Universidad Tecnológica Ecotec

Facultad de Ingenierías, arquitectura y ciencias de la naturaleza ingeniería en tecnologías de la información

Título del trabajo:

Desarrollo de un procedimiento de seguridad para la red implementada de los esquemas de la Estación Naval Penitenciaria de Ecuador “ESNAPE”.

Línea de Investigación:

Tecnologías de la información y comunicación

Modalidad de titulación:

Trabajo de integración curricular

Carrera:

Ingeniería en tecnologías de la información

Título a obtener:

Ingeniero en tecnologías de la información

Autor (a):

Andie Paúl Guanoluisa Chávez

Tutores:

Mgtr. Marcos Espinoza

Samborondón – Ecuador

2025

DEDICATORIA

Esta tesis está dedicada con profunda gratitud y amor a los pilares de mi vida y a mis compañeros de trayectoria académica.

A mis queridos padres, cuyo inquebrantable apoyo, guía y sacrificio han sido la piedra angular de cada logro que he alcanzado. Su aliento ha sido mi fortaleza, y su fe en mí, el motor de cada noche de insomnio y de mi incansable búsqueda de la excelencia. Debo este hito a los valores que me inculcaron y a los sueños que me ayudaron a alcanzar.

A mi querido hermano, Justin Sebastián Guanoluisa, gracias por ser mi constante fuente de inspiración y motivación. Sus palabras de aliento y su genuino orgullo por mi progreso me han ayudado a superar momentos de duda y me han recordado por qué sigo adelante.

A los dedicados funcionarios del área de Tecnologías de la Información y la Comunicación (TIC) de la Gobernación de la Provincia del Guayas, les expreso mi más sincero agradecimiento. Su mentoría, orientación técnica y constante motivación fueron fundamentales para ampliar mi perspectiva y agudizar mi disciplina. Su profesionalismo y generosidad dejaron una huella imborrable en mi trayectoria académica. Al personal de la Fiscalía de Durán, les agradezco profundamente su invaluable apoyo y enseñanzas. Su compromiso con la justicia y la integridad me inspiró a cursar mis estudios de derecho con propósito y responsabilidad. Las lecciones que adquirí bajo su guía han enriquecido tanto mis conocimientos como mi carácter.

Finalmente, a mis compañeros de la Universidad Estatal, cuya camaradería y colaboración se convirtió en un capítulo importante de mi vida. Nuestras luchas compartidas, las largas noches preparando presentaciones, debates, disertaciones orales para simulaciones de audiencias en tribunales y el incansable trabajo en equipo nos permitieron llegar hasta el final de la carrera de derecho. El 11 de julio de 2025 pudimos egresar, siendo este un testimonio de nuestra unidad, perseverancia y dedicación a la profesión jurídica.

Para cada uno de ustedes, este logro es tanto suyo como mío.

AGRADECIMIENTO

Ante todo, ofrezco mi más profunda gratitud a Dios por guiarme en cada paso de este camino. En momentos de incertidumbre y fatiga, su presencia me brindó la luz y la sabiduría que me sostuvieron. Sin la gracia divina, este logro no habría sido posible.

A mis queridos padres, su apoyo incondicional, sus sacrificios y su amor incondicional han sido la base sólida sobre la que se asienta este logro. Su fortaleza me ha inspirado y su confianza en mi potencial ha alimentado mi ambición. Cada logro que alcanzo es un reflejo de su dedicación a mi futuro.

A mi hermano menor, Justin Guanoluisa, gracias por su inagotable aliento y su espíritu alegre. Su fortaleza silenciosa y su fe en mí fueron un recordatorio constante para seguir adelante.

A los profesionales del área de Tecnologías de la Información y la Comunicación de la Gobernación de la Provincia del Guayas, les agradezco sinceramente su apoyo y guía. Sus conocimientos técnicos, motivación y mentoría han sido fundamentales para moldear mi perspectiva académica y profesional. A los profesores de la Facultad de Ingeniería de la Universidad Tecnológica Ecotec, gracias por su dedicación y experiencia. Sus conocimientos y guía me han convertido una mejor persona.

Sobre todo, extiendo mi más sincero agradecimiento a la Armada del Ecuador. Ha sido un verdadero honor desarrollar esta tesis en una de las instituciones más prestigiosas y respetadas de nuestro país. Su confianza y colaboración han enaltecido este proyecto académico, y me enorgullece haberlo llevado a cabo bajo su distinguido nombre.

A cada uno de los antes mencionados, les ofrezco mi sincera y eterna gratitud.

ANEXO No. 9

PROCESO DE TITULACIÓN
CERTIFICADO DE APROBACIÓN DEL TUTOR

Samborondón, 04 de Agosto de 2025

Magíster
Erika Ascencio Jordán
Facultad de Ingenierías, Arquitectura y Ciencias de la Naturaleza
Universidad Tecnológica ECOTEC

De mis consideraciones:

Por medio de la presente comunico a usted que el trabajo de titulación TITULADO: **Propuesta de fortalecimiento de la seguridad de redes wifi en entornos sensibles de la comunicación en la Estación Naval Penitenciaria de Ecuador**, fue revisado, siendo su contenido original en su totalidad, así como el cumplimiento de los requerimientos establecidos en la guía para su elaboración, por lo que se autoriza al estudiante: **GUANOLUISA CHAVEZ ANDIE PAUL,** para que proceda con la presentación oral del mismo.

ATENTAMENTE,

Firmado electrónicamente por:
MARCOS ANTONIO ESPINOZA MINA

Marcos Antonio Espinoza Mina, Ph.D.
Tutor

ANEXO No. 10

PROCESO DE TITULACIÓN
CERTIFICADO DEL PORCENTAJE DE COINCIDENCIAS
DEL TRABAJO DE TITULACIÓN

Habiendo sido revisado el trabajo de titulación TITULADO: **Propuesta de fortalecimiento de la seguridad de redes wifi en entornos sensibles de la comunicación en la Estación Naval Penitenciaria de Ecuador**, elaborado por GUANOLUISA CHAVEZ ANDIE PAUL fue remitido al sistema de coincidencias en todo su contenido el mismo que presentó un porcentaje del 4% mismo que cumple con el valor aceptado para su presentación que es inferior o igual al 10% sobre el total de hojas del documento. Adicional se adjunta print de pantalla de dicho resultado.


Informe de originalidad de Safeassign • Enviado el vie., 01 ago. 2025 16:56

ENTREGA ATRASADA - Documento Final del Proyecto Integrador Curricular (WORD)

PROYECTO INTEGRADOR

Puntuación total: 4 % Riesgo bajo

ANDIE PAUL GUANOLUISA CHAVEZ

Número total de informes	Coincidencia máxima	Coincidencia promedio	Enviado el	Conteo de palabras promedio
1	4 %	4 %	01/08/25	37.095

Contenido adicional 4 %

Conteo de palabras: 37.095
Origen: Andie Paul Guanoluisa Chávez - Documento Final.docx

ATENTAMENTE,

MARCOS ANTONIO ESPINOZA MINA

MARCOS ANTONIO ESPINOZA MINA, Ph.D.
Tutor

Índice

Contenido

Índice de Tablas

Índice de Ilustraciones

Índice de Figuras

RESUMEN

Esta tesis presenta el diseño de un procedimiento integral de seguridad para controlar y gestionar los accesos a la red, adaptado dentro de un área critica, tal y como lo es un reparto militar, y en este caso es la Estación Naval Penitenciaria de Ecuador “ESNAPE”.

El procedimiento define roles y responsabilidades para el personal militar técnico dentro de la ESNAPE y la DIRTIC, con el respaldo de protocolos de registro formales (Anexos A y B). Los dispositivos se registran utilizando sus direcciones MAC, previamente investigadas por medio de la herramienta DNS Checker y se les asignan IP fijas, que posteriormente se validan y agrupan para facilitar su administración, lo cual garantiza la trazabilidad, la autorización de dispositivos y el acceso seguro a internet a través de una red WiFi dentro del reparto naval por medio del firewall Fortinet FG-70F, donde se realizan las configuraciones adecuadas y los permisos de accesos a la red, implementada con puntos de acceso Ubiquiti U6-LR y el controlador Cloud Key Gen2 Plus. La interfaz de Fortinet facilita el aprovisionamiento de usuarios, la vinculación de IP/MAC y la monitorización, cabe mencionar que el propósito principal presente proyecto, no se enfoca en el desarrollo técnico en sí mismo, sino que se enfoca tanto en el diseño como en la formalización de un procedimiento operativo. Por lo tal, la simulación técnica antes mencionada se la empleo como complemento para observar no solo la factibilidad, sino también la eficiencia, además de la coherencia del flujo del procedimiento propuesto dentro del presente proyecto. Además, para evitar la saturación de los grupos de IP, se aplican mecanismos de desactivación durante los ciclos de rotación del personal militar.

Las tareas de monitoreo se centralizan a través de la interfaz del controlador de Ubiquiti, lo que permite el seguimiento en tiempo real de los dispositivos del personal militar que se encuentre haciendo uso de la red, el consumo de ancho de banda, el estado de la conexión y las asociaciones de puntos de acceso. La disponibilidad del servicio está sujeta a áreas de cobertura estrictas, y cualquier mantenimiento o interrupción se comunica con antelación. Además, se describen prácticas operativas sostenibles, que incluyen análisis continuo del tráfico, restricción de puertos no autorizados, evaluaciones de vulnerabilidad e informes mensuales de seguridad.

La solución propuesta mejora la gobernanza institucional, agiliza el acceso a la red y fortalece la infraestructura digital frente a los riesgos de ciberseguridad en constante evolución dentro de la Estación Naval Penitenciaria de Ecuador “ESNAPE”.

Palabras Clave: Seguridad de red, Firewall, Controladora Ubiquiti, autenticación IP/MAC.

ABSTRACT

This thesis presents the design of a comprehensive security procedure to control and manage network access, adapted to a critical area, such as a military facility, in this case the Ecuadorian Naval Penitentiary Station (ESNAPE).

The procedure defines roles and responsibilities for technical military personnel within ESNAPE and DIRTIC, supported by formal registration protocols (Annexes A and B). Devices are registered using their MAC addresses, previously investigated using the DNS Checker tool, and are assigned fixed IP addresses, which are subsequently validated and grouped for ease of management. This ensures traceability, device authorization, and secure internet access through a Wi-Fi network within the naval facility using the Fortinet FG-70F firewall. The appropriate configurations and network access permissions are implemented, implemented with Ubiquiti U6-LR access points and the Cloud Key Gen2 Plus controller. The Fortinet interface facilitates user provisioning, IP/MAC binding, and monitoring. It is worth mentioning that the primary purpose of this project is not focused on technical development per se, but rather on the design and formalization of an operational procedure. Therefore, the aforementioned technical simulation was used as a complement to observe not only the feasibility but also the efficiency and coherence of the proposed procedure flow within this project. Furthermore, to avoid IP pool saturation, deactivation mechanisms are implemented during military personnel rotation cycles.

Monitoring tasks are centralized through the Ubiquiti controller interface, allowing real-time tracking of military personnel devices using the network, bandwidth consumption, connection status, and access point associations. Service availability is subject to strict coverage areas, and any maintenance or interruptions are communicated in advance. Additionally, sustainable operational practices are described, including continuous traffic analysis, unauthorized port restriction, vulnerability assessments, and monthly security reports.

The proposed solution improves institutional governance, streamlines network access, and strengthens the digital infrastructure against the constantly evolving cybersecurity risks within the Ecuadorian Naval Penitentiary Station "ESNAPE."

Keywords: Network security, Firewall, Ubiquiti Controller, IP/MAC authentication.

Introducción

Actualmente se está viviendo una transformación digital constante, por lo que la seguridad de las redes inalámbricas adquirió una importancia y preocupación considerable dentro de empresas u organizaciones a nivel global. Bajo este contexto, se debe destacar que las instituciones militares, al igual que otras instituciones enfrentan desafíos particulares, esto es debido a que, al ser un entorno estratégico, manejan información sensible y donde no solo la confidencialidad, sino también la integridad y disponibilidad de la información y los datos son imprescindible para garantizar el mejor funcionamiento de la institución y también de la protección de la información en cuanto al orden público.

Aún más actualmente debido a que Ecuador se encuentra bajo tensión interna, nunca antes visto desde el retorno a la democracia, esto es debido a la declaratoria de "Conflicto Armado Interno", instaurado desde el año 2024. Dicha medida fue tomada por el Presidente Daniel Noboa en respuesta al incremento de violencia provocada por grupos delictivos, lo que ha conllevado a la presencia de las Fuerzas Armadas y Policiales no solo en lugares públicos, sino también en lugares estratégicos, tal y como es el caso de las zonas penitenciarias, además, de cumplir funciones importantes como el resguardo, la custodia y la rehabilitación de las personas privadas de la libertad (PPL), e incluso, muchas de ellas se encuentran relacionadas con casos de alta sensibilidad; por esto mismo se debe garantizar que la red de comunicaciones no solo debe ser eficiente, sino también debe ser segura y estar protegida ante cualquier amenaza cibernética. Por tal razón, la Estación Naval Penitenciaria de Ecuador (ESNAPE) es un claro ejemplo de ello, ya que dicha institución cuenta con una infraestructura de red que desempeña un rol importante dentro de la coordinación operativa y también en el manejo de los datos sensibles. Por lo que bajo este contexto, el presente proyecto propone el desarrollo de un procedimiento de seguridad operativo para controlar, administrar y también supervisar los accesos a la red WiFi del reparto naval ESNAPE, tomando en cuenta que esta área critica demanda protocolos que se adapten a la realidad institucional de la Armada del Ecuador.

El avance de la tecnología ha contribuido a la implementación de las redes WiFi como soluciones eficientes para la transmisión de datos, sin embargo, dicha facilidad también ha derivado en nuevos desafíos en cuanto a la exposición de estas redes como lo es a las vulnerabilidades, los ataques cibernéticos, accesos no autorizados, y también las filtraciones de la información. Además, las redes WiFi poseen ciertas vulnerabilidades propias las cuales pueden ser explotadas por agentes maliciosos. Los últimos estudios realizados han señalado la importancia de fortalecer la seguridad en redes inalámbricas dentro de los entornos sensibles, tal y como lo es del caso de las instituciones militares. Uno de los ejemplos de dichas investigaciones son las realizadas por autores como Kizza (2020), las cuales han

demostrado que la aplicación de no solamente de protocolos avanzados de cifrado, sino también de la autenticación multifactor pueden mitigar riesgos asociados a accesos no autorizados, además de los ataques de intercepción de datos. El autor Guamán (2024) en su investigación llamada “Seguridad de la Información en las Fuerzas Armadas del Ecuador para la predicción de ciberataques en redes militares” resalta esa necesidad imperiosa de instaurar mecanismos de seguridad con el objetivo de proteger la información dentro de un entorno de redes para los sistemas de institucione militares, como es el caso de las Fuerzas Armadas del Ecuador.

Cabe destacar que, sin ninguna política de seguridad apropiada, las redes WiFi se pueden convertir en uno de los objetivos más vulnerables dentro de cualquier infraestructura de TI. Además, se debe conocer que en la actualidad dentro de la región de Latinoamérica existen varias instituciones del ámbito militar que han adoptado medidas de seguridad básicas para las redes que manejan, sin embargo, no muchas de las veces implementan estrategias completas o robustas que abarquen los nuevos avances en ciberseguridad.

También, es importante mencionar que la pandemia del COVID-19 aceleró la digitalización en varios ámbitos (GCF Global, 2025). Lo que a su vez provocó un incremento en cuanto a las ciber amenazas, espionajes y fugas de información, por lo que existe una creciente necesidad de implementar varias medidas de seguridad más robustas en las redes WiFi utilizadas dentro de instalaciones sensibles.

Bajo este contexto, el presente proyecto se enfoca en poder desarrollar un procedimiento de seguridad para la red de la Estación Naval Penitenciaria de Ecuador (ESNAPE). Cuyo objetivo es el de poder analizar el estado actual de las redes WiFi y los protocolos que se encuentran vigentes dentro de dicho reparto militar, identificando así, aquellas vulnerabilidades existentes, lo que a su vez tiene como propósito proponer un conjunto de soluciones que contribuyan a que estos protocolos o procesos activos, no solo sean más seguro, sino también más confiable, además de que pueda contribuir a mitigar aquellos riesgos existentes dentro de la institución.

La Estación Naval Penitenciaria de Ecuador es una instalación militar, la cual representa un entorno seguro en cuanto a las redes de comunicación, ya que estas son de suma importancia. Como se sabe, las redes WiFi son un medio para la transmisión de datos, por lo que requieren medidas de seguridad, las cuales deben ser robustas con el fin de no solo prevenir los accesos no autorizados, sino también los posibles ciberataques. El presente proyecto se enfatiza en analizar y también en mejorar la seguridad de las redes dentro de un entorno sensible, esto se lo hace con la finalidad de salvaguardar no solamente la integridad de las comunicaciones, sino también la información que se maneja dentro de la instalación.

Entonces, se puede decir que la “ESNAPE” es una institución que posee una infraestructura de red WiFi la cual desempeña un papel importante en cuanto a la coordinación operativa y también en el manejo de datos confidenciales.

En referencia a la pertinencia del tema, cabe mencionar que este proyecto es sumamente relevante ya que tiene potencial para fortalecer las políticas de seguridad dentro del reparto militar, en donde la disponibilidad del servicio para el cumplimiento de las funciones del personal militar activo, asegurándose así de que los controles de acceso sean más estrictos, además de que los procedimientos de seguridad contribuya a la gestión operativa, por lo que no solo se debe seguir criterios de seguridad, sino también un orden jerárquico y trazabilidad. En donde si se llegara a implementar se podría lograr optimizar el uso del servicio de red, lo que evitaría la sobrecarga de los dispositivos del personal militar, o también el uso inadecuado de los recursos de la red WiFi de la Estación Naval Penitenciaria de Ecuador. Todas las acciones antes mencionadas no solo se encargarán de contribuir a proteger la información sensible y confidencial, sino que también ayudaría a la disponibilidad del servicio, y a su vez permitirá un control más efectivo de las operaciones que se realicen internamente, lo que contribuirá así una respuesta rápida y pertinente ante una posible incidencia.

Ante estos desafíos, surge la necesidad imperiosa de realizar el presente proyecto, ya que la tecnología avanza día a día, pero esto a su vez trae consigo riesgos trascendentales, en cuanto al ámbito de la seguridad, ya que, sin políticas de seguridad estrictas y robustas, el reparto militar ESNAPE se expone a vulnerabilidades que pueden comprometer la disponibilidad de sus servicios, impidiendo así que el personal militar activo pueda realizar sus funciones dentro del área penitenciaria. Por tal razón, el desarrollo del presente proyecto es indispensable ya que las herramientas tecnológicas dentro de la ESNAPE no garantizan la protección adecuada por si solas, por ende, es fundamental, pertinente y conducente el desarrollo de un procedimiento de seguridad la cual constituya una propuesta de gestión operativa con el fin de regular y tambien el de administrar el acceso a la red WiFi de la Estación Naval Penitenciaria de Ecuador “ESNAPE”.

Además, el presente proyecto se fundamentará en un marco actualizado y también, estará basado en evidencias con el fin de que a futuro se puedan realizar implementaciones de seguridad en las demás instalaciones críticas dentro del Ecuador.

Planteamiento del Problema

En el contexto actual, en referencia a la seguridad de las redes inalámbricas, estas forman parte esencial de cualquier empresa u organización que utilicen información sensible, tal y como es el caso de las instituciones militares, ya que dichas instituciones manejan información sensible o clasificada. Por tal motivo es que las redes WiFi representan una herramienta imprescindible tanto para la conectividad como para el intercambio de datos, pero también es importante tener en cuenta que dichas redes tienden a sufrir múltiples vulnerabilidades, las cuales pueden ser aprovechadas por terceros con intenciones malintencionadas.

La Estación Naval Penitenciaria de Ecuador (ESNAPE), enfrenta un desafío sumamente complicado en referencia a la seguridad de sus redes WiFi, ya que esta institución no escapa de esa realidad. Como toda institución, la infraestructura de red inalámbrica que posee es un activo fundamental para la operatividad constante como la gestión y manejo correcto de la información importante y también para la comunicación interna, así como el acceso a aquellos sistemas que gestionan la información sensible o confidencial para la seguridad de la institución. Sin embargo, se ha podido identificar que actualmente la infraestructura que posee la Estación Naval Penitenciaria (ESNAPE) no cuenta con un marco solido en cuanto a la seguridad, esto quiere decir que el reparto militar no cuenta con un procedimiento operativo estandarizado, el cual se enfoque en el control y gestión del acceso de dispositivos a la red WiFi de dicho reparto, por tal razón se han registrado casos que afectan no solo a la seguridad de la información dentro de la Estación Naval Penitenciaria de Ecuador, sino también a la eficiencia administrativa y disponibilidad del servicio, debido a ello, existe una alta probabilidad de que este reparto militar se exponga a varias amenazas, tales como, el acceso no autorizado a los datos sensibles, ataques de denegación de servicios (DoS), intercepción de los datos, y demás acciones que pueden convertirse en un catalizador para comprometer la integridad de las operaciones que se realizan dentro de la ESNAPE.

Bajo este contexto se puede constatar que existe una necesidad imperiosa de desarrollar un procedimiento operativo robusto, formal y replicable, el cual tenga como objetivo regular el acceso de los dispositivos a la red WiFi de la Estación Naval Penitenciaria (ESNAPE) de manera no solo segura, sino también eficiente, la cual se base en roles establecidos, solicitudes formales, corresponsabilidad técnica y administrativa entre repartos navales como lo es la ESNAPE y la DIRTIC y también en controles periódicos de supervisión; por lo que por medio de un correcto desarrollo de un procedimiento de seguridad adaptado a las necesidad y capacidades de la Estación Naval Penitenciaria de Ecuador se puede contribuir a asegurar no solo la confidencialidad, sino también la integridad y disponibilidad

de la información que se aloja dentro de un entorno crítico y sensible como lo es un reparto militar.

Stallings (2017) mencionaba que la falta de protocolos adecuados, al igual que la carencia de segmentación de redes, como nulas políticas de accesos y la falta de capacitación de las buenas prácticas de seguridad al personal, podrían constituir en una de las debilidades más graves ya que dicha debilidad podría ser explotada por agentes malintencionados en cualquier momento.

Con lo descrito anteriormente, la problemática central que busca abordar el presente proyecto sería la falta de un esquema de seguridad estructurado, el cual permita gestionar de manera adecuada aquellos riesgos vinculados al uso inadecuado de las redes WiFi en una instalación estratégica, como un área militar, específicamente la Estación Naval Penitenciaria (ESNAPE). Dicha deficiencia no solo podría limitar las acciones que se tomen frente a un posible incidente, sino que también podría aumentar la posibilidad de que se concreten ataques que puedan afectar de forma directa la confidencialidad operativa del entorno militar.

En el ámbito internacional, existen varios estándares y buenas practican en cuanto al aseguramiento de las redes WiFi dentro de entornos críticos. Un ejemplo es que, el Centro Criptológico Nacional de España (2021) el cual publicó recomendaciones precisas en cuanto a la seguridad de las redes WiFi en empresas u organizaciones, algunas de dichas recomendaciones son las siguientes:

1) Evitar el uso de redes WiFi abiertas o sin cifrado: Esta recomendación hace referencia a que las redes abiertas o sin cifrado dan la posibilidad de que cualquier persona se pueda conectar, lo que provoca que se expongan a la intercepción de los datos.
2) Separación de las redes del resto de la infraestructura: Dicha recomendación incentiva a separar la red WiFi de la red interna, ya sea por medio de VLANs o también por un Firewall, esto ayuda a minimizar los riesgos de ataques.
3) Controlar el acceso de los dispositivos: Esta recomendación trata del proceso IP/MAC para que los dispositivos autorizados se puedan conectar. Cabe destacar que esta es una de las recomendaciones que se adecuan al presente proyecto ya que el control de acceso de los dispositivos a la red WiFi por medio de registro IP/MAC Address asegura que solo los dispositivos autorizados puedan tener acceso a la red WiFi de la Estación Naval Penitenciaria de Ecuador, lo que contribuye a reducir el riesgo de intrusiones.
4) Monitoreo continuo de la red: Dentro de esta recomendación se hace alusión a la supervisión Activia para detectar comportamientos anómalos. Es

importante mencionar que el “monitoreo continuo de la red WiFi” también es parte del presente proyecto ya que la supervisión activa permite en este caso al militar técnico poder detectar los comportamientos inusuales, al igual que nos accesos no autorizados o en otros casos, los intentos de ataque.

5) Auditar: Esta recomendación hace referencia a la auditoria y al registro de eventos de conexión, por ello se debe mantener los logs de acceso, los cuales permiten realizar análisis si se llegara a presentar incidencias, además de que permite constatar de que se cumplan las políticas de una empresa u organización.
6) Formar a los usuarios de las buenas prácticas: Otra de las recomendaciones es la de realizar programas de concientización para el personal, esto se lo hace con el propósito de reducir los errores humanos, por ejemplo, compartir las credenciales o también el acceso a las redes inseguras.

De igual manera, Estados Unidos por medio de su Instituto Nacional de Estándares y Tecnología (2024) pudo desarrollar el “Marco de Ciberseguridad 2.0”, en el cual, dicho marco provee varias directrices significativas que contribuyen a gestionar aquellos riesgos de ciberseguridad dentro de las instituciones. Sin embargo, la aplicación como tal de dichos marcos normativos y técnicos dentro de país, específicamente dentro de una infraestructura de seguridad como la Estación Naval Penitenciaria (ESNAPE) aún es nula, lo cual intensifica aún más la problemática que existe.

Por lo tanto, se volvió esencial desarrollar una investigación aplicada, la cual contempló un análisis técnico en cuanto al estado en el que se encontraba la red, identificando sus componentes clave, todo esto con el propósito proseguir con el apartado operativo para la posterior formulación del procedimiento de seguridad para el reparto militar ESNAPE, en donde no solo se contempla las políticas, sino también de procedimientos al alcance de la institución y del personal con el que cuenta, además de considerar las capacidades técnicas y también de aquellos recursos de los que se dispone, por lo que el presente proyecto establece un procedimiento integral de gestión del acceso a la red WiFi del la ESNAPE, por medio del uso combinado entre los dispositivos de red y las políticas de seguridad para garantizar no solo la disponibilidad, sino también un acceso seguro, controlado y también eficiente en cuanto al servicio de la red WiFi del reparto naval.

El presente proyecto no se limita únicamente a la identificación de la problemática, sino que, su propósito fue desarrollar soluciones prácticas, las cuales eran adaptables al contexto de la Estación Naval Penitenciaria (ESNAPE), esto es debido a que pudieran ser implementadas de manera progresiva y con un enfoque sostenible. La solución para

desarrollar un procedimiento de seguridad dentro de la instalación ESNAPE abarcó lo siguiente: Análisis de la red y componentes clave dentro de la Estación Naval Penitenciaria de Ecuador, Identificación de los roles y responsabilidades del personal militar técnico; Creación y formulación de documentos de solicitudes para el registro de dispositivos de los militares activos entrantes por medio de formularios institucionales; Proceso de registro y asociación de la IP y Mac Address de los dispositivos; Supervisión constante del uso de los servicios de red; Control del número de dispositivos por cada uno de los militares dentro del reparto naval; Auditoria de los dispositivos conectados y la Liberación de los dispositivos inactivos, procedimiento final que se hace durante el periodo de ingreso y salida del personal militar a la Estación Naval Penitenciaria de Ecuador.

El propósito del proyecto no solamente fue la de asegurar que el acceso a los recursos de la red del reparto militar ESNAPE por parte del personal militar activo se realice tanto en orden como con trazabilidad y también responsabilidad, cumpliendo así con los principios de seguridad y eficiencia dentro del ámbito operativo, sino también a un aumento en cuanto a la cultura dentro de la institución con respecto a la protección de sus datos e información sensible, además de la ejecución de las buenas prácticas de seguridad digital. Esto permitiría evitar tanto las improvisaciones, como las conexiones no autorizadas y también el descontrol del servicio de la red WiFi del reparto naval, lo que a su vez garantizaría que el uso de los recursos tecnológicos de la ESNAPE se encuentre alineados con aquellas necesidades que requiere. Por tal razón, la Estación Naval Penitenciaria podría operar de manera correcta dentro de un entorno más seguro, y a su vez, asegurando la continuidad de aquellas funciones que realiza de manera diaria, sin comprometer la integridad de las comunicaciones que se dan de manera interna, ni tampoco la confidencialidad de aquellos datos críticos o sensibles.

Objetivos de la investigación

Objetivo general

Desarrollar un procedimiento de seguridad para la red WiFi de la Estación Naval Penitenciaria (ESNAPE), por medio del análisis de la configuración que se posee y la aplicación correcta de controles operativos para fortalecer la gobernanza del reparto militar, el control interno y garantizar la protección de la información de la institución y asegurar la continuidad de las operaciones dentro de un entorno crítico.

Objetivos Específicos

- Analizar la topología de la red WiFi de la Estación Naval Penitenciaria de Ecuador (ESNAPE).
- Identificar los roles y responsabilidades del personal militar técnico encargados de la gestión operativa del acceso a la red del reparto naval, incluyendo el registro y monitoreo de dispositivos.
- Diseñar un nuevo procedimiento de gestión operativa para el acceso de la red WiFi, que se adapte a las capacidades tecnológicas y organizativas de la Estación Naval Penitenciaria de Ecuador (ESNAPE).
- Evaluar el modelo del procedimiento de diseñado para el acceso a la red WiFi, que permita valorar su eficacia y aplicabilidad para una mejor gestión operativa dentro de la Estación Naval Penitenciaria de Ecuador (ESNAPE).

Justificación de la Investigación

Ante el panorama crítico por el que se encuentra el Ecuador, el estado se ha visto en la necesidad de declarar un conflicto armado interno a causa del incremento de organizaciones delictivas, por lo que es imprescindible fortalecer las capacidades de reacción de las instituciones encargadas del orden público. Bajo este contexto, la Armada del Ecuador ha sido desplegada para desempeñar funciones estratégicas en áreas criticas como los centros penitenciarios, dichos lugares son donde la seguridad no puede únicamente restringirse a espacios físicos, sino que también demanda un control de medios de comunicaciones internas para el personal militar, en este caso, los accesos a la red WiFi del reparto naval ESNAPE.

