ESCUELA DE POSGRADO NEWMAN

MAESTRÍA EN
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

" Propuesta para mejorar la gestión de la Infraestructura de la red de datos la Fuerza Aérea Ecuatoriana, Quito – 2022 "

Trabajo de Investigación
para optar el Grado a Nombre de la Nación de:

Maestro en
Gestión de Tecnologías de la Información

Autores:
Lic. Gamboa Alabuela, Jonathan William
Lic. Gamboa Alabuela, Jefferson Paúl

Docente Guía:
Mtra. Julissa Vargas Fuentes

TACNA – PERÚ

2022

INFORME DE ORIGINALIDAD

19%	19%	2%	5%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

ÍNDICE GENERAL

ÍNDICE DE TABLAS

Resumen

La presente investigación se basa en proponer una mejora en la gestión de la infraestructura de red de la Fuerza Aérea Ecuatoriana (FAE), en razón que actualmente no se dispone de una estandarización tanto en hardware como en software para una óptima gestión sin limitaciones de compatibilidad, para esto se utilizará un enfoque mixto tanto cualitativo como cuantitativo mediante una investigación aplicada para lograr implementar una política de gestión de la red de datos de la FAE mediante estándares propios, apegados tanto a normas internacionales como necesidades institucionales, para mantener una administración adecuada de la red así como una escalabilidad que no limite la dimensión de la misma y perdure en el tiempo.

Palabras clave: propuesta de mejora, infraestructura, red, hardware, software, políticas de gestión, seguridad informática, estándares, internet, intranet.

Introducción

La presente investigación tiene como objetivo mejorar la gestión de la red de datos de la Fuerza Aérea Ecuatoriana mediante la exploración de nuevas tecnologías que permitan tener estándares propios, apegados tanto a normas internacionales como necesidades institucionales, para mantener una administración adecuada de la red.

En el primer capítulo encontraremos como se ha planteado el problema y la metodología que se ha utilizado, así mismo se puede observar que está dirigida a un grupo de administradores y usuarios de TIC.

En el segundo capítulo se hace necesario conocer a que se refiere la gestión en diferentes aspectos como la gestión financiera, infraestructura de red, seguridad de la información y en otras aristas que comprenden el manejo de la red, así como la conceptualización de algunos elementos que se conjugan dentro de ella.

Llegando al tercer capítulo exponemos a la Fuerza Aérea como una entidad pública que ha trazado su historia y su filosofía organizacional en la que se destaca su misión que consiste en desarrollar la capacidad militar aeroespacial, que garantice la defensa de la soberanía e integridad territorial; y, apoyar con su contingente al desarrollo nacional y a la seguridad pública y del Estado.

En el cuarto capítulo una vez estudiado como se podría mejorar la gestión de la red de datos se hace una propuesta basada en una nueva tecnología que permitiría

tener un mejor control de la red mediante la implementación de una arquitectura de red diferente.

Y por último en el quinto capítulo se sugiere una implementación paulatina de una nueva tecnología que permita llegar mejor al usuario final manteniendo las políticas de seguridad para la transferencia de datos y tener un mejor manejo y control de la red.

Capítulo I

Antecedentes del Estudio

1.1. Título del Tema:

Propuesta de mejora de la gestión de la infraestructura de la red de datos la Fuerza Aérea Ecuatoriana, Quito – 2022.

1.2. Planteamiento del Problema:

La presente investigación busca diseñar una propuesta de mejora para la gestión de la infraestructura de red de la fuerza aérea ecuatoriana en el año 2022, basada en la renovación de los equipos activos y cableado estructurado del edificio principal

La actual infraestructura de red de la Fuerza Aérea fue instalada en el año de 1996, en un primer diagnóstico se ha podido identificar: cortes en la transmisión de datos, lentitud en la transmisión y recepción de datos a través de la red, además los servicios informáticos simultáneos como telefonía IP, video llamadas, aplicaciones, etc., tienen que proveerse de manera limitada a los usuarios, debido a que no existe una estandarización clara y definida para el cableado estructurado, en tal virtud actualmente la Fuerza Aérea cuenta con un cableado de categoría 5E ceñido a la norma EIA/TIA 568B y el cableado vertical (backbone) con fibra óptica OM4 y OM2 multimodo, otro aspecto que se considera importante dentro de la infraestructura de red son los equipos activos, que actualmente siguen funcionando con pocas fallas a pesar de que ya han cumplido con su vida útil, tendiendo a la obsolescencia, ocasionando: la disminución paulatina de los puntos de red, ralentización en el acceso a los diferentes sistemas y servicios informáticos

de la Fuerza Aérea, limitado crecimiento para impresoras y nuevos usuarios, lentitud en la transmisión y recepción de datos a través de la red, falta de alta disponibilidad de red y vulnerabilidad de la información disponible en la red, en vista que convergen varias redes en un mismo equipo, estos diagnósticos detallados se deben a una deficiente política para la adquisición de equipos nuevos y a un plan de renovación tecnológica que establezca puntos importantes como la inversión, gestión lógica de la red, capacitación continua y transferencia de conocimientos para contar con profesionales internos que administren la red de datos.

De no ser atendidos los puntos anteriormente mencionados se podría llegar a tener incompatibilidad con los elementos activos que conforman la red provocando una caída de los servicios, así como la limitación en lo que se refiere a escalabilidad. En lo que se refiere a la obsolescencia de equipos de no ser actualizados repercutirá en la falla masiva al tratarse de equipos centrales o a su vez impidiendo la transmisión de los datos en los puntos terminales. Tocando el punto del personal que administra la red sin capacitación previa estarían desprovistos de los conocimientos necesarios para solventar problemas críticos o a su vez repeler los ataques constantes y la fuga de información seria masiva puesto que las políticas de seguridad de la información no se han plasmado en su totalidad.

Para poder mejorar los puntos mencionados es necesario crear una política de gestión de la red en la cual se especifique los estandarización de equipos para manejar una sola línea, facilitando la administración de los mismos la conexión y

operatividad, así como dimensionar la escalabilidad para el crecimiento ordenado de la red; además un análisis de inversión de capital que permita una renovación de al menos el 50% de la red, en los puntos más críticos; así mismo la creación de una matriz automatizada que evidencie un plan de renovación constante y los límites de ejecución, ligado a todo esto es necesario contar con un plan de carrera en el cual se asigne competencias específicas de los profesionales en tic y a su vez incluir procedimientos para mitigar las diferentes amenazas haciendo hincapié en la implantación de las políticas de seguridad de la información.

1.3. Objetivos de la Investigación:

- Mejorar la gestión de la red de datos de la Fuerza Aérea Ecuatoriana mediante la exploración de nuevas tecnologías que permitan tener estándares, apegados a normas internacionales y necesidades institucionales, para mantener una administración adecuada de la red, así como una escalabilidad que no limite la dimensión de la misma y perdure en el tiempo.

- Determinar las necesidades críticas de la red mediante un mapeo que identifique los puntos estratégicos del funcionamiento de los componentes que no pueden fallar, para evitar colapsos en la misma y determinar opciones de financiamiento de capital para actualizar o reemplazar solo lo necesario.

- Analizar los diferentes componentes de la red, teniendo como base su funcionamiento y prestaciones, para un cambio oportuno que evite la obsolescencia tecnológica.

- Mantener personal capacitado acorde a las necesidades de implementación de mejoras de la red mediante capacitaciones brindadas por la institución o autoeducación que permitan certificarse profesionalmente para que realicen una actualización constante de la red.

