seguridad serán ejecutadas únicamente en el Cantón Militar de Popayán - Tercera División como fue autorizado, no podrán realizarse desde ninguna otra unidad militar.
- No se interrumpirá el servicio de red inalámbrica a los usuarios del Cantón Militar durante la ejecución de las pruebas de penetración, ni de ningún otro servicio informático.
- No se modificarán los parámetros de configuración de los dispositivos de la red inalámbrica del Cantón Militar ni de autenticación de los usuarios del Ejército para navegar en Internet.
- No se afectará ni se modificarán los parámetros de configuración de ningún dispositivo de toda la infraestructura de la red de datos del Ejército Nacional de Colombia.
- Se permite el uso de herramientas de hackeo informático ético que no violen las políticas de seguridad del Ejército Nacional de Colombia en cuanto al tratamiento de la información encontrada, la cual es considerada de orden clasificado y restringido, es decir, que no expongan públicamente ningún tipo de información o datos que pueda comprometer la seguridad de la información desde el Cantón Militar de Popayán.

- Se restringen las pruebas de penetración informática únicamente a los puntos de acceso de la red inalámbrica del Cantón Militar de Popayán, no se autorizan pruebas de penetración contra las terminales, dispositivos de interconexión ni ningún otro activo de red diferente, por cuánto estás labores están restringidas y autorizadas únicamente al personal militar que labora en el área de seguridad informática en la institución, por protocolos de seguridad de contrainteligencia militar interna de la red del Ejército Nacional de Colombia.
- Se debe suspender inmediatamente las pruebas de penetración si se logra acceder al área de almacenamiento SAN con los servidores que contienen información militar confidencial y de acceso restringido en la ciudad de Bogotá.

Cordialmente,

SP. DEGO ANDRES VALENCIA HOLGUIN
Suboficial Comunicaciones Tercera División

Correo: diego.valencia@ejercito.mil.co
diegoholguinv1979@gmail.com
Celular: 3112870090

CAROLINA RODRIGUEZ

TE. YEIMY CAROLINA RODRIGUEZ RODRIGUEZ
B6-Comunicaciones C5

Correo: yeimy.rodriguez@ejercito.mil.co
caritoesunica@gmail.com
Celular: 3502479042

ANEXO C. Escala de valoración de metodologías de pruebas de penetración bajo definición de riesgos de la norma NTC-ISO 27001

Se presenta la definición de vulnerabilidades, amenazas y riesgos de la norma NTC-ISO 27001 para evaluar objetivos de control y controles como parte del proceso del sistema de gestión de seguridad de la información. Esta norma proporciona asesoría y orientación sobre las mejores prácticas de apoyo a los controles especificados, los cuales se describen a continuación (ISO 27001, 2006).

Este anexo contiene la escala de valoración de riesgos para seleccionar la metodología adecuada a implementarse para gestión de seguridad de la información en la red inalámbrica del Cantón Militar de Popayán.