La necesidad y realización del presente proyecto se encuentra justificado en base a la necesidad imperiosa de instaurar un procedimiento de seguridad eficaz dentro de la red de la Estación Naval Penitenciaria (ESNAPE), esta última es una institución estatal importante ya que opera dentro de un entorno sumamente sensible, donde no solo la disponibilidad, sino también la confidencialidad y la integridad de la información son esenciales debido a la naturaleza crítica de las actividades operativas realizadas dentro de la instalación naval. Esto es debido a que la carencia de un protocolo de seguridad operativo robusto para controlar los accesos a la red WiFi supone un alto riesgo, en especial si se tiene en cuenta la rotación constante del personal militar que presta servicios dentro de la ESNAPE y por consiguiente, la exposición a amenazas tecnológicas, ya sean internas o externas. Se debe tener en cuenta que actualmente, la Estación Naval Penitenciaria (ESNAPE) cuenta con una red WiFi ya implementada, no obstante, esta misma no cuenta con un procedimiento protocolar y

estructurado el cual permita no solo regular, sino también administrar controlar y monitorear de manera sistemática aquellos dispositivos que se encuentren conectados en la red, ni tampoco que se designe responsabilidades evidentes al personal dentro de la institución. Cabe destacar que, la ausencia de dichos procedimientos involucra de manera potencial un mal control en referencia a los accesos, además de dificultar la protección adecuada frente a posibles incidencias, lo cual conlleva a un aumento de riesgos potenciales de seguridad dentro de la institución naval. Por tal motivo, la propuesta del proyecto no busca enfocarse en aspectos técnicos, sino en diseñar un procedimiento claro, practico y también funcional, el cual se adapte a las capacidades del reparto naval, además de ajustarse a la estructura institucional de la ESNAPE, lo cual permita al personal militar técnico a poder ejecutar sus responsabilidades de manera clara, ordenada y sobre todo segura.

Entonces, el desarrollo del presente proyecto se enfoca en establecer un procedimiento operativo, el cual se compone de los siguientes ejes:

- Análisis de la red y componentes clave dentro de la Estación Naval Penitenciaria de Ecuador.
- Identificación de los roles y responsabilidades del personal militar técnico y posterior asignaciones de funciones.
- Creación y formulación de documentos de solicitudes para el registro de dispositivos de los militares activos entrantes por medio de formularios institucionales.
- Proceso de registro y asociación de la IP y Mac Address de los dispositivos.
- Supervisión constante del uso de los servicios de red.
- Control del número de dispositivos por cada uno de los militares dentro del reparto naval.
- Auditoria de los dispositivos conectados.
- Liberación de los dispositivos inactivos.
- Y también la validación del mismo.

Este procedimiento propuesto dentro del presente proyecto no solamente es una guía técnica, sino que también es un modelo de gobernanza técnico-operativo dentro de un área critica como lo es un reparto militar, además de que se encarga de mejorar la capacidad de respuesta ante posibles incidentes, sino que también refuerza la supervisión, además de la rendición de cuentas que se hace dentro de las instituciones militares. De igual manera, con los roles y responsabilidades ya asignadas al personal técnico de la institución se promueve una cultura, la cual está orientada a la seguridad y también al manejo responsable de aquellos recursos tecnológicos con los que se cuenta.

Es importante resaltar que el incremento significativo de los diferentes dispositivos conectados a la red inalámbrica, ya sea de las instituciones públicas o privadas, en muchos casos, viene acompañado de un aumento considerable de amenazas enfocadas a estas mismas tecnologías. Como ejemplo se tiene el informe de Cisco denominado “Cyber Threat Trends Report: From Trojan Takeovers to Ransomware Roulette” (2024), en dicho informe se hace referencia a las redes WiFi de las empresas, las cuales representan uno de los objetivos principales de ataques, en especial, cuando estas mismas empresas no cuentan con procedimiento adecuado ni controles establecidos. Es por tal motivo que dentro del informe antes referido se destaca la exigencia de una adecuada implementación de estrategias de seguridad que permitan disminuir el impacto de los ciberataques.

Dentro del mismo informe de Cisco el cual se ha mencionado con anterioridad, se sostiene que aquellas empresas que se encargan de implementar estrategias de seguridad pueden llegar a reducir aproximadamente más del 70% del impacto generado por ciberataques, esto refuerza la necesidad imperiosa de la iniciativa del presente proyecto en referencia a un entorno crítico como lo es la ESNAPE.

Por consiguiente, el presente proyecto no solo se enfoca en cubrir una problemática técnica-operativa, sino que también busca poder generar soluciones totalmente prácticas y que se adapten al contexto de la institución naval, además de estar motivado por una responsabilidad social y por un compromiso académico de poder contribuir al fortalecimiento de aquellos sistemas de seguridad de las redes WiFi dentro de las instituciones públicas, específicamente, una institución de alta sensibilidad como lo es la Estación Naval Penitenciaria de Ecuador “ESNAPE” y de tal manera, contribuir a mejorar los niveles de protección dentro de un entorno crítico y sensible, e incluso, en donde se ve inmersa no solo la seguridad nacional, sino también la operatividad de la misma institución. Además, el presente proyecto aspira a generar resultados que puedan llegar a ser replicados en las demás instituciones públicas del país que posean características similares, y a su vez, promover una cultura no solo de prevención, sino también de fortalecimiento de las aptitudes y capacidades técnicas de los funcionarios responsables de la gestión de las redes.

CAPÍTULO I

MARCO TEORICO

CAPÍTULO I

MARCO TEÓRICO

El marco teórico del presente proyecto está fundamentado en los conceptos, principios y también en las teorías que respaldan tanto el diseño como la implementación de las medidas de seguridad en referencia a las redes inalámbricas, específicamente dentro de un entorno sensible como lo es una Estación Naval de Ecuador “ESNAPE”. Cabe mencionar que, el punto de este análisis permitirá comprender de una mejor manera los aspectos técnicos y operativos que sustentan el presente proyecto, al igual que los desafíos que surgen en relación a una mejora en cuanto a la gestión operativa con el objetivo de regular y administrar los accesos de los dispositivos a la red WiFi dentro de un contexto de un área critica como lo es un reparto militar de la Armada del Ecuador.

1.- Antecedentes de la Investigación

En el Ecuador, el 9 de enero del año 2024 bajo el marco de declaratoria de “Conflicto Armado Interno” el presidente Daniel Noboa emitió el Decreto Ejecutivo No. 111 debido a los altos índices de violencia, además de actos terroristas y la presencia del crimen organizado en varios ámbitos como en lo social e institucional. Por tal motivo, en concordancia con el Artículo 5 del Decreto No. 111 (PRESIDENCIA DE LA REPÚBLICA DEL ECUADOR, 2024) se ordenó a las Fuerzas Armadas realizar operaciones militares enmarcándose en el Derecho Internacional Humanitario y a su vez respetando los Derechos Humanos con el fin de neutralizar a los grupos criminales en base a lo establecido en el Artículo 4 del mismo Decreto Ejecutivo.

Debido a este antecedente, las Fuerzas Armadas se movilizaron según lo dispuesto por el Gobierno, en donde una de las nuevas asignaciones y competencias que se le dio a esta organización militar fue la de retomar el control de todos los Centros de Privación de Libertad (CPL) del país.

Bajo este contexto la administración del sistema carcelario tuvo que modificarse con el fin de tratar de dotarlo de medios necesarios como el recurso humano, financiero y, sobre todo medios tecnológicos que se encuentren a la altura de sus funciones, especialmente en cuanto se refiere a la seguridad pública. Por tal razón, para cumplir con las nuevas funciones encomendadas por el gobierno, el 6 de mayo del año 2024 las Fuerzas Armadas ordenaron la creación de un nuevo Reparto Militar denominada “Estación Naval Penitenciaria de Ecuador (ESNAPE)”, y a su vez, dicho reparto se divide de la siguiente forma:

- Centro de Privación de Libertad (CPL).
- Centro de Rehabilitación Social (CRS).

2.- Marco Fundamental

1.2.1.- Fundamentos de la Problemática de Investigación

En referencia a las redes inalámbricas, estas han adquirido un papel fundamental en este siglo XXI ya que han transformado la forma en que todas las instituciones manejan la comunicación y el intercambio de información, permitiendo mayor flexibilidad y accesibilidad, más aún en entornos críticos debido a la gestión de información estratégica. Cabe destacar, que su implementación en entornos sensibles, como instalaciones penitenciarias e instituciones de gobierno, plantea retos importantes, esto es debido a su vulnerabilidad que conlleva los ataques cibernéticos, ya que las redes WiFi en muchos casos son susceptibles a intercepciones de datos y accesos no autorizados, en especial cuando no cuentan con protocolos de seguridad.

En el contexto específico de la Estación Naval Penitenciaria "ESNAPE", la importancia de un control y administración de los accesos de los dispositivos a la red inalámbrica se radica en su papel para la comunicación interna y también en el manejo de información clasificada, lo que conlleva a desafíos importantes debido a su latente riesgo de accesos indebidos a la red WiFi del reparto militar lo que puede llevar a casos de vulnerabilidades a ataques cibernéticos, por esta razón, el control de acceso a las redes WiFi es fundamental para garantizar no solo el acceso a internet por parte del personal militar activo, sino también para los propios servicios internos, los cuales deben ser realizados de manera organizada, segura y también eficientes, e incluso la protección de la integridad de toda la información, además de garantizar la correcta operatividad de la instalación naval. Ya que, en un caso de acceso no autorizado, este podría comprometer los datos que resguarda la institución.

Por lo cual, el presente proyecto no solamente responde a la urgencia operacional de la Estación Naval Penitenciaria de Ecuador “ESNAPE”, sino que también el valor de la propuesta de este proyecto radica en:

- Proponer un modelo que pueda ser replicable dentro de otros repartos de la Armada del Ecuador.
- Abordar el acceso a las redes WiFi desde una perspectiva tanto organizacional como de procesos, no únicamente técnica.
- Contribuir a una mejora continua de la gestión dentro de la Estación Naval Penitenciaria de Ecuador “ESNAPE” en cuanto a las redes WiFi y sus servicios digitales.

Además de estar dentro de un marco tanto legal como normativo, lo cual implica garantizar la seguridad de aquellos datos dentro de las entidades del estado. Ya que, la implementación de parámetros de seguridad contribuye a prevenir los accesos no autorizados, lo que a su vez lo protege de ciberataques, asegurando así la integridad de los sistemas del reparto militar.

Cabe mencionar que una buena seguridad en las redes WiFi puede contribuir a la protección de la información sensible, evitando así que aquellos usuarios no autorizados puedan acceder a dicha red, lo que especialmente importante dentro de aquellos entornos donde se gestiona información crítica (Aryaka, 2023).

1.2.2.- Fundamentos de Administración y Control de Recursos de la Red

Tanto una adecuada administración como el correcto control de los recursos de las redes son importantes para garantizar el funcionamiento no solo efectivo, sino también seguro en referencia a las infraestructuras de TI. Esto conlleva, por ejemplo, la supervisión del tráfico de las redes, además de la gestión de los dispositivos que se encuentran conectados y también, la implementación de políticas de acceso. Por lo cual, una gestión eficaz contribuye tanto a identificar como a resolver problemas de manera rápida, al igual que optimizar su rendimiento, sumado a esto, el garantizar la disponibilidad de los servicios de una empresa u organización (International IT, 2022).

Se debe destacar que la gestión de red abarca la supervisión y el control de no solo la monitorización, sino también la configuración, la protección, al igual que los recursos y servicios de dicha red (Hewlett Packard Enterprise, 2025). Todo esto conlleva a mantener tanto la fiabilidad como la seguridad de la infraestructura, además de que una correcta administración de las redes puede facilitar la distribución eficiente de los recursos disponibles, por ejemplo, el ancho de banda y también la capacidad de los servidores, lo que asegura que las aplicaciones críticas puedan recibir los recursos que necesitan sin desperdicios.

1.2.3.- Rol del Personal Designado en la Gestión de Conectividad

Los funcionarios o personal designados dentro de cualquier institución ya sea pública o privada dentro del país, realizan un papel indispensable en la gestión de la conectividad, ya que son los encargados de no solo la implementación, sino también del mantenimiento de las políticas de seguridad, además de asegurar el adecuado funcionamiento de la red. La constante capacitación, además de la conciencia en cuanto a las buenas prácticas en ciberseguridad son indispensables ya que pueden contribuir a prevenir errores humanos, los cuales pueden poner en riesgo la seguridad de la red. Por tal motivo, tanto el conocimiento como las habilidades para emplear de manera correcta aquellas herramientas que permitan no solo instalar, sino también el dar soporte y mantenimiento a sus redes informáticas, estas

labores son fundamentales para todo el personal designado para la gestión de la conectividad.

Es importante mencionar que la gestión de la información dentro un ámbito institucional exige que el personal esté implicado en cuanto a las políticas de información, y también en los procedimientos organizacionales, ya que estos promueven el manejo seguro de la información, por ejemplo, el intercambio y almacenamiento de la misma (Contreras Díaz, Rivero Amador, González Pérez, & Ding, 2021).

3.- Marco Conceptual

1.3.1.- Redes Inalámbricas (WiFi, SSID, VLAN y Direccionamiento)

Las redes inalámbricas, también conocidas como WiFi, son las que permiten la conexión de todos los dispositivos a una red de manera inalámbrica, haciendo uso de las ondas de radios con el objetivo de poder transmitir los datos, lo que significa que no hay necesidad de usar cables físicos. Se debe mencionar que la evolución constante de la tecnología y las redes WiFi se han llegado a convertir en activo esencial de la infraestructura de las diferentes empresas u organizaciones, especialmente, en el caso de las instituciones militares.

En cuanto al Service Ser Identifier (SSID), este es un identificador único, el cual se encarga de distinguir a una red determinada. Por tal razón, aquellos dispositivos que requieran conectarse a una red WiFi tienen que hacer uso del SSID adecuado (Masoud, Jaradat, & Alia, 2021). Es importante conocer que, al desactivar la función de difusión de SSID permite al usuario contar con una capa de seguridad adicional, esto es debido al ocultar la red de aquellos usuarios no autorizados, pero, aun así, dicha medida no garantizaría una protección adecuada por si sola, por tal motivo es necesario que se complemente con otros mecanismos de seguridad, tal es el caso de técnicas de cifrado y autenticación.

En referencia a la Virtual Local Area Networks (VLAN), estas tienen la facultad de segmentar una red física con el fin de crear redes independientes (Zepeda Vega). En cuanto a la ventaja de segmentar una red es que permite facilitar la administración de una red, además de mejorar la seguridad, esto último es posible al aislar las diversas clases de tráfico.

Ahora, en relación al direccionamiento de la IP, esta es importante debido a que permite tanto la identificación como la localización de dispositivos dentro de una red. Cabe mencionar que, cada uno de los dispositivos que se encuentren conectados dentro de una red WiFi debe contar con una dirección IP única, la cual permita a dicho dispositivo poder comunicarse con otros dispositivos, además de acceder a los recursos que se comparten.

Finalmente, es fundamental conocer que una asignación apropiada de las direcciones IP, en conjunto con la aplicación de VLAN y una correcta configuración del SSID, ayuda a una adecuada gestión, además de contar con una red segura.

1.3.2.- Correlación entre el Direccionamiento IP, MAC Address y Usuarios Registrados

La dirección IP al igual que la dirección de la MAC Address son identificadores fundamentales dentro de la administración de las redes WiFi. Pero, en el caso de la dirección IP, esta puede ser modificada dependiendo siempre de la configuración propia de la red, ya sea estática o dinámica. Mientras que en el caso de la dirección de la MAC Address es única para cada uno de los dispositivos existentes y que se le es asignado durante su fabricación, por ejemplo, dispositivos celulares inteligentes; las computadores y laptops; dispositivos de red como routers, switches; dispositivos IoT como cámaras de seguridad, etc.

Ahora, asociar tanto las direcciones IP como la MAC Address con los usuarios correspondientes otorga la posibilidad de una trazabilidad eficiente dentro de las redes WiFi. Dicha práctica es fundamental dentro de los entornos críticos, tal es el caso de las instituciones militares como lo es la Estación Naval Penitenciaria de Ecuador “ESNAPE”, ya que en dichas instituciones es crucial realizar monitoreos constantes, además de controlar adecuadamente el acceso a sus redes WiFi.

Ahora, al vincular correctamente todas estas direcciones en conjunto con las credenciales de los usuarios de la institución, se puede identificar de manera rápida cualquier actividad ilícita, sospechosa o inusual y a su vez, contrarrestarlas con la toma de medidas adecuadas.

La implementación de aquellos sistemas que cumplan la función tanto de registrar como gestionar dichas asociaciones puede facilitar la detección de todos los dispositivos no autorizados, y permitiendo a su vez prevenir estos accesos no autorizados en la red de la institución. Sumado a eso se debe permitir la aplicación de políticas de seguridad que se adapten no solo a la institución, sino también a los perfiles de los usuarios y a los dispositivos que se utilizan.

1.3.3.- Control de acceso a las redes WiFi por medio de autenticación y políticas de acceso

Para cualquier empresa u organización el control de los accesos a sus redes WiFi es una estrategia indispensable, más aún en instituciones importantes donde se manejan datos sensibles como lo son las instituciones militares, esto se lo hace con el fin de garantizar que solamente los usuarios y dispositivos autorizados cuenten con los accesos a los recursos de la red. Dicho esto, se debe presentar varios de los métodos para implementar dicho control,

entre los cuales se destacan: La autenticación de los usuarios; El control de los accesos basados en los roles; Control de acceso al nivel de la red y El control de los accesos a nivel de las aplicaciones.

- **Autenticación de los usuarios:** La acción de la verificación de los usuarios por medio de sus credenciales como lo son sus nombres de usuarios y contraseñas, las tarjetas de identificaciones o la autenticación por medio de un dispositivo biométrico. Todo este proceso se encarga de asegurar que solo el personal autorizado pueda acceder a la red WiFi de la institución.
- **Control de Acceso en base a roles:** Esto hace referencia a asignar determinados permisos a los usuarios dependiendo de las funciones que realizan dentro de la institución. Un ejemplo puede ser el administrador de la red, dicho administrador tendrá el acceso a la opción de configuraciones avanzadas, mientras que el caso de un usuario estándar, este solo podrá tener acceso a los recursos básicos.
- **Control de los accesos a nivel de la red:** Dicho control trata de la implementación de las restricciones en aquellos dispositivos de la red, como es el caso de los routers y switches, esto se lo hace con el fin de controlar el flujo de tráfico, además de limitar el acceso a ciertas direcciones IP o también a puertos específicos.
- **Control del acceso a nivel de las aplicaciones:** Al establecer medidas dentro de las aplicaciones se puede controlar el acceso a varias funcionalidades, además de ciertos datos, esto se lo puede hacer implementando ciertos mecanismos, por ejemplo, la autenticación adicional o también, la verificación en dos pasos.

Todas estas estrategias antes mencionadas contribuyen al fortalecimiento de la seguridad de la red WiFi, además de proteger los datos críticos en contra de los accesos no autorizados dentro de la institución.

Implementar medidas para fortalecer la seguridad de la red WiFi es fundamental ya que permite reducir de manera significativa los riesgos a posibles ataques, ya que si no se lo hace se deja a las redes WiFi expuestas a una variedad de amenazas, que incluyen ataques como:

- **Man-in-the-Middle:**

Este tipo de amenaza permite a los atacantes no solamente poder interceptar la comunicación entre los diferentes dispositivos conectados a una red, sino que también manipular dicha comunicación (National Institute of Standards and Technology, 2022).

- **Inyección de Paquetes Maliciosos:**

Esta amenaza hace referencia a la inserción de datos maliciosos dentro de una red con el propósito de comprometer la integridad de esta.

- **Suplantación de Puntos de Acceso Legítimos:**

Estas amenazas son especialmente graves en escenarios donde se manejan datos sensibles, esto es debido a que pueden derivar en pérdidas económicas, interrupciones operativas y daños en la reputación de la institución. Esto es debido a que los atacantes se encargan de crear puntos de accesos falsos con el objetivo de engañar a los usuarios y así poder obtener sus datos de ingreso.

- **Ataques de Intercepción de Datos:**

Los atacantes pueden capturar información que se transmite entre dispositivos conectados a la red. Esta técnica, conocida como sniffing, es común cuando no se utilizan métodos de cifrado apropiados.

- **Suplantación de Identidad (Phishing):**

Este ataque se lo puede realizar mediante la creación de puntos de acceso fraudulentos; aquí los atacantes buscan engañar a los usuarios para que se conecten a redes no seguras, exponiendo así sus credenciales y datos (Rosero Tejada, 2021).

- **Exploits de Configuración Débil:**

Esta amenaza se da debido a la falta de actualizaciones en el firmware de los dispositivos y también por dejar las configuraciones por defecto, lo que provoca que las redes queden vulnerables a exploits (Rashid , Asif Ali, Kamlesh, Shibin, & Munwar, 2020).

1.3.4.- La Gestión de los Dispositivos Conectados a la Red WiFi y las Buenas Prácticas

Una correcta gestión de todos aquellos dispositivos conectados a una red WiFi es importante ya que así se puede mantener tanto su seguridad como su rendimiento. Por lo tal las buenas prácticas son fundamentales, en este caso, Jesús García (2008) menciona que algunas de estas prácticas pueden incluir el manteamiento de un inventario de todos los dispositivos de manera actualizada, a su vez se debe implementar políticas de actualizaciones y también de los correspondientes parches de software.

A esto se debe sumar una adecuada segmentación de la red WiFi con el propósito de aislar los dispositivos conectados en base a su función o nivel de riesgo.

También es importante la recomendación del uso de dispositivos de monitoreo, los cueles se encarguen de detectar en tiempo real todas esas amenazas potenciales en tiempo real, además de los comportamientos inusuales. Tal es el caso de las instituciones militares, las cueles son considerados entornos sensibles, debido a que la seguridad es indispensable

y dichas prácticas pueden ayudar a prevenir los accesos no autorizados, garantizando así la continuidad operativa de su red WiFi.

Por lo mencionado anteriormente es que la Estación Naval Penitenciaria de Ecuador “ESNAPE” siguiendo con las buenas prácticas, cuenta con dispositivos de monitoreo, como por ejemplo el Firewall de la marca FORTINET, cuyo modelo es el FG-70F, también está la Controladora Cloud Key Gen2 Plus de la marca UBIQUITI, que con el uso combinado de dichos dispositivos con políticas de seguridad informática permiten contar con un procedimiento integral que se enfocado en la gestión del acceso de los dispositivos del personal militar activo a la red WiFi de la ESNAPE.

1.3.5.- Monitoreo y Disponibilidad del Servicio de la Red WiFi

El monitoreo continuo de la red WiFi es fundamental para poder asegurar no solo la disponibilidad de dicha red, sino también para detectar posibles intentos de intrusiones o fallos. Un correcto monitore incluye ciertos criterios esenciales como la supervisión del ancho de banda, también de la latencia, la intensidad de la señal, además de la tasa de errores. Cabe destacar que las herramientas tanto de análisis como de diagnóstico otorgan la facilidad de poder identificar los cuellos de botella, además de las interferencias o aquellos dispositivos maliciosos. En instituciones importantes donde la conectividad es imprescindible para las operaciones diarios como es el caso de las instituciones militares, el poder garantizar la disponibilidad de los servicios de WiFi es considerada como una prioridad estratégica.

Bajo este contexto, la Estación Naval Penitenciaria de Ecuador “ESNAPE” hace uso de una Controladora (Cloud Key Gen2), la cual pertenece a la línea UniFi perteneciente a Ubiquiti, en donde su función principal es la de no solo administrar, sino también monitorear los dispositivos de la red, como es el caso de los Puntos de Accesos, Switches, etc.

1.3.6.- Norma Internacional: ISO/IEC 27001 y su Implementación en entornos militares

La normativa internacional ISO/IEC 27001 es un estándar que se encarga de establecer todos aquellos requisitos tanto para la creación, implementación, mantenimiento y también para la mejora constante de un sistema de seguridad (National Quality Assurance, 2022).

También se debe mencionar que la normativa ISO/IEC 27001, es la cual establece directrices para la gestión de la seguridad de la información, abarcando aspectos como la evaluación de riesgos y la implementación de controles de acceso, las cuales pueden ser aplicables dentro de diferentes empresas u organizaciones, e incluso, las instituciones militares, para lo cual, el desarrollo de un correcto procedimiento para regular y administrar los accesos a la red WiFi de la Estación Naval Penitenciaria de Ecuador “ESNAPE” se debe

basar en la Normativa ISO/IEC 27001, ya que su incorporación dentro del ámbito de las instituciones militares asegura un enfoque sistemático en cuanto a la protección de la información, algunas de las políticas ISO/IEC 27001 que pueden incorporarse a los repartos militares como lo es el caso de la ESNAPE pueden ser:

- **Políticas para el Control de Acceso:**

Dentro de esta política se hace referencia a establecer reglas concisas en cuanto a quien puede tener acceso a los recursos. Ahora, en el caso de la Estación Naval Penitenciaria de Ecuador “ESNAPE”, esto puede conllevar a restringir el acceso no solo a los sistemas, sino también a la red WiFi y documentación según los rangos del personal militar, al igual que sus funciones y también en el nivel de autorización de dicho personal uniformado.

- **Políticas de Gestión de Activos:**

Esta política alude al aseguramiento de todos los equipos, al igual que los sistemas, los cuales deben estar debidamente identificados, además de clasificados y protegidos. En el caso concreto de la Estación Naval Penitenciaria de Ecuador “ESNAPE” esto incluiría hasta los dispositivos personales del personal militar activo como los celulares o tablets o dispositivos institucionales utilizados dentro de las operaciones tácticas que se realizan en el reparto naval.

- **Política de Uso Aceptable:**

Dicha política se encarga de regular el uso tanto de los sistemas como de los dispositivos por parte del personal. Ahora, dentro del contexto de la Estación Naval Penitenciaria de Ecuador “ESNAPE” se podría evitar que el personal militar haga uso de los recursos del reparto naval para uso personal o que se haga uso de aplicaciones no autorizadas.

- **Políticas de la Gestión de los Riesgos:**

Esta política evoca a establecer un proceso tanto para identificar y evaluar incidentes. En el caso concreto de la Estación Naval Penitenciaria de Ecuador “ESNAPE”, dicha política se la puede cumplir por medio del monitoreo de los dispositivos que se encuentren conectados a la red WiFi por medio de la controladora de red.

- **Políticas de Gestión de Incidentes:**

Esta política de la Normativa ISO 27001 establece el como no solamente se tiene que reportar, sino también investigar aquellos incidentes los cuales afecten la seguridad de la

información. En cuanto al ámbito militar, esta política permitiría una respuesta rápida en casos de accesos no autorizados o filtraciones.

En el caso de Ecuador se encuentra vigente la Ley Orgánica de Personal y Disciplina de las Fuerzas Armadas, en donde en su Artículo 196, numeral 12 se establece que son faltas atentatorias todas las acciones que comprometan la seguridad, tal es el caso del incumplimiento de un protocolo establecido (Ministerio de Defensa Nacional del Ecuador, 2023). Por lo que la falta de atención ante esta política de gestión de incidentes puede conllevar a consecuencias tanto para la ESNAPE como para su personal.

- **Política de Concientización:**

Esta política hace referencia a que se debe promover a que todo el personal se encuentre capacitado en cuanto a las buenas prácticas dentro del ámbito de la seguridad. Ahora, dentro de un contexto militar, esta política podría reforzar la disciplina digital, además de reducir el riesgo de los errores humanos.

Finalmente, dicha normativa internacional contribuye no solo a la implementación de controles adecuados, sino también a proponer políticas de seguridad adecuadas, además de ayudar a identificar los posibles riesgos.

1.4. Marco Situacional

1.4.1.- Contexto de Conectividad Controlada en la ESNAPE

La Estación Naval Penitenciaria de Ecuador “ESNAPE” como reparto militar al igual que los demás repartos dentro del país, opera en torno a un marco normativo riguroso, el cual se encarga de regular no solo las comunicaciones, sino también la seguridad de la información, específicamente la Directiva General Permanente emitida por la Comandancia General de la Armada.

Se debe tener en cuenta que la ESNAPE es un nuevo reparto militar el cual surgió en el año 2024, en dicho reparto se cuenta una infraestructura avanzada la que está orientada a mitigar los riesgos en cuanto a los posibles ciberataques, por tal razón, las políticas de ciberdefensa dentro de los entornos militares como el caso de la ESNAPE, se encuentran enfocadas en dar protección a la integridad, además de la confidencialidad de los datos que se manejan garantizando así un entorno tecnológico seguro, pero que a su vez se pueda apoyar a la labor de todos aquellos militares que realizan sus funciones tanto de protección, operativas, logísticas, abastecimiento, y demás dentro de un espacio crítico como lo es la penitenciaria.

Néstor Ganuza en su Guía de Ciberdefensa (2020) hace mención a que dentro del entorno militar se tiene un interés colectivo, el cual es el de reforzar las capacidades de ciberdefensa dentro de cada uno de los entornos militares con el fin de garantizar la seguridad de los sistemas institucionales, al igual que su información e infraestructura. Esto se lo hace con el objetivo de aportar en asegurar no solo los intereses de la institución como tal, sino también en los intereses nacionales en contra de potenciales amenazas cibernéticas, para ello dichas instituciones deben de planificar, diseñar, desarrollar y también desplegar todas sus capacidades en ciberseguridad.

En el caso de las instituciones militares de Ecuador, se requiere contar con una conectividad controlada, la cual permita el acceso seguro a los recursos de sus redes WiFi, pero sin comprometer la seguridad operativa de la institución, tal como es el caso de la ESNAPE. Por lo que esto conlleva a la implementación de medidas tanto técnicas como operativas, las cueles regulen el acceso adecuado a la red, pero a su vez, asegurando que solo el personal uniformado autorizado logre no solo conectarse, sino también acceder a la información crítica. Con este contexto se debe tener en cuenta que en la ESNAPE aún no se cuenta con un procedimiento formal para solicitar el acceso a la red WiFi de dicho reparto, por ende, es importante que se proponga incluir un documento de solicitud para formalizar así el registro de los militares, esto podría contribuir tanto al control como a la gestión de acceso dentro de un ámbito operativo-administrativo.

1.4.2.- Control de Tráfico de la Red

El control de tráfico de la red WiFi al igual que el registro de los dispositivos personas por usuario dentro de dicha red militar son prácticas fundamentales, las cuales ayudan a prevenir los accesos no autorizados y a su vez garantizar el correcto seguimiento de las actividades dentro de la red, en este caso, dentro de la red WiFi de la ESNAPE. El despliegue de sistemas de autenticación que cumplan la función de vincular las Direcciones IP con las MAC Address con el personal uniformado permite una mejor gestión en cuanto a los dispositivos conectados. Esto quiere decir que, asociar tanto la IP con la MAC Address del militar activo dentro del Firewall Fortinet es más que una acción técnica, ya que contribuiría a contar tanto con un mayor control como ordenado y personalizado en cuanto a que usuario esta haciendo uso de los recursos de la red dentro de la ESNAPE.

También, el monitoreo constante del tráfico de la red contribuye a detectar posibles comportamientos inusuales que presuntamente puedan ser intentos de intrusión o también, puedan ser vistos como una forma de mal usar los recursos de la red.