1.4. Metodología:

1.4.1. Tipo y Diseño de investigación

1.4.1.1. Tipo de investigación

De acuerdo con la naturaleza del presente trabajo esta investigación será de tipo aplicada descriptiva con un enfoque mixto tanto en el aspecto cuantitativo como cualitativo (Sampieri, 2000). Siendo de tipo exploratorio dado que busca descubrir mediante los conocimientos adquiridos tanto procesos como políticas que permitan el crecimiento y fortalecimiento de la red como protagonista principal de las TIC dentro de la FAE. Con un enfoque mixto se analizará tanto los datos cuantitativos como números de equipos, así como históricos de inversión y del lado cualitativo las políticas vigentes que necesiten ser cambiadas para mejorar los procesos de administración de la red que es la parte importante de las TIC.

1.4.1.2. Diseño de la investigación

Se usara una investigación no experimental ya que se busca explorar los datos en su forma real, los cuales no serán manipulados en la recolección de los mismos.

1.4.2. Población y Muestra

1.4.2.1. Población

La población corresponde a todos quienes manejan la red de datos enfocándose principalmente en los administradores y solo en los usuarios directivos que utilizan la misma en el proceso de toma de decisiones.

1.4.2.2. Muestra

Se realizara con una muestra no estadística en razón que la cantidad de administradores no es amplia así se podrá obtener un análisis de datos correctos, siendo siempre un número impar para no entrar en datos parejos

27 administradores

1.5. Técnicas e instrumentos

1.5.1. Técnicas:

Se utilizará un modelado de BMPN para identificar los puntos críticos que obstaculizan la constante evolución de la red, así mismo se determinara las aristas dentro de la infraestructura que son el punto clave para una mejor gestión.

Además, se realizó un análisis de toda la infraestructura de red de la Fuerza Aérea Ecuatoriana usando metodologías de Hacking Ético que fueron proporcionadas por el Comando de Ciberdefensa de Fuerzas Armadas, mismas que se dividen en:

- Defensa
- Exploración
- Respuesta

1.5.2. Instrumentos:

El modelado de BPMN necesitará la alimentación de los diferentes procesos por parte de los administradores se determinará y se simulará como estos se pueden mejorar o cambiar.

Se analizará los datos obtenidos por el comando de ciberdefensa para establecer los puntos de vulnerabilidad.

1.6. Justificación:

Justificación Teórica.

Este justificación implica describir los vacíos encontrados en el conocimiento (Bedoya, 2020) y en razón que esta investigación al estar dentro de una institución con doctrina (FAE, 2018), pretende plantear mediante el análisis del conocimiento propuesto, mejoras para crear nuevas aproximaciones doctrinales respaldadas en el avance tecnológico tanto de medios material y equipo que permitan la mejora continua y evitar el desgaste tecnológico acelerado.

Así mismo se sumerge en la entrega de políticas que si bien pueden ser flexibles estas mejoraran tanto la inversión como el anejo y administración de la red de datos de la FAE.

Justificación Práctica.

Para un justificación práctica es necesario ahondar en la presente investigación presentara nuevas estrategias que permitan verificar inmediatamente los puntos críticos y necesarios para el correcto funcionamiento y administración de la red, estableciendo puntos críticos que permitan actualizaciones oportunas de la misma, así como una inversión escalable tanto para evitar la obsolescencia (Vega, 2012) así como el ahorro del capital.

Justificación Metodológica.

Se realizará una investigación aplicada descriptiva en razón que este método permite establecer variables representativas para tratar de predecir un factor que a mediano o largo plazo incurra en problemas dentro de la red de datos que maneja la FAE.

También se orienta en un enfoque mixto ya que se necesitan valores exactos para su respectivo análisis de toda la infraestructura de red así como cualitativo que describa las funciones de la misma. Esto permitirá establecer una estrategia que combine ambos enfoques para la administración de la red de datos y a su vez esta se escalable en el tiempo mitigando los efectos colaterales de obsolescencia tecnológica (Vega, 2012) y evitando malas inversiones.

1.7. Definiciones:

Entendiendo de manera conceptualizada la gestión, son todas las actividades que en conjunto con las decisiones y políticas implementadas en una empresa se conseguirá administrar de la mejor manera un problema o situación, es así que gestionar uno de los elementos fundamentales de una organización como es su infraestructura tecnológica, es una actividad que resulta complicada, en especial cuando existe un gran número de dispositivos o se encuentran dispersos geográficamente y además que debe abarcar el hardware, el software, los elementos de red, un sistema operativo (SO) y el almacenamiento de datos (Peña & Anías, 2019)

1.8. Alcances y limitaciones:

Alcances:

El alcance de la presente investigación explorará el actual sistema de gestión de la infraestructura de red de la Fuerza Aérea Ecuatoriana, para el personal que labora en el departamento de tecnologías de la información y comunicaciones en la institución mencionada.

La propuesta abarcará al rediseño e implementación de una nueva infraestructura de red física y lógica para la Fuerza Aérea Ecuatoriana, la misma que está enfocada en el sector de la defensa nacional.

Limitaciones:

- Resistencia por partes de los directivos y personal subordinado para la implementación de buenas prácticas para el uso de herramientas e infraestructura tecnológica que permita mejorar el desempeño del procesado de la información considerando que al pertenecer al sector defensa se requiere de una alta disponibilidad de la información.

- La falta de capacitación o transferencia de conocimientos en la implementación de nuevas tecnologías, afectando aún más la situación por la rotación obligatoria del personal militar.

- Reducción presupuestaria que se ve afectada anualmente, mismo que no permite mantener un equilibrio tecnológico para ser implementado en la Dirección de Tecnologías de la Información y Comunicaciones, originando falta

de adquisición de equipamiento moderno y capacitación continua para una mejor gestión interna.

Capitulo II

Marco Teórico

2.1. Conceptualización de las variables o tópicos clave

Gestión

Interacción coordinada con los medios y recursos disponibles en la institución teniendo como fin el logro óptimo de un objetivo, el mismo que permitirán reflejar el cumplimiento de la misión establecida por la empresa.

Gestión financiera

Planificación enfocada hacia los recursos que la empresa dispone, para administrar y orientar de la mejor manera la adquisición, renovación o mantenimiento de lo que se desea implementar, considerando las limitaciones y las priorizaciones establecidas.

Gestión de la seguridad informática

Mitigación de los riesgos que pueden hacer vulnerable a una empresa enfocada en la infraestructura tecnológica, mediante el establecimiento de políticas, lineamientos, prácticas y estrategias para el uso de la tecnología implementada.

Gestión de la Infraestructura de Red

En el presente trabajo de investigación se conceptualizará la variable Gestión de la Infraestructura de Red la misma que se articulará con la gestión de la seguridad de la información dentro de la organización de estudio.

La infraestructura de red son los recursos tecnológicos disponibles dentro de una empresa tanto de hardware como software, que permiten conectividad, comunicación, administración y operación de la red de datos, proporcionando la mejor ruta, para una comunicación continua entre usuarios, aplicaciones y servicios tecnológicos.

La infraestructura de red compone toda la conexión técnicamente analizada y categorizada de la red, es el conjunto de cables, adaptadores, conectores, etc., por los cuales transita toda la información digital, sin embargo las empresas están adoptando nuevos modelos de TI basados en la red, como la nube informática móvil e Internet of Things (IoT), que aumenta el valor y la importancia de la red corporativa, (Kerravala, 2014)

Gestión de la seguridad de la información

La gestión de la seguridad de la información se encuentra normada y respaldada en las normas ISO que tratan a cerca de la seguridad de la información, abarcando varias de sus dimensiones como un glosario estándar, requisitos para poder implementar un Sistema de Gestión de Seguridad de la Información (SGSI), buenas prácticas de un SGSI y proporcionar las directrices apropiadas de cuando se deben realizar diferentes evaluaciones a la seguridad para el tratamiento de los datos para evitar ser blanco de ataques.