RIESGO, AMENAZA O VULNERABILIDAD		METODOLOGÍA | MARCO					
		OSSTMM	OWASAP	ISAAF	NIST	PTES	PTF
A.5 POLÍTICA DE SEGURIDAD		**6**	**6**	**5**	**6**	**5**	**1**
A.5.1 Política de seguridad de la información		**6**	**6**	**5**	**6**	**5**	**1**
A.5.1.1	Documento de política de seguridad de la información	3	3	2	3	2	0
A.5.1.2	Revisión de política de seguridad de la información	3	3	3	3	3	1
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		**33**	**24**	**9**	**31**	**12**	**5**
A.6.1 Organización interna		**24**	**17**	**0**	**23**	**7**	**0**
A.6.1.1	Compromiso de la dirección con la seguridad de la información	3	3	0	3	2	0
A.6.1.2	Coordinación de seguridad de la información	3	3	0	3	2	0
A.6.1.3	Asignación de responsabilidades para seguridad de la información	3	2	0	2	0	0
A.6.1.4	Proceso de autorización para servicios de procesamiento de información	3	3	0	3	0	0
A.6.1.5	Acuerdos sobre confidencialidad	3	1	0	3	0	0
A.6.1.6	Contacto con autoridades	3	1	0	3	0	0
A.6.1.7	Contacto con grupos de interés especiales	3	1	0	3	0	0
A.6.1.8	Revisión independiente de seguridad de la información	3	3	0	3	3	0
A.6.2 Partes externas		**9**	**7**	**9**	**8**	**5**	**5**
A.6.2.1	Identificación de riesgos relacionados con las partes externas	3	3	3	3	2	3
A.6.2.2	Consideraciones de seguridad para clientes	3	3	3	3	3	2
A.6.2.3	Consideraciones de seguridad en acuerdos con terceras partes	3	1	3	2	0	0
A.7 GESTIÓN DE ACTIVOS		**15**	**3**	**9**	**14**	**5**	**3**
A.7.1 Responsabilidad por los activos		**9**	**0**	**9**	**9**	**5**	**3**
A.7.1.1	Inventario de activos	3	0	3	3	3	3
A.7.1.2	Propiedad de activos	3	0	3	3	2	0
A.7.1.3	Uso aceptable de activos	3	0	3	3	0	0
A.7.2 Clasificación de la información		**6**	**3**	**0**	**5**	**0**	**0**
A.7.2.1	Directrices de clasificación	3	2	0	3	0	0
A.7.2.2	Etiquetado y manejo de información	3	1	0	2	0	0
A.8 SEGURIDAD DE LOS RECURSOS HUMANOS		**24**	**10**	**0**	**23**	**0**	**0**
A.8.1 Antes de la contratación laboral		**9**	**7**	**0**	**9**	**0**	**0**
A.8.1.1	Roles y responsabilidades	3	3	0	3	0	0
A.8.1.2	Selección	3	1	0	3	0	0
A.8.1.3	Términos y condiciones laborales	3	3	0	3	0	0
A.8.2 Durante la vigencia de la contratación laboral		**9**	**3**	**0**	**8**	**0**	**0**
A.8.2.1	Responsabilidades de la dirección	3	3	0	3	0	0
A.8.2.2	Educación, formación y concientización sobre la	3	0	0	3	0	0