1.4.3.- Configuración y Distribución de los Access Point y Controladora

Tanto la configuración como la distribución acertada de los Access Point y la controladora como tal, son indispensables ya que permiten asegurar no solo una cobertura optima, sino también una gestión de manera centralizada de la red WiFi. Por lo cual, los Access Point tienen que ser ubicados de manera estratégica con el fin de cubrir las áreas que sean necesarias. En cuanto a la controladora Cloud Key Gen2 Plus, esta permite la administración de forma centralizada de todos los Access Point de modelo U6-LR, ambos de la marca Ubiquiti, lo que a su vez puede facilitar la implementación de las políticas de seguridad y también del monitoreo continuo del estado de la red WiFi de la institución.

1.4.4.- Firewall Fortinet y Políticas en el Reparto Militar

La ejecución de políticas de seguridad por medio del dispositivo Firewall de la marca Fortinet dentro de las instituciones militares, como es el caso de la ESNAPE, puede añadir una capa extra de protección contra posibles ciberataques o filtrado de información. Disco dispositivo de modelo FG-70F permite la implementación no solo de políticas de filtrado de contenido, sino también del control de las aplicaciones, al igual que la prevención de posibles intrusiones y el establecimiento de conexiones seguras en cuanto a las VPN. La configuración asertiva de dichas políticas es fundamental para mantener tanto la integridad como la confidencialidad de la información en las redes WiFi militares.

1.5. Marco Contextual

1.5.1.- Procedimiento Operativo para el Registro de IP/MAC Address

Los procedimientos operativos en referencia tanto al registro como la liberación de las direcciones IP y las MAC Address en las redes de entornos militares debe ser totalmente rígidas, además de estar documentadas. En dicho procedimiento se incluye la asignación de las direcciones IP por medio del dispositivo Firewall de marca Fortinet, cuyo modelo es el Fortigate (FG-70F) a aquellos dispositivos que el personal uniformado requiera, esto es debido a que el dispositivo como tal otorga la posibilidad de gestionar todos estos registros de forma eficiente, y a su vez, se asegura tanto la integridad como la protección de la infraestructura de TI de la institución militar. Ahora, en referencia a la liberación de estas direcciones IP, este proceso se lo lleva a cabo para aquellos dispositivos ya no son usados por parte del personal uniformado de la Estación Naval Penitenciaria de Ecuador “ESNAPE”.

Cabe destacar que el cumplimiento de todo este procedimiento ayuda no solo a mantener un control riguroso y preciso de aquellos dispositivos conectados a la red WiFi de la ESNAPE, sino que también contribuye a prevenir los posibles accesos no autorizados a dicha red.

1.5.2.- Definición de los Permisos y Roles para la Configuración de los Equipos de Red

Asignar y especificar tanto los permisos como los roles en referencia a la configuración de equipos de red es imprescindible, esto es debido a que así se puede prevenir los cambios no autorizados que en ciertos casos puede llegar a comprometer la seguridad de la infraestructura. Bajo este contexto, el personal que se encarga de la administración de red debe contar con permisos diferentes en base a sus responsabilidades, además de que todas las acciones que se lleven a cabo tienen que ser registradas para posteriormente se pueda realizar una investigación, análisis o auditoria y también dar un mejor seguimiento a los cambios realizados. Dicha auditoria puede ayudar a validar el servicio de la red institucional, permitiendo identificar y también corregir los posibles usos indebidos, además de posibles casos de vulnerabilidades y a su vez poder corregirlas.

Toda esta práctica antes mencionada contribuye a una gestión no solo controlada, sino también segura de aquellos equipos de red de la Estación Naval Penitenciaria de Ecuador “ESNAPE”.

1.5.3.- La Gestión de los Usurarios Inactivos dentro de la Red y Políticas de Depuración

La adecuada gestión de aquellos usuarios que se encuentren en estado “inactivos” dentro de la red WiFi de la ESNAPE, y también la implementación de políticas para dicha depuración son fundamentales, ya que pueden contribuir a la reducción de posibles accesos no autorizados. En este contexto, los registros de la IP y MAC de los dispositivos del personal que no han sido utilizadas por un determinado periodo tienen que ser eliminadas, además de seguir un procedimiento para revisar de manera regular la red del reparto militar.

1.5.4.- Monitoreo y Reporte de los Dispositivos Conectados

Tanto el monitoreo periódico como un adecuado reporte de los dispositivos conectados a la red WiFi de la institución, pueden ser prácticas imprescindibles, ya que se así se puede detectar algún incidente de seguridad, además de poder responder de manera rápida a ese posible incidente. Por tal razón, las instituciones que implementan sistemas de monitoreos pueden identificar una variedad de escenarios, por ejemplo, comportamientos inusuales, dispositivos no autorizados, uso inadecuado de los recursos de la red, y más.

1.6. Marco Tecnológico

1.6.1. Controladora (Cloud Key Gen2 Plus)

La controladora modelo Cloud Key Gen2 Plus de la marca UBIQUITI es un dispositivo potente, el cual fue diseñado para centralizar la administración de las redes (Ubiquiti, 2020).

Dicho dispositivo funciona como un servidor pequeño pero autónomo el cual permite gestionar de manera fácil los diferentes dispositivos por medio de una sola interfaz, y esto es posible sin la necesidad de depender de los servicios externos en la nube.

Algunas de las funciones principales de esta controladora son:

- **Gestión Centralizada:**

La controladora Cloud Key Gen2 Plus permite administrar los puntos de accesos, además de los switches, las cámaras IP y demás equipos pertenecientes al ecosistema UniFi y todo esto desde esta única herramienta.

- **Supervisión Remota:**

La controladora cuenta con una arquitectura hibrida, esto quiere decir que permite acceder a la red me manera segura desde cualquier lugar, y a su vez, mantener la privacidad de los datos.

- **Interfaz Intuitiva:**

La controladora hace uso del software UniFi Controller, el cual ofrece una mejor experiencia a los usuarios en cuanto a la eficiencia para configurar y monitorear los dispositivos.

1.6.2.- Firewall (FortiGate 70F)

El firewall modelo FortiGate 70F es un dispositivo de última generación, el cual fue desarrollado por Fortinet, dicho dispositivo fue diseñado para ofrecer una protección avanzada dentro de las redes de las empresas u organizaciones (Fortinet, 2025). Cabe destacar que este dispositivo no solo se centra en cumplir con funciones tradicionales de los propios firewalls, tal es el caso de las funciones de filtrado y también controlar el tráfico dentro de las redes, sino que también integra nuevas tecnologías como, por ejemplo, la inspección profunda de paquetes, herramientas de inteligencia artificial y el acceso a la red basado en la confianza cero, el cual es un enfoque ZTNA.

Algunas de las funciones principales de este Firewall son:

- **Filtrado de Tráfico:**

Posee un filtrado inteligente en cuanto al tráfico, ya que analiza en tiempo real quellos datos que circulan por la red, e incluso si dichos datos estan cifrados, esto lo hace para poder detectar y bloquear posibles amenazas tal es el caso de malware o accesos no autorizados.

- **Control de Aplicaciones:**

El firewall tiene la capacidad de establecer políticas para el uso tanto del software como el de los servicios, esto contribuye a mantener no solo el cumplimiento normativo, sino también el de reducir los riesgos.

- **FortiGuard:**

Estos servicios pertenecientes al firewall modelo FortiGate 70F incluyen protecciones contra amenazas, las cuales se basan en inteligencia artificial, tal es el caso de los antivirus, IPS, filtrado web, y demás.

1.6.3.- Access Point

Los access point (AP) también se los conoce como puntos de accesos inalámbricos, los cuales son dispositivos de red que permiten conectar equipos como smartphones, laptops, tablets, y demás dispositivos a una red local, sin hacerlo por medio de cables (CISCO, 2025). Se puede decir que los acces point funcionan como un puente entre una red cableada (LAN) y los dispositivos inalámbricos, lo que facilita no solo la comunicación, sino también el acceso a los recursos, por ejemplo, el internet, impresoras o servidores.

CAPITULO II

METODOLOGÍA DEL PROCESO DE INVESTIGACIÓN

CAPÍTULO II

METODOLOGÍA DEL PROCESO DE INVESTIGACIÓN

2.1. Enfoque de la investigación

Para la realización de la presente investigación se determinó que el enfoque más apropiado será el cuantitativo, esto se fundamenta por la recolección de los datos esenciales, por tal razón se los realizará por medio de instrumentos estructurados, tal es el caso de las encuestas de preguntas cerradas. Además, la información recopilada por dicho instrumento será procesada con el propósito de ser presentada de manera numérica a través del uso de herramientas estadísticas, por ejemplo, cuadros o gráficos, que ayuden a una fácil comprensión e interpretación de los resultados. Dicha elección está fundamentada en la necesidad de conocer no solo las percepciones, sino también las experiencias del personal militar designado dentro del reparto de la ESNAPE.

Por otro lado, este enfoque también utiliza la recolección y el análisis de datos para contestar preguntas de investigación ya que confía en la medición numérica, el conteo y frecuentemente en el uso de la estadística para establecer con exactitud patrones de comportamiento de una población (Monje Álvarez, 2011).

En este caso, el objetivo es mejorar la seguridad de la red dentro del ámbito operativo en la Estación Naval Penitenciaria de Ecuador “ESNAPE” por medio del desarrollo de un procedimiento de seguridad que contribuya a la gestión operativo dentro del reparto naval para regular y también administrar el acceso a la red WiFi, por lo cual abarca describir los procesos administrativos, al igual que formular modelos de documentos de registros y establecer los responsables operativos, por lo que el proyecto de la presente tesis no se centra en pruebas técnicas de los sistemas de la ESNAPE, sino que el objetivo es el desarrollo de una propuesta la cual sea aplicada para una futura implementación dentro del reparto naval, para ello, el enfoque cuantitativo el cual fue elegido para la presente investigación permitirá establecer relaciones causa-efecto entre variables como es el caso del uso de dispositivos no registrados dentro del área penitenciaria, la percepción sobre políticas de seguridad, y tambien la efectividad de los procedimientos actuales, lo que brindará resultados no solo objetivos, sino tambien medibles, los cuales fundamenten el desarrollo del nuevo procedimiento de seguridad para la red de la Estación Naval Penitenciaria de Ecuador (ESNAPE).

2.2. Tipo de Investigación

Una vez que se haya recabado toda la información pertinente se procederá a utilizar el método descriptivo. Hernández, Fernández y Baptista (2011) mencionan que este tipo de

estudios permite especificar las características o propiedades más significativas de personas, grupos, poblados o de cualquier fenómeno con el cual se desarrollará el estudio. Básicamente con la descripción se hará una medición de la información a través de estadísticas y porcentajes se podrá determinar los rasgos principales de las mayorías para definir un patrón específico.

En términos prácticos, el tipo de investigación seleccionado permite, por ejemplo, el uso de encuestas y entrevistas con el fin de recopilar información detallada sobre las necesidades, desafíos y expectativas específicas del personal militar dentro de la Estación Naval Penitenciaria de Ecuador “ESNAPE”.

Dentro de este contexto, el enfoque descriptivo se centraría en la realización de un análisis exhaustivo del estado actual de la red WiFi de la Estación Naval Penitenciaria de Ecuador (ESNAPE), además de los procesos operativos involucrados en el registro de dispositivos de los usuarios, además de la autenticación de estos últimos, proporcionando así una base sólida que permitirá definir de manera clara aspectos fundamentales, los cuales requerirán una intervención y posterior desarrollo de un nuevo procedimiento. En este sentido, permitirá cumplir con el objetivo de desarrollar un procedimiento de seguridad para una correcta gestión operativa enfocada en regular y administrar los accesos de los dispositivos a la red de la ESNAPE que se adapte a la capacidad y realidad de dicho reparto militar, esto es debido a que se plantea una nueva estructura de gestión administrativa en cuanto al acceso a la red WiFi del reparto militar, en donde se incluye los roles y responsabilidades, flujos y también documentos de solicitudes.

2.3. Técnicas e instrumentos para la recolección de datos

Para realizar el correspondiente levantamiento de información se hará uso de la técnica de las encuestas con el uso de instrumentos, específicamente de los cuestionarios de preguntas cerradas, con el cual se busca cumplir con los objetivos específicos antes definidos dentro del proyecto:

- Analizar la topología de la red WiFi de la Estación Naval Penitenciaria de Ecuador (ESNAPE).
- Identificar los roles y responsabilidades del personal militar técnico encargados de la gestión operativa del acceso a la red del reparto naval, incluyendo el registro y monitoreo de dispositivos
- Diseñar un nuevo procedimiento de gestión operativa para el acceso de la red WiFi, que se adapte a las capacidades tecnológicas y organizativas de la Estación Naval Penitenciaria de Ecuador (ESNAPE).
- Evaluar el modelo del procedimiento de diseñado para el acceso a la red WiFi,

que permita valorar su eficacia y aplicabilidad para una mejor gestión operativa dentro de la Estación Naval Penitenciaria de Ecuador (ESNAPE).

2.4. Delimitación de la Investigación

La presente investigación se la realizó en la Estación Naval Penitenciaria de Ecuador (ESNAPE), la cual es un reparto militar ubicado en la provincia del Guayas, ciudad de Guayaquil, Km 16.5 Vía a Daule, dicha investigación se centró en el análisis operativo de la red ya establecida dentro del reparto militar, sin considerar la adquisición de equipamiento físico.

La duración del análisis abarcó desde el mes de octubre del año 2024 hasta el mes de febrero del año 2025. En cuanto a la población que fue objeto de estudio, esta fue el personal militar designado por la Armada del Ecuador, los cuales requerían conectividad a la red del reparto por medio de sus dispositivos personales o institucionales, al igual que el personal uniformado técnico, los cuales son los responsables de la administración de los accesos a la red, todo esto para realizar sus operaciones militares dentro de este centro penitenciario.

2.5. Universo y Muestra de la Investigación

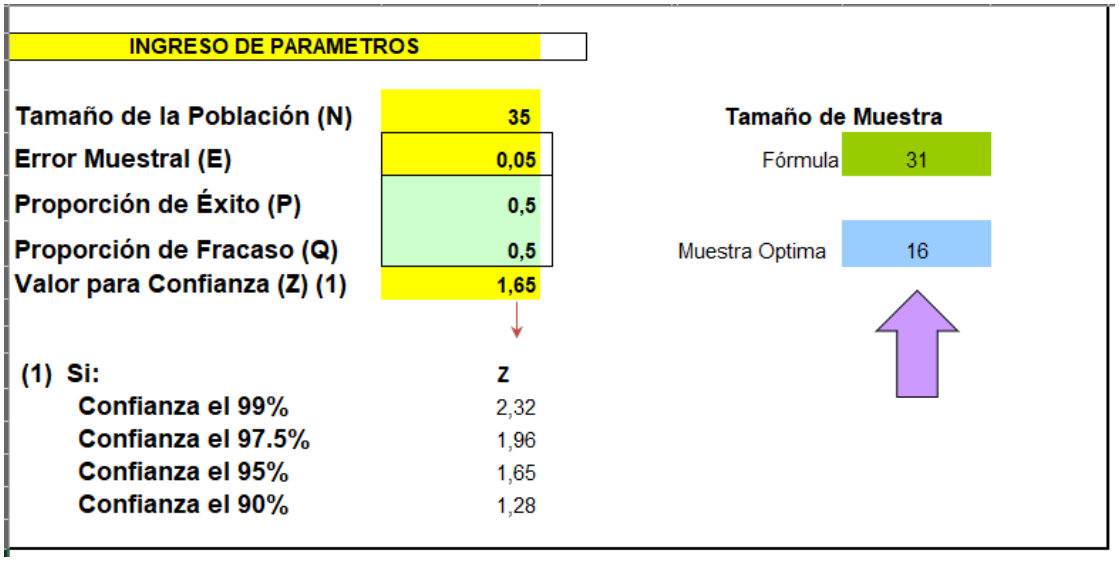
La población objeto de estudio estaba conformada por parte del personal militar activo dentro del reparto denominado ESNAPE, los cuales requerían contar con acceso a la red WiFi de dicho reparto en el marco de sus funciones, tanto operativas, como técnicas y administrativas. La muestra para la presente investigación fue seleccionada por medio de un muestreo no probabilístico por conveniencia, teniendo en cuenta solo al personal militar activo dentro del reparto naval, los cuales ya contaban con acceso a internet y excluyendo al personal que se encontraba dentro de este centro de privación de libertad como a los Agentes de la Policía Nacional y Agentes de Seguridad Penitenciaria.

En total, se llegó a encuestar a 35 militares activos dentro de la Estación Naval Penitenciaria de Ecuador que representaban distintas funciones dentro del reparto militar. Además, para la presente muestra se establecieron criterios de inclusión, como, por ejemplo, pertenecer a la Armada del Ecuador, haber solicitado acceso a la red del reparto militar, adicional, cumplir con funciones que requieran conectividad a la red de la ESNAPE.

A través de todo el proceso de muestreo se buscó recopilar información indispensable que refleje de forma precisa tanto las opiniones como la perspectiva del personal militar, así como el funcionamiento de la red interna de la ESNAPE. Esto permitió abordar de forma efectiva los objetivos específicos establecidos en la presente investigación, además de facilitar la formulación de un plan estratégico específico para el desarrollo de un procedimiento

de seguridad que contribuya a una mejor gestión operativa para no únicamente regular los accesos a la red inalámbrica, sino también administrarlos, consiguiendo así garantizar que los accesos a la red WiFi y también los servicios internos de la red de la Estación Naval Penitenciaria de Ecuador “ESNAPE” se los realice de manera organizada, segura y también eficiente. Dicho esto, con el fin de obtener una mayor comprensión en cuanto a los procesos y políticas que posee la Estación Naval Penitenciaria de Ecuador, por lo que se llevó a cabo entrevistas al personal militar técnico designado por la Armada. Esta entrevista que fue llevada a cabo permitió una visión interna de la operatividad y los desafíos que enfrenta el reparto militar en referencia a la seguridad de la red wifi del reparto militar.

Ilustración 1 Cálculo del tamaño de muestra para poblaciones finitas.



Nota. Ilustración propia que muestra la fórmula para el cálculo del tamaño de la población seleccionada que pertenece a los 35 militares activos del reparto ESNAPE.

2.6. Variables de Estudio

Las variables analizadas dentro de la presente investigación se definieron en base a los objetivos específicos establecidos dentro del proyecto.

La primera variable, definida como “El análisis de la topología de Red WiFi del reparto naval” se encuentra enmarcada en el análisis de la estructura actual de la conectividad de los elementos físicos y lógicos dentro de la red de la ESNAPE, ya que era indispensable conocer cómo se encuentra distribuida la red de dicho reparto naval para poder llevar a cabo el desarrollo del procedimiento operativo en cuanto a la gestión de acceso a la red WiFi de la Estación Naval Penitenciaria de Ecuador, porque en base a esa misma topología se debía estructurar y formular procedimiento para hacer segura a la red WiFi del reparto naval, ya que dicha red se encuentra dentro de un área crítica . En cuanto a la segunda variable, esta se

define en “Roles y Responsabilidad del Personal Militar Técnicos encargados de la gestión operativa del acceso a la red del reparto naval, incluyendo el registro y monitoreo de dispositivo”, aquí se representa los niveles tanto de intervención, como de validación y también el control dentro del proceso operativo de acceso. En referencia a la tercera variable, esta es “El diseño de un procedimiento de gestión operativa para el acceso de la red WiFi, que se adapte a las capacidades tecnológicas y organizativas de ESNAPE”, dicha variable permite no solo definir, sino también estructurar y estandarizar los pasos a seguir para un correcto acceso de los dispositivos a la red WiFi de la Estación Naval Penitenciaria de Ecuador, en donde se abarca la identificación de los roles y responsabilidades del personal militar técnico y posterior asignaciones de funciones; también la formulación de documentos de solicitudes para el registro de dispositivos de los militares activos entrantes por medio de formularios institucionales; el proceso de registro y asociación de la IP y Mac Address de los dispositivos; la supervisión constante del uso de los servicios de red; el control del número de dispositivos por cada uno de los militares dentro del reparto naval; al igual que la auditoria de los dispositivos conectados y también la liberación de los dispositivos inactivos. Ahora, la cuarta variable es la “Administración y Monitoreo de la Red”, la cual se enfoca en todas aquellas acciones para salvaguardar la seguridad operativa de la red del reparto militar por medio del seguimiento y control de los dispositivos que se encuentren conectados.

Tabla 1. Matriz de Operacionalización de Datos

Variables	Contextualización	Indicadores	Instrumentos
Topología de Red WiFi.	Análisis del diseño y segmentación de la red de la Estación Naval Penitenciaria de Ecuador (ESNAPE).	Segmentación de las áreas del reparto militar, puntos de accesos e interconexiones.	Encuestas y observación.
Roles y Responsabilidad del Personal Militar Técnico.	Identificación de las responsabilidades del personal militar técnico en el proceso de acceso de los dispositivos.	Flujo de autorización y niveles jerárquicos de aprobación.	Encuestas y entrevistas.
Diseño del procedimiento propuesto.	Estandarización de procesos y validación de accesos.	Cantidad de registros, tiempos de respuesta, y nivel de satisfacción con	Encuestas.

		soluciones propuestas.	
Evaluación del procedimiento.	Seguimiento e identificación de mejoras.	Identificación de mejoras y nivel de satisfacción.	Encuestas y observación.

Fuente: Elaboración propia (2025).

2.7. Métodos de Estudio

Dentro del ámbito metodológico dentro de la presente investigación, se hizo uso de diferentes métodos de estudio con el objetivo de entender y también mejorar el procedimiento de seguridad para una mejor en la gestión operativa de los accesos de dispositivos a la red perteneciente al reparto militar ESNAPE, por lo que en primer lugar, el método empleado para el presente trabajo investigativo fue el de la observación y medición, debido a que en primera instancia se deberá recabar datos que ayuden a identificar el problema y aquellas características principales dentro del reparto militar en respecto al tema a estudiarse. También, para complementar el enfoque elegido, el cual fue cuantitativo, se empleó métodos observacionales dentro del ámbito del flujo operativo técnico dentro de la Estación Naval Penitenciaria de Ecuador (ESNAPE). Dichas observaciones tenían el objetivo de comprender las actividades realizadas por el personal militar técnico. Por tal razón, este componente fue indispensable ya que permitió ajustar la propuesta metodológica con una perspectiva realista del entorno en donde se desarrolla el proyecto.

En segundo lugar, con el fin de recolectar toda la información empírica, por tanto, se hizo uso de encuestas que, mediante la aplicación de un banco de preguntas estructurados, las cueles eran de preguntas cerradas y de opción múltiple a la muestra seleccionada que en este caso era el personal militar interno de la Estación Naval Penitenciaria de Ecuador (ESNAPE), además de entrevistas con el propósito de recopilar datos directamente de la población objeto de estudio.

Por un lado, las encuestas realizadas a la población de estudio permiten tener una mayor facilidad en referencia al análisis estadístico, esto es debido a que las respuestas obtenidas pueden ser cuantificadas de manera más asequible, además, este método de estudio asegura que la población de estudio, que en este caso es el personal militar, respondan seleccionando una de las respuestas predefinidas, haciendo que este método facilite la recopilación tanto de datos específicos como estructurados, lo que contribuye a que la información sea concisa en referencia a las opiniones del grupo de la muestra estudiada.

Y, en cuanto a las entrevistas, estas fueron dirigidas al personal militar activo dentro del reparto de la ESNAPE, en donde dichas entrevistas proporcionaron una mayor comprensión en cuanto a los procesos internos, además de los desafíos que enfrentaba la Estación Naval Penitenciaria de Ecuador (ESNAPE). Aquí se incluyeron debates y opiniones en cuanto al procedimiento operativo que se encontraba vigente en ese momento y las posibles áreas de mejora.

Tras esto, se evaluaron las respuestas de las encuestas, además de analizar las transcripciones de las entrevistas con el objetivo de extraer información valiosa.

2.8. Instrumentos de Recolección de Datos

Dentro del presente proyecto de investigación se hizo uso de múltiples técnicas e instrumentos tanto para la recopilación como para el análisis de datos de manera exitosa, por ello, las encuestas fueron uno de los instrumentos fundamentales, dicho instrumento permitió obtener datos cuantificables en referencia no solo a la percepción, sino también al conocimiento y experiencia del personal militar activo con respecto a un procedimiento de seguridad de red, además de la aceptación de una propuesta de mejora. Las preguntas fueron diseñadas basándose únicamente en aquellos componentes clave de un procedimiento de seguridad, como es el caso la identificación de los roles y responsabilidades del personal militar técnico, formulación de documentos de solicitudes para el registro de dispositivos de los militares activos entrantes, los pasos a seguir en cuanto al proceso de registro y asociación de la IP y Mac Address de los dispositivos, el control del número de dispositivos por cada uno de los militares dentro del reparto naval, la auditoria de los dispositivos conectados y también la liberación de aquellos dispositivos inactivos. Y para complementar las encuestas, tambien se aplicaron cuestionarios con una escala Likert al personal militar que conformaba la población de estudio dentro del presente proyecto de investigación. Este tipo de cuestionario permitió al personal uniformado expresar sus opiniones y evaluaciones en una escala de respuesta, lo que facilitó la cuantificación de sus percepciones y expectativas en relación a los procedimientos vigentes en cuanto al acceso a la red WiFi dentro de la ESNAPE. Las escalas Likert resultaron especialmente útiles tanto para medir las actitudes, como es el caso de los niveles de acuerdo o desacuerdo.

También se llevaron a cabo entrevistas, en donde se hizo uso de preguntas abiertas. Este nuevo enfoque aplicado a los entrevistados contribuyó a proporcionar respuestas no solo detalladas, sino también beneficiosas, esto es debido a que no se encontraban limitadas por respuestas predefinidas como es el caso de las encuestas que también se habían realizado. Dichas entrevistas con preguntas abiertas promovieron la expresión de opiniones propias, además de experiencias personales, lo que, sin duda, contribuyó a la obtención de

una mejor comprensión de los desafíos y las perspectivas de una propuesta para un nuevo procedimiento de seguridad para la correcta gestión operativa enfocada en regular y también administrar el acceso de los dispositivos del personal militar a la red WiFi dentro del reparto naval ESNAPE.

Una vez realizado las encuestas como las entrevistas, se procedió a la recopilación de los mismos, por tal razón se empleó la técnica de análisis de datos para procesar y examinar la información recopilada, lo cual se explicará de manera más completa en el punto del procesamiento y análisis de datos.

2.9. Procesamiento y Análisis de los Datos

En conjunto con lo anteriormente presentado en cuanto a los Métodos e Instrumentos de Recolección de Datos, ya en referencia al proceso de procesamiento y análisis de datos dentro de la presente investigación se aplicó un método el cual estuvo basado en técnicas estadísticas descriptivas, en donde los datos que se recolectaron por medio de las encuestas fueron posteriormente tabulados en hojas de cálculo, en donde se estructuraron en base a las variables de estudio establecidas, las cuales contribuyeron a facilitar la interpretación de los datos recolectados previamente. Por esta razón, las respuestas obtenidas fueron procesadas utilizando hojas de cálculos de la herramienta ofimática Excel, debido a que se hicieron operaciones estadísticas que contribuyeron a la extracción de información y que a su vez proporcionó una visión más clara de la situación en la que se encontraba la Estación Naval Penitenciaria de Ecuador (ESNAPE) por medio de las encuestas. También se realizaron gráficos de barras o pasteles que permitieron representar de manera visual los resultados obtenidos y que a su vez influyeron en el enriquecimiento del análisis estadístico, además de que facilitaron la presentación de los resultados, además de que se pudo asegurar una presentación no solo efectiva, sino también comprensible para el público objetivo, con ello se puede decir que este enfoque no solo destaca los resultados, sino que también enfatiza la importancia de la visualización de datos dentro de la presente investigación.

Este procedimiento estadístico fue útil y pertinente, no solo para identificar tendencias, sino también para evaluar la eficiencia de los protocolos vigentes dentro de la ESNAPE, además de que funcionó como base objetiva para diseñar un nuevo procedimiento para una mejora en la gestión operativa la cual pueda tanto regular como administrar de mejor manera los accesos de los dispositivos a la red de la Estación Naval Penitenciaria de Ecuador, por lo cual se ajustó no solo a las necesidades del reparto militar, sino también a sus capacidades, por tal razón permitió validar la necesidad de un procedimiento de seguridad más estructurado, formalizado y seguro para la red de la Estación Naval Penitenciaria de Ecuador (ESNAPE).

Una vez que se concluyó con el análisis dentro de la herramienta ofimática Excel, se procedió a la presentación de hallazgos, por tal razón dichos hallazgos fueron llevados a cabo con profesionalismo mediante la herramienta ofimática Microsoft Word. En este punto, no solo había que limitarse a resumir resultados, por lo que Word se convirtió en una herramienta indispensable para la realización de informes detallados.

La inclusión de gráficos realizados previamente en la herramienta de Excel desempeñó un rol importante tanto en la claridad como en la accesibilidad de estos informes, lo que aseguraba una presentación no solo efectiva, sino tambien comprensible para el personal militar técnico y los oficiales. Este enfoque aplicado no solo se centra en destacar los resultados, sino que también hace énfasis en la importancia de la visualización de los datos de la investigación.

2.10. Fases de Investigación y Resultados Esperados

2.10.1. Fase 1: Analizar la topología de la red WiFi de la Estación Naval Penitenciaria de Ecuador (ESNAPE)

Dentro de esta primera fase por medio de un diagnóstico profundo se pudo identificar los aquellos elementos importantes dentro de la red WiFi de la Estación Naval Penitenciaria de Ecuador, en donde se hizo un mayor enfoque en la distribución de los puntos de accesos, la cobertura dentro del reparto militar, y los mecanismos de monitoreo disponibles por medio de la Controladora Cloud Key Gen2 Plus.

Es importante mencionar que para llevar a cabo este diagnóstico se realizó una observación directa a la distribución de la red dentro del reparto naval, además de que se aplicaron entrevistas al personal militar técnico, además de los militares activos dentro de la ESNAPE, esto se lo hizo con el fin de conocer las opiniones individuales, sino también para evaluar la eficacia del procedimiento vigente, además de la frecuencia en casos de accesos no autorizados y la percepción del personal uniformado en cuanto a los accesos de los dispositivos a la red WiFi de la Estación Naval Penitenciaria de Ecuador.

Resultados Esperados en la Fase 1:

Se espera contar con una visión completa de las debilidades operativas actuales dentro del reparto militar ESNAPE, además de la percepción que hay en cuanto a la gestión de acceso de los dispositivos a la red, esto quiere decir que se espera contar con una visión más amplia y funcional de la topología de red WiFi de la ESNAPE, incluyendo la capacidad de control en cuanto a los dispositivos conectados; esto es importante para que sirva como base en el diseño de medidas de mejora en el desarrollo de un procedimiento operativo para la Estación Naval Penitenciaria de Ecuador.