Seguridad de la información

La Seguridad de la Información, se refiere a que los datos tanto físicos como digitales sean íntegros y se encuentren disponibles en el momento oportuno para

su manejo, así como mantengan la privacidad y seguridad debido a su importancia.

ITIL

Son un conjunto de buenas prácticas que se utilizan para la administración de los servicios de TI, su desarrollo y operación, fortaleciendo la comunicación y reduciendo los cotos de TI, además que mejora la calidad del servicio.

Escalabilidad

Aspecto complejo e importante en el diseño de una infraestructura de TI, para establecer su capacidad de adaptación a través del tiempo y ante el crecimiento institucional para mantener un rendimiento eficaz frente a mayores cargas.

Topología de red

La topología de red es un mapa o disposición de la red, que puede ser física o lógica para el intercambio de datos, es la manera en la que se establece el diseño de la red para optimizar el flujo de datos con base en las necesidades propias de la empresa planteando los mejores caminos de la señales transmitidas o recibidas.

Red LAN

Red de computadoras que permite el intercambio de datos entre ellas o con servicios y aplicaciones albergadas a nivel local, la comunicación entre ellas se las considera dentro de un espacio de menor tamaño.

Modelado de procesos en BPMN

Partiendo de la primicia que “Un modelo de negocio describe las bases sobre las que una empresa crea, proporciona y capta valor” (Ostenwalder, 2011). Es necesario mencionar que en esto se basara la presente investigación, si bien se está analizando una empresa que no ofrece una rentabilidad es necesario gestionarla como si lo fuese, es ahí donde entra el Modelado de procesos en BPMN lo que permitirá constantemente simular la efectividad de los procesos a proponer.

2.2. Importancia de las variables o tópicos clave

Para entender la investigación de esta propuesta de mejora comenzamos con la definición de gestión. “Acción o trámite que, junto con otros, se lleva a cabo para conseguir o resolver una cosa.” (GESTIÓN | Definición de GESTIÓN Por Oxford Dictionary En Lexico.Com y También El Significado de GESTIÓN, n.d.), y al entender su definición inferimos que para la gestión correcta de lo que hemos planteado necesitamos de varios enfoques y participaciones de usuarios y administradores, nos enfocamos en algo muy importante como es la gestión, en vista que proponemos mejorar la forma en la que actualmente está estructurada la infraestructura de red de la Fuerza Aérea Ecuatoriana, siendo una empresa del sector público destinado a la defensa de la soberanía su alcance es de nivel nacional y su infraestructura de red debe ser implementada junto con buenas prácticas internacionales que han dado buenos resultados hasta el momento, en vista que a pesar del gran crecimiento tecnológico en todos los campos, también ha crecido exponencialmente las necesidades de cómputo, almacenamiento y

procesamiento de datos, llevando al límite las arquitecturas actuales (Beltrán & Sevillano, 2013) que necesitan una mejor gestión.

Una parte importante de cómo mejorar la infraestructura de red, también es darle el enfoque de innovación tecnológica, caracterizada por la presencia de dos elementos representados por la novedad y la explotación comercial, (Trott, 2005), dependerá mucho de los administradores de red que esta idea tenga frutos, no siempre lo que se propone se cumple, debido a varias limitaciones que los proyectos pueden presentar en la actualidad, y más aun considerando que la tecnología se actualiza constantemente, es así que la propuesta debería plantear una mejora que sea escalable.

Como lo menciona la revista de tecnología e Innovación en Educación Superior, “A medida que las organizaciones crecen, resulta más complejo administrar y mantener su infraestructura, haciéndose necesaria la búsqueda de herramientas para facilitarlo y fortalecer la aplicación de medidas preventivas y correctivas, con el objetivo de reducir al mínimo los incidentes y mantener el nivel de operación esperado.” (González, 2021), es necesario que la empresa cuente con un propuesta de mejora que permita solventar las fallas actuales que presenta la infraestructura de red, que es un punto primordial para la comunicación que debe mantener la empresa a nivel nacional, sin embargo un alcance mucho mayor sería rediseñar toda la gestión de las TI pero que demanda de una mayor investigación que solvente todas las falencias a distintos niveles, debido a que en estos tiempos TI es un soporte principal de toda organización que maneja grandes cantidades de información.

Como bien, hemos limitado la propuesta de mejora hacia la gestión de la infraestructura de red, podemos establecer que esta investigación aplicada, buscará una mejor administración de la comunicación interna a nivel local (red LAN), la misma que tendrá varias aristas desde la planificación hasta la ejecución propiamente dicha, entendiendo que no siempre implementar buenas prácticas va de la mano de invertir exorbitantes cantidades de dinero que permitan mantener sistemas de vanguardia a la tecnología, en razón que la aplicación de ciertas políticas tanto de seguridad como para mantener un estándar incluso llegan a constituir un ahorro de recursos, otra manera de entender esta investigación aplicada es nombrarla como una administración de redes a nivel local, “El término administración de redes es definido como la suma total de todas las políticas, procedimientos que intervienen en la planeación, configuración, control, monitoreo de los elementos que conforman a una red con el fin de asegurar el eficiente y efectivo empleo de sus recursos. Lo cual se verá reflejado en la calidad de los servicios ofrecidos” (Altamirano, 2003) y como nos dice esta última parte la gestión correcta de la infraestructura de red se ve reflejada en cada usuario final pueda obtener un servicio totalmente funcional y oportuno.

Un punto muy importante a plasmar en esta investigación es la administración de la seguridad dentro de la red local, para esto debemos diferenciar términos como seguridad informática y seguridad de la información, los cuales bajo normas ISO se complementan, pues si bien la seguridad informática protege los tangibles y no tangibles electrónicos (hardware y software) la seguridad de la información establece seguridades, para que la información que en estos se concentren no

sea violentada y su integridad sea confiable, por lo tanto una mejora continua y la aplicación de políticas de seguridad harán una administración segura de la red LAN, como lo menciona un artículo de la Universidad de Pereira “La información es el instrumento fundamental para el funcionamiento de las empresas y la operación de los negocios, esto hace que la información deba protegerse como el activo más importante de la organización”, (Isabel Ladino et al., 2011), actualmente las TI son sumamente utilizadas por las empresas, generando que muchas ocasiones sean vulnerables al no contar con una buena administración que como hemos mencionado implica establecer varios enfoques, o pudiendo implementar varios lineamientos como la Norma ISO/IEC 27000, para establecer la importancia de implementar un sistema de gestión de seguridad de la información que a la vez está involucrada con dar seguridad a la red LAN.

Una vez planteada la generalización de la investigación aplicada en dónde hemos establecido desde lo que significa gestión hasta el uso de normas aceptadas internacionalmente, es momento de plantear conceptos más técnicos que nos permitan mejorar la infraestructura de red.

Diseño de redes.

Una administración adecuada y un diseño de red apegado a normas técnicas es un gran reto, pues no es simplemente realizar conexiones físicas y establecer una comunicación digital interna, una buena gestión requiere de varias características para que permanezca en el tiempo y sea escalable, definida como “la capacidad de mejorar recursos para ofrecer una mejora (idealmente) lineal en

la capacidad de servicio" (Villaroel Salvatierra, 2011), debemos considerar que no está definido un diseño estándar del que se pueda tomar referencia, más bien existen vario parámetros establecidos para cada red dependiendo de los tipos y necesidades que se presentan, con esta propuesta buscaremos establecer los requisitos mínimos en la implementación y auditoría de una red.