	seguridad de la información						
A.8.2.3	Proceso disciplinario	3	0	0	2	0	0
A.8.3 Terminación o cambio de contratación laboral		**6**	**0**	**0**	**6**	**0**	**0**
A.8.3.1	Responsabilidades en terminación	2	0	0	2	0	0
A.8.3.2	Devolución de activos	2	0	0	1	0	0
A.8.3.3	Retiro de derechos de acceso	2	0	0	3	0	0
A.9 SEGURIDAD FÍSICA Y DEL ENTORNO		**27**	**12**	**10**	**21**	**11**	**4**
A.9.1 Áreas seguras		**16**	**10**	**6**	**11**	**6**	**0**
A.9.1.1	Perímetro de seguridad física	3	3	1	3	3	0
A.9.1.2	Controles de acceso físico	3	3	1	3	3	0
A.9.1.3	Seguridad de oficinas, recintos e instalaciones	3	1	1	2	0	0
A.9.1.4	Protección contra amenazas externas y ambientales	3	3	1	3	0	0
A.9.1.5	Trabajo en áreas seguras	2	0	1	0	0	0
A.9.1.6	Áreas de carga, despacho y acceso público	2	0	1	0	0	0
A.9.2 Seguridad de los equipos		**11**	**2**	**4**	**10**	**5**	**4**
A.9.2.1	Ubicación y protección de equipos	3	2	1	3	2	1
A.9.2.2	Servicios de suministro	3	0	1	2	1	1
A.9.2.3	Seguridad del cableado	3	0	2	3	2	2
A.9.2.4	Mantenimiento de equipos	1	0	0	1	0	0
A.9.2.5	Seguridad de equipos fuera de las instalaciones	1	0	0	1	0	0
A.9.2.6	Seguridad en reutilización oeliminación de los equipos	0	0	0	0	0	0
A.9.2.7	Retiro de activos	0	0	0	0	0	0
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES		**86**	**70**	**28**	**81**	**30**	**22**
A.10.1 Procedimientos operacionales y responsabilidades		**10**	**9**	**0**	**10**	**0**	**0**
A.10.1.1	Documentación de procedimientos de operación	3	3	0	3	0	0
A.10.1.2	Gestión del cambio	3	2	0	3	0	0
A.10.1.3	Distribución de funciones	3	2	0	3	0	0
A.10.1.4	Separación de instalaciones de desarrollo, ensayo y operación	1	2	0	1	0	0
A.10.2 Gestión de la prestación del servicio por terceras partes		**9**	**0**	**3**	**8**	**3**	**3**
A.10.2.1	Prestación del servicio	3	0	3	3	3	3
A.10.2.2	Monitoreo y revisión de servicios por terceras partes	3	0	0	3	0	0
A.10.2.3	Gestión de cambios en servicios por terceras partes	3	0	0	2	0	0
A.10.3 Planificación y aceptación del sistema		**6**	**6**	**4**	**6**	**4**	**4**
A.10.3.1	Gestión de la capacidad	3	3	2	3	2	2
A.10.3.2	Aceptación del sistema	3	3	2	3	2	2
A.10.4 Protección contra códigos maliciosos y móviles		**6**	**6**	**4**	**4**	**6**	**4**
A.10.4.1	Controles contra códigos maliciosos	3	3	2	2	3	2
A.10.4.2	Controles contra códigos móviles	3	3	2	2	3	2
A.10.5 Respaldo		**3**	**3**	**0**	**3**	**0**	**0**
A.10.5.1	Respaldo de la información	3	3	0	3	0	0
A.10.6 Gestión de la seguridad de las redes		**6**	**6**	**6**	**6**	**6**	**0**
A.10.6.1	Controles de las redes	3	3	3	3	3	0
A.10.6.2	Seguridad de servicios de la red	3	3	3	3	3	0
A.10.7 Manejo de los medios		**11**	**6**	**3**	**12**	**3**	**3**
A.10.7.1	Gestión de medios removibles	3	0	0	3	0	0
A.10.7.2	Eliminación de medios	2	0	0	3	0	0
A.10.7.3	Procedimientos para manejo de la información	3	3	0	3	0	0
A.10.7.4	Seguridad de la documentación del sistema	3	3	3	3	3	3
A.10.8 Intercambio de la información		**13**	**9**	**4**	**13**	**4**	**4**
A.10.8.1	Políticas y procedimientos para intercambio de información	3	3	0	3	0	0
A.10.8.2	Acuerdos para el intercambio	3	2	0	3	0	0
A.10.8.3	Medios físicos en tránsito	2	1	1	2	1	1
A.10.8.4	Mensajería electrónica	2	0	0	2	0	0
A.10.8.5	Sistemas de información del negocio	3	3	3	3	3	3
A.10.9 Servicios de comercio electrónico		**4**	**7**	**0**	**4**	**0**	**0**