2.10.2. Fase 2: Identificación de los roles y responsabilidades del personal militar técnico encargados de la gestión del acceso a la red, registro y monitoreo de dispositivos

Por medio de la observación directa y también por las entrevistas dirigidas al personal militar técnico delegados encargados de la red, se pudo levantar información sobre el proceso operativo que se encontraba en vigencia en ese momento dentro del reparto militar ESNAPE. Esto permitió mapear los procesos que se llevaban a cabo, además de los tiempos estimados y la validación por parte del personal involucrado. Por tal razón se planea establecer tareas como el registro de IP/MAC, la liberación de los usuarios inactivos y también el monitoreo continuo de aquellos dispositivos ya conectados.

- **Resultados Esperados en la Fase 2:**
  Dentro de esta segunda fase se espera contar con una estructura más clara en cuanto a las responsabilidades del personal militar técnico dentro de la ESNAPE, lo que pude llegar a facilitar la gestión para que sea más eficaz, además de controlar el acceso a la red, y asegurar a su vez que cada uno del personal técnico militar cumpla con sus funciones tanto en el registro como en el monitoreo y liberación de dispositivos.

2.10.3. Fase 3: Diseño del procedimiento de seguridad

Por medio de un análisis operativo en conjunto con los resultados de la fase del diagnóstico, se organizó un nuevo procedimiento el cual contempla varios apartados que contribuirán a una mejora en cuanto a la gestión operativa de los accesos de dispositivos del personal militar a la red WiFi de la ESNAPE, dicho procedimiento se compone no solamente de establecer los roles y responsabilidades del personal militar técnico, sino también la formulación de documentos de solicitudes para el registro de dispositivos de los militares activos, además del proceso de registro y asociación de la IP y Mac Address de los dispositivos, la supervisión en cuanto al uso de los servicios de red, el control del número de dispositivos por cada uno de los militares dentro del reparto naval, las auditorias de los dispositivos que se encuentren conectados y finalmente, la liberación de los dispositivos inactivos.

Dicho procedimiento fue propuesto de tal forma estandarizada y de tal manera que sea adaptable a la realidad de la Estación Naval Penitenciaria de Ecuador (ESNAPE).

- **Resultados Esperados en la Fase 3:**
  Contar con un procedimiento conciso y eficiente el cual no solo reduzca los márgenes de error, sino que también tenga como objetivo mejorar la seguridad operativa de la red de la Estación Naval Penitenciaria de Ecuador (ESNAPE).

2.10.4. Fase 4: Evaluación y retroalimentación del procedimiento propuesto

Dentro de esta fase se dio paso a la evaluación y retroalimentación del procedimiento diseñado para el acceso a la red WiFi dentro del reparto militar ESNAPE, además de presentar los resultados obtenidos a todas las partes involucradas, lo que incluye al personal militar técnico y los usuarios que vienen a ser el personal uniformado ya sean tripulantes u oficiales.

- **Resultado Esperado en la Fase 4:**
  Validar el impacto que puede generar la aplicabilidad de una nueva propuesta de un procedimiento de seguridad que contribuya a una mejora en la gestión operativa por parte del personal militar técnico de la Estación Naval Penitenciaria de Ecuador, para regular y también administrar los accesos del dispositivo a la red WiFi del reparto naval, además de compartir recomendaciones adicionales para la sostenibilidad en el tiempo.

CAPÍTULO III

ANÁLISIS DE RESULTADOS

CAPÍTULO III

ANÁLISIS DE RESULTADOS

El análisis de los resultados es considerado como una fase crucial dentro de cualquier proyecto de investigación, haciendo énfasis en la etapa de convergencia en donde los datos son recopilados de forma meticulosa, además del procesado correspondiente (Bermúdez Rubio, Cuenca Rivera, García Murillo, Gutiérrez Gómez, & Portela Ramírez, 2021).

Dentro de este capítulo se expone los resultados que se obtuvieron a lo largo del desarrollo del presente proyecto “Desarrollo de un procedimiento de seguridad en la red para la implementación de los esquemas de la Estación Naval Penitenciaria de Ecuador”, por lo que para llevar a cabo esto fue considerado no solo la implementación por etapas en referencia al procedimiento de seguridad propuesto, sino que también para el desarrollo de la presente investigación se ha llevado a cabo un proceso meticuloso tanto de recopilación de datos cuantitativos por medio de encuestas, además de su procesamiento, con el propósito de valorar tanto la viabilidad como la aceptación y eficacia de un nuevo modelo de gestión de seguridad para la red WiFi de la ESNAPE, también, dicho proceso fue respaldado por herramientas estadísticas avanzadas.

Cabe mencionar que los resultados obtenidos adquieren una importancia trascendente en referencia al procedimiento operativo dentro de la Estación Naval Penitenciaria de Ecuador (ESNAPE), donde dichos resultados son parte de una etapa imprescindible en donde la información recolectada cobra una importancia significativa. Por tal razón, el análisis que se llevó a cabo no solo se limitó a las percepciones del personal militar activo de la ESNAPE encuestado, sino que también incluye una descripción cronológica pertinente en referencia a las actividades realizadas, las cuales, cabe destacar, se encuentran vinculadas de manera directa con las fases metodológicas del presente proyecto, lo que sin lugar a dudas, permite evidenciar de manera concreta la progresiva consolidación de la propuesta, la cual es el procedimiento de seguridad técnico-operativo que se diseñó.

De acuerdo a la metodología implementada dentro del presente proyecto, en primer lugar, se realizará la presentación del desarrollo del proyecto por fases y en segundo lugar, se presentará los resultados empíricos obtenidos de la metodología cuantitativa aplicada dentro del presente proyecto.

3.1. Resultados del Análisis Funcional por Fases

3.1.1.- Fase 1: Análisis de la topología de la red WiFi de la Estación Naval Penitenciaria de Ecuador "ESNAPE".

Dentro de la primera fase del proyecto, esta se centró en no solo conocer, sino tambien comprender de manera detallada el cómo está estructurada la red inalámbrica de la Estación Naval Penitenciaria "ESNAPE", reparto militar perteneciente a la Armada del Ecuador. Es importante destacar que, debido a la naturaleza reservada del propio entorno militar, el acceso físico a los componentes críticos de la red de la ESNAPE fue limitado. Sin embargo, para poder llevar a cabo el presente proyecto de manera satisfactoria y proponer un procedimiento de seguridad realista y que se adapte a las capacidades de la Estación Naval Penitenciaria de Ecuador, se solicitó colaboración directa con el personal técnico del reparto militar ESNAPE. Como resultado de dicha colaboración directa, se obtuvo una imagen oficial del mapa de distribución de la red de la ESNAPE, la cual representa la distribución tanto física como lógica de los dispositivos de red desplegados dentro de este reparto militar, ya que el presente proyecto se debía hacer en base a la topología crear un procedimiento para hacer segura esa red, ya que la ESNAPE se encuentra dentro de un área crítica como lo es una zona penitenciaria.

El mapa proporcionado por los técnicos de la ESNAPE incluye los puntos de acceso inalámbrico, además de los dispositivos activos y sobre todo disponibles dentro del reparto naval como lo son los switches, el firewall y la controladora de red. Es gracias a esta información importante que se pudo lograr un análisis exhaustivo para comprender la forma en que están conectados los distintos dispositivos, además de la segmentación de la red, al igual que la existencia de VLANs, tambien y el flujo de datos desde la conexión inicial del usuario hasta su validación y salida a internet a través del proveedor CEDIA.

Se debe mencionar que, adicionalmente, se realizó la evaluación de aquellos componentes técnicos utilizados, en este caso, los equipos marca Ubiquiti en los puntos de acceso, así como la configuración general de la red, la cual presenta una estructura jerárquica básica típica de redes.

Cabe destacar que dentro del ámbito operativo del reparto militar ESNAPE, gracias a esta fase inicial enfocada en el análisis, se pudo determinar aquellos puntos críticos los cuales deben fortalecerse en referencia al control de los accesos a la red WiFi de este reparto, en donde a su vez se destaca ese necesidad de no únicamente limitar el uso de la red para el personal militar activo, sino que también no existan casos de accesos no autorizados a dicha red WiFi, ya que como se lo ha mencionado, la ESNAPE al ser una instalación militar es

considerada un área sumamente crítica y más aún cuando está dentro de una zona penitenciaria.

Es aquí donde no se pudo constatar que existe una conexión poco controlada, debido a la falta de un procedimiento formal no solo de autorización, sino también de monitoreo y trazabilidad en cuanto al acceso a la red WiFi de del reparto naval, lo cual puede traer consigo posibles vulnerabilidades, lo que evidentemente puede generar un escenario propenso a accesos no autorizados dentro de la red de la Estación Naval Penitenciaria de Ecuador "ESNAPE", más aún siendo una institución perteneciente al ámbito militar y de alta sensibilidad como lo es la ESNAPE.

3.1.2.- Resultado Obtenido de la Fase 1: Análisis de la topología de la red WiFi de la Estación Naval Penitenciaria de Ecuador "ESNAPE".

Como efecto de la ejecución de esta fase, se pudo consolidar un entendimiento completo en cuanto al estado actual de la red WiFi dentro del reparto militar ESNAPE. El análisis exhaustivo del mapa de red permitió sentar las bases para estructurar una propuesta de seguridad, la cual evidentemente debía estar alineada a las capacidades tecnológicas existentes dentro de la Estación Naval Penitenciaria de Ecuador.

Dentro de la Fase 1 " Análisis de la topología de la red WiFi de la Estación Naval Penitenciaria de Ecuador" se pudo detectar que la red del reparto militar ESNAPE no cuenta con un procedimiento formal, lo cual representa una debilidad crítica. La visualización detallada de la topología fue indispensable para identificar los puntos donde deben implementarse medidas como la doble autenticación basada en direcciones IP/MAC, el monitoreo continuo de accesos, la liberación de IP de aquellos usuarios inactivos, y el monitoreo de equipos conectados por medio de la controladora WiFi. En este sentido, el acceso a la conectividad se la daba de manera manual sin un registro pertinente, con direcciones IP distribuida de forma dinámica y sin contar con un control preciso de las direcciones MAC Address de los dispositivos, de igual manera, por medio de encuestas se pudo evidenciar que múltiples militares contaban con más de un dispositivo registrado, lo que podría generar un margen de incidencias, además de dificultar un proceso de administración y auditoria.

Finalmente, para concluir la primera fase se puede decir que dicha fase fue determinante esto es debido a que en primer lugar, se pudo constatar que existe la necesidad de implementar un procedimiento el cual sea más riguroso, y que no solo contemple la autorización en base a los roles específicos dentro del reparto naval, sino también la identificación de los usuarios a la asociación a sus dispositivos, además de que el diseño del

procedimiento propuesto no se desarrollaría en el vacío, sino alineado a una comprensión clara de cómo opera actualmente la red del reparto militar ESNAPE. Dicha información sirvió como punto de inicio técnico y tambien estratégico para todo lo que restaba del proyecto, asegurando así que las decisiones posteriores fueran coherentes y que estuvieran adaptadas a la infraestructura ya implementada dentro de la Estación Naval Penitenciaria de Ecuador.

3.1.3.- Fase 2: Identificación de Roles y Responsabilidades del Personal Militar Técnico

Durante la segunda fase, se pudo llevar a cabo un proceso de análisis funcional del personal técnico militar dentro de la ESNAPE encargado de tanto de la administración, como el mantenimiento y monitoreo de la red WiFi del reparto militar. Por lo que para poder llevar un correcto desarrollo de la fase 2, se estableció contacto con los funcionarios responsables operativos tanto del reparto militar ESNAPE como de la Dirección de Tecnologías de la Información y Comunicaciones (DIRTIC), identificando así sus funciones, las herramientas utilizadas y tambien los protocolos internos en cuanto a la validación de dispositivos del personal militar.

Inicialmente dentro de la Fase 2 se pudo evidenciar que el registro de dispositivos de todo el personal militar se lo realizaba únicamente desde el sistema de control local del reparto ESNAPE, esto quiere decir que no se contaba una participación de ningún otro reparto naval. La falta de un procedimiento robusto ha facilitado la aparición de casos de accesos no autorizados a la red WiFi de la Estación Naval Penitenciaria de Ecuador, lo que sin lugar a dudas representaba un riesgo no solo a nivel operativo, sino tambien a la seguridad estratégica dentro de un área critica como lo es un reparto militar, como la ESNAPE.

3.1.4.- Resultados Obtenidos de la Fase 2: Identificación de Roles y Responsabilidades del Personal Militar Técnico:

Es debido a lo realizado en esta segunda fase y a lo presentado anteriormente que uno de los resultados más significativos dentro de esta segunda fase fue la de establecer una estructura que sea tanto jerárquica como funcional con el fin de que se establezca de manera comprensible la gestión del acceso a la red WiFi del reparto naval. Además, en cuanto al nivel operativo, se pudo determinar que este control de acceso de los dispositivos a la red WiFi no debería recaer únicamente en un solo funcionario, al contrario, esta responsabilidad debería ser una labor compartida entre los militares técnicos de la propia ESNAPE.

Ahora, gracias a la información recopilada dentro de la Fase 2, se procedió con la estructuración del procedimiento por medio de un modelo de flujo operativo, el cual define

con precisión tanto las actividades como las decisiones por cada uno de las partes involucradas.

1.- Militar solicitante: Son el personal uniformado perteneciente a la Armada del Ecuador quienes ingresan a realizar funciones dentro de la Estación Naval Penitenciaria de Ecuador “ESNAPE” (cada dos meses hay un relevo de personal), además de que son quienes iniciaran el proceso.

2.- Militar técnico de la ESNAPE: Son los militares designados dentro de área técnica de la Estación Naval Penitenciaria de Ecuador “ESNAPE”, los cuales son tripulantes especialistas dentro del ámbito informático y son quienes deberán receptar la solicitud inicial, además de verificar la información proporcionada por el militar solicitante.

3.- Militar Oficial del área de tecnologías de la información y comunicación de la ESNAPE: Es el oficial especialista al mando del área técnica de la Estación Naval Penitenciaria de Ecuador y será quien tenga la potestad de aprobar o denegar las solicitudes del personal militar entrante para el acceso a la red WiFi de la ESNAPE.

4.- Militar técnico del reparto designado (DIRTIC): Son los militares activos dentro de área de tecnologías de la Dirección de Tecnologías de la Información y Comunicaciones (DIRTIC), los cuales son tripulantes especialistas dentro del ámbito informático y quienes receptan los documentos de la ESNAPE, además de ejecutar los registros de las MAC Address y también asignar una IP dentro del Firewall Fortigate.

5.- Oficial de Seguridad Informática (OSI): Es el oficial especialista, denominado OSI, quien está al mando del área de tecnologías de la Dirección de Tecnologías de la Información y Comunicaciones (DIRTIC), y será quien administre y monitoree los dispositivos conectados por medio de la Controladora para remitir informes mensuales a la ESMAAR.

Finalmente, gracias a esta segunda fase, se pudo cimentar las bases organizativas para garantizar así que el nuevo procedimiento de seguridad dentro de la Estación Naval Penitenciaria de Ecuador sea factible de implementar dentro de las condiciones reales de este mismo reparto militar.

3.1.5.- Fase 3: Diseño del Procedimiento de Seguridad

Con base en todos los hallazgos de las dos fases anteriores, se pudo elaborar un procedimiento técnico-operativo el cual debía estar destinado a estandarizar el proceso de autorización, además del control y monitoreo de los dispositivos con accesos a la red inalámbrica del reparto militar ESNAPE. Es por tal razón que dicho procedimiento fue

diseñado para cubrir todo el ciclo de vida del acceso de los disipativos a la red WiFi de la Estación Naval Penitenciaria de Ecuador, y esto va desde la solicitud inicial, la validación, el registro de IP desde la ESNAPE y la DIRTIC como doble factor de autenticación, hasta el monitoreo posterior a la conexión. Es precisamente dentro de esta fase en donde se definió de manera clara y tácita las etapas que comprende desde la recepción de la solicitud, validación técnica, aprobación jerárquica, configuración de acceso mediante dirección IP y MAC Address de doble validación, Consultas de los usuarios ingresados, la liberación de aquellas IP de usuarios sin actividad, el monitoreo de los equipos conectados dentro de la controladora de la ESNAPE.

Asimismo, se procedió a elaborar un diagrama de flujo, también de formularios estandarizados para facilitar la adopción del procedimiento por parte del personal militar técnico. Cabe mencionar que este diseño se adaptó específicamente a la realidad y a los recursos con los que cuenta ESNAPE, y esto se lo pudo hacer sin requerir inversiones adicionales ya sea de hardware o software.

3.1.6.- Resultados Obtenido de la Fase 3: Diseño del Procedimiento de Seguridad

Con los resultados obtenidos anteriormente dentro de la Fase 1 y Fase 2, se pudo identificar esa latente necesidad de estructurar el procedimiento, el cual no solo formalice, sino también regule los accesos de los dispositivos a la red WiFi de la Estación Naval Penitenciaria de Ecuador “ESNAPE”. Por lo cual, dentro de la presente Fase se llevó a cabo el desarrollo del diseño de un procedimiento técnico-operativo, dentro del cual no solo establezca los roles y responsabilidades de manera clara, sino también los pasos destallados, además de los controles específicos tanto para poder garantizar la seguridad, y también la trazabilidad, además de la correcta gestión en cuanto a los dispositivos que se conectan dentro de la red WiFi de la ESNAPE.

El resultado que se obtuvo dentro de la Fase 3 fue un procedimiento estructurado, práctico y adaptado a la realidad y capacidad del entorno militar de la Estación Naval Penitenciaria de Ecuador, además que este 3 conllevo a una delimitación de los roles operativos, ya que esto fue fundamental para el desarrollo del procedimiento propuesto, el cual también se fundamentó en dos componentes importantes:

1.- Los roles y responsabilidades del personal militar involucrados, y

2.- Flujo técnico-operativo en cuanto al registro de dispositivos del personal uniformado y la validación del acceso de los mismos.

En cuanto a los roles y responsabilidades del personal militar involucrados, aquí es donde se pudo definir de manera estructurada los siguientes perfiles, además de su intervención dentro del desarrollo del presente procedimiento:

1.- Militar solicitante:

- Es aquel militar que ingresa a realizar funciones dentro de la Estación Naval Penitenciaria de Ecuador “ESNAPE” y quien requiere el acceso a la red WiFi del reparto militar.
- Es quien inicia el proceso por medio de la entrega del Anexo A, en donde este declara no solo sus datos personales como sus nombres, apellidos, rango, reparto y demás, sino que también el tipo de dispositivo que desea registrar, y si es personal o institucional, la MAC Address de ese dispositivo.

2.- Militar técnico de la ESNAPE:

- Es el militar del área técnica de la Estación Naval Penitenciaria de Ecuador “ESNAPE”, quien deberá no solo receptar la solicitud inicial, sino también verificar que no exista duplicidad de registro, o que el militar solicitante no exceda los dispositivos permitidos.
- Debe remitir la solicitud inicial al otro reparto interviniente, en este caso se propuso la participación de la DIRTIC, por medio del correo institucional de la Armada (Zimbra).
- También se debe encargar de realizar tanto la activación como liberación de los dispositivos según se den los relevos del personal militar a la ESNAPE, todo esto se lo tendrá que realizar dentro del Firewall Fortigate.
- Finalmente, es quien deberá realizar informes semanales a la DIRTIC en referencia a los dispositivos activos para su auditoria correspondiente.

3.- Militar Oficial del área de tecnologías de la información y comunicación de la ESNAPE:

- Es quien aprueba o deniega de manera formal la solicitud de registro previa.
- Una vez que aprueba la solicitud inicial deberá completar el documento Anexo B para remitirlo al militar técnico de la ESNAPE.
- También se debe encargar del monitoreo contino de todos los dispositivos autorizados y que cuenten con acceso a la red WiFi de la ESNAPE.

4.- Militar técnico del reparto designado (DIRTIC)

- Es quien tendrá que receptar las solicitudes provenientes de la ESNAPE y a su vez remitirlas al Oficial de Seguridad Informática (OSI).
- Es quien se encargará de ejecutar los registros de las MAC Address de los dispositivos solicitantes además de asignar una IP dentro del Firewall Fortigate.
- Una vez realizadas sus funciones deberá comunicar por medio del correo institucional (Zimbra) al militar técnico de la ESNAPE para que pueda habilitar el acceso de los dispositivos correspondientes.

5.- Oficial de Seguridad Informática (OSI)

- Deberá verificar la documentación enviada por la ESNAPE.
- Encargado de la Controladora de la Armada del Ecuador para administrar y monitorear las conexiones activas dentro de la ESNAPE para remitir informes mensuales a la ESMAAR.

En cuanto al Procedimiento Técnico-operativo propuesto dentro del presente proyecto, se compone de los siguiente:

1.- El procedimiento empieza con la solicitud inicial por parte del militar entrante a la ESNAPE, por medio del Anexo A.

2.- Revisión técnica por parte del equipo de tecnología de la ESNAPE, verificando que los datos del dispositivo correspondan, el número de dispositivos del usuario y que no exista duplicidad.

3.- Validación por el Oficial de TICS de la ESNAPE para su aceptación o rechazo.

4.- Remisión dirigida a DIRTIC en donde se incluya los Anexos A y B por medio de correo institucional (Zimbra).

5.- Configuraciones técnicas de los dispositivos por medio de:

- Registro del dispositivo por la MAC y asignación por IP dentro del Firewall Fortinet modelo FG-70F.
- Monitoreo de los dispositivos por medio de la Controladora (Cloud Key Gen2).

6.- La activación del acceso lo realiza el militar técnico de la ESNAPE según el procedimiento operativo.

7.- El monitoreo y posterior auditoría debe ser reportado mensualmente por el Oficial de Seguridad Informática (OSI) de la DIRTIC a la ESMAAR.

Todo este diseño realizado dentro de la Fase 3 tiene el objetivo de no solo estandarizar el procedimiento, sino también, promover las transparencias, además de delimitar las responsabilidades del personal militar técnico dentro de la ESNAPE por niveles jerárquicos, por tal razón se pudo lograr delimitar las funciones específicas de cada una de las partes involucradas en cuanto al control de acceso a la red WiFi de la ESNAPE.

Este nuevo enfoque funcional permitió estructurar el procedimiento de seguridad propuesto de tal manera que cada rol tenga asignaciones específicas, además de responsabilidad compartida pero delimitada. Además de permitir un control formal y sobre todo más seguro en cuanto a los dispositivos conectados a la red WiFi del reparto naval, y esto a su vez puede contribuir a la reducción de los riesgos en torno a la seguridad y también a los accesos no autorizados.

Cabe mencionar que el presente procedimiento de seguridad no solo responde a la necesidad de fortalecer la seguridad digital, sino que también mejora la eficiencia en la gestión de usuarios militares. Ya que, al estar alineado con los roles previamente identificados, además de la infraestructura disponible, dio paso a convertirse en una herramienta viable y sostenible a largo plazo.

3.1.7.- Fase 4: Evaluación y retroalimentación del procedimiento propuesto

Finalmente, la fase 4 consistió en someter el procedimiento de seguridad ya diseñado para la gestión de los accesos de los dispositivos del personal militar de la ESNAPE a la red WiFi de dicho reparto naval, mediante una evaluación preliminar, dicha evaluación se la hizo por medio de la aplicación de entrevistas al personal militar activo dentro de la Estación Naval Penitenciaria de Ecuador "ESNAPE", incluyendo tambien al personal militar técnico ya que estos últimos son los que interactúan con la red. En referencia a la evaluación realizada, dicha entrevista consistió en preguntas que evaluaban la viabilidad del procedimiento propuesto dentro del reparto militar, además de la percepción sobre la seguridad, la experiencia de conectividad, y tambien la aceptación del modelo propuesto, y sobre todo, lo que se buscaba dentro de esta fase por medio de las entrevistas era mejorar la propuesta planteada en el proyecto con base en criterios tanto operativos como técnicos. Todo este proceso permitió

validar, desde una perspectiva empírica, la pertinencia de la propuesta formulada dentro del presente trabajo de investigación.

Cabe mencionar que, como complementación se la Fase 4 fue sometida a una encuesta Likert, la cual es una herramienta de medición utilizada en este caso para recopilar datos en cuanto a la percepción y aceptación del procedimiento propuesto, en donde el personal militar encuestado tuvo que responder seleccionado una de las opciones de escala dentro de la encuesta Likert para indicar el nivel de acuerdo o desacuerdo en cuanto al procedimiento del presente proyecto. Finalmente, se consideró tambien la posibilidad de poder implementar este modelo dentro de otros repartos militares de la Armada del Ecuador como medida estandarizada.

3.1.8.- Resultados Obtenidos de la Fase 4: Evaluación del Nuevo Procedimiento de Seguridad:

Una vez que se elaboró el procedimiento técnico-operativo, este fue sometido a un proceso de evaluación tal y como se establece dentro de la Fase 4, dicho proceso fue de evaluación cualitativa en donde participaron las partes involucradas, en este caso, los militares dentro de la Estación Naval Penitenciaria de Ecuador “ESNAPE”, incluyendo al personal técnico y oficial de TICS.

El objetivo principal de la Fase 4 denominada “Evaluación del Nuevo Procedimiento de Seguridad” fue obtener no solo las observaciones pertinentes, sino también validar la viabilidad del flujo planteado dentro de la propuesta, además de mejorar esta última en base a los criterios tanto operativos como técnicos.

1.- Herramientas de Evaluación

- Entrevistas al personal militar de arma, técnicos y oficial de TICS de la Estación Naval Penitenciaria de Ecuador “ESNAPE”.
- Encuesta Likert aplicada al personal uniformado para medir la percepción del procedimiento por medio de escalas que permiten a dichos militares indicar su grado tanto de acuerdo como de desacuerdo.
- Simulación de flujo documental con el objetivo de detectar posibles cuellos de botella o redundancia en cuanto al control.

2.- Hallazgos Principales y Retroalimentación Pertinente

a) Viabilidad Operativa Aceptable: El personal militar técnico pudieron indicar que el procedimiento realizado es viable en términos logísticos, además de que puede ser implementado dentro de los esquemas actuales de la ESNAPE.
b) Preocupación en los tiempos de respuesta: Durante la presente fase se señalo que los tiempos de verificación y posterior validación podrían extenderse en referencia a los horarios (no laborales y fines de semana), por lo cual se sugirió que se definieran los tiempos de respuestas.
c) Necesidad de Programas de Capacitación: Se propuso realizar capacitaciones o explicaciones al personal militar en cuanto a las condiciones del uso de la red WiFi del reparto naval, los tipos de dispositivos autorizados y la cantidad máxima, además de las consecuencias del mal uso de la red de la ESNAPE.

3.- Mejora del Procedimiento en Base a las Retroalimentaciones

Con toda la información recopilada en cuanto a las observaciones, se pudo llevar a cabo los siguientes ajustes dentro del diseño inicial:

- Se procedió a incluir los plazos, o tiempo que se demore en aplicar el procedimiento, en este caso se tiene lo siguiente: Los militares del área técnica de ESNAPE tendrán desde las 09:00 am hasta las 12:00 pm aceptará las solicitudes y validarlas. Conforme a estas solicitudes se deberá enviar por correo institucional Zimbra todo este listado para que desde las 14:00 pm hasta las 16:00 pm sean aprobadas dichas solicitudes para su posterior registro por parte del área de tecnología de DIRTIC.
- Se tendrá que incorporar un documento denominado Anexo C, el cual incluya una guía resumida para los militares solicitantes.

Como resultado de la última fase "Evaluación del nuevo procedimiento de seguridad", los resultados que se obtuvieron indicaron una alta aceptación del procedimiento de seguridad por parte del personal militar activo dentro de la Estación Naval Penitenciaria de Ecuador. La mayoría de los militares entrevistados consideraron que el nuevo modelo propuesto mejora de manera significativa el control de acceso a la red WiFi de los dispositivos, además de la seguridad, además de calificar dicho procedimiento por medio de la encuesta Likert. También, el personal militar pudo expresar su predisposición para adoptar el procedimiento de seguridad propuesto, pero siempre que existan programas de capacitaciones previas, además de que haya un soporte técnico adecuado. Dicha validación

cualitativa pudo complementar el diseño técnico y operativo del procedimiento de seguridad que se propuso, confirmando así su viabilidad y utilidad real en el contexto de un área critica como lo es la Estación Naval Penitenciaria de Ecuador.

Finalmente, dentro del Capítulo III denominado “Análisis de Resultados” dentro del presente proyecto en cuanto a la Fase 4, se pudo evidenciar la evolución de la propuesta del proyecto que se llevo a cabo, el cual abarco un diagnóstico inicial, para pasar posteriormente por un diseño detallado en cuanto al procedimiento técnico-operativo, hasta llegar a la parte final correspondiente a la viabilidad y validación por medio de retroalimentaciones de las partes involucradas, en este caso, el personal militar de la Estación Naval Penitenciaria de Ecuador “ESNAPE”.

Este procedimiento propuesto no solo tiene como objetivo regular los accesos de los dispositivos a la red WiFi del reparto naval, sino que también busca contribuir a una mejora en la cultura institucional en referencia a la seguridad de la redes, las cuales están orientadas a un área critica como lo es un reparto militar penitenciario.

3.2. Encuestas

Para complementar el Capítulo III dentro del presente trabajo de investigación, y de acuerdo a la metodología implementada se presentan las preguntas formuladas dentro de las encuestas realizadas el personal militar dentro de la ESNAPE, esto se lo hizo con el fin de evaluar no solo a percepción, sino también el conocimiento en cuanto a los accesos a la red y la seguridad en el registro de los dispositivos del personal militar activo. Se debe mencionar que las encuestas consistieron en preguntas cerradas con opciones múltiples, lo que contribuye a un análisis cuantitativo de los resultados, además de su representación en gráficos.

Cada una de las preguntas que se presentarán fueron formuladas de manera adecuada para poder obtener información que contribuya a evaluar la efectividad de los procesos vigentes dentro de la Estación Naval Penitenciaria de Ecuador. Por tal razón, los datos que fueron generados fueron utilizados para la elaboración de los gráficos, los cuales reflejaran de manera visual las tendencias pertinentes, las cuales fundamentan las decisiones metodológicas y operativas en referencia al nuevo procedimiento propuesto dentro del presente proyecto.

A continuación, se incluyen las preguntas que fueron realizadas al personal militar dentro de la ESNAPE junto con los resultados obtenidos.