Para entender de mejor manera la propuesta debemos definir claramente la funcionalidad de la red, para la cual estamos mejorando su gestión, además que al plantear el tema de escalabilidad, conseguimos una infraestructura adaptable y administrable en el tiempo y con las debidas transferencias de conocimientos; hablamos de éste último punto debido a que nuestra investigación está centrada en una institución pública del sector de defensa en la cual, muchas de las personas que cumplen con las funciones de planificadores y ejecutores de distintos proyectos trabajan en la institución de manera temporal y variable, es ahí que entra un énfasis en cómo las políticas para la gestión de la red permitirán que sea administrable con el pasar del tiempo y los recursos no se desperdicien.

De una manera técnica el diseño físico de las redes, identifica la ubicación física y función de los equipos activos de red junto con sus servidores, debido a que no todos los servidores a ser interconectados proveen los mismos servicios. Si no se encuentran ubicados adecuadamente, previa una planificación los costos de interconexión serían mucho más altos, es así que podemos iniciar recopilando los datos y necesidades de los usuarios y administradores, una vez realizado esto procedemos al análisis respectivo en dónde acoplamos cada necesidad con

nuestro espacio físico con base en las capacidades económicas y tecnológicas que se disponga pero siempre asignando una adecuada priorización.

Como parte del diseño físico de la red debemos plantear una topología que satisfaga de manera general los requerimientos recopilados, analizar qué tipo de cableado será el que se deba utilizar, el mismo que dependerá del tráfico de red, la seguridad, la distancia y una vez más el alcance económico, pudiendo implementar cable UTP de categoría 7A y fibra óptica, otro apartado son los equipos activos de red como los routers y switchs los mismo que son el centro de toda la infraestructura de red, al ser equipos que permiten establecer una comunicación continua y fiable por la red, una vez conseguido el análisis del diseño físico, podemos realizar un modelo de diseño lógico que permita a la red tener un tráfico continuo de datos sin estancamientos ni limitaciones además de establecer prioridades con base en los requerimientos que se mencionó anteriormente.

Complementando la mejora en la gestión de la infraestructura de red, debemos documentar todos los cambios que se van realizando a través del tiempo, en vista que existen partes que son removidas o actualizadas sin alterar el diseño planteado, es así que debemos contar con diagramas físicos de la red, los tipos de cable implementados junto con su longitud y características, la ubicación exacta de cada punto y equipo perteneciente a la red y la aplicación de normas internacionales para el cableado estructurado, como la norma TIA/EIA-606, cuyo objetivo es dar los lineamientos de administración y, consecuentemente, de identificación de un sistema de cableado estructurado, (de la Fuente, 2003).

Si bien hemos hablado de varios aspectos para mejorar nuestra infraestructura de red, ITIL nos abre el campo para establecer buenas práctica que mejorarán nuestra administración de las TI, “La gestión de servicios de TI es el instrumento mediante el cual un área puede empezar a adoptar una actitud proactiva en relación con la satisfacción de las necesidades de la organización, lo cual contribuye a evidenciar su participación en la generación de valor, (Cestari et al., n.d.), recordemos que todas las aplicaciones y servicios de negocio están soportadas por la infraestructura de TI, y al ser nuestro espacio de objeto, una institución de alcance nacional su infraestructura de red y comunicación se vuelve un factor crítico, es así que una adecuada gestión es de suma importancia para el nivel táctico y estratégico presente en la institución, las redes actualmente son tan complejas que su mantenimiento también depende de una buena planificación establecidas por buenas prácticas, y como mencionamos al ser un factor crítico dentro de la institución, los usuarios confían sumamente en la disponibilidad, integridad y seguridad que la red presenta, sea la comunicación o las aplicaciones propias desarrolladas, y se verán demasiado afectados si la red presenta limitaciones o intermitencias.

Uniendo todo lo anteriormente planteado es necesario implementar un ¿Cómo? se puede mejorar la administración y gestión que se realiza de la red, entendiendo diferentes conceptos y partiendo que la economía es el limitante principal, es necesario ahondar en un modelo como si esta institución fuese un negocio, es ahí donde se propone implementar un modelo de procesos en BPMN, que logre dar

soluciones a problemas futuros y determine los puntos claves para una mejor gestión de la red tanto física como lógica, innovando dentro del ámbito público.

2.3. Análisis comparativo

Para realizar un análisis comparativo se recoge 2 tópicos principales en los que se basa la presente investigación y los cuales estarán sumergidos en el modelado de BPMN, por un lado la gestión de la seguridad informática y por el otro la gestión de la seguridad de la información.

Tabla 1 *Análisis comparativo*

SEGURIDAD INFORMÁTICA	SEGURIDAD DE LA INFORMACIÓN
Gestión financiera:	
Vista desde la gestión financiera para brindar una seguridad informática es necesario siempre un aumento de recursos puesto que a mayor nivel de vanguardia tecnológica se presente existe un menor nivel de sectores vulnerables.	En este mismo aspecto dentro de la seguridad de la información no siempre se requiere aumento de inversión para implementar políticas que ayuden a plasmar una cultura que permita la seguridad de la información.
Los recursos económicos que se asignan a la seguridad informática siempre llegan a ser cortos puesto que se requiere una innovación continua	Los recursos asignados para seguridad de la información pueden ser más pequeños y duraderos puesto que esto se basa también en el accionar de los usuarios.

SEGURIDAD INFORMÁTICA	SEGURIDAD DE LA INFORMACIÓN
Implementación:	
Se limita la implementación de todas las normas de seguridad a la calidad y cantidad de equipos que se posea	La implementación en este aspecto no siempre está limitada a los equipos depende más de cómo estos se controlan y supervisan.
Toma de decisiones:	
Siempre se verá afectado y en menor impacto dentro de la toma de decisiones aun siendo un riesgo es aceptado comúnmente por los directivos.	Es mucho más importante que la seguridad informática en sí, aun al ir de la mano con esta, es mucho más importante porque la información de una empresa es lo más importante ya sea de cualquier naturaleza.
Modelado en BPMN	
En ocasiones dentro del modelado se debe omitir ciertos procesos para salvaguardar la información	No se podría omitir procesos críticos, puesto que la información quedaría expuesta.

2.4. Análisis crítico

La presente investigación se orienta en un modelado de procesos en BPMN que permite una simulación del funcionamiento de los mismos, y si bien no se aplica como procesos dentro de un negocio que presenta una rentabilidad,

mejorará la forma de gestionar la red, desde su concepción hasta los servicios finales que ofrecen.

Se puede comparar un factor de renta económica que ofrece un negocio común, con el aumento de calidad de los servicios que entregaría la FAE con un mejoramiento de la gestión de su infraestructura de red, así como el ahorro de inversión en capital que no sea prioritario, es entonces una ventaja muy particular el tratar una empresa que no ofrece una rentabilidad como un negocio común para poder mejorar en todos los ámbitos.

Si bien la economía es un factor limitante, los diferentes caminos dentro de una buena gestión, tanto en la parte del hardware que requiere muchas veces una inversión grande de capital, como la parte de software que se basa en el ingenio con el que se maneja el hardware, permitirán una innovación continua, que junto con una supervisión efectiva permitan que la tecnología no se estanque y permita el soporte tecnológico en todos los ámbitos.