A.10.9.1	Comercio electrónico	0	2	0	0	0	0
A.10.9.2	Transacciones en línea	2	2	0	2	0	0
A.10.9.3	Información disponible al público	2	3	0	2	0	0
A.10.10 Monitoreo		**18**	**18**	**4**	**15**	**4**	**4**
A.10.10.1	Registro de auditorías	3	3	0	3	0	0
A.10.10.2	Monitoreo del uso del sistema	3	3	2	3	2	2
A.10.10.3	Protección de la información del registro	3	3	2	3	2	2
A.10.10.4	Registros del administrador y del operador	3	3	0	3	0	0
A.10.10.5	Registro de fallas	3	3	0	3	0	0
A.10.10.6	Sincronización de relojes	3	3	0	0	0	0
A.11 CONTROL DE ACCESO		**72**	**69**	**65**	**69**	**65**	**65**
A.11.1 Requisito del negocio para el control de acceso		**3**	**3**	**2**	**3**	**2**	**2**
A.11.1.1	Política de control de acceso	3	3	2	3	2	2
A.11.2 Gestión del acceso de usuarios		**12**	**12**	**9**	**12**	**9**	**9**
A.11.2.1	Registro de usuarios	3	3	3	3	3	3
A.11.2.2	Gestión de privilegios	3	3	2	3	2	2
A.11.2.3	Gestión de contraseñas para usuarios	3	3	2	3	2	2
A.11.2.4	Revisión de los derechos de acceso de los usuarios	3	3	2	3	2	2
A.11.3 Responsabilidades de los usuarios		**6**	**3**	**3**	**3**	**3**	**3**
A.11.3.1	Uso de contraseñas	3	3	3	3	3	3
A.11.3.2	Equipo de usuario desatendido	3	0	0	0	0	0
A.11.3.3	Política de escritorio despejado y de pantalla despejada	0	0	0	0	0	0
A.11.4 Control de acceso a las redes		**21**	**21**	**21**	**21**	**21**	**21**
A.11.4.1	Política de uso de servicios de red	3	3	3	3	3	3
A.11.4.2	Autenticación de usuarios para conexiones externas	3	3	3	3	3	3
A.11.4.3	Identificación de equipos en las redes	3	3	3	3	3	3
A.11.4.4	Protección de puertos de configuración y diagnóstico remoto	3	3	3	3	3	3
A.11.4.5	Separación en las redes	3	3	3	3	3	3
A.11.4.6	Control de conexión a las redes	3	3	3	3	3	3
A.11.4.7	Control de enrutamiento en la red	3	0	3	3	3	3
A.11.5 Control de acceso al sistema operativo		**18**	**18**	**18**	**18**	**18**	**18**
A.11.5.1	Procedimientos de ingreso seguros	3	3	3	3	3	3
A.11.5.2	Identificación y autenticación de usuarios	3	3	3	3	3	3
A.11.5.3	Sistema de gestión de contraseñas	3	3	3	3	3	3
A.11.5.4	Uso de las utilidades del sistema	3	3	3	3	3	3
A.11.5.5	Tiempo de inactividad de sesión	3	3	3	3	3	3
A.11.5.6	Limitación del tiempo de conexión	3	3	3	3	3	3
A.11.6 Control de acceso a las aplicaciones y a la información		**6**	**6**	**6**	**6**	**6**	**6**
A.11.6.1	Restricción de acceso a la información	3	3	3	3	3	3
A.11.6.2	Aislamiento de sistemas sensibles	3	3	3	3	3	3
A.11.7 Computación móvil y trabajo remoto		**6**	**6**	**6**	**6**	**6**	**6**
A.11.7.1	Computación ycomunicaciones móviles	3	3	3	3	3	3
A.11.7.2	Trabajo remoto	3	3	3	3	3	3
A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN		**41**	**48**	**33**	**38**	**34**	**33**
A.12.1 Requisitos de seguridad de los sistemas de información		**3**	**3**	**3**	**3**	**3**	**3**
A.12.1.1	Análisis y especificación de los requisitos de seguridad	3	3	3	3	3	3
A.12.2 Procesamiento correcto en las aplicaciones		**11**	**12**	**11**	**11**	**11**	**11**
A.12.2.1	Validación de datos de entrada	3	3	3	3	3	3
A.12.2.2	Control de procesamiento interno	3	3	3	3	3	3
A.12.2.3	Integridad del mensaje	3	3	3	3	3	3
A.12.2.4	Validación de datos de salida	2	3	2	2	2	2
A.12.3 Controles criptográficos		**6**	**6**	**5**	**6**	**5**	**5**
A.12.3.1	Política sobre uso de controles criptográficos	3	3	3	3	3	3
A.12.3.2	Gestión de llaves	3	3	2	3	2	2
A.12.4 Seguridad de los archivos del sistema		**5**	**9**	**4**	**4**	**5**	**4**