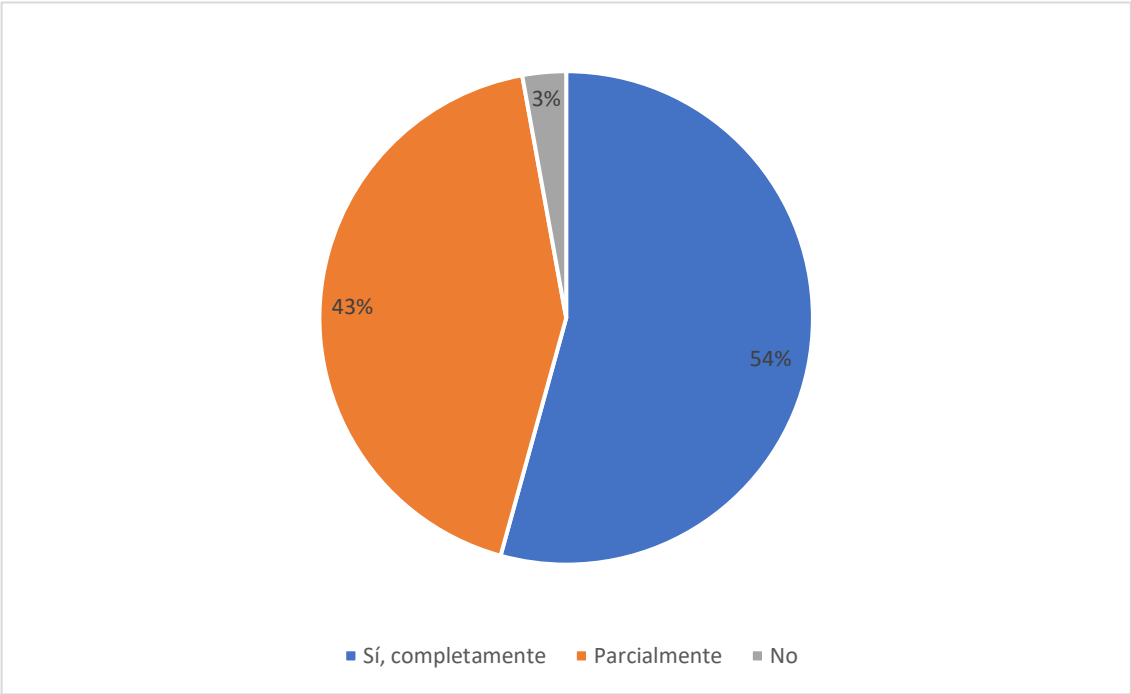
3.2.1. Preguntas de las Encuestas

Tabla 2 Pregunta 1

¿Conoce el procedimiento actual de registro de dispositivos para acceso a la red WiFi institucional?	Frecuencia	Porcentaje
Sí, completamente	19	54%
Parcialmente	15	43%
No	1	3%
Total	35	100%

Fuente: Elaboración propia (2025)

Ilustración 2 Pregunta 1



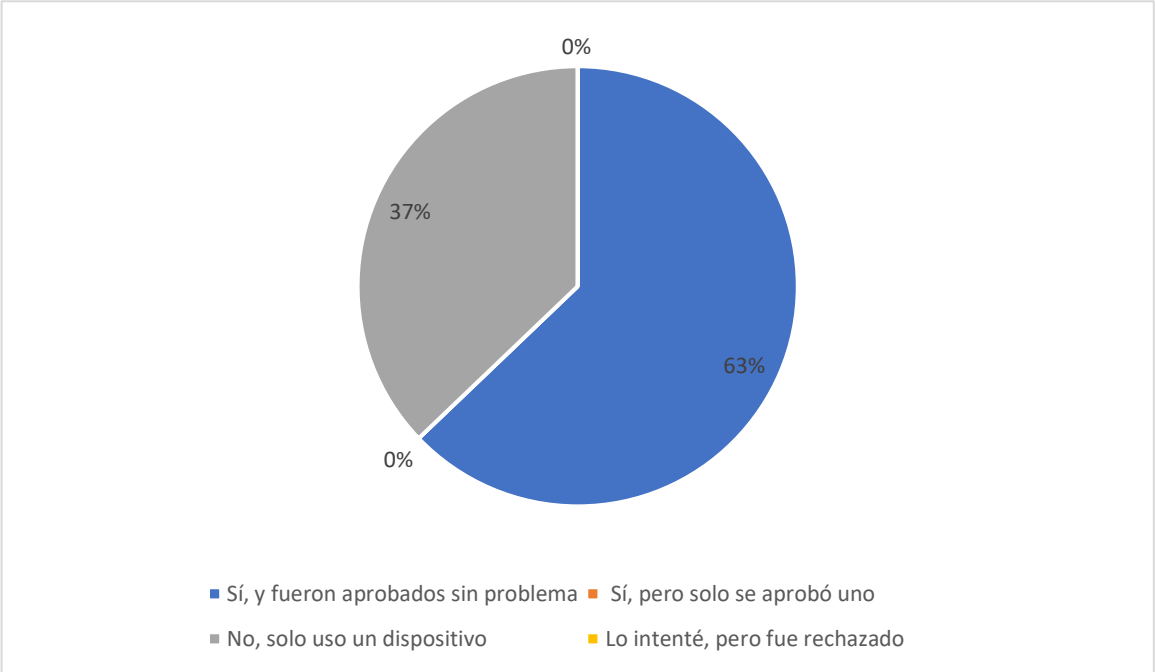
Fuente: Elaboración propia (2025)

Tabla 3 Pregunta 2

¿Ha solicitado previamente el registro de más de un dispositivo?	Frecuencia	Porcentaje
Sí, y fueron aprobados sin problema	22	63%
Sí, pero solo se aprobó uno	0	0%
No, solo uso un dispositivo	13	37%
Lo intenté, pero fue rechazado	0	0%
Total:	35	100%

Fuente: Elaboración propia (2025)

Ilustración 3 Pregunta 2



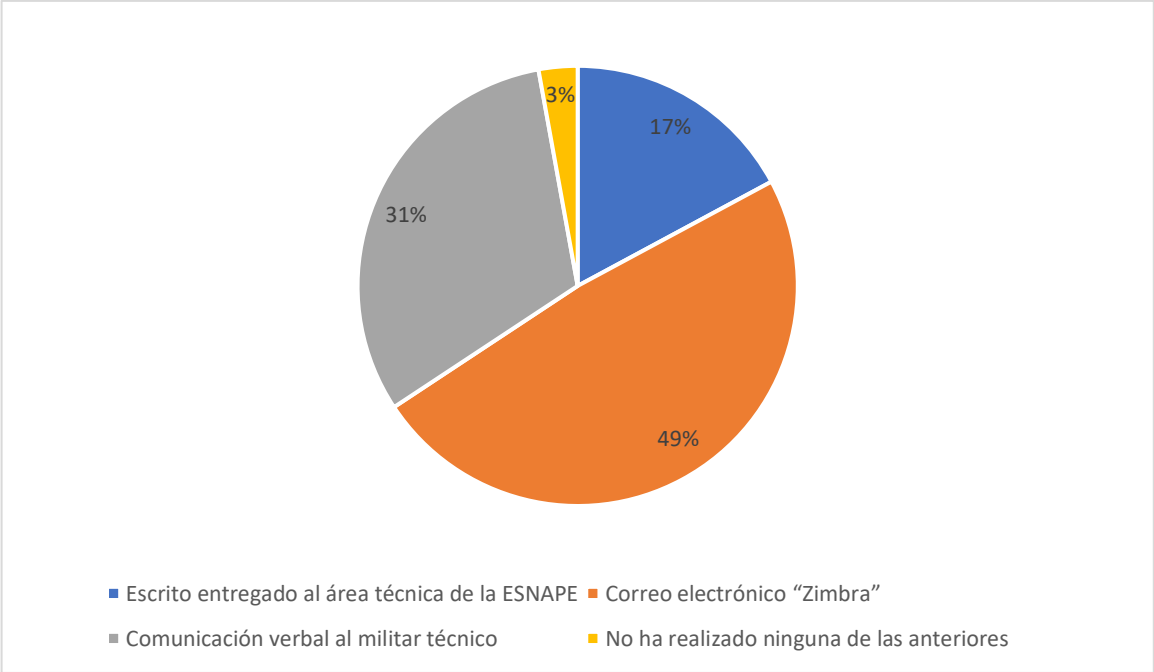
Fuente: Elaboración propia (2025)

Tabla 4 Pregunta 3

¿A través de qué medio realizó el proceso de acceso a la red WiFi de la ESNAPE?	Frecuencia	Porcentaje
Escrito entregado al área técnica de la ESNAPE	6	17%
Correo electrónico “Zimbra”	17	49%
Comunicación verbal al militar técnico	11	31%
No ha realizado ninguna de las anteriores	1	3%
Total:	35	100%

Fuente: Elaboración propia (2025)

Ilustración 4 Pregunta 3



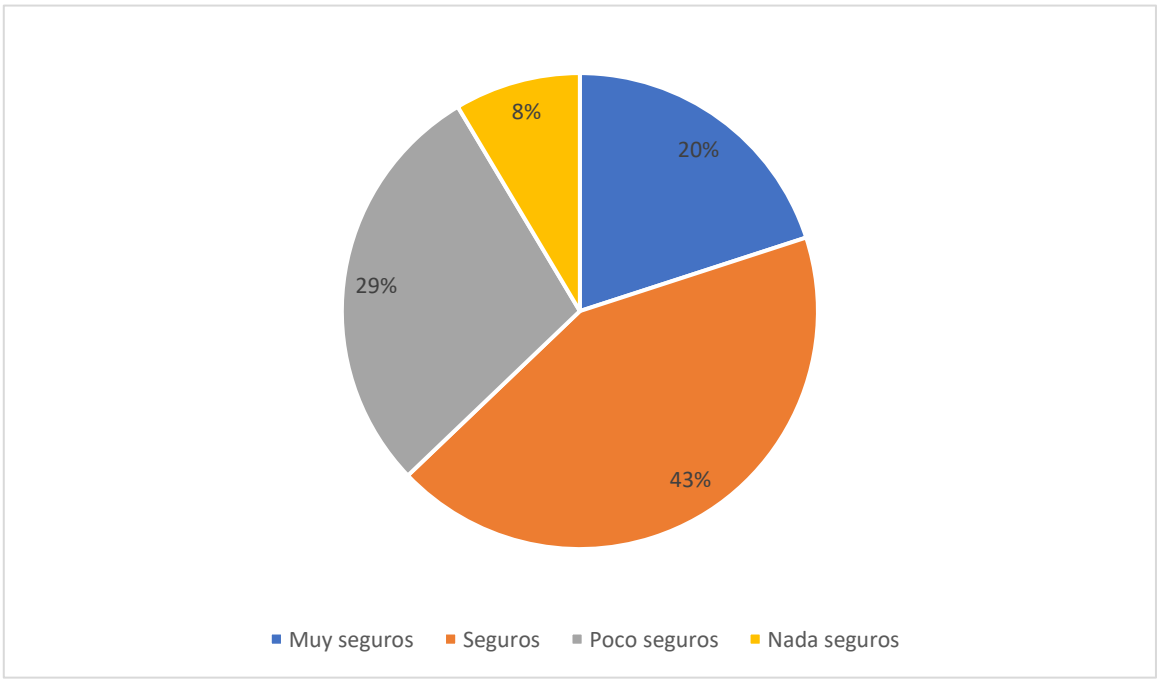
Fuente: Elaboración propia (2025)

Tabla 5 Pregunta 4

¿Considera que los medios a través de los cuales realizó su solicitud de acceso a la red son seguros?	Frecuencia	Porcentaje
Muy seguros	7	20%
Seguros	15	43%
Poco seguros	10	29%
Nada seguros	3	8%
Total:	35	100%

Fuente: Elaboración propia (2025)

Ilustración 5 Pregunta 4



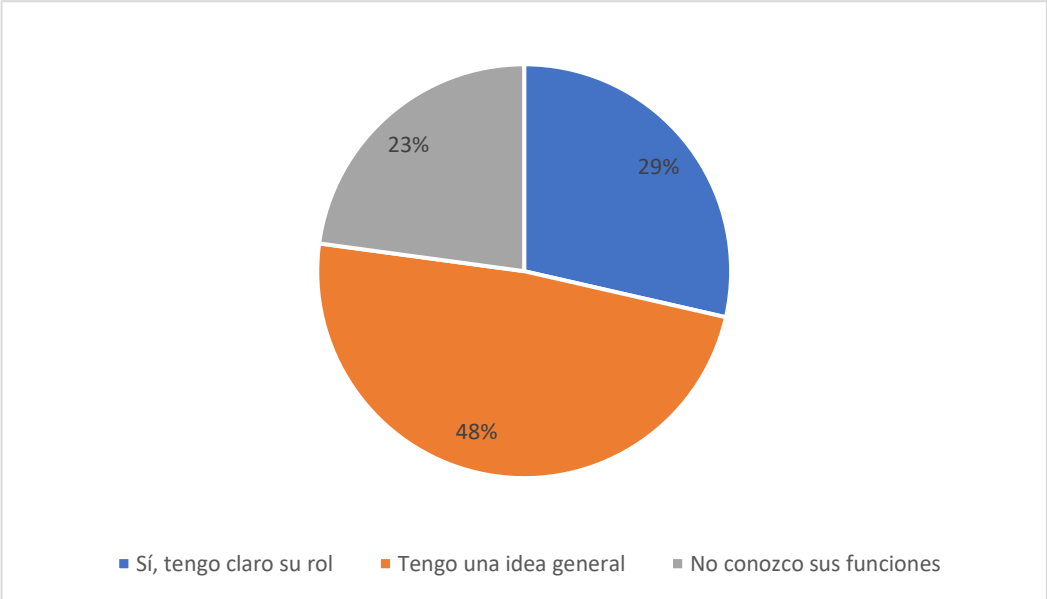
Fuente: Elaboración propia (2025)

Tabla 6 Pregunta 5

¿Conoce cuáles son las funciones específicas del personal militar técnico designado en la ESNAPE?	Frecuencia	Porcentaje
Sí, tengo claro su rol	10	29%
Tengo una idea general	17	48%
No conozco sus funciones	8	23%
Total	35	100%

Fuente: Elaboración propia (2025)

Ilustración 6 Pregunta 5



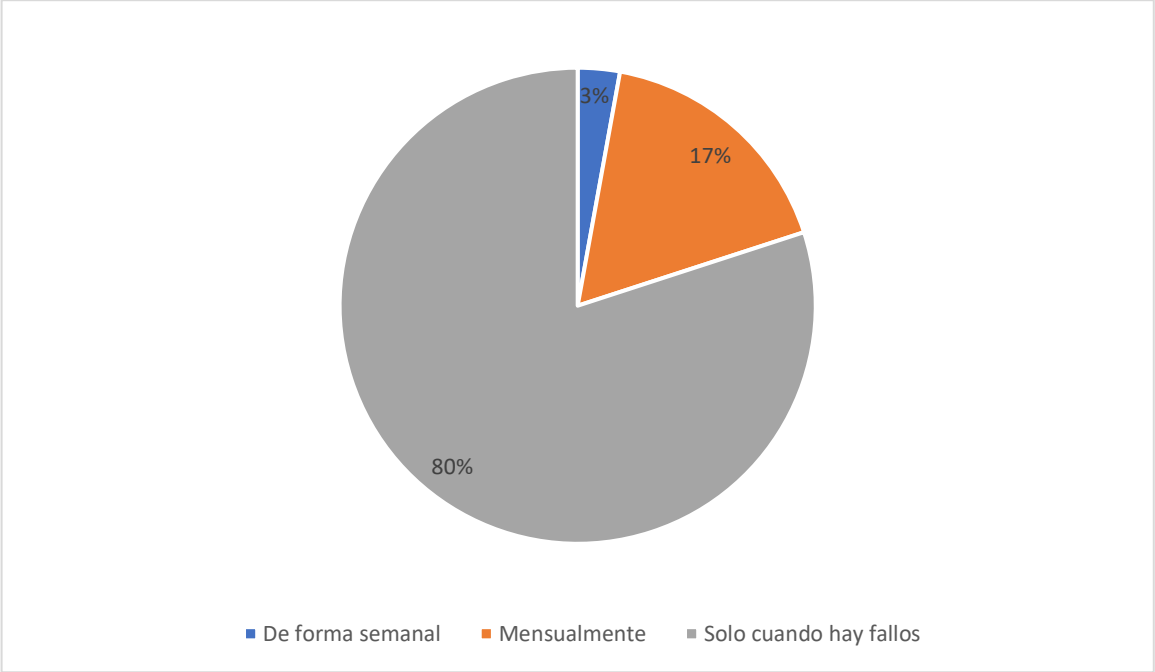
Fuente: Elaboración propia (2025)

Tabla 7 Pregunta 6

¿Con qué frecuencia el personal militar técnico informa sobre el estado de los dispositivos conectados?	Frecuencia	Porcentaje
De forma semanal	1	3%
Mensualmente	6	17%
Solo cuando hay fallos	28	80%
Total	35	100%

Fuente: Elaboración propia (2025)

Ilustración 7 Pregunta 6



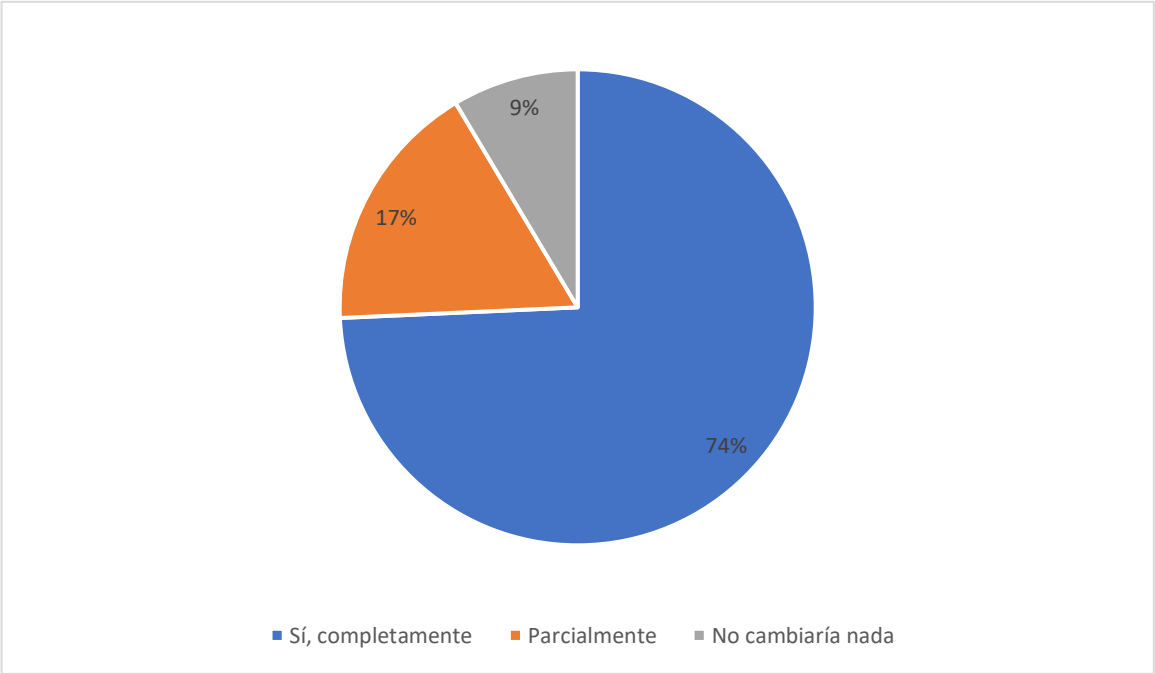
Fuente: Elaboración propia (2025)

Tabla 8 Pregunta 7

¿Cree que la implementación de un nuevo procedimiento documentado y estandarizado mejoraría el control de acceso de dispositivo a la red WiFi de la ESNAPE?	Frecuencia	Porcentaje
Sí, completamente	26	74%
Parcialmente	6	17%
No cambiaría nada	3	9%
Total	35	100%

Fuente: Elaboración propia (2025)

Ilustración 8 Pregunta 7



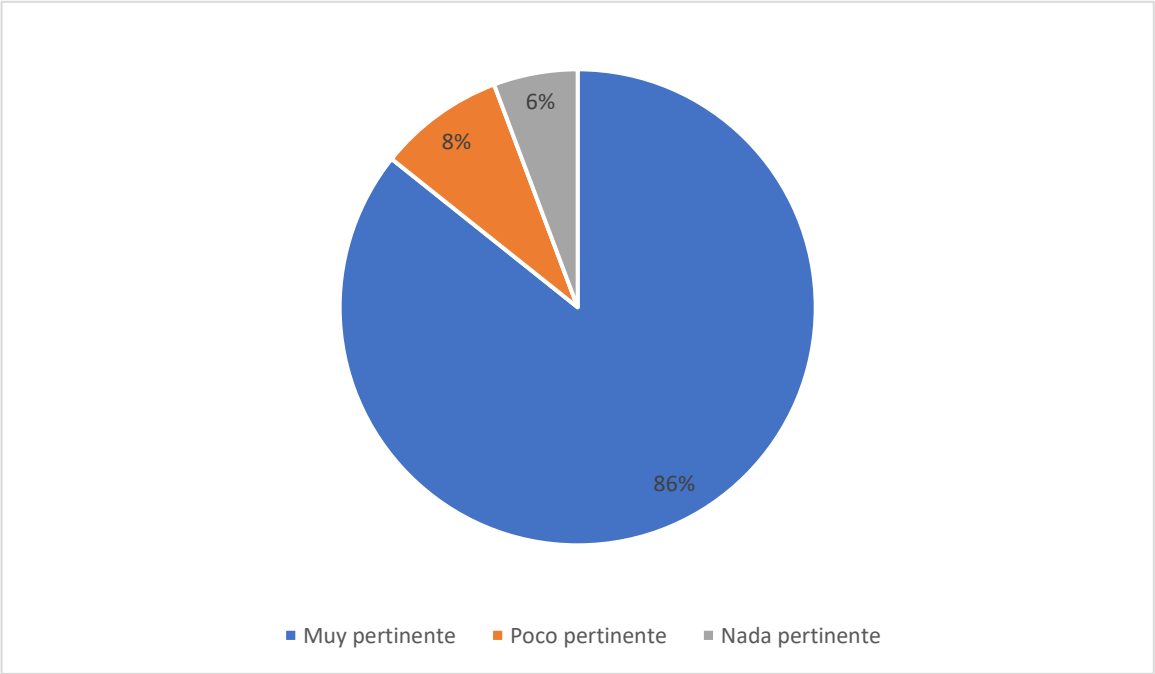
Fuente: Elaboración propia (2025)

Tabla 9 Pregunta 8

¿Considera pertinente establecer roles y responsabilidades claros para el personal técnico de la ESNAPE y de la DIRTIC encargados del registro de dispositivos de los usuarios?	Frecuencia	Porcentaje
Muy pertinente	30	86%
Poco pertinente	3	8%
Nada pertinente	2	6%
Total	35	100%

Fuente: Elaboración propia (2025)

Ilustración 9 Pregunta 8



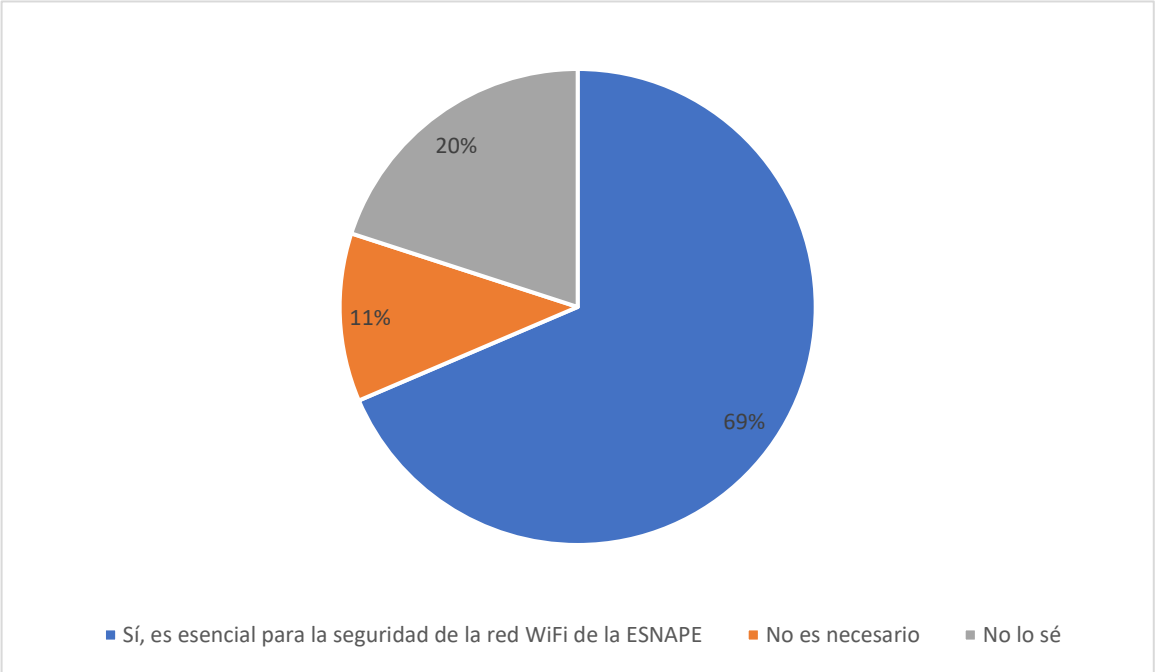
Fuente: Elaboración propia (2025)

Tabla 10 Pregunta 9

¿Considera importante que cada dispositivo de los militares dentro de la ESNAPE sea asociado a una IP y MAC Address?	Frecuencia	Porcentaje
Sí, es esencial para la seguridad de la red WiFi de la ESNAPE	24	69%
No es necesario	4	11%
No lo sé	7	20%
Total	35	100%

Fuente: Elaboración propia (2025)

Ilustración 10 Pregunta 9



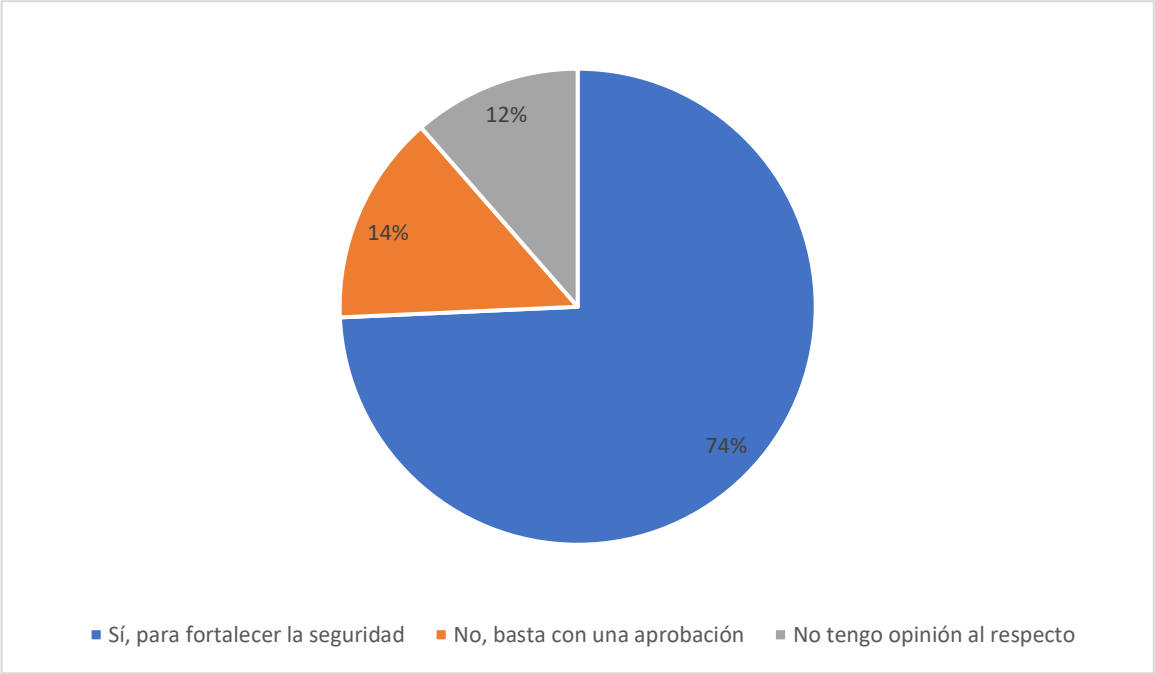
Fuente: Elaboración propia (2025)

Tabla 11 Pregunta 10

¿Cree que el nuevo procedimiento debería incluir fases de validación y doble autorización?	Frecuencia	Porcentaje
Sí, para fortalecer la seguridad	26	74%
No, basta con una aprobación	5	14%
No tengo opinión al respecto	4	12%
Total	35	100%

Fuente: Elaboración propia (2025)

Ilustración 11 Pregunta 10



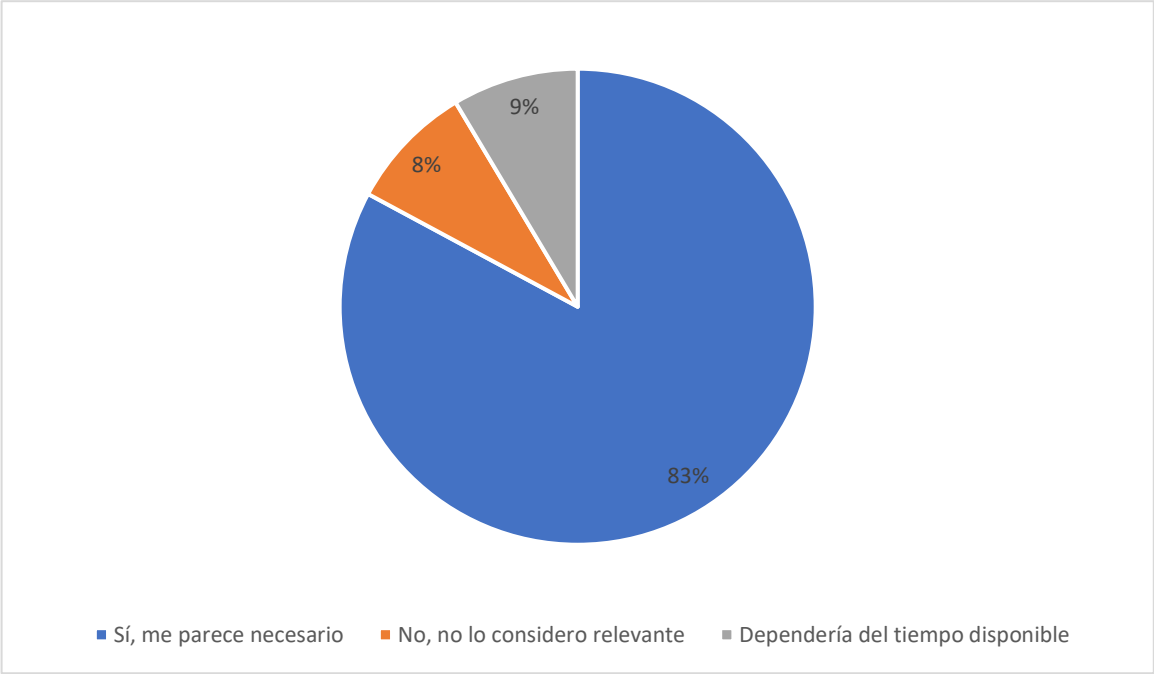
Fuente: Elaboración propia (2025)

Tabla 12 Pregunta 11

¿Estaría dispuesto a capacitarse sobre el uso del nuevo procedimiento de seguridad de red?	Frecuencia	Porcentaje
Sí, me parece necesario	29	83%
No, no lo considero relevante	3	8%
Dependería del tiempo disponible	3	9%
Total	35	100%

Fuente: Elaboración propia (2025)

Ilustración 12 Pregunta 11



Fuente: Elaboración propia (2025)

3.3. Datos de Cada Pregunta

Pregunta 1: ¿Conoce el procedimiento actual de registro de dispositivos para acceso a la red WiFi institucional?