No se puede abarcar todos los ámbitos en los que una red de datos tiene un impacto, en razón que constantemente siguen apareciendo nuevos requerimientos que incluso son atípicos si se basan en estadísticas predictivas, pero el hecho de que se cuente con bases sólidas para la gestión de la misma logra que se mantenga siempre controlados estos eventos, se podría decir que se logra una estandarización de cómo resolver los problemas oportunamente emitiendo soluciones anticipadas.

Pero se podría decir que al aplicar nuevas estrategias es mejor crear propias políticas y estándares, sin embargo viéndolo desde un lado rentable como se mencionó anteriormente, es un concepto alejado de la realidad pretender crear nuevas políticas y estándares, que ciertamente no se pretende una copia de estos pero facilitan mucho una gran mejora de la gestión de una infraestructura de red.

Por último el tiempo siempre será una carta en contra de cualquier innovación puesto que las ideas así como la tecnología que las acompaña crecen a pasos agigantados pero que mejor reto que fusionar el pasado con un futuro incierto que en este caso hablando de tecnología, se refiere a hardware casi obsoleto con software vanguardista o viceversa, los cuales se hacen funcionales gracias a una gestión apropiada y la toma de decisiones oportunas de los directivos.

Capítulo III

Marco Referencial

3.1. Reseña histórica

La Fuerza Aérea Ecuatoriana (FAE), forma parte de las Fuerzas Armadas del Ecuador. Su historia data de 1912 pero fue oficialmente constituida el 27 de octubre de 1920, ubicada desde sus inicios en el sector norte de la ciudad de Quito en la parroquia de Cotocollao, con la creación de la primera escuela de aviación militar, tras su camino ha logrado un desarrollo institucional notable que llegó a ser en sus inicios una de las pocas fuerzas aéreas en América del Sur, además una de las pocas que ha desarrollado combate con otros países (Perú 1981 y 1995), pero también ha enfrentado a conflictos internos en los que ha participado activamente.

Mediante Decreto Ejecutivo Nro. 2091 de diciembre 31 de 1943, el presidente constitucional de la República, Carlos Alberto Arroyo del Río, creó la Comandancia General de Aeronáutica y en su artículo primero dispone que la Fuerza Aérea dependerá directamente del Ministerio de Defensa Nacional, quedando por consiguiente modificada la Ley Orgánica de las Fuerzas Armadas.

La Ley Orgánica de las Fuerzas Armadas, que se expidió en la administración del presidente de la República Dr. José María Velasco Ibarra y se publicó en el Registro Oficial N.272, de agosto 28 de 1944, aporta la información fundamental para determinar fechas y precisar el marco legal en que se sustentará la

conformación de la Fuerza Aérea Ecuatoriana, como una de las ramas de las Fuerzas Armadas, sin relación de dependencia de la Fuerza Terrestre.

En la misma ley se consagra la iniciación de la Fuerza Aérea, con su naturaleza jurídica y organizaciones propias dentro de las Fuerzas Armadas, al tenor de los artículos 1, 3, 9, 12, 14 y 16 que constituyen el andamiaje jurídico y basamento de conformación de la Fuerza Aérea como una de las ramas de las Fuerzas Armadas. (Plan Estratégico Institucional de Defensa, 2017)

En el año 2018 mediante acuerdo del Ministerio de Defensa Nacional se expide el Estatuto Orgánico de Gestión Organizacional por Procesos del Comando Conjunto de las Fuerzas y con diferente acuerdo ministerial se expide el ESTATUTO ORGÁNICO DE GESTIÓN ORGANIZACIONAL POR PROCESOS DE LA FUERZA AÉREA ECUATORIANA como órgano subordinado al Comando Conjunto.

3.2. Filosofía organizacional

Del Direccionamiento Estratégico

La Fuerza Aérea Ecuatoriana se alinea con la misión y define su estructura institucional, sustentada en su base legal y direccionamiento estratégico, determinadas en la matriz de competencias y modelo de gestión de la Defensa.

Misión

"Desarrollar la capacidad militar aeroespacial, que garantice la defensa de la soberanía e integridad territorial; y, apoyar con su contingente al desarrollo nacional y a la seguridad pública y del Estado."

Visión

"Ser una Fuerza Aérea disuasiva, respetada y aceptada por la sociedad; pionera en el desarrollo aeroespacial nacional."

3.3. Diseño organizacional.

Estructura organizacional de gestión por procesos

Procesos Institucionales

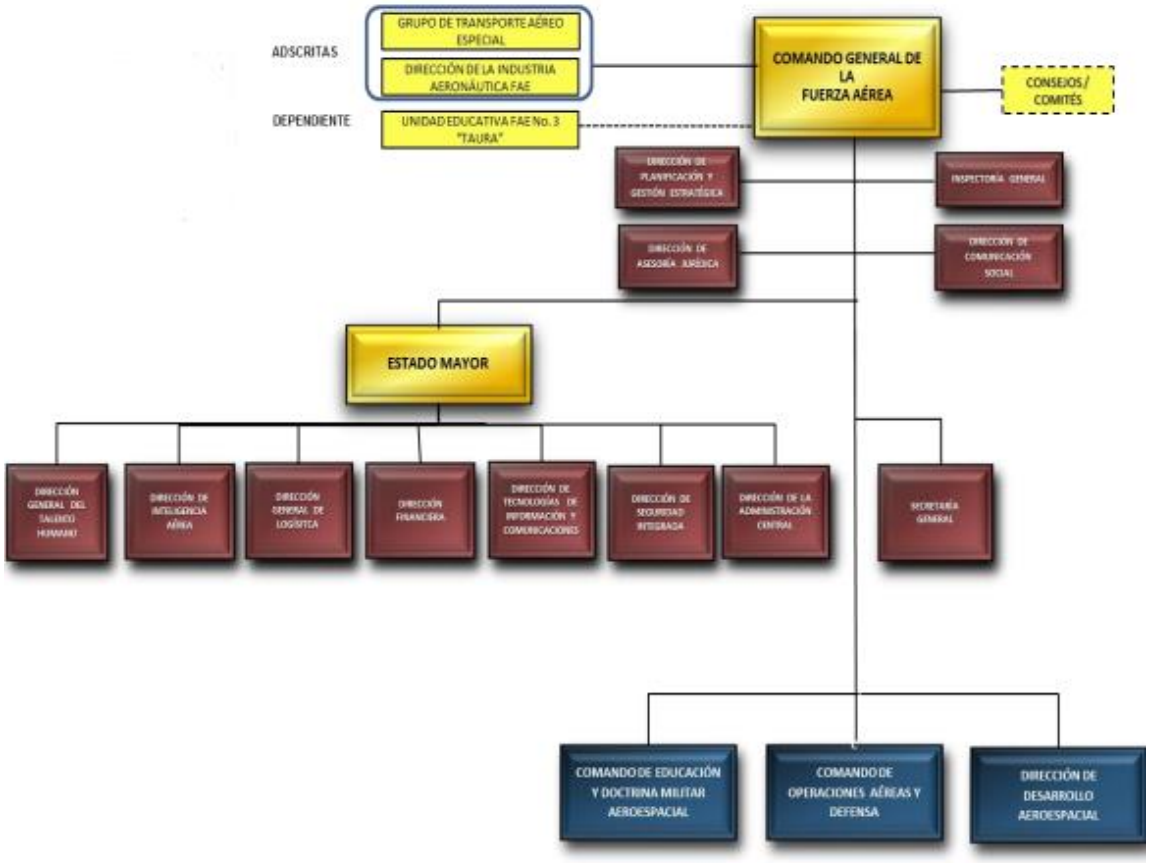
Para cumplir con la misión de la Fuerza Aérea Ecuatoriana determinada en su planificación estratégica y modelo de gestión, se gestionarán los siguientes procesos en la estructura institucional:

Gobernantes.- Son aquellos procesos que proporcionan directrices, políticas y planes estratégicos, para la dirección y control de la Fuerza Aérea Ecuatoriana.