A.12.4.1	Control del software operativo	3	3	2	2	3	2
A.12.4.2	Protección de datos de prueba del sistema	2	3	2	2	2	2
A.12.4.3	Control de acceso al código fuente de los programas	0	3	0	0	0	0
A.12.5 Seguridad en los procesos de desarrollo y soporte		**13**	**15**	**7**	**11**	**7**	**7**
A.12.5.1	Procedimientos de control de cambios	3	3	0	2	0	0
A.12.5.2	Revisión técnica de aplicaciones después de cambios en sistema operativo	3	3	3	3	3	3
A.12.5.3	Restricciones en cambios a paquetes de software	2	3	1	1	1	1
A.12.5.4	Fuga de información	3	3	3	3	3	3
A.12.5.5	Desarrollo de software contratado externamente	2	3	0	2	0	0
A.12.6 Gestión de la vulnerabilidad técnica		**3**	**3**	**3**	**3**	**3**	**3**
A.12.6.1	Control de vulnerabilidades técnicas	3	3	3	3	3	3
A.13 GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN		**15**	**14**	**4**	**11**	**6**	**4**
A.13.1 Reporte sobre los eventos y las debilidades de la seguridad de la información		**6**	**6**	**4**	**6**	**6**	**4**
A.13.1.1	Reporte sobre eventos de seguridad de la información	3	3	2	3	3	2
A.13.1.2	Reporte sobre debilidades de la seguridad	3	3	2	3	3	2
A.13.2 Gestión de los incidentes y las mejoras en la seguridad de la información		**9**	**8**	**0**	**5**	**0**	**0**
A.13.2.1	Responsabilidades yprocedimientos	3	3	0	3	0	0
A.13.2.2	Aprendizaje debido a incidentes de seguridad de la información	3	2	0	2	0	0
A.13.2.3	Recolección de evidencia	3	3	0	0	0	0
A.14 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO		**14**	**12**	**1**	**13**	**1**	**1**
A.14.1 Aspectos de seguridad de la información, de la gestión de la continuidad del negocio		**14**	**12**	**1**	**13**	**1**	**1**
A.14.1.1	Inclusión de seguridad de la información en proceso de gestión de continuidad del negocio	3	3	0	3	0	0
A.14.1.2	Continuidad del negocio y evaluación de riesgos	3	3	1	3	1	1
A.14.1.3	Desarrollo e implementación de planes de continuidad que incluyen seguridad de la información	3	2	0	2	0	0
A.14.1.4	Estructura para planificación de continuidad del negocio	3	2	0	3	0	0
A.14.1.5	Pruebas, mantenimiento y reevaluación de planes de continuidad del negocio	2	2	0	2	0	0
A.15 CUMPLIMIENTO		**29**	**26**	**12**	**28**	**14**	**12**
A.15.1 Cumplimiento de los requisitos legales		**17**	**14**	**4**	**16**	**4**	**4**
A.15.1.1	Identificación de la legislación aplicable	3	3	0	3	0	0
A.15.1.2	Derechos de propiedad intelectual (DPI)	3	2	0	3	0	0
A.15.1.3	Protección de los registros de la organización	3	2	0	3	0	0
A.15.1.4	Protección de datos y privacidad de la información personal	3	2	2	3	2	2
A.15.1.5	Prevención del uso inadecuado de servicios de procesamiento de información	3	3	0	2	0	0
A.15.1.6	Reglamentación de los controles criptográficos	2	2	2	2	2	2
A.15.2 Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico		**6**	**6**	**4**	**6**	**4**	**4**
A.15.2.1	Cumplimiento con políticas y normas de seguridad	3	3	2	3	2	2
A.15.2.2	Verificación del cumplimiento técnico	3	3	2	3	2	2
A.15.3 Consideraciones de la auditoría de los sistemas de información		**3**	**3**	**2**	**3**	**3**	**2**
A.15.3.1	Controles de auditoría de sistemas de información	3	3	2	3	3	2
A.15.3.2	Protección de las herramientas de auditoría de los sistemas de información	3	3	2	3	3	2
VALORACIÓN TOTAL		**362**	**294**	**176**	**335**	**183**	**150**