La mayoría de los militares dentro de la ESNAPE que conforman la población de la investigación indicaron conocer parcialmente el procedimiento vigente dentro del reparto militar, un 43% para ser exacto, lo cual pone en evidencia una brecha en la socialización de los protocolos técnicos en la Estación Naval Penitenciaria de Ecuador. Aunque un número relevante, el 54% afirma conocerlo completamente, pero, aun así, la paridad con quienes no lo conocen demuestra una falta de comunicación institucional sen cuanto a los procesos formales.

Pregunta 2: ¿Ha solicitado previamente el registro de más de un dispositivo?

El resultado obtenido dentro de la pregunta 2 es que el 63% del personal militar ha obtenido la aprobación de registros a múltiples dispositivos, lo que demuestra que existe cierta flexibilidad en referencia a dicho registro dentro de la ESNAPE.

Este resultado refuerza la necesidad imperiosa de definir de manera clara las políticas en cuanto a la cantidad de dispositivos permitidos por cada uno de los miembros uniformados del reparto militar ESNAPE dentro del nuevo procedimiento de seguridad.

Pregunta 3: ¿A través de qué medio realizó el proceso de acceso a la red WiFi de la ESNAPE?

Se pudo constatar que el medio más usado para solicitar el acceso a la red de la Estación Naval Penitenciaria de Ecuador fue por medio de correo electrónico (Zimbra), con una cifra del 49%. Sin embargo, lo que se destacó notablemente es la cantidad significativa del personal militar que ha recurrido no solo a la comunicación verbal, sino también a no realizar alguna solicitud para el acceso a la red del reparto militar ESNAPE. Esto demuestra que existe un vacío en cuanto a la estandarización de los canales o medios para solicitar el acceso a la red WiFi dentro del reparto.

Pregunta 4: ¿Considera que los medios a través de los cuales realizó su solicitud de acceso a la red son seguros?

Los resultados que se obtuvieron dentro de la encuesta realizada, específicamente en la pregunta 4, validan esa necesidad de no solo estandarizar, sino también reforzar el sistema por el cual se solicite el acceso a la red del reparto militar ESNAPE, además de la

incorporación de herramientas formales como es el caso de la documental y también de un registro robusto. Que exista un 37% en cuanto a la percepción negativa del personal militar en referencia al proceso vigente dentro de la ESNAPE confirma que dicho proceso era vulnerable, además de carecer de legitimidad operativa.

Por ello mismo se debe realizar la implementación de un nuevo procedimiento que sea seguro, para esto debe haber un flujo con su respectiva validación, además de delimitar los roles y responsabilidades del personal militar técnico, para buscar revertir la percepción por parte de los uniformados, además de fortalecer la seguridad y confianza dentro de la ESNAPE en cuanto a sus procedimientos.

Pregunta 5: ¿Conoce cuáles son las funciones específicas del personal militar técnico designado en la ESNAPE?

Un grupo considerable del personal militar encuestado perteneciente al universo de la muestra supo manifestar por medio de los resultados obtenidos que hay un 48% de militares que conocen de manera general las funciones que realiza el personal militar técnico. Dicho resultado demuestra la pertinencia y necesidad de detallar los roles y responsabilidades de este mismo personal técnico militar, tal y como se lo propone dentro del segundo objetivo específico dentro de la presente investigación.

Cabe destacar que toda esta falta de definición podría comprometer no solo la trazabilidad de roles y responsabilidades, sino también la eficiencia operativa dentro de la Estación Naval Penitenciaria de Ecuador.

Pregunta 6: ¿Con qué frecuencia el personal militar técnico informa sobre el estado de los dispositivos conectados?

La mayor parte del personal militar encuestado respondió con un 80% que reciben información por parte del equipo militar técnico solo cuando se presenta un fallo. Este resultado demuestra una falta de monitoreo continuo y proactivo.

La falta de un monitoreo constante puede comprometer no solo la estabilidad, sino también la seguridad de la red dentro de la Estación Naval Penitenciaria de Ecuador “ESNAPE”, por tal razón se demuestra la imperiosa necesidad y pertinencia de implementar medidas de auditoras como lo son informes periódicos como parte del nuevo procedimiento de seguridad propuesto en el presente proyecto.

Pregunta 7: ¿ Cree que la implementación de un nuevo procedimiento documentado y estandarizado mejoraría el control de acceso de dispositivo a la red WiFi de la ESNAPE?

La propuesta establecida dentro del presente proyecto en referencia a un nuevo procedimiento de seguridad para la red WiFi de la ESNAPE recibe un amplio respaldo, con un 74% por parte del personal uniformado dentro del reparto militar. Este resultado demuestra que, si existe una predisposición por parte del personal dentro de la Estación Naval Penitenciaria de Ecuador para mejorar los protocolos vigentes, además de que este mismo personal militar estaría de acuerdo con adaptarse a los cambios estructurados, siempre y cuando se garantice una mayor seguridad.

Pregunta 8: ¿Considera pertinente establecer roles y responsabilidades claros para el personal técnico de la ESNAPE y de la DIRTIC para que sean los encargados del registro de dispositivos de los usuarios?

Una cantidad del 86% del personal militar encuestado considera que es muy pertinente establecer de manera clara tanto los roles como las responsabilidades del personal militar técnico, esto demuestra una amplia coincidencia en cuanto a las necesidades de estructurar de manera formal las funciones técnicas dentro de la gestión de la red WiFi de la Estación Naval Penitenciaria de Ecuador.

Cabe destacar que el resultado obtenido demuestra la relevancia y pertinencia del análisis funcional realizando dentro de las fases anteriores en el presente proyecto. Además, el amplio respaldo a esta propuesta refuerza la implementación de flujos de trabajo, los cueles estén formalizados, con asignaciones claras y especificas en cuanto a los roles y responsabilidades, también los tiempos de respuesta y el manejo documental, tal y como se lo propone dentro del desarrollo de un procedimiento operativo más seguro para la red WiFi de la Estación Naval Penitenciaria de Ecuador “ESNAPE”.

Pregunta 9: ¿Considera importante que cada dispositivo de los militares dentro de la ESNAPE sea asociado a una IP y MAC Address??

El resultado obtenido dentro de esta pregunta demuestra un número considerable de militares, con un 69% que considera fundamental un registro de los dispositivos por medio del proceso asociación de IP/MAC Address.

Aquí se puede constatar una conciencia en referencia a la importancia del control de los dispositivos a los accesos a la red del reparto militar ESNAPE. Este resultado también

demuestra que un gran número de militares aprecian la seguridad digital, además de que dicho resultado respalda la implementación de un nuevo procedimiento de seguridad, el cual debe ser más estricto.

Pregunta 10: ¿Cree que el nuevo procedimiento debería incluir fases de validación y doble autorización?

Dentro del resultado que se pudo obtener se puede constatar que un 74% del personal militar encuestado respaldó la implementación de un proceso de doble validación. Además de esto, dicho resultado se puede interpretar como que existe una preocupación en torno a la seguridad operativa dentro de la Estación Naval Penitenciaria de Ecuador “ESNAPE”.

El resultado obtenido da como respuesta el fortalecimiento del diseño de un procedimiento el cual esté basado en doble capa de autorización, tal y como se lo ha venido planteando en el presente proyecto. Para ello fue indispensable conocer los roles y responsabilidades del personal militar técnico dentro de la ESNAPE, además de la colaboración de la DIRTIC para poder llevar a cabo esta doble autorización por medio del proceso de IP/MAC Address.

Pregunta 11: ¿Estaría dispuesto a capacitarse sobre el uso del nuevo procedimiento de seguridad de red?

Dentro de los resultados de esta pregunta se obtuvo una amplia respuesta positiva con un 83%, esto demuestra el interés por parte del personal militar por adaptarse a nuevos procesos que no solo mejoren la seguridad, sino también el control.

Dicha aceptación es fundamental tanto para la evaluación como la aplicación de manera efectiva del nuevo procedimiento de seguridad para la red WiFi de la Estación Naval Penitenciaria de Ecuador. Además de revelar una cultura institucional favorable en torno a un aprendizaje técnico-operativo.

3.4. Interpretación de los Resultados de las Encuestas

Objetivo 1: Analizar la topología de la red WiFi de la Estación Naval Penitenciaria de Ecuador (ESNAPE).

Los resultados obtenidos por medio de las encuestas revelan que, aunque el personal técnico y operativo dentro de la ESNAPE tiene un conocimiento parcial en referencia al procedimiento de conexión a la red, existe una evidente necesidad de mejorar la comprensión tanto en su estructura como en su funcionamiento. La mayoría del personal militar activo

encuestado manifestaron tener solo un entendimiento general de cómo se lleva a cabo el registro de dispositivos, lo que sin lugar a dudas, evidencia la insuficiencia de los actuales mecanismos de capacitación o divulgación interna sobre la topología de red. Bajo este contexto, fue fundamental practicar el método de observación directa, además de contar con un recurso visual especifico, como lo fue el mapa de red proporcionado por el equipo técnico de la Estación Naval Penitenciaria de Ecuador, lo que a su vez permitió analizar de manera detallada la arquitectura de la red interna de este reparto militar. Cabe mencionar que esta topología muestra cómo están conectados los dispositivos, al igual que la ubicación de los puntos de acceso y tambien la asignación lógica en cuanto a las direcciones IP, los cuales son aspectos imprescindibles para comprender el entorno operativo en el cual se desarrolla el presente proyecto y su propuesta de procedimiento de seguridad.

Por lo presentado anteriormente, es que este análisis previo no solo fue útil, pertinente y conducente sino tambien crucial, esto es debido a que permite aterrizar técnicamente la propuesta, adaptándola así a la realidad del reparto militar ESNAPE sin la necesidad de solicitar o contar con un presupuesto, lo cual resultaba inviable.

Objetivo 2: Identificar los roles y responsabilidades del personal militar técnico encargados de la gestión del acceso a la red, registro y monitoreo de dispositivos.

Los hallazgos que se obtuvieron por medio de las encuestas realizadas reflejaron una desconexión entre lo que el personal militar percibe como el procedimiento de registro y lo que realmente ejecuta el personal militar técnico. Si bien es cierto que existe conciencia de que debe haber una trazabilidad en el acceso, se debe mencionar que la ejecución de estos procesos no ha sido uniforme. Algunos de los militares indicaron que su solicitud para que sus dispositivos cuenten con acceso a la red del reparto fue realizada por medios informales, como es el caso de la comunicación verbal, lo que a su vez implica una falta de sistematización.

Todos estos resultados demuestran la necesidad de delimitar y especificar de manera clara los roles y responsabilidades del personal militar técnico, estableciendo así aquellas responsabilidades específicas como es el caso de la recepción y verificación del documento de solicitud por parte de los usuarios para su aceptación o denegación, la verificación de MAC Address y su posterior registro desde la ESNAPE y DIRTIC, asociación de la IP/MAC al usuario solicitante desde la ESNAPE, Consulta de los usuarios ingresados, continuando con la Liberación de los usuarios inactivos y el Monitoreo continuo por medio de la Controladora WiFi.

3.5. Entrevista

Entrevista Con el Oficial de Seguridad de la Información (OSI)

Duración Estimada: 30 minutos

Sección 1: Estado actual y necesidades de la red dentro del reparto militar

Entrevistador: Desde su experiencia como encargado técnico, ¿cómo describiría la situación actual de la red WiFi dentro de la ESNAPE?

OSI: En términos generales, la red dentro de este reparto funciona con estabilidad. Considerando que la ESNAPE es un nuevo reparto militar que se concibió debido a la declaratoria de CONFLICTO ARMADO INTERNO emitido el 9 de enero del 2024 por medio del decreto No. 111, en donde se establece que las Fuerzas Armadas deben tomar el control dentro de las cárceles, por tal razón para cumplir con esta orden, la Armada del Ecuador, por medio del oficio No. OF-ARE-ESMAAR-LOG-2024-0019-R, se dispuso la creación de un nuevo reparto naval el cual opere dentro de las instalaciones del complejo penitenciario en Guayaquil, el cual fue denominado Estación Naval Penitenciaria de Ecuador “ESNAPE”.

Sin embargo, no contamos aún con protocolos formales de autorización e incluso muchos de los registros de acceso se hacen manualmente.

Entrevistador: ¿Considera que el diseño actual de la red cumple con los estándares de seguridad adecuados?

OSI: Diría que parcialmente, ya que la ejecución de este proyecto se enfocó en el desarrollo de una red WiFi optimizada para entornos críticos como lo es una instalación penitenciaria, estableciendo estándares y protocolos de seguridad los cuales estuvieran adaptados a las necesidades del personal militar en funciones. Con esto quiero decir que la estructura fue pensada en la cobertura como tal, pero no necesariamente para seguridad avanzada. Ha habido casos donde se ha detectado vulnerabilidades relacionadas con accesos no registrados y dispositivos personales sin control adecuado.

Sección 2: Gestión y control de los accesos de dispositivos a la red WiFi del reparto naval “ESNAPE”

Entrevistador: ¿Qué procesos siguen actualmente para registrar o autorizar dispositivos en la red interna?

OSI: En la práctica, cuando un usuario ya sea un tripulante u oficial desea conectarse a la red, debe solicitar la asistencia de un miembro del personal técnico que se encuentre disponible. Este militar técnico se hace responsable de registrar el dispositivo dentro del firewall de la Armada.

Entrevistador: ¿Qué actores están involucrados en la gestión operativa de la red?

OSI: Somos tres técnicos que compartimos funciones, dos tripulantes y un oficial. Cualquiera de los compañeros tripulantes puede hacerse responsable de registrar el dispositivo del militar solicitante y posteriormente registrarlo y el oficial es quien se encarga de asegurarse que el proceso se lleve a cabo de forma eficiente. Sin embargo, esta distribución no está documentada formalmente.

Sección 3: Percepción del nuevo procedimiento propuesto

Entrevistador: ¿Qué opinión tiene sobre la propuesta de un procedimiento de seguridad más estructurado?

OSI: Nos parece una muy buena iniciativa. Es más, ya hemos discutido que una metodología más completa ayudaría a evitar duplicidades al igual que errores de registro lo que permitiría una mejor auditoría en caso de incidentes. Si el procedimiento fuera con base documental, sería perfecto.

Sección 4: Retos y viabilidad de implementación

Entrevistador: ¿Cuáles considera que serían los principales desafíos para implementar este procedimiento?

OSI: Considero que el reto más complejo sería lograr que el procedimiento que se propone quede verdaderamente establecido y claro dentro de la operatividad de la Estación Naval Penitenciaria de Ecuador. Debido a la rotación constante del personal militar, este cambio se da cada dos meses, siendo esta una orden directa de los altos mandos debido a la naturaleza critica del reparto, por eso es fundamental que cada nuevo militar conozca al detalle el procedimiento actualizado, además de que lo aplique con rigurosidad. Sin duda esto implicaría no solo capacitar de forma continua, sino también asegurar que existan mecanismos de seguimiento, además de documentación que permitan mantener tanto la trazabilidad como la coherencia operativa, y esto debe ser independiente del relevo de personal militar.

Entrevistador: ¿Considera viable aplicar este procedimiento en otros repartos de la Armada del Ecuador?

OSI: Considero que podría ser replicable. Siempre y cuando se adapte a la infraestructura de cada uno de los repartos navales, es una propuesta realista y útil.

3.5.1. Interpretación de los Resultados de la Entrevista

Los datos que fueron obtenidos por medio de esta entrevista con el Oficial de Seguridad de la Información (OSI) revelan aspectos fundamentales no solo para validar la necesidad, sino también la aplicabilidad del procedimiento propuesto en el presente proyecto.

En primer lugar, se confirma que, si bien la red cuenta con estabilidad funcional, su estructura carece de mecanismos formales de control, además de un correcto sistema de registros aumentan el riesgo de casos de accesos no autorizados.

En cuanto a la percepción a nivel operativo, se puede demostrar una apertura clara en cuanto a la implementación de un procedimiento seguro y estructurado, el cual ordene las responsabilidades, además de que permita el registro y monitoreo de accesos, lo cual se lo puede llevar a cabo conociendo la segmentación lógica de la red y también con el uso de herramientas para el registro y validación de dispositivos con los recursos actuales de la Estación Naval Penitenciaria de Ecuador “ESNAPE”.

Finalmente, se pudieron identificar ciertos desafíos como es el caso de la capacitación y la implementación de herramientas básicas, pero dichos desafíos no representan barreras insuperables. Esta entrevista refuerza la viabilidad del procedimiento propuesto dentro del presente proyecto, además de respaldar su replicabilidad en otros repartos navales, evidentemente, esto debe ser siempre que se adapten a las condiciones técnicas de estos repartos.

Con lo presentado anteriormente, se puede decir que estos hallazgos ratifican una vez más la pertinencia del diseño elaborado de un procedimiento más seguro, además de que se sugiere un alto nivel de aceptación institucional en referencia a su futura implementación.

CAPÌTULO IV

PROPUESTA

CAPÍTULO IV

PLAN ESTRATÉGICO OPERATIVO-TECNOLÓGICO

4.1. Propuesta del Procedimiento de Seguridad de la Red WiFi para la Estación Naval Penitenciaria de Ecuador “ESNAPE”

4.1.1.- Descripción de la Propuesta

Dentro del presente capítulo el cual hace referencia a la propuesta del proyecto, se presenta dicha propuesta formal en cuanto al procedimiento de seguridad estructurado tanto de gestión de acceso como de control de la red inalámbrica dentro del reparto militar denominado Estación Naval Penitenciaria (ESNAPE), el cual forma parte de un plan estratégico de seguridad tecnológica para una de las instituciones públicas más críticas del país como lo es la Armada del Ecuador dentro de su reparto ESNAPE. Cabe destacar que, a diferencia de iniciativas más genéricas en otras instituciones o contextos, la presente propuesta está netamente enfocada en el entorno militar de Ecuador, donde no solo la disponibilidad, sino también la integridad y la confidencialidad de la información representan pilares importantes para la operatividad diaria de este reparto militar en donde se desarrolla el presente proyecto. Y, contando con la base al diagnóstico previo realizado en fases anteriores como lo fue mediante encuestas, entrevistas, observación directa y análisis documental, se pudieron identificar algunas debilidades en referencia al control de dispositivos conectados, además de la ausencia de trazabilidad, procesos manuales poco eficientes y también la inexistencia de un protocolo formalizado.

Ahora, esta propuesta tiene como objetivo desarrollar un procedimiento de seguridad a nivel operativo, el cual se encargue de regular el acceso a la red WiFi de la Estación Naval Penitenciaria de Ecuador “ESNAPE”, por medio de no solo la verificación, sino también la validación y autorización de los dispositivos requirentes del personal militar designado a realizar funciones dentro del reparto naval. La presente propuesta como tal surge debido a los riesgos de seguridad latentes en cuanto a los accesos no autorizados de dispositivos, esto es debido a que dichos accesos no controlados pueden comprometer no solo la integridad, sino también la confidencialidad y la disponibilidad de los recursos de la red WiFi de la ESNAPE.

En referencia a la propuesta, esta se centra en la definición clara en cuanto a los roles y responsabilidades dentro del reparto naval, también de la implementación de controles tanto operativos como administrativos, además del uso eficiente de las herramientas existentes dentro de la infraestructura tecnología de la Estación Naval Penitenciaria de Ecuador. Con

esto se procurará que solamente los dispositivos que ya hayan sido previamente autorizados, además de que hayan sido debidamente registrados tengan acceso a la red WiFi de la ESNAPE, lo que a su vez contribuiría a reforzar no solo el principio de mínima exposición, sino también la trazabilidad de eventos, además de la transparencia del procedimiento. Entonces, para poder lograrlo se ha desarrollado un procedimiento estructurado, el cual inicia por medio de una solicitud formal para requerir el acceso a internet por parte del personal militar asignado al reparto naval, esto continua con el proceso de revisión y validación técnica de los dispositivos por parte de los militares técnicos de la ESNAPE, además de el registro de los dispositivos solicitantes dentro del Firewall de la Armada. Y para complementarlo, se propone el uso de los sistemas de monitoreo existentes dentro de la ESNAPE, tal es el caso de la Controladora Cloud Key Gen2, por medio de la cual se puede realizar un monitoreo contante de los dispositivos conectados dentro de la red, incluido los switches y los AP, además de los dispositivos que están en lineo o apagados y sobre todo la IP, y el nombre a quien le pertenece, esto es para realizar reportes semanales y mensuales en referencia a la conectividad, lo que permite contar con un control activo del estado de la red WiFi de la ESNAPE.

Cabe destacar que, la propuesta del presente proyecto reconoce el uso de las herramientas existentes dentro de la ESNAPE como es el caso del Firewall Fortinet modelo FG-70F y también la Controladora Cloud Key Gen2 de marca UBIQUITI, sin embargo, el enfoque central de este proyecto es dentro del ámbito operativo, esto quiere decir que, se prioriza el desarrollo del diseño del procedimiento, además de las responsabilidades de las partes involucradas y también la gestión documental la cual respalde cada acción dentro del procedimiento. No obstante, el conocimiento técnico de las herramientas antes mencionadas pertenecientes a los esquemas actuales de la Estación Naval Penitenciaria de Ecuador es importantes como contexto, sin embargo, no constituyen el eje central de la presente propuesta de este proyecto.

Es por todas estas razones que la presente propuesta tiene como objetivo principal estandarizar el acceso a la red WiFi del reparto militar ESNAPE, asegurando así que cada dispositivo ya sea personal o institucional esté previamente autorizado, además de monitoreado y adecuadamente registrado, sin comprometer tanto la funcionalidad como la seguridad de los sistemas institucionales.

4.2. Introducción

Dentro de los entornos de seguridad institucional, en especial, dentro de áreas criticas como un reparto militar, específicamente la Estación Naval Penitenciaria de Ecuador, los accesos no autorizados a las redes WiFi representan una amenaza importante. Entonces, la

necesidad, pertinencia y conducencia de diseñar el presente procedimiento estructurado se dio debido a los casos recurrentes de inconsistencias detectadas en la gestión de usuarios y dispositivos conectados a la red WiFi de la Estación Naval Penitenciaria de Ecuador “ESNAPE”. Durante el proceso se pudo observar que, aunque existía infraestructura ya instalada, la cual constaba de Access Points Ubiquiti, Firewall Fortinet, Controladora Cloud Key Gen2, su utilización como tal no respondía a criterios estandarizados en cuanto a control, y mucho menos a un procedimiento de seguridad de red WiFi que sea sostenible, esto quiere decir que la ausencia de un procedimiento operativo formal enfocado al control de acceso de los dispositivos a la red WiFi de la ESNAPE no solo limita la capacidad de este reparto en cuanto a la respuesta ante posibles incidentes, sino también genera riesgos, tal es el caso de la exposición de su información, además de dificultar tanto la supervisión tecnológica como su auditoria.

Bajo este contexto, la falta de una documentación clara no solo en referencia a los roles, sino también en los permisos, registro de dispositivos y monitoreo de tráfico originaba vulnerabilidades, las cuales podían dar como resultados casos de accesos no autorizados, consumo no regulado del ancho de banda institucional, además de `posibles riesgos para la confidencialidad de la información dentro del reparto naval. También se pudo detectar una ausencia de procesos formales en referencia a dar de baja a dispositivos sin actividad o que pertenecían al personal militar saliente, provocando así una saturación del conjunto de direcciones IP’s.

Con todo lo presentado anteriormente es que surgió esa motivación para el desarrollo de un procedimiento el cual pueda articular las capacidades técnicas existentes dentro del reparto militar ESNAPE, además de los lineamientos operativos claros, también las responsabilidades definidas y mecanismos de supervisión efectivos. Por lo que la propuesta se enfoca en la transformación de un sistema funcional, pero fragmentado, dentro de un entorno tanto controlado como trazable y resiliente. Esto quiere decir que la propuesta dentro del presente proyecto surge como una alternativa operativa con el fin de enfrentar dicha problemática, y a su vez, brindar un mecanismo no solo ordenado, sino también seguro y auditable, el cual permita controlar que solamente los dispositivos debidamente autorizados, verificados y también registrados puedan acceder a la red WiFi de la ESNAPE. Cabe destacar que, al establecer no solamente controles claros, sino también documentos se puede fortalecer tanto la gobernanza tecnológica dentro del reparto naval, al igual que se puede promover una cultura de responsabilidad entre aquel personal uniformado que cumple funciones dentro de la ESNAPE.

Finalmente, la estructura del presente procedimiento diseñado en el proyecto incluye:

1.- Ingreso de solicitud por parte del personal uniformado entrante por medio de documentación del Anexo A.

2.- Verificación de la información por medio de una revisión técnica por parte del equipo de tecnología de la ESNAPE, verificando que los datos del dispositivo correspondan, el número de dispositivos del usuario y que no exista duplicidad.

3.- Validación institucional de la información por parte del Oficial de TICS de la ESNAPE para su aceptación o rechazo.

4.- Remisión dirigida a DIRTIC en donde se incluya los Anexos A y B por medio de correo institucional (Zimbra).

5.- Configuraciones técnicas de los dispositivos por medio de:

- Registro del dispositivo por la MAC y asignación por IP dentro del Firewall Fortinet modelo FG-70F.
- Monitoreo de los dispositivos por medio de la Controladora (Cloud Key Gen2).

6.- La activación del acceso por parte del militar técnico de la ESNAPE según el procedimiento operativo y liberación de usuarios inactivos.

7.- Monitoreo y posterior auditoría por el Oficial de Seguridad Informática (OSI) de la DIRTIC a la ESMAAR.

Todo este procedimiento antes mencionado está diseñado con el propósito de ser aplicable, además de replicable dentro de otros repartos navales y también medible. Por lo tanto, el presente proyecto no solo tiene como finalidad resolver la necesidad operativa exacta dentro de la Estación Naval Penitenciaria de Ecuador, sino también establecerse como base para posteriores mejoras dentro del ámbito de la seguridad en la red WiFi del reparto naval, centrándose en el marco de las políticas vigentes dentro de la Armada del Ecuador.

4.3. Definición de Objetivos

4.3.1.- Objetivo General de la Propuesta

El objetivo de la propuesta dentro del presente proyecto es:

Establecer un procedimiento operativo estandarizado que permita verificar, validar, registrar y también monitorear los dispositivos conectados a la red Wifi de la Estación Naval Penitenciaria de Ecuador “ESNAPE”, por medio del aprovechamiento de la infraestructura

tecnológica ya implementada y existente dentro de este reparto militar, asegurando la trazabilidad, control y complimiento de las funciones internas.

4.3.2.- Objetivos Específicos de la Propuesta

- Analizar el estado actual de la red WiFi de la Estación Naval Penitenciaria de Ecuador, identificando las debilidades operativas con el control de acceso a su red.
- Diagnosticar las políticas, procesos y partes involucradas en la gestión del acceso a la red WiFi, con énfasis en el ámbito y funcionamiento operativo, sin profundizar el apartado técnico, con el fin de establecer una base de conocimiento del reparto naval.
- Establecer los lineamientos, roles, responsabilidades y componentes claros para diseñar un procedimiento operativo seguro y efectivo, contemplando las buenas prácticas en la gestión de accesos, adaptándose a las capacidades y estructura jerárquica para asegurar la asegure la trazabilidad en la Estación Naval Penitenciaria de Ecuador.
- Desarrollar la propuesta del procedimiento de seguridad operativo para regular el acceso a la red WiFi de la Estación Naval Penitenciaria de Ecuador, por medio de la validación en simulaciones dentro de un entorno controlado.
- Recolectar retroalimentaciones del personal militar sobre la propuesta desarrollada, identificando las observaciones y verificar la viabilidad del procedimiento de seguridad desde una perspectiva operativa, sentando las bases para su implementación.

4.4. Análisis de la Situación Actual de la ESNAPE (Diagnóstico Interno)

Por medio de la revisión técnica y empírica de los procesos operativos vigentes dentro de la red WiFi de la Estación Naval Penitenciaria de Ecuador “ESNAPE”, se pudieron detectar las siguientes fortalezas, oportunidades, debilidades y amenazas:

Tabla 13 FODA del Plan Estratégico

Fortalezas (F):

Aspecto	Análisis
Infraestructura instalada de alto nivel.	El reparto militar ESNAPE cuenta con equipos como los Access Points Ubiquiti U6-LR y Firewall Fortinet FG-70F con licenciamiento UTP, lo que sin lugar a duda permite un entorno técnico robusto,

	adecuado para implementar medidas avanzadas de control y monitoreo.
Personal técnico dispuesto a implementar mejoras.	El personal técnico militar activo dentro de la ESNAPE no solo demuestra compromiso, sino también iniciativa, lo que contribuye a la adaptación de nuevas propuestas y el fortalecimiento operativo del sistema de acceso.
Red segmentada con VLANs para operativos y administrativos.	La división de la red de la ESNAPE en VLANs permite un control lógico más preciso, aislando a su vez el tráfico por funciones, además de mejorar la seguridad general del sistema.

Oportunidades (O):

Aspecto	Análisis
Posibilidad de replicar este procedimiento en otros repartos militares pertenecientes a la Armada del Ecuador.	La estandarización de la propuesta del actual procedimiento puede permitir la posibilidad de ampliar su impacto positivo dentro del reparto militar ESNAPE, promoviendo así las prácticas uniformes de seguridad.
Aceptación institucional sobre la necesidad de un procedimiento formal.	Existe una predisposición dentro del reparto naval, lo que facilita la implementación del nuevo procedimiento de seguridad, a su vez de que se reduce resistencias y favoreciendo así la adopción gradual en torno a los niveles jerárquicos.
Disponibilidad de herramientas de monitoreo disponibles como la controladora WiFi.	Contar con recursos tecnológicos importantes permite no solo supervisar, sino también ajustar y auditar el proceso de

	conexión, reforzando así tanto su trazabilidad como su efectividad operativa dentro del reparto militar.

Debilidades (D):

Aspecto	Análisis
Duplicidad de registros, saturación de IP's y falta de trazabilidad histórica.	La falta de mecanismos normalizados ha generado redundancia en los registros de dispositivos, lo que contribuye a un agotamiento de rangos IP disponibles y ausencia de historial verificable contribuye a los accesos no autorizados, todo esto dificulta la supervisión técnica.
Ausencia de base documental y formatos normalizados.	La falta de documentos oficiales que definan tanto los roles, como los procedimientos y creación de formularios estructurados impide la estandarización y continuidad operativa dentro de la Estación Naval Penitenciaria de Ecuador, especialmente en contextos de rotación frecuente del personal militar dentro de este reparto.