Sustantivos.- Son aquellos procesos que realizan las actividades esenciales para proveer de los servicios y productos que se ofrece a sus clientes y/o usuarios, los mismos que se enfocan a cumplir la misión de la Fuerza Aérea Ecuatoriana.

Adjetivos.- Son aquellos procesos que proporcionan productos o servicios a los procesos gobernantes y sustantivos, se clasifican en procesos adjetivos de asesoría y de apoyo.

Fig. 1 Estructura Orgánica de Nivel Central



Fuente: Estatuto orgánico de gestión organizacional por procesos de la Fuerza Aérea Ecuatoriana.

La Estructura Institucional de La Fuerza Aérea Ecuatoriana antes detallada se ha establecido para el cumplimiento de sus competencias, atribuciones, misión y visión y gestión de sus procesos.

Estructura Descriptiva.- Para la descripción de la estructura definida para la Fuerza Aérea Ecuatoriana, se establece la misión, atribuciones y

responsabilidades; así como los entregables de sus distintos procesos internos, en este trabajo de investigación nos centraremos en el nivel de apoyo directamente en la Dirección de Tecnologías de la Información y Comunicaciones, encargada de la gestión de las TI en apoyo al cumplimiento de la misión de la FAE.

Y la misión de la Dirección de Tecnologías de Información y Comunicaciones es: Gestionar el empleo de Tecnologías de Información y Comunicaciones permanentemente con seguridad, mediante su desarrollo, implementación, administración y mantenimiento; a fin de contribuir al direccionamiento estratégico, desarrollo de capacidades aéreas y apoyo al desarrollo nacional.

3.4. Productos y/o servicios.

La dirección de Tecnologías de Información y Comunicaciones tiene como servicios los siguientes:

- Dirigir la automatización e integración de los sistemas de tecnologías de la información y comunicaciones (TIC´S) de conformidad a las normas legales y técnicas inherentes a las operaciones y procesos administrativos;
- Gestionar las directrices, lineamientos, procedimientos, planes de continuidad e instructivos internos para el equipamiento en hardware y software, uso y mantenimiento de los sistemas de información, comunicaciones y seguridad para el fortalecimiento del sistema de tecnologías de la información y comunicación.
- Gestionar los requerimientos en la institución de las TIC´S;

- Dirigir y coordinar el cumplimiento de normas internas y manuales técnicos para la administración del sistema de tecnologías de la información y comunicación;
- Gestionar los proyectos de las TIC´S de conformidad a la planificación institucional;
- Planificar y gestionar la infraestructura relacionada con las TIC´S;
- Gestionar la integridad, disponibilidad y seguridad de la información, garantizando la efectiva operación de los sistemas de información y comunicaciones;
- Supervisar el cumplimiento de los procedimientos de seguridad de la información.
- Dirigir la elaboración del Plan Integral de TIC'S; y,
- Supervisar la aplicación de las políticas, normas y regulaciones relacionadas con la ciberdefensa.

Entregables (Productos):

- Directivas, regulaciones, procedimientos, e instructivos en el ámbito de las TIC'S.
- Plan de contingencia de tecnologías de la información y comunicaciones.
- Sistemas y aplicaciones informáticos para interoperar con sistemas gubernamentales.
- Proyectos de innovación, modernización y renovación del sistema de tecnologías de la información y comunicaciones.
- Informes de análisis de factibilidad y vulnerabilidades de las TIC'S.

- Manuales técnicos y procedimientos de operación y mantenimiento.
- Informes técnicos y de seguridad de TIC´S.
- Plan de contingencia para asegurar la continuidad de funcionamiento de instalaciones, equipos, redes y servicios de tecnologías de la información; y
- Plan de mantenimiento de la infraestructura tecnológica.
- Informe de cumplimiento de procedimientos de seguridad de la información y la ciberdefensa.

3.5. Diagnóstico organizacional

Matriz FODA

"El análisis FODA consiste en realizar una evaluación de los factores fuertes y débiles que, en su conjunto, diagnostican la situación interna de una organización, así como su evaluación externa, es decir, las oportunidades y amenazas" (Talancón, 2007)

Tabla 2 *Oportunidades y amenazas de la organización.*

OPORTUNIDADES	AMENAZAS
Existe la apertura que brindan las organizaciones para realizar convenios que permitan las capacitaciones y transferencias de conocimiento para las nuevas tecnologías de la información.	La recesión económica de impacto directo en las instituciones públicas provocada por la pandemia mundial del COVID-19, se presenta la obsolescencia tecnológica debido al continuo y acelerado avance de la misma.

OPORTUNIDADES	AMENAZAS
Se dispone de centros de capacitación propios que permiten disponer de profesionales actualizados.	Las guerras no convencionales que buscan vulnerar la seguridad informática y robar la información, además los accesos que se autoriza al personal (usuario final) llegan a constituir un peligro para la seguridad de la información
Como parte del sector de la defensa nacional, es una institución con experiencia histórica que se preserva en el tiempo y aceptación en la sociedad.	El avance constante de la tecnología y los incrementos en sus precios de equipos y sistemas nos restringe a mantenernos a la par con la tecnología.

Tabla 3 *Comparativo FODA*

FORTALEZAS	FORTALEZA VS OPORTUNIDAD	FORTALEZA VS AMENAZA
Se cuenta con una buena cultura organizacional que genera el compromiso del	Aprovechar el compromiso del personal para que las instituciones de convenio actualicen los	Fomentar la creación de proyectos de TI con el mínimo de recursos o a través de la autogestión.

FORTALEZAS	FORTALEZA VS OPORTUNIDAD	FORTALEZA VS AMENAZA
personal con la institución Se ha establecido un buen plan de carrera profesional del personal militar de la Fuerza Aérea. Cuenta con instalaciones adecuadas para la implementación de tecnologías actuales requeridos	conocimientos del personal. Aplicar el plan de carrera de manera eficiente para generar capacitación interna. Fomentar que organizaciones a la vanguardia tecnológica se interesen por las TI del sector defensa.	Aprovechar el capital humano interno fomentando la aplicación de su intelecto para el desarrollo de la tecnología. Implementar sistemas de seguridad informática acordes a la tecnología usadas por posibles enemigos externos. Elaborar un cronograma de rotación que no disminuya la capacidad operativa en las TIC.
DEBILIDADES	**DEBILIDAD VS OPORTUNIDAD**	**DEBILIDAD VS AMENAZA**
Las TIC dentro de la institución no han	Aprovechar la comunicación presente	Establecer políticas que permitan sobresalir a las

FORTALEZAS	FORTALEZA VS OPORTUNIDAD	FORTALEZA VS AMENAZA
generado una notable importancia para su actualización continua.	con otras instituciones para implementar planes que permitan sobresalir a las TI sobre otras tecnologías.	TI con un costo mínimo o con el empleo de estándares internacionales.
El personal técnico de las TIC rota constantemente sin la debida planificación de la transferencia de conocimiento	Planificar un eficiente cronograma de rotación que permita la eficiente transferencia de conocimientos.	Establecer un periodo considerable para que el personal capacitado sea un soporte fundamental en las TIC y evitar que el personal se convierta en indispensable.
Deficiente distribución económica de los recursos asignados para la implementación y actualización de las TI.	Destacar más el uso de las TI dentro de la sociedad a fin de elevar una imagen como Fuerza Aérea acorde a la vanguardia tecnológica.	Fomentar el uso de tecnología de vanguardia a niveles superiores del mando institucional para garantizar la disponibilidad, confiabilidad e integridad

FORTALEZAS	FORTALEZA VS OPORTUNIDAD	FORTALEZA VS AMENAZA
		de los sistemas de información.