Amenazas (A):

Aspecto	Análisis
Riesgos de acceso no autorizado y pérdida de confidencialidad.	La falta de mecanismos confiables tanto de verificación como de trazabilidad, al igual que la autenticación dual IP/MAC, ha permitido que existan casos de ingresos de dispositivos no registrados o manipulados, lo que ha generado que se comprometa la integridad de la red WiFi del reparto militar

	ESNAPE, al igual que la privacidad de los datos institucionales.
Saturación del servicio por uso indebido de dispositivos no verificados.	El registro no controlado de múltiples dispositivos del personal militar, ya sean dispositivos personales o institucionales, y sin criterios técnicos establecidos, ha generado congestión en los recursos de red, afectando la disponibilidad del servicio y generando vulnerabilidades operativas dentro del reparto militar ESNAPE.
Dificultades en la continuidad del control ante cambios rotativos del personal militar.	Dentro de la Estación Naval Penitenciaria de Ecuador está establecida la orden o política de los altos mandos en referencia a la rotación frecuente del personal militar asignado a la ESNAPE, dicha rotación se da cada dos meses, lo que supone un riesgo en cuanto a la aplicación constante del procedimiento, ya que cada relevo requiere capacitación específica, además de un compromiso institucional para mantener la coherencia operativa del procedimiento de seguridad.

4.5. Plan de Actividades de Implementación del Procedimiento

Actividad 1: Diagnostico situacional del entorno inalámbrico de la ESNAPE y levantamiento de información

Esta primera actividad tuvo como objetivo conocer a detalle el estado en que se encontraba la red WiFi de la Estación Naval Penitenciaria de Ecuador, por ejemplo, los dispositivos conectados, mecanismos actuales de seguridad, y demás. Dicho diagnostico permitió identificar aquellas brechas operativas, además de validar la necesidad imperiosa del procedimiento propuesto, además del levantamiento de información de dicho entorno en cuanto a la conectividad WiFi del reparto naval, considerando principalmente el ámbito operativo para regular el acceso a la red y su uso.

Para poder llevar a cabo esta primera parte del plan de actividades se realizó una revisión documental de la distribución de la red WiFi de la ESNAPE para conocer a que red se iba a aplicar el presente proyecto, además de entrevistas con el personal militar técnico, al igual que al personal militar dentro del reparto naval quieren hacen suso de los servicios de red.

Dentro de esta esta actividad se pudo identificar la cantidad de usuarios que requerían conexión a la red de la ESNAPE, además del tipo de dispositivos que usualmente se conectan a dicha red y el procedimiento que se encontraba vigente para permitir o denegar el acceso de los dispositivos a la red WiFi del reparto naval.

Finalmente, esta primera actividad realizada fue fundamental, ya que sirvió como base para poder estructurar y desarrollar un procedimiento de seguridad operativa formal, el cual se adapte a las necesidades reales de la Estación Naval Penitenciaria de Ecuador, alineándose no solo a las políticas del reparto naval, sino también a las capacidades existentes dentro de la ESNAPE.

Actividad 2: Planteamiento del procedimiento operativo para regular los accesos a la red WiFi de la ESNAPE

En base a toda la información recopilada anteriormente, se procedió con el desarrollo del procedimiento de seguridad operativo, el cual permita regular de forma segura los accesos a la red WiFi de la Estación Naval Penitenciaria de Ecuador. Dicho procedimiento fue estructurado en varios ejes, los cuales incluyeron una solicitud de acceso, la autorización por parte del personal militar técnico designado, el registro de los dispositivos autorizados y el monitoreo constante de su uso.

Asimismo, se estableció de forma clara los roles de las partes involucradas, por ejemplo, siendo en este caso la DIRTIC el reparto encargado tanto en administrar el acceso al igual que gestionar los privilegios de los usuarios. También esta la ESNAPE el reparto solicitante de estos accesos. Además, como parte del procedimiento se incluyo la aplicación de dos formularios los cuales fueron formulados y presentados a la autoridad, el Anexo A y Anexo B.

En referencia al Anexo A, este documento es la solicitud para el registro del personal militar entrante a la ESNAPE a cumplir con sus funciones. En cuanto al Anexo B, es el documento para solicitar el perfil de administrador por parte del oficial de TICS de la ESNAPE, el cual contara con mayores privilegios operativos dentro de la red WiFi del reparto militar.

Actividad 3: Formulación y elaboración de formatos oficiales internos para el registro de dispositivos (Anexos A y B)

Dentro de la actividad 3 se contemplo la formulación y posterior elaboración de dos documentos para el reparto naval, los cuales sean primordiales para registrar y autorizar los accesos de los dispositivos a la red WiFi de la ESNAPE. Los documentos propuestos denominados “Anexo A y Anexo B” fueron evaluados junto con el personal militar técnico para su aceptación y su uso, además de ser socializados con el personal de uniformado en funciones. Dichos documentos fueron concebidos como parte del presente proyecto, pero, además, son los únicos instrumentos válidos que pueden ser usado por el personal militar para el registro y autorización de los dispositivos ya sean personales o institucionales dentro de la red WiFi de la Estación Naval Penitenciaria de Ecuador.

En cuanto al Anexo A, este documento será usado por el personal designado a cumplir funciones dentro de la ESNAPE, los cuales requerirán acceso a la red WiFi. Cabe mencionar que se ha establecido que solamente se podrán registrar un máximo de hasta dos dispositivos por militar, los cuales serán debidamente identificados por la Mac Address.

Mientras que el Anexo B, es el documento que será utilizado únicamente por el militar autorizado el cual administre la red, en este caso, es el oficial de TICS de la ESNAPE, en donde además de sus datos personales, deberá incluir los datos del dispositivo del militar solicitante, además de contar con la autorización de la DIRTIC. Es importante destacar que ambos documentos formulados contienen campos de identificación, tal es el caso del grado que ostenta el militar en ese momento, además del área de trabajo, el tipo de dispositivo, y los datos técnicos, al igual que las firmas de los responsables en la autorización, esto último es útil para garantizar la trazabilidad del proceso, dicho proceso conta de lo siguiente:

1.- El militar solicitante, es quien inicia el proceso por medio del formulario de solicitud para requerir el acceso a la red dentro del reparto naval, en donde, por medio del Anexo A, en el cual dicho militar declara no solo sus datos personales como sus nombres, apellidos, rango, reparto y demás, sino que también el tipo de dispositivo que desea registrar, y si es personal o institucional, la MAC Address de ese dispositivo. Se debe destacar que dicha solicitud deberá ser tomada como una declaración de responsabilidad.

2.- Los militares técnicos de la Estación Naval Penitenciaria de Ecuador “ESNAPE” serán los responsables de recibir esta solicitud inicial, además de verificar que dichos dispositivos cumplan con ciertos requisitos, tal es el caso de no haber duplicidad del registro,

que no sobrepase el límite de dispositivos por militar, y que también corresponda a un dispositivo autorizado ya sea celulares y laptos.

3.- Tras realizar estas acciones, se deberá remitir el requerimiento, en donde el responsable será el Militar Técnico de Estación Naval Penitenciaria de Ecuador al Oficial de TICS, en donde este último tendrá la potestad de aceptar o denegar la solicitud inicial.

4.- Conforme al procedimiento, el Oficial de TICS deberá realizar el Anexo B y en conjunto con el Anexo A será enviado al militar técnico de ESNAPE para que este a si vez será quien remita la documentación por correo electrónico institucional (Zimbra) a la DIRTIC para su legalización.

5.- El militar técnico de DIRTIC será quien receptes las solicitudes (Anexo A y Anexo B) y deberá informar al Oficial de Seguridad de la Información para su verificación correspondiente.

6.- El procedimiento con los Anexos A y Anexo B elaborados dentro del presente proyecto terminan con el Oficial de Seguridad de la Información de DIRTIC quien tendrá la función de verificar las solicitudes de registro provenientes de ESNAPE.

Cabe mencionar que su uso obligatorio garantiza no solo la trazabilidad, sino también la legalidad administrativa del procedimiento, además de la mejora en la gestión documental del control de acceso a la red WiFi del reparto naval, ya que aplicar de manera rigurosa los formatos previamente diseñados como parte del presente proyecto, y aprobados por las autoridades para estandarizar de manera pertinente la solicitud de acceso a la red WiFi dentro del reparto ESNAPE (Anexo A para usuarios finales y Anexo B para administradores) garantizan que el proceso de autorización sea documentado no solo de forma estandarizada, sino también controlada.

Actividad 4: Desarrollo del procedimiento operativo para controlar los accesos a la red WiFi de la ESNAPE

Como parte fundamental del desarrollo del presente proyecto se propuso procedimiento operativo no solo seguro, sino también formalizado y detallado el cual permita gestionar de forma segura los accesos de los dispositivos del personal militar a la red WiFi de la Estación Naval Penitenciaria de Ecuador. Cabe mencionar que esta actividad 4 plantea el desarrollo propositivo de dicho procedimiento el cual puede ser adoptado una vez que se realicen tanto los ajustes técnicos como las validaciones permitentes dentro de este entorno crítico como lo es este reparto naval.

Ahora, en referencia al procedimiento desarrollado, este contempla una distribución especifica en cuanto a los roles del personal militar técnico, estableciendo así de manera precisa los encargados de no solo ejecutar cada acción, sino también bajo que condiciones, y también con que niveles de validación, todo esto es con el objetivo de garantizar tanto la trazabilidad como el control y también la eficiencia dentro de la gestión de acceso de los dispositivos a la red WiFi de la ESNAPE.

Con lo presentado anteriormente, se distinguen los siguientes roles y responsabilidades del personal militar técnico extraídas del procedimiento propuesto:

Roles y responsabilidades instituidos en el procedimiento propuesto

1.- Militar solicitante de la ESNAPE:

- Son los militares de tropa u oficiales designados a prestar servicios dentro de la Estación Naval Penitenciaria de Ecuador “ESNAPE” y quien requiere el acceso a la red WiFi del reparto naval. Por lo que el proceso inicia por medio de la entrega del Anexo A, en donde este declara no solo sus datos personales como sus nombres, apellidos, rango, reparto y demás, sino que también el tipo de dispositivo que desea registrar, y si es personal o institucional, la MAC Address de ese dispositivo.

2.- Militar técnico de la ESNAPE:

- El militar técnico de la ESNAPE es quien recepta la solicitud inicial (Anexo A) realizada por el militar activo dentro del reparto naval.
- Se encargará de verificar que no solo no exista duplicidad de dispositivos, sino también que no haya un exceso de dispositivos por cada militar, además de que la MAC Address corresponda a los dispositivos permitidos, en este caso celulares o laptops. Cabe mencionar que se estableció que el máximo de dispositivos permitidos por cada uno de los militares será de dos dispositivos.
- Una vez aprobada las solicitudes por parte del Oficial de TICS de la ESNAPE, el militar técnico deberá remitir dichas solicitudes a DIRTIC por medio del correo electrónico institucional (Zimbra).
- Una vez que DIRTIC se ha encargado de registrar la IP y MAC Address de los dispositivos, el técnico militar de la ESNAPE conforme al procedimiento desarrollado deberá realizar lo siguiente dentro del Firewall Fortinet FG-70F:
    - Activar los dispositivos solicitados, los cuales siguieron previamente el procedimiento y hayan sido autorizados.
    - Desactivar los dispositivos del personal militar relevado.

- Debe remitir cada viernes o tras cada relevo del personal militar un listado actualizado de aquellos dispositivos activos dentro de la red WiFi de la ESNAPE a la DIRTIC para efectos tanto de auditoria como de control.

3.- Oficial de TICS de la ESNAPE:

- Militar oficial designado en la ESNAPE, quien aprueba o deniega de manera formal la solicitud de registro presentado por el personal militar entrante.
- Como oficial dentro del personal militar será responsable no solo del control sino también de la trazabilidad del procedimiento dentro del reparto naval.
- Tiene la función tanto de supervisar como de monitorear todos los dispositivos autorizados y que cuenten con acceso a la red WiFi de la ESNAPE.
- Como el militar más antiguo dentro del área de tecnologías de la ESNAPE contará con acceso administrativo a la Controladora Cloud Key Gen2. Esto será por medio de las credenciales asignadas por parte de la DIRTIC.

4.- Militar técnico de DIRTIC:

- Militar técnico designado por la DIRTIC, quien recibe las solicitudes provenientes de la Estación Naval Penitenciaria de Ecuador por medio del correo institucional (Zimbra).
- Las solicitudes de la ESNAPE deberá remitirlas al Oficial de Seguridad Informática (OSI) de DIRTIC para su validación correspondiente.
- Se encargará de ejecutar los registros de IP y MAC Address de los dispositivos solicitantes dentro del Firewall Fortigate FG-70F.
- Una vez realizadas sus funciones deberá comunicar por medio del correo institucional (Zimbra) al militar técnico de la ESNAPE para que este último proceda tanto con la activación como con la asignación de permisos.

5.- Oficial de Seguridad Informática de DIRTIC:

- Deberá revisar y validar todos los documentos de solicitudes enviadas por la ESNAPE.
- Encargado de supervisar y auditar las conectividades de todos los dispositivos del personal militar que fueran aprobados.
- Como el militar más antiguo dentro del área de tecnologías de la DIRTIC deberá remitir mensualmente informes a la ESMAAR sobre el control de las

conexiones y también del acceso a la red WiFi de la ESNAPE del personal uniformado.

Esta parte del procedimiento evidentemente contempla la fase documental elaborada en cuanto a los Anexo A y Anexo B, por medio de los cuales el personal militar únicamente podrá solicitar el acceso a la red WiFi de la ESNAPE, además de la asignación como administrador, obviamente, dependiendo del rol asignado.

Además, durante el avance de la presente actividad se realizaron simulaciones controladas haciendo uso de la herramienta DNS CHECKER para verificar las direcciones MAC de los dispositivos dentro de la documentación del Anexo A, además de que por medio de la maquina virtual VMware, esto se lo hizo con el objetivo de recrear escenarios de asignaciones de direcciones IP además de asociales con direcciones de Mac Address, además del establecimiento de los registros a la conexión de red por medio del Firewall, todo esto se lo hizo con el fin de evitar intervenir con la infraestructura de la ESNAPE para no causar afectaciones a su operatividad. El propósito de esto fue no solo observar, sino también documentar como funcionaria el procedimiento propuesto tanto en la fase técnica como en la fase organizacional. Cabe mencionar que, estas simulaciones se las realizaron con las configuraciones del Firewall FG-70F, sin embargo, se debe aclarar que el objetivo principal del presente proyecto no se enfoca en el desarrollo técnico en sí mismo, sino que se enfoca tanto en el diseño como en la formalización de un procedimiento operativo. Por lo tal, la simulación técnica antes mencionada se la empleo como complemento para observar no solo la factibilidad, sino también la eficiencia, además de la coherencia del flujo del procedimiento propuesto dentro del presente proyecto. Esto quiere decir que, se prioriza un enfoque operativo y organizacional, centrado en el establecimiento tanto de roles como de responsabilidades, además de los mecanismos de control los cuales puedan ser adaptados por la ESNAPE como parte de su política interna de seguridad operativa.

Con el desarrollo de la actividad 4 se logró definir claramente que ningún miembro de las Fuerzas Armadas podría acceder a la red WiFi de la ESNAPE sin cumplir con el protocolo de validación, el cual por medio del procedimiento desarrollado en el presente proyecto incluye la revisión técnica, solicitudes documentadas, la validación jerárquica y también el registro técnico. Esto quiere decir que, el procedimiento propuesto no solo garantiza la responsabilidad compartida entre la ESNAPE y la DIRTIC, sino también la distribución de funciones de forma equitativa, logrando así evitar la concentración de las funciones, además de un mejor control para una mayor seguridad dentro del ámbito operativo de la Estación Naval Penitenciaria de Ecuador.

Finalmente, la presente actividad concluye con el desarrollo integral del procedimiento propuesto dentro del proyecto, el cual se encuentra alineado no solo con las normativas de seguridad de la Estación Naval Penitenciaria de Ecuador, sino también, se encuentra adaptado a la realidad y capacidad de dicho reparto naval, lo cual permite su futura implementación tanto efectiva como segura, en caso de que la presente propuesta del proyecto sea oficialmente acogido por los altos mandos militares pertenecientes a la Armada del Ecuador.

Actividad 5: Evaluación de los resultados obtenidos, validación de la propuesta del proyecto y retroalimentación

Para finalizar se llevó a cabo una evaluación cualitativa en cuanto a los resultados del desarrollo del procedimiento propuesto dentro del presente proyecto, por tal razón se realizaron entrevistas al personal dentro de la Estación Naval Penitenciaria del Ecuador. Si bien es cierto que la implementación no fue inmediata, el proyecto que se efectuó fue socializado no solo con el oficial de TICS de la ESNAPE, sino también con los militares técnicos y el personal uniformado dedignado a prestar servicios dentro del reparto naval, recibiendo así una respuesta positiva, además de sugerencias constructivas. Cabe destacar que la validación que se realizó de la presente propuesta se apoyó en la revisión correspondiente del contenido por parte de los militares del área técnica de la Estación Naval Penitenciaria de Ecuador, quienes enfatizaron la viabilidad del procedimiento propuesto de este proyecto, además de su claridad y potencial para ser aplicado de manera segura y eficiente dentro del reparto naval. Dicha aceptación no solo refuerza el impacto operativo positivo del presente proyecto, sino que también tiene una gran posibilidad de ser implementado de manera formal, y a su vez de ser exitoso. Para complementar esta actividad, se diseñó y también se distribuyó una encuesta Likert al personal militar técnico activo en la Estación Naval Penitenciaria de Ecuador con el objetivo de no solo evaluar los niveles de claridad del procedimiento, sino también su aplicabilidad y también la pertinencia de la propuesta presentada en el presente proyecto, en donde se obtuvieron resultados positivos.

Ahora, una de las recomendaciones compartidas ante la presentación de la propuesta del proyecto fue dejar establecido que los oficiales técnicos tanto de la ESNAPE como de la DIRTICE deben ejecutar acciones de revisión técnica y administrativa de forma mensual, por tal razón aquí fue donde se deben incluir auditorías de registros, análisis de tráfico, informes de consumo y también la verificación de cumplimiento de roles. Cabe destacar que la interacción y colaboración constante entre la ESNAPE y la DIRTIC permitirá que el procedimiento evolucione de forma proactiva, alineándose con los cambios

tecnológicos y también las necesidades operativas emergentes, garantizando así la sostenibilidad del sistema de seguridad de red WiFi del reparto naval.

Se instó incluir programas de capacitaciones cortas para el personal militar quienes solicitan el acceso a la red WiFi, en especial a las partes involucradas dentro del procedimiento para su correcto funcionamiento. A esto se debe sumar la incorporación de un "diagrama de procedimiento para el registro", en donde no solo se muestre el flujo de la propuesta realizada en el presente proyecto, sino también plasmar de manera clara el rol del personal militar técnico, los militares solicitantes y los oficiales del área técnica hasta cumplir con lo estipulado dentro del procedimiento de seguridad para regular y controlar los accesos a la red WiFi de la Estación Naval Penitenciaria de Ecuador. Además de indicar que era importante conocer los responsables de la aprobación de la documentación elaborada (Anexo A y Anexo B), y como resultado se opto por establecer que ambos documentos presentarán las firmas de los militares involucrados.

De igual manera se sugirió que el resultado final del proyecto realizado en cuando al procesamiento de seguridad para el control de los accesos a la red WiFi sea difundido al personal militar dentro de la ESNAPE, dicha tarea fue llevada a cabo, además de mantener un canal de retroalimentación con el personal militar técnico para poder identificar posibles inconvenientes durante la ejecución del procedimiento propuesto o posibles contratiempos que enfrente el personal uniformado de la ESNAPE en su aplicación. En este contexto, se puede dar el caso de la rotación del personal militar que presta servicios dentro de la ESNAPE o también la finalización del tiempo de servicios, por lo que en estos casos se instó seguir el procedimiento desarrollado para dar la baja de los dispositivos pertenecientes al personal uniformado que sea reasignado a otro reparto o salga del mismo, al igual de aquel militar designado que cuente con acceso de administrador. Es por este motivo que se dejó constancia de las retroalimentaciones como parte de información valiosa tanto para mejorar como para ajustar el procedimiento desarrollado antes de una aplicación formal, de tal manera que dicho procedimiento se mantenga alineado no solo a los protocolos internos de la ESNAPE, sino también a la estructura jerárquica exclusiva de la Armada del Ecuador.

Finalmente, esta última etapa dentro de la actividad 5 refuerza aún más el enfoque del proyecto, el cual es una propuesta proactiva, que esta orientada tanto a una mejora continua como para el fortalecimiento en referencia a la gestión de los accesos a la red WiFi dentro de la Estación Naval Penitenciaria de Ecuador.

4.6. Plan de Implementación Estratégico

Dentro de este apartado se describirá el plan estratégico de implementación de la propuesta del presente proyecto de tesis, por lo cual se desarrolló un cronograma de actividades clave que permitan tanto la ejecución organizada como coordinada y también efectiva del nuevo procedimiento de seguridad para controlar el acceso a la red WiFi de la Estación Naval Penitenciaria de Ecuador.

Cabe mencionar que este plan no solo considera aspectos técnicos, sino también operativos y administrativos, los cuales están alineados con los roles del personal militar técnico dentro de la ESNAPE y la DIRTIC. Además, cada una de las actividades que se presentan cuentan con un tiempo estimado de desarrollo y también un indicador tangible, el cual servirá como evidencia de su cumplimiento, esto se lo hizo con el propósito de garantizar un desarrollo tanto organizado como coherente y medible del presente proyecto, el cual es el procedimiento operativo para regular los accesos a la red WiFi de la ESNAPE, por lo que se planteo un plan de desarrollo estratégico conformado por diversas actividades centrales. Cada uno de estos ejes esta enfocada en consolidar aquellos lineamientos operativos los cuales permitan fortalecer no solo la seguridad, sino también la el control del reparto militar en los accesos de los dispositivos a la red WiFi del mismo, permitiendo así mejorar los niveles de seguridad dentro de la Estación Naval Penitenciaria de Ecuador, además de la trazabilidad y también la responsabilidad funcional.

Tabla 14 Plan de Desarrollo de Actividades Estratégicas de Implementación

Actividad	Responsable	Tiempo Estimado	Indicador de Éxito
Levantamiento de información del entorno de la Estación Naval Penitenciaria de Ecuador “ESNAPE”.	Autor del proyecto en colaboración con el personal militar técnico.	1 mes.	Información detallada de la distribución de la red de la ESNAPE, además del entorno actual de la gestión de accesos y dispositivos con conexión.
Planteamiento del procedimiento operativo del proyecto para regular	Autor del proyecto, Militar técnico y Oficial	1 mes.	Propuesta que contemple tanto las responsabilidades, como

los accesos a la red WiFi de la ESNAPE	TIC de la ESNAPE y DIRTIC.		los flujos en el registro de los dispositivos, y las normativas de acceso a la red WiFi de la ESNAPE.
Elaboración de formatos oficiales internos para el registro de dispositivos (Anexos A y B)	Autor del proyecto en colaboración con el personal militar técnico	2 meses.	Documentos concluidos para solicitar el acceso a la red WiFi de la ESNAPE, además de la administración de la misma (Anexo a y Anexo B), revisados y aprobados por el personal militar.
Diseño del procedimiento operativo para controlar el acceso a la red WiFi de la ESNAPE	Autor del proyecto, Militar técnico y Oficial TIC de la ESNAPE y DIRTIC.	2 meses	Procedimiento de seguridad a nivel operativo, verificado el cual detalla los roles (personal uniformado, militares técnicos, y oficiales administradores), flujo de validación (revisión, autorización y registro), control de dispositivos por militar (máximo 2 dispositivos), y finalmente, la trazabilidad dentro del reparto naval.
Sociabilización del procedimiento propuesto	Autor del proyecto, Militar técnico y Oficial TIC de la	1 mes.	Entrevistas con el personal militar técnico para demostrar la viabilidad de la propuesta del proyecto.

	ESNAPE y DIRTIC.		
Análisis y retroalimentación del procedimiento propuesto	Autor del proyecto, Militar técnico y Oficial TIC de la ESNAPE y DIRTIC.	Permanente	Realización de entrevistas al personal militar del área de tecnologías, además del análisis de los resultados obtenidos por medio de la encuesta tipo Likert aplicadas a La población objeto de estudio en cuanto al acceso a la red WiFi del reparto naval. El procedimiento propuesto se considera exitoso cuando más del 85% del personal militar involucrado dentro de las encuestas calificaron con la calificación más alta tanto la utilidad, como la claridad y también la aplicabilidad de la propuesta del presente proyecto. Además de que las retroalimentaciones otorgadas fueron integradas en la versión final del proyecto.

Fuente: Elaboración propia (2025)

Ilustración 13 Cronograma del Plan Estratégico del Procedimiento de Seguridad de Red WiFi de la ESNAPE (Oct. 2024 – Jul. 2025)

Actividad	oct-24	nov-24	dic-24	ene-25	feb-25	mar-25	abr-25	may-25	jun-25	jul-25
1. Análisis del entorno de la ESNAPEI (diagnóstico de situación actual del reparto naval)	•	•								
2. Levantamiento de información sobre normativa interna, roles operativos y equipos activos.		•	•							
3. Definición de objetivos estratégicos del procedimiento operativo			•	•						
4. Diseño del procedimiento operativo para la ESNAPE (roles, protocolos, medidas y controles)				•	•					
5. Análisis operativo del procedimiento propuesto con base en referencias técnicas estandarizadas, sin implementación directa, de las herramientas como firewalls Fortinet y escenarios de control como los simulados en VMware					•	•				
6. Validación de la propuesta mediante criterios de seguridad, viabilidad y replicabilidad						•	•			
7. Ajustes y mejora continua del procedimiento tras validación							•	•		
8. Elaboración del documento formal del procedimiento operativo								•	•	
9. Revisión por parte de autoridades institucionales (ENAPE)									•	
10. Socialización del procedimiento y capacitación básica al personal designado										•

Fuente: Elaboración propia (2025)

4.7. Estrategias Aplicadas al Entorno Operativo de Seguridad de Red en la ESNAPE

Por medio de los análisis antes realizados y el desarrollo del procedimiento de seguridad del presente proyecto en cuanto a su propuesta de la gestión y control de accesos a la red WiFi dentro de la Estación Naval Penitenciaria de Ecuador, se planteo las siguientes estrategias, las cuales están orientadas no solo a la seguridad, sino también eficiente y trazable en el contexto de un entorno militar el cual pertenece a un área critica, adaptadas a las características y necesidades de dicho reparto militar. Por tal razón, a continuación, se detallan las estrategias tecnológicas principales propuestas dentro del presente proyecto, con un enfoque orientado a la seguridad, la sostenibilidad operativa y la trazabilidad del uso de recursos de la ESNAPE.

1.- Solicitud de Registro y Autenticación de Dispositivos

Descripción:

Una de las piezas fundamentales dentro del procedimiento propuesto en el presente proyecto consiste en establecer por medio de una solicitud escrita el registro de dispositivos los dispositivos del personal militar, estos pueden ser laptops y celulares, los cuales pueden ser de uso personal e incluso dispositivos que pertenecientes a la propia Armada del Ecuador, los cuales muchas veces son conferidos a ciertos militares para sus actividades.

Dicha solicitud está conformada por los formatos del Anexo “A” y “B”, recopila la dirección MAC del dispositivo, su procedencia, el tipo de usuario y otros datos claves que permitirán su posterior autorización o rechazo. Las funcionalidades claves de la misma son:

- Validación del límite máximo de dispositivos permitidos por usuario.
- Asociación de dispositivos con rangos operativos (personal permanente o rotativo).
- Clasificación de dispositivos según origen: institucional o personal.

Beneficios:

- Facilita la auditoría y control por parte de DIRTIC.
- Permite establecer políticas diferenciadas de uso según tipo de usuario y dispositivo.

Indicadores de Éxito en Entorno Controlado:

- Número de dispositivos registrados correctamente.
- Consistencia entre los registros físicos y los digitales reflejados en la red dentro del Firewall Fortinet.

2.- Formulación de Documentación Operativa (Solicitudes, Guías y Flujograma)

Descripción:

Se realizaron jornadas para socializar el procedimiento propuesto dentro del presente proyecto, dicha actividad fue dirigida al personal militar que prestaba servicios en la ESNAPE, además del personal militar técnico. Las jornadas antes mencionadas se centraron en explicar no solo los objetivos, sino también los beneficios y las diferentes fases del procedimiento para un mayor control de los accesos a la red WiFi del reparto naval.

Beneficios:

- Reducción de errores humanos por interpretación errónea.
- Fácil entendimiento del procedimiento para el personal militar asignado a prestar servicios en el reparto naval.

Indicadores de Éxito:

- Documentación elaborada para el procedimiento (Anexo A y Anexo B, roles y responsabilidades del personal involucrado y flujograma del procedimiento).
- Nivel de utilidad apreciada por los militares activos del reparto naval (resultados obtenidos por medio de entrevistas no estructuradas al personal militar y retroalimentaciones de los mismos).

3.- Validación del Procedimiento Propuesto por Simulaciones en Entorno Controlado

Descripción:

Antes de una implementación a futuro, como parte del proyecto se realizaron ejercicios simulados para que se pueda constatar la aplicabilidad del procedimiento propuesto dentro de un entorno controlado, por lo cual se simuló todo el procedimiento, iniciando desde la solicitud realizada por el militar entrante, en donde este declara sus datos personales, además del rango, reparto, dispositivo que desea registrar, y si es personal o institucional, la MAC Address de dicho dispositivo; seguido de la recepción de ese documento (Anexo A), realizada por el militar activo dentro del reparto naval, además de verificar que no haya un exceso de dispositivos por cada militar (estableció que el máximo de dispositivos permitidos por cada uno de los militares será de dos dispositivos), además de que la MAC Address corresponda a los dispositivos permitidos (se dejó establecido el uso de celulares y laptops), en este último se hizo uso de la herramienta “DNS Cheker”. Una vez comprobada la información en este escenario se continuo con el procedimiento propuesto pasando por el Oficial de TICS (como militar más antiguo del área, contará con acceso administrativo a la Controladora Cloud Key Gen2, por medio de las credenciales asignadas por parte de la DIRTIC). Continuando con el escenario de simulación se hizo uso de la herramienta VMware para simular el Firewall Fortinet FG-70F de la Armada se procedió a ejecutar los registros de IP y MAC Address de los dispositivos solicitantes en esta simulación dentro del Firewall Fortigate FG-70F, esto fue para activar los dispositivos solicitados, los cuales siguieron previamente el procedimiento y hayan sido autorizados, además de desactivar los dispositivos del personal militar relevado. Todo esto se lo hizo para replicar el procedimiento propuesto dentro del presente proyecto, además de comprobar su viabilidad dentro del reparto naval, además de su coherencia y la factibilidad del procedimiento desarrollado.

Beneficios:

- Mejor seguridad y robustez en cuanto a la operatividad del procedimiento técnico-operativo desarrollado.
- Refuerzo de la preparación del personal militar técnico para escenarios reales.
- Mayor confianza por parte del reparto naval en la propuesta presentada dentro del presente proyecto.
- Reducción de incidentes relacionadas con el acceso no autorizado.

Indicadores de Éxito:

- Cantidad de simulaciones realizadas.
- Tiempos de respuesta dentro del proceso de registro durante las simulaciones.
- Reuniones para afirmar la factibilidad del procedimiento dentro del reparto naval.
- Opiniones y sugerencias derivadas de estas simulaciones realizadas.
- Prevención de saturación del pool de IPs disponibles.
- Mayor control sobre el uso real de la red.
- Número de IPs liberadas para su reutilización eficiente.

4.- Sociabilización de la Propuesta Desarrollada del Procedimiento para Regular los Accesos a la Red WiFi de la ESNAPE

Descripción:

Se realizaron jornadas para socializar el procedimiento propuesto dentro del presente proyecto, dicha actividad fue dirigida al personal militar que prestaba servicios en la ESNAPE, además del personal militar técnico. Las jornadas antes mencionadas se centraron en explicar no solo los objetivos, sino también los beneficios y las diferentes fases del procedimiento para un mayor control de los accesos a la red WiFi del reparto naval.

Beneficios:

- Designación de roles y responsabilidades claras para su cumplimiento dentro del proceso.
- Trazabilidad de auditorías internas, y también del seguimiento operativo.
- Mayor control sobre el uso real de la red.
- Facilita la rotación del personal operativo sin comprometer la seguridad del sistema.
- Identificación automática de dispositivos inactivos mediante la monitorización.
- Prevención de la saturación en la asignación de nuevas direcciones IP.
- Garantizar que solo los dispositivos activos tengan acceso a la red.

Indicadores de Éxito:

- Aceptación por parte del personal uniformado en operaciones del reparto naval.

- Prevalidación para la inclusión del procedimiento propuesto en la normativa interna de la Armada del Ecuador.

4.8. Evaluación sobre el Plan Estratégico Tecnológico

La Puntuación (1) siendo la más baja y la Puntuación (5) siendo la más alta.

Tabla 15 Evaluación del plan estratégico tecnológico aplicado a la administración del acceso a la red Wifi de la ESNAPE

Criterios de Evaluación	Puntuación	Justificación
Claridad y concisión del resumen del plan estratégico.	4	El plan estratégico presenta una estructura clara, con objetivos bien definidos, estrategias alineadas a los requerimientos operativos de la ESNAPE, y una redacción precisa que refleja una planificación lógica, aunque puede ampliarse en términos de visualización de resultados a largo plazo.
Grado de inclusión de objetivos, estrategias y relevancia para el colectivo institucional.	5	Se incluyen metas específicas, responsables, cronograma y actividades que responden directamente a necesidades reales del reparto naval, como la restricción y control de acceso a la red WiFi de la ESNAPE.
Viabilidad técnica y operativa del plan estratégico.	5	El plan es altamente factible, ya que se adapta a las capacidades técnicas actuales de la ESNAPE, incluyendo el uso de infraestructura ya existente como firewalls Fortinet y controladores Ubiquiti, eliminando la necesidad de adquisiciones externas costosas.
Evaluación de recursos necesarios y su disponibilidad.	4	Se ha considerado adecuadamente el personal técnico y los equipos disponibles; sin embargo, se recomienda documentar de forma más precisa la asignación de turnos de gestión durante períodos de relevo o contingencia.
Claridad y precisión de los indicadores de éxito y resultados esperados.	5	Se incluyen indicadores como la reducción de incidentes de conexión no autorizada, eficiencia en el control del uso del wifi institucional y monitoreo de actividad de red, lo que permite evaluar el impacto operativo.
Posibles impactos positivos en el colectivo institucional a corto y largo plazo.	5	El impacto es notoriamente favorable, especialmente en seguridad informática, eficiencia del uso de recursos de red y orden administrativo, con sostenibilidad asegurada por la continuidad del personal militar técnico calificado.
Inclusión de las partes involucradas dentro del reparto para la elaboración del plan.	4	Aunque se contempló la participación de técnicos y oficiales TIC, podría incorporarse un módulo de retroalimentación más amplio para recoger sugerencias de personal operativo en el campo.
Estrategia de comunicación para la implementación del plan.	4	Se establecen vías formales de comunicación institucional como correo Zimbra y oficios diseñados, pero se recomienda implementar mecanismos complementarios como paneles informativos o boletines técnicos.

Nivel de innovación en las soluciones tecnológicas propuestas.	5	La propuesta destaca por adaptar el control de red de una forma avanzada mediante la asociación de IP/MAC y monitoreo en tiempo real, con prácticas poco comunes en entornos militares convencionales.
Adecuación de tecnologías seleccionadas al entorno institucional.	5	El uso de DNS Checker, el Firewall Fortinet y la Controladora Ubiquiti resulta apropiado y eficiente, respetando las restricciones operativas, el entorno seguro y las limitaciones presupuestarias propias del reparto ESNAPE.

Fuente: Elaboración propia (2025)

Conclusiones

La implementación de un plan tecnológico estratégico para la administración del acceso a la red WiFi dentro de la Estación Naval Penitenciaria de Ecuador (ESNAPE) ha demostrado ser una iniciativa necesaria y eficaz, basada en la realidad institucional y la capacidad operativa del entorno militar. La ejecución del presente proyecto de tesis ha facilitado un mayor nivel de control, organización y seguridad en el manejo de la red WiFi institucional, garantizando que solo el personal autorizado y los equipos verificados puedan acceder a la infraestructura digital sensible.

Una de las conclusiones más significativas de este proyecto reside en relación con el análisis de la topología y distribución de la red de la ESNAPE, ya que su revisión era importante debido a que se debía conocer a que red se quería dar seguridad con el desarrollo del procedimiento para controlar los accesos a dicha red, además de comprender no solo las limitaciones, sino también las fortalezas de la misma. Además, por medio de este análisis se pudo establecer un punto de inicio tanto realista como coherente contemplando las condiciones operativas del reparto naval.

Identificar tanto los roles como las responsabilidades de las partes involucradas dentro de la gestión de los accesos a la red WiFi permitió definir las funciones que cumplen cada uno de los militares del área técnica, además de conocer que dichos actores no solo cuentan con un papel clave en referencia a la configuración y mantenimiento de la red, sino que además manejan el rol de administradores para la vigilancia de los dispositivos conectados en la red. Toda esta indagación realizada permitió establecer un proyecto cuya propuesta en parte distribuya las responsabilidades de manera eficaz, además de fortalecer el rol del recurso más importante dentro de una institución, la cual es el recurso humano, con el propósito de afianzar la parte activa y a su vez garantizar la operatividad de la conectividad, en especial dentro de un área critica como lo es la ESNAPE.

Otra conclusión enfocada en el diseño del procedimiento, se desarrollo una propuesta completa orientada al fortalecimiento de la administración de los accesos de los dispositivos a red WiFi del reparto militar, por lo que dicha propuesta se enfocó en hacer uso exclusivamente de los recursos con los que ya contaba la ESNAPE, evitando propuestas que escapen de las capacidades del propio reparto. El diseño presentado estableció no solo protocolos claros y secuenciales para los registros, sino también para la validación y el monitoreo de los dispositivos con acceso a la red WiFi, permitiendo así un mayor control del reparto militar, además de que para ello se contempló la estructura jerárquica del personal de la Armada del Ecuador dentro de la ESNAPE, y a su vez, adaptándolo a los medios de

autorización y niveles de responsabilidades. También, la eficiencia obtenida mediante un sistema de registro centralizado basado en direcciones MAC y vinculación IP. Al limitar el acceso exclusivamente a los dispositivos registrados, principalmente computadoras portátiles y teléfonos inteligentes, la ESNAPE ha fortalecido su estrategia de ciberseguridad y minimizado los riesgos de accesos no autorizado. La inclusión de un flujo de trabajo estructurado de aprobación y verificación, con la participación de técnicos tanto de la ESNAPE como del DIRTIC, garantiza ese doble factor de seguridad, fomentando una cultura de responsabilidad en la gestión de la información. Además, con los procedimientos estandarizados de control de acceso digital implementados, la transición entre el personal, especialmente durante la rotación o reasignación, se vuelve más manejable y predecible. Al integrar la gestión de acceso en los flujos rutinarios de documentación y comunicación (como las solicitudes oficiales y los correos electrónicos de Zimbra), el proyecto también contribuye a la optimización de las tareas administrativas, que a menudo sobrecargan a las unidades operativas.

Otra de las conclusiones en cuanto al procedimiento propuesto fue que este mismo se sometió a una fase de evaluación tanto conceptual como operativa, lo que permitió recoger las sugerencias por parte del personal militar involucrado. Dicha evaluación confirmo que la propuesta desarrollada es factible dentro de la ESNAPE, además de responder de manera acertada a las necesidades tanto de control como de trazabilidad y también de seguridad en referencia a la demanda del acceso a la red inalámbrica del reparto militar. Si bien es cierto que la propuesta aún no está en una fase de implementación inmediata, se pudo constatar un nivel alto de aceptación, lo que representa un paso fundamental hacía una futura aplicación del mismo.

El factor humano no se ha descuidado. Al asignar claramente los roles y responsabilidades a los militares técnicos de la ESNAPE, los oficiales de TIC y el personal de la DIRTIC, el plan fomenta la coordinación entre repartos navales y el desarrollo profesional. El énfasis en la documentación, la capacitación y la elaboración de informes programados promueve un entorno donde se comparten y mantienen las mejores prácticas. Además, los procedimientos técnicos implementados, en particular los realizados a través del firewall de Fortinet y el controlador de red de Ubiquiti, demuestran la viabilidad del proyecto. Los protocolos de configuración, que abarcan desde el registro de dispositivos y la asignación de IP/MAC hasta la monitorización en tiempo real y las auditorías periódicas, se han adaptado cuidadosamente para satisfacer las necesidades de una institución militar sin incurrir en costes adicionales de infraestructura. Esto reafirma la alineación del plan con las políticas

institucionales y su adaptabilidad a los recursos existentes, evitando así la necesidad de inversiones externas o cambios drásticos en la infraestructura digital.

Finalmente, el procedimiento propuesto por medio del presente proyecto constituye una herramienta imprescindible para mejorar la gestión operativa dentro de los accesos de dispositivos a la red WiFi del reparto naval, lo que demuestra que, con una planificación adecuada, la contemplación de las limitaciones institucionales y el uso eficiente de las herramientas existentes, es totalmente posible modernizar los procedimientos sin sacrificar el control, la disciplina ni la integridad operativa. El resultado es un modelo escalable y replicable que potencialmente puede extenderse a otras unidades de las Fuerzas Armadas, sentando un precedente para futuras integraciones tecnológicas dentro de un contexto donde el Ecuador ha sido declarado en estado de Conflicto Armado Interno.

Recomendaciones

Tras el desarrollo del plan tecnológico estratégico para la gestión del acceso inalámbrico en la Estación Naval Penitenciaria de Ecuador (ESNAPE), se han formulado varias recomendaciones clave para garantizar la sostenibilidad, la mejora continua y la posible expansión del sistema. Estas recomendaciones buscan no solo fortalecer la infraestructura operativa establecida por medio del presente proyecto, sino también fomentar una cultura más amplia de responsabilidad digital e innovación tecnológica dentro del reparto naval.

En primer lugar, se debe implementar protocolos estandarizados para la adecuada gestión del personal militar dentro del reparto naval, esto debe ser en base a los roles operativos que cumple cada uno de las partes involucradas en el proceso de registro de accesos a la red y también el monitoreo, por lo que se recomienda establecer de manera formal las funciones de cada uno de los militares dentro del área de tecnologías, por tal razón, el protocolo tiene que incluir funciones especificas como las propuestas en el presente proyecto, tal es el caso del registro de los dispositivos, monitoreo en tiempo real, además de una gestión de alertas internas que ya depende netamente de la propia Armada del Ecuador. Dicho enfoque operativo permite no solo reforzar la trazabilidad, sino también mejorar la eficiencia en cuanto a la los accesos a la red WiFi de la ESNAPE y también su debida supervisión.

En segundo lugar, se recomienda adoptar la propuesta del presente proyecto como guía operativa para la Estación Naval Penitenciaria de Ecuador, dado que el procedimiento elaborado se desarrollo considerando tanto la realidad como las capacidades actuales del reparto naval, por tal razón se exhorta la validación formal del presente proyecto para ser tomado como guía operativa dentro del reparto, debido a que la propuesta desarrollada esta constituida en una base tanto ordenada como realista, la cual puede emplearse como herramienta para capacitar al personal militar, además de estandarizar las funciones y a su vez, facilitar posibles auditorias en cuanto al uso de la red WiFi.

Otra recomendación es que se debe simular más escenarios controlados para evaluar el procedimiento planteado, con el objetivo de constatar el desempeño de los militares involucrados dentro de situaciones específicas en cuanto a la gestión accesos a la red WiFi; este paso es importante tenerlo en cuenta debido a que aportará a valorar no solo la aplicabilidad del procedimiento presentado dentro de más escenarios, sino también identificar posibles mejoras, además de ajustar si es necesario los tiempos, roles, además de los recursos en relación a las funcionalidades operativas dentro de la ESNAPE.

Además, se debe implementar un mecanismo para socializar el procedimiento ante posibles cambios o la rotación del personal militar, sobre todo esta última ya que esta dinámica es habitual dentro de las instituciones militares, no solo de la Armada, sino también del Ejercito y la FAE, por tal razón se recomienda establecer medidas para compartir el procedimiento cada vez y cuando se designe a un nuevo personal a prestar servicios dentro de la ESNAPE, en especial aquellos que sean designados a cumplir funciones relacionadas a la gestión de los accesos a la red inalámbrica. Por tal razón, se pueden realizar dinámicas de sociabilización para una corta inducción técnica, además de la entrega de información del proceso e incluso, comprobar los conocimientos mediante capacitaciones en referencia al proceso de los registros, lo que puede garantizar que cada equipo militar designado a realizar funciones en la ESNAPE pueda aplicar de manera correcta el procedimiento, no solo para preservar la continuidad operativa, sino también para evitar posibles errores provenientes de la falta de conocimientos al procedimiento.

Otra recomendación importante es mejorar la comunicación entre los repartos navales de la ESNAPE y el DIRTIC mediante el establecimiento de una plataforma para el envío y seguimiento de solicitudes. Si bien el procedimiento desarrollado se apoya en el correo electrónico (Zimbra) y documentos oficiales, un sistema de flujo de trabajo digital integrado podría mejorar la transparencia, además de agilizar los procesos de aprobación y permitir actualizaciones del estado de las solicitudes de los usuarios en tiempo real. Esta herramienta también podría generar notificaciones automáticas, mejorando los tiempos de respuesta y reduciendo la dependencia del seguimiento manual.

También se recomienda reforzar continuamente la concientización sobre la seguridad de los datos y el uso responsable de la red entre todos los usuarios registrados. Los programas breves y periódicas de concienciación mediante correos electrónicos o breves sesiones informativas presenciales pueden ayudar a recordar a los usuarios sus responsabilidades al acceder a los recursos institucionales de internet, incluyendo la importancia de proteger sus credenciales personales, evitar instalaciones no autorizadas y reportar anomalías.

Finalmente, si bien el proyecto ha generado mejoras significativas en cuanto a la gestión y control de los accesos de dispositivos a la red WiFi de la ESNAPE, su éxito a largo plazo dependerá de la adaptabilidad, la colaboración y una mentalidad proactiva. Al invertir en auditorías de sistemas, formación de usuarios, análisis de datos y difusión de políticas, así la ESNAPE puede garantizar que los beneficios de esta iniciativa perduren y evolucionen en respuesta a las nuevas demandas y exigencias del reparto militar.

Bibliografía

Aryaka. (24 de Enero de 2023). *Seguridad de la red: Protección de sus activos digitales*. Obtenido de Aryaka.com: https://www.aryaka.com/es/blog/network-security/

Bermúdez Rubio, D., Cuenca Rivera, P. E., García Murillo, P. G., Gutiérrez Gómez, G., & Portela Ramírez, A. J. (2021). Sugerencias para escribir análisis de resultados, conclusiones y recomendaciones en tesis y trabajos de grado. *Dialnet, 8*(1), 1-12. doi:https://doi.org/10.15332/24224529.6608

Centro Criptológico Nacional. (Julio de 2021). *Recomendaciones de seguridad en redes Wi-Fi corporativas.* Obtenido de CCN-CERT: https://www.ccn-cert.cni.es/es/informes/informes-de-buenas-practicas-bp/3137-ccn-cert-bp-11-recomendaciones-redes-wifi-corporativas/file.html?utm_

CISCO. (2024). *Cyber Threat Trends Report: From Trojan Takeovers to Ransomware Roulette.* Obtenido de Cisco.com: https://www.cisco.com/c/dam/en/us/products/collateral/security/cyber-threat-trends-report.pdf

CISCO. (Abril de 2025). *¿Qué es un punto de acceso inalámbrico?* Obtenido de Cisco.com: https://www.cisco.com/site/us/en/learn/topics/small-business/what-is-an-access-point.html#tabs-9da71fbd27-item-1288c79d71-tab

Contreras Díaz, Y. d., Rivero Amador, S., González Pérez, M. M., & Ding, B. (2021). La Gestión de Información en el contexto institucional y el rol de los directivos. *Scielo*, 1-21. Obtenido de http://scielo.sld.cu/pdf/ics/v32n1/2307-2113-ics-32-01-e1798.pdf

Correa Castillo, B. L. (2024). Evaluación de vulnerabilidades del protocolo WPA3 SAE con el esquema Dragonblood en una red Wi-Fi domiciliaria y de oficina pequeña. *Universidad Nacional de Loja*, 1-231. Obtenido de https://dspace.unl.edu.ec/jspui/bitstream/123456789/28854/1/ByronLenin_CorreaCastillo.pdf

Fortinet. (7 de Abril de 2025). *FortiGate 70F Series.* Obtenido de fortinet.com: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-70f-series.pdf

Ganuza, N. (2020). *GUÍA DE CIBERDEFENSA ORIENTACIONES PARA EL DISEÑO, PLANEAMIENTO, IMPLANTACIÓN Y DESARROLLO DE UNA CIBERDEFENSA MILITAR.* Obtenido de Junta Interamericana de Defensa: https://jid.org/wp-content/uploads/2022/01/Ciberdefensa10.pdf?utm_source

García Romanos , J. (2008). La gestión de la configuración y la gestión de activos como una gestión del conocimiento. *Redalyc, 4*(1), 18-35. Obtenido de https://www.redalyc.org/pdf/922/92217123004.pdf

GCF Global. (2025). *Seguridad en redes wifi*. Obtenido de GCFGlobal.org: https://edu.gcfglobal.org/es/seguridad-en-internet/seguridad-en-redes-wifi/1/

Guamán Seis, J. A. (2024). *Seguridad de la Información en las Fuerzas Armadas del Ecuador para la predicción de ciberataques en redes militares [Tesis de Doctorado, Universidad de Guadalajara].* Repositorio Institucional. Obtenido de

https://riudg.udg.mx/visor/pdfjs/viewer.jsp?in=j&pdf=20.500.12104/104668/1/DCUCEA10154FT.pdf

Hernández Sampieri , R., Fernández Collado, C., & Baptista Lucio , P. (Junio de 2011). *METODOLOGÍA DELA INVESTIGACIÓN.* Obtenido de Universidad Veracruzana: https://www.uv.mx/personal/cbustamante/files/2011/06/metodologia-de-la-investigaci%C3%83%C2%B3n_sampieri.pdf

Hewlett Packard Enterprise. (2025). *¿Qué es la gestión de red?* Obtenido de Hpe.com: https://www.hpe.com/lamerica/es/what-is/network-management.html?utm_source

International IT. (5 de Julio de 2022). *¿Qué es la Gestión de Red y por qué es importante?* Obtenido de Internationalit.com: https://www.internationalit.com/post/qu%C3%A9-es-la-gesti%C3%B3n-de-red-y-por-qu%C3%A9-es-importante?lang=es&utm=

Kizza, J. M. (2020). *Guide to Computer Network Security.* Chattanooga: Department of Computer Science and Engineering University of Tennessee. doi:10.1007/978-3-319-55606-2

Masoud, M. Z., Jaradat, Y., & Alia, M. (2021). IEEE802.11 Access Point's Service Set Identifier (SSID) for Localization and Tracking. *Tech Science Press, 71*(3), 1-18. doi:10.32604/cmc.2022.023781

Ministerio de Defensa Nacional del Ecuador. (24 de Enero de 2023). *LEY ORGÁNICA DE PERSONAL Y DISCIPLINA DE LAS FUERZAS ARMADAS.* Obtenido de defensa.gob.ec: https://www.defensa.gob.ec/wp-content/uploads/downloads/2023/02/LEY-ORGANICA-DE-PERSONAL-Y-DISCIPLINA-DE-LAS-FUERZAS-ARMADAS_ene_2023.pdf

Monje Álvarez, C. A. (2011). *METODOLOGÍA DE LA INVESTIGACIÓN CUANTITATIVA Y CUALITATIVA Guía didáctica.* Obtenido de Universidad Veracruz: https://www.uv.mx/rmipe/files/2017/02/guia-didactica-metodologia-de-la-investigacion.pdf

National Institute of Standards and Technology. (19 de Enero de 2022). *Guide to Bluetooth Security.* Obtenido de Nvlpubs.nist.gov: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf

National Institute of Standards and Technology. (Febrero de 2024). *The NIST Cybersecurity Framework (CSF) 2.0.* Obtenido de nvlpubs.nist.gov: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

National Quality Assurance. (2022). *ISO 27001:2022 GUÍA DE IMPLEMENTACIÓN DE SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.* Obtenido de Nqa.com: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

PRESIDENCIA DE LA REPÚBLICA DEL ECUADOR. (9 de Enero de 2024). *Decreto Ejecutivo No. 111.* Obtenido de Secretaría General de Comunicación de la Presidencia: https://www.comunicacion.gob.ec/wp-content/uploads/2024/01/Decreto_Ejecutivo_No._111_20240009145200_20240009145207.pdf

Rashid , N., Asif Ali, l., Kamlesh, K., Shibin, D., & Munwar, A. (2020). Survey on Wireless Network Security. *Springer Nature Link*, 2-21. doi:https://link.springer.com/article/10.1007/s11831-021-09631-5

Rosero Tejada, L. (15 de Septiembre de 2021). *El phihing como riesgo informático, técnicas y prevención en los canales electrónicos: un mapeo sistemático.* Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/21699/4/UPS-GT003573.pdf

Stallings, W. (2017). *CRYPTOGRAPHY AND NETWORK SECURITY - PRINCIPLES AND PRACTICE* (7 ed.). Edinburgh Gate: Pearson. Obtenido de https://dl.hiva-network.com/Library/security/Cryptography-and-network-security-principles-and-practice.pdf

Tareef, A., Abadleh, A., Alkasasbeh, A., & Alghamdi, M. (Julio de 2024). *Enhancing Wi-Fi Security by Preventing Backward Compatibility Attacks on WPA3 Protocols.* doi:10.21203/rs.3.rs-4830716/v1

Ubiquiti. (2020). *UniFi Cloud Key Gen2 Plus Datasheet.* Obtenido de Ubiquiti: https://dl.ubnt.com/datasheets/unifi/UniFi_Cloud_Key_G2_Plus_DS.pdf

Zepeda Vega, D. (s.f.). *Diseño de Redes LAN Tecnologías de conmutación.* Obtenido de Consejo Nacional de Universidades - Nicaragua: https://www.uazuay.edu.ec/sites/default/files/public/redes_de_datos_lan2.pdf

Anexos

Anexo 1.- Cuestionario dirigido al personal militar activo dentro de la Estación Naval Penitenciaria de Ecuador

Pregunta 1: ¿Conoce el procedimiento actual de registro de dispositivos para acceso a la red WiFi institucional?

a) Sí, completamente
b) Parcialmente
c) No

Pregunta 2: ¿Ha solicitado previamente el registro de más de un dispositivo?

a) Sí, y fueron aprobados sin problema
b) Sí, pero solo se aprobó uno
c) No, solo uso un dispositivo
d) Lo intenté, pero fue rechazado

Pregunta 3: ¿A través de qué medio realizó el proceso de acceso a la red WiFi de la ESNAPE?

a) Escrito entregado al área técnica de la ESNAPE
b) Correo electrónico “Zimbra”
c) Comunicación verbal al militar técnico
d) No ha realizado ninguna de las anteriores

Pregunta 4: ¿Considera que los medios a través de los cuales realizó su solicitud de acceso a la red son seguros?

a) Muy seguros
b) Seguros
c) Poco seguros
d) Nada seguros

Pregunta 5: ¿Conoce cuáles son las funciones específicas del personal militar técnico designado en la ESNAPE?

a) Sí, tengo claro su rol
b) Tengo una idea general
c) No conozco sus funciones

Pregunta 6: ¿Con qué frecuencia el personal militar técnico informa sobre el estado de los dispositivos conectados?

a) De forma semanal
b) Mensualmente
c) Solo cuando hay fallos

Pregunta 7: ¿Cree que la implementación de un nuevo procedimiento documentado y estandarizado mejoraría el control de acceso a la red?

a) Sí, completamente
b) Parcialmente
c) No cambiaría nada

Pregunta 8: ¿Considera pertinente establecer roles y responsabilidades claros para el personal técnico de la ESNAPE y de la DIRTIC para que sean los encargados del registro de equipos de los usuarios?

a) Muy pertinente
b) Poco pertinente
c) Nada pertinente

Pregunta 9: ¿Considera importante que cada dispositivo sea registrado mediante IP y MAC Address?

a) Sí, es esencial para la seguridad de la red WiFi de la ESNAPE
b) No es necesario
c) No lo sé

Pregunta 10: ¿Cree que el nuevo procedimiento debería incluir fases de validación y doble autorización?

a) Sí, para fortalecer la seguridad
b) No, basta con una aprobación
c) No tengo opinión al respecto

Pregunta 11: ¿Estaría dispuesto a capacitarse sobre el uso del nuevo procedimiento de seguridad de red?

a) Sí, me parece necesario
b) No, no lo considero relevante

c) Dependería del tiempo disponible

Anexo 2.- Guía de entrevista dirigida al Oficial de Tecnologías de la Información y Comunicación de ESNAPE

Sección 1: Estado actual y necesidades de la red dentro del reparto militar

Desde su experiencia como encargado técnico, ¿cómo describiría la situación actual de la red WiFi dentro de la ESNAPE?

¿Considera que el diseño actual de la red cumple con los estándares de seguridad adecuados?

Sección 2: Gestión y control de acceso a la red

¿Qué procesos siguen actualmente para registrar o autorizar dispositivos en la red interna?

Entrevistador: ¿Qué actores están involucrados en la gestión operativa de la red?

Sección 3: Percepción del nuevo procedimiento propuesto

¿Qué opinión tiene sobre la propuesta de un procedimiento de seguridad más estructurado?

Sección 4: Retos y viabilidad de implementación

¿Cuáles considera que serían los principales desafíos para implementar este procedimiento?

¿Considera viable aplicar este procedimiento en otros repartos de la Armada del Ecuador?

Anexo 3.- Documento Anexo A, solicitud para el acceso a la red WiFi de la Estación Naval Penitenciaria de Ecuador “ESNAPE”.

Figura 1 Anexo "A" del Procedimiento

DOCUMENTACIÓN DE SOLICITUD PROPUESTA PARA ACCESO A LA RED WIFI DE LA ESNAPE

ANEXO "A"

SOLICITUD DE REGISTRO PARA EL ACCESO A LA RED WIFI DE LA ESTACIÓN NAVAL PENITENCIARIA DE ECUADOR "ESNAPE"

La red **WiFi de ESNAPE** está configurada con privilegios únicamente para:

ACCESO A INTERNET:

- SITIOS Y SERVICIOS GUBERNAMENTALES.
- SITIOS INFROMATIVOS Y DE CONSULTAS.
- SITIOS DE REDES SOCIALES.
- SITIOS REQUERIDOS POR NECESIDAD INSTITUCIONAL

DATOS DEL PERSONAL SOLICITANTE:

NOMBRES: _____

APELLIDOS: _____

GRADO: _____

REPARTO: _____ DEPARTAMENTO: _____

TIPO DE DISPOSITIVO: _____

MAC ADDRESS DEL DISPOSITIVO _____

ORIGEN DEL DISPOSITIVO: REPARTO: ☐ PERSONAL: ☐

NOTA: SOLO SE PERMITIRÁ MÁXIMO EL REGISTRO DE DOS (2) DISPOSITIVOS POR USUARIO

SOLICITADO POR	**AUTORIZADO POR**
_____	_____
GRADO – NOMBRES	**GRADO – NOMBRES**
CARGO	**CARGO**

Anexo 4.- Anexo B, solicitud para la administración de la red en la ESNAPE

Figura 2 Anexo "B" del Procedimiento

DOCUMENTACIÓN PROPUESTA PARA LA ADMINISTRACIÓN DE LA RED WIFI DE LA ESNAPE

ANEXO "B"

SOLICITUD PARA LA ADMINISTRACIÓN DE LA RED WIFI DE LA ESTACIÓN NAVAL PENITENCIARIA DE ECUADOR "ESNAPE"	
La red **WiFi de ESNAPE** está configurada con privilegios únicamente para:	
ACCESO A INTERNET: • SITIOS Y SERVICIOS GUBERNAMENTALES. • SITIOS INFROMATIVOS Y DE CONSULTAS. • SITIOS DE REDES SOCIALES. • SITIOS REQUERIDOS POR NECESIDAD INSTITUCIONAL	
DATOS DEL ADMINISTRADOR DESIGNADO: NOMBRES: _____ APELLIDOS: _____ GRADO: _____ CARGO EN LA ESNAPE: _____ IP Y MAC DEL DISPOSITIVO PARA LA ADMINISTRACIÓN: _____ _____	
NOTA: TERMINADO EL TIEMPO DE SERVICIO INSTITUCIONAL SE TENDRÁ QUE COMUNICAR A LA DIRTIC PARA PROCEDER A ELIMINAR LA CUENTA DE ADMINISTRADOR	
SOLICITADO POR _____ **GRADO – NOMBRES** **CARGO** **ESNAPE**	**AUTORIZADO POR** _____ **GRADO – NOMBRES** **CARGO** **DIRTIC**

Anexo 5.- Flujo desarrollado para la propuesta realizada en el presente proyecto, para plasmar de manera clara el rol del personal militar técnico, los militares solicitantes y los oficiales del área técnica hasta cumplir con lo estipulado dentro del procedimiento de seguridad para regular y controlar los accesos a la red WiFi de la Estación Naval Penitenciaria de Ecuador desarrollado en el presento proyecto.

Figura 3 Flujo Desarrollado del Procedimiento Propuesto para el Registro y Acceso de Dispositivos a la Red WiFi de la ESNAPE

Anexo 6.- Sociabilización del Nuevo Procedimiento de seguridad al personal militar activo para el acceso a la red WiFi de la Estación Naval Penitenciaria de Ecuador