De lo que se puede analizar en la matriz FODA es que tanto las debilidades y amenazas presentes son un problema para la correcta administración de las TIC dentro de la organización, en este caso la Fuerza Aérea Ecuatoriana; en tal virtud, se debería aprovechar las estrategias planteadas para superar esta deficiencia que existe en la actualidad. Realizar una adecuada planificación permitirá desarrollar mucho más las estrategias planteadas a fin de convertirlas en un buen aporte para la administración de las TIC, más aún en un escenario cambiante que exige una tecnología vanguardista, las amenazas representan un riesgo inminente, puesto que el escenario en guerras no convencionales que se desarrollan en el ámbito del ciberespacio en estos tiempos ha causado pérdidas irreparables de información, con un costo muy alto así en incluso fracturas irreparables.

Siendo las amenazas factores externos que en muchas de las ocasiones son incontrolables como la pandemia del COVID-19, es necesario robustecer las políticas de gestión de las TIC para establecer planes de contingencia que permitan el correcto funcionamiento de las organizaciones aun sin la supervisión constante del personal inmerso en esto.

Por otro lado dentro de las oportunidades se puede destacar la experiencia y años que ha estado activa la institución, al ser una institución pública, dispone de una excelente infraestructura y personal calificado, actualmente su principal fortaleza recae en disponer de una buena cultura organizacional que permite la administración central a través de procesos establecidos en un estatuto debidamente legalizado, además que cuenta con un prestigio local y nacional.

Las oportunidades que presenta la institución deben ser explotadas al máximo, la falta de recursos podrían ser solventados con la autogestión que permita el crecimiento de la institución, es decir al pertenecer al sector de la defensa, se debe realizar convenios interinstitucionales que para aplicar cambios tecnológicos a un menor costo y no caer siempre en la obsolescencia tecnológica, debido a que actualmente se enfrenta a instituciones con tecnología de punta, además una estrategia que se debe fortalecer, es plantear mejores políticas institucionales enfocadas en la tecnología sin que exista el conflicto de intereses.

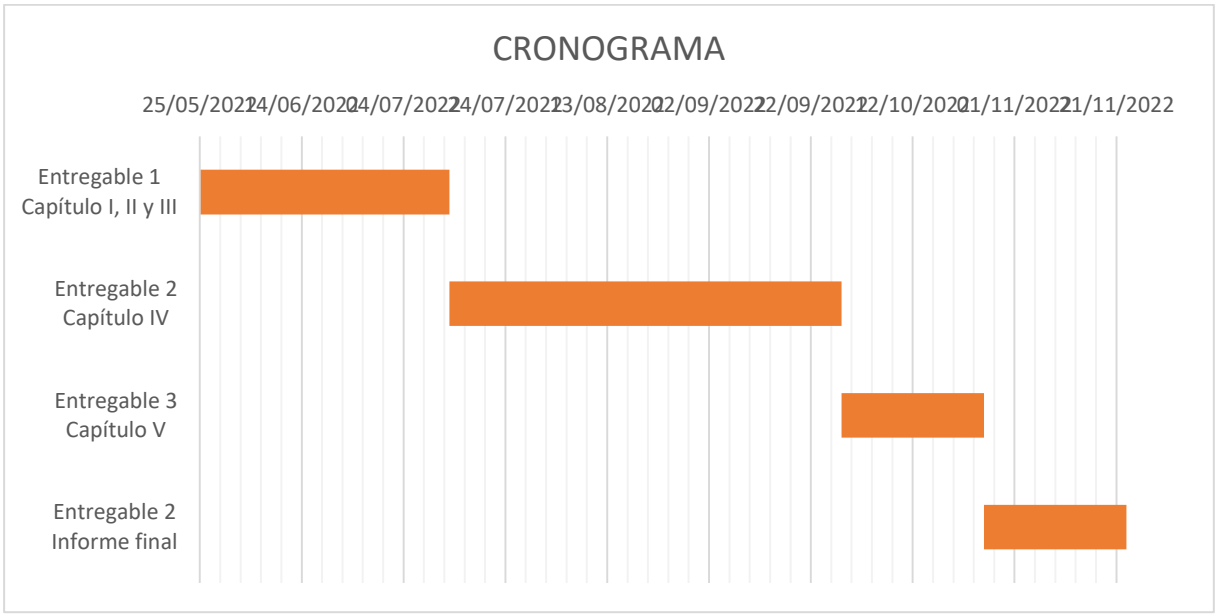
Aprovechar las oportunidades abre una brecha grande al éxito de cualquier institución, más aún si se cuenta con centros de capacitación propios en los cuales la experimentación debe ser una de las aristas que apuntale los cambios tecnológicos, puesto que si bien una inversión en equipos es primordial lo es más contar con personal certificado que pueda propagar conocimientos tecnológicos.

Luego del Análisis FODA, con la finalidad de controlar y minimizar las amenazas presentes, se deben aplicar estrategias enfocadas en potenciar las oportunidades planteadas y fortalezas aprovechando el compromiso del personal con la

institución, lo que genera un sentido de pertenencia para alcanzar los objetivos propuestos, sumado a esto las diferentes capacitaciones logran un alto conocimiento tecnológico y experticia, que al ser debidamente administrado se traduce en la transferencia de conocimientos técnicos que permitan un correcto funcionamiento de los distintos sistemas soportados por las TIC, multiplicando así tanto oportunidades y fortalezas, logrando con esto, no depender estrictamente del recurso económico; además el mejoramiento de políticas ya establecidas para que estas sean claras logrará una correcta administración de las TIC, ya sea en situaciones normales así como en situaciones adversas, estableciendo puntos críticos de afección lo que fomentaría el uso de tecnología de vanguardia para demostrar así a los niveles superiores como lo es el mando institucional los beneficios de las TIC que actualmente prestan, a fin de que la inversión en tecnología se mantenga en el tiempo pudiendo ser escalable evitando inconvenientes por la rápida obsolescencia o por problemas de incompatibilidad y más aún si estas TIC apoyan directamente a la consecución de los objetivos institucionales.

El mejoramiento continuo tanto de políticas como estrategias que se han obtenido del análisis FODA debe ser evaluado periódicamente puesto que un mundo tecnológico dinámico exige siempre una constante actualización, para que tanto personal material y equipo converjan para afrontar nuevas amenazas, impedir debilidades y multiplicar oportunidades que apuntalen fortalezas.

Diagrama Gantt



Capitulo IV

Resultados

4.1. Marco metodológico

De acuerdo con la naturaleza del presente trabajo esta investigación será de tipo aplicada descriptiva con un enfoque mixto tanto en el aspecto cuantitativo como cualitativo (Sampieri, 2000). Siendo de tipo exploratorio dado que busca descubrir mediante los conocimientos adquiridos tanto procesos como políticas que permitan el crecimiento y fortalecimiento de la red como protagonista principal de las TIC dentro de la FAE. Con un enfoque mixto se analizará tanto los datos cuantitativos como números de equipos, así como históricos de inversión y del lado cualitativo las políticas vigentes que necesiten ser cambiadas para mejorar los procesos de administración de la red que es la parte importante de las TIC.

Además, se realizó un análisis de toda la infraestructura de red de la Fuerza Aérea Ecuatoriana usando metodologías de Hacking Ético que fueron proporcionadas por el Comando de Ciberdefensa de Fuerzas Armadas, mismas que se dividen en:

- Defensa
- Exploración
- Respuesta

El análisis de vulnerabilidades será interpretado por el departamento de Tecnologías de la Información y Comunicaciones y serán presentados en reportes.

Para la presentación de resultados, se aplicaron entrevistas al personal del departamento TIC y a personal externo del departamento que vendrían a representar a clientes externos, buscando identificar aspectos relacionados con buenas prácticas empresariales y dominio en determinadas áreas asociadas a la gestión de la información.

Para el desarrollo de la propuesta, se usaron gráficos de pastel, de acuerdo con las herramientas utilizadas, se tiene lo siguiente:

Revisión de archivo documental: Revisión de la información obtenida del análisis de vulnerabilidades como marco de referencia, obtenido directamente de los archivos de la FAE.

Entrevistas: se realizaron entrevistas abiertas al personal militar responsable de los procesos internos que garantizan la continuidad de los servicios a través de la red, se enfocaron las preguntas a diagnosticar vulnerabilidades, necesidades y características que posee la infraestructura de red.

La población de estudio corresponde a los administradores de la red siempre en un número impar para no tener datos parejos y mejorar la toma de decisiones y los principales usuarios que están ligados a la red:

- 27 Administradores de la RED
- 07 usuarios principales

Para la selección de la muestra de usuarios principales se realizó una selección a conveniencia de acuerdo a la disponibilidad de información y voluntad de participación en el estudio.

La población de estudio se la realizará al personal de la fuerza aérea ecuatoriana para cumplir con los objetivos planteados tomamos una muestra probabilística conformada por:

- Usuarios externos personal fuera del
- Integrantes del departamento tic de la FAE

Para seleccionar a los usuarios externos se lo hace a conveniencia tomando en cuenta la disponibilidad del personal y de existir voluntad de participación

4.2. Diagnóstico

El diagnóstico de la infraestructura de red de la Fuerza Aérea Ecuatoriana se analizó las siguientes dimensiones:

4.2.1. Gestión de los servicios críticos de la FAE

La actividad principal de la fuerza aérea ecuatoriana es la de brindar el apoyo a la misión de fuerzas armadas adoptando las nuevas tecnologías que puedan satisfacer la demanda actual que exige la defensa nacional es así que la funcionalidad de los servicios deberían estar disponibles las 24 horas los 7 días dela semana

Al pertenecer al sector de la defensa nacional la integridad de los datos que maneja la FAE a nivel nacional depende de la buena gestión de la seguridad de la información que debe seguir de acuerdo a normas de internacionales y militares

4.2.2. Identificación de riesgos dos puntos áreas vulnerables de la FAE

A través de la identificación de los riesgos de los servicios críticos de la FAE podemos considerar el impacto que ocasionaría un evento en el que se impida el funcionamiento operativo de la red representando pérdidas de información y en especial vulnerabilidad a la información calificada

Actualmente los departamentos de TIC de la FAE integran la mayoría de servicios que utilizan información militar, el riesgo de seguridad informática y la falta de normas y o políticas claras compromete las áreas de la organización en especial aquellas que disponen de información de la defensa nacional

4.2.3. Entrevistas

Tabla 4 *Procedimiento de recolección de información*

Técnicas	**Procedimiento** ¿Cuándo? Segunda semana de julio de 2022
	¿Cómo? Se realizaron entrevistas al personal del departamento TIC (2 técnicos) También se entrevistó a 3 clientes externos
Entrevista	¿Dónde? En las instalaciones de la Fuerza Aérea Ecuatoriana
	¿Cuándo? Tercera semana de julio de 2022

4.2.3.1. Análisis de las entrevistas

En lo que respecta a la información que atraviesa la infraestructura de red y considerando las expectativas del personal que hace uso de las TIC y los servicios de información, se tiene lo siguiente:

En la primera pregunta se considera la posibilidad de haber recibido ataques cibernéticos de cualquier índole por parte de terceros, los entrevistados pertenecientes al personal del departamento TIC al igual que los clientes señalan que dichos ataques, no han sido frecuentes en los últimos años sin embargo empresas qué son consideradas públicas han tenido ataques continuos en el presente año, lo cual es sumamente negativo debido a que manejan políticas similares de seguridad, en algunos casos se ha visto comprometido todo el sistema de la empresa obligando a detener actividades operativas y administrativas disminuyendo la eficiencia en el cumplimiento de las operaciones, un diseño ineficiente de infraestructura de red colapsa los servicios cuándo se presenta demasiados usuarios que buscan el mando y control de las operaciones.

El primer entrevistado perteneciente al departamento tic señaló:

“En los años que lleva perteneciendo al departamento tic de la FAE no ha sufrido ataques cibernéticos recurrentes, sin embargo se han creado los denominados ataques de denegación de servicios disminuyendo la realización de las actividades propias e inclusive la pérdida de información útil, haciendo que sea algo frustrante para el personal”.

En relación con la pregunta dos: los entrevistados coinciden en que, la situación de ataques cibernéticos se ha presentado al menos entre cuatro o cinco veces es decir un promedio bajo en consideración con el resto de empresas públicas que han sufrido diferentes ciberataques

En relación con la pregunta tres: Con esta pregunta se pretendió verificar si el personal externo conoce de la buena administración de la infraestructura de red sin embargo manifestaron total desconocimiento al respecto, técnico del departamento TIC señaló que actualmente la gestión de infraestructura de red no tiene una política clara ni estandarizada

Un entrevistado del departamento tic añadió que “han existido anteriormente proyectos por mejorar infraestructura de red y aumentar la seguridad de la misma basados en las sugerencias que han recibido del personal de la parte operativa, considerando que los técnicos de bajo nivel son los que reciben directamente las quejas por corte de los servicios de la red, sin embargo hasta el momento no se han implementado nuevos proyectos ni innovaciones”

La pregunta destinada al personal del departamento tic fue la número 4, sobre sí consideraban una marca en específico para mantener la infraestructura de red considerando además la seguridad

Un entrevistado del departamento tic mencionó “En lo personal considero que las marcas dentro del primer cuadrante de Gardner desempeñan muy bien las necesidades que busca mantener la Fuerza Aérea Ecuatoriana pero todo debe ir acompañado de buenas prácticas y políticas establecidas”

En relación a la pregunta 5: En esta pregunta se buscó identificar la percepción que tienen los entrevistados sobre la calidad de la actual tecnología usada en la infraestructura de red con la que cuenta la FAE, varios coincidieron en que los servicios informáticos prestados son buenos, sin embargo son limitados cuando existe un alto tráfico de usuarios lo que reduce la operatividad de las actividades

En relación a la pregunta 6, en la que sugiere una posibilidad de aumentar la calidad de los servicios a través del cambio de topología de red sea física y lógica, ante esto se manifestó que debe ser imprescindible estar a la par de las nuevas tecnologías y no considerar únicamente las topologías típicas presentes.

Un entrevistado del departamento TIC manifestó que un mejor sistema de infraestructura de red haría que el tráfico de usuario sea más fluido.

En relación a la pregunta 7: se cuestionó de manera general si la existencia de problemas en la red es común o se da en casos específicos, ante lo cual los clientes externos e internos del departamento TIC, señalaron qué es algo habitual cuándo hay horas pico de trabajo, en tal virtud es imprescindible mejorar la calidad de la red.

Siguiendo con esta pregunta la número ocho planteaba evaluar la calidad de los servicios en términos generales que presta la Fuerza Aérea a todo su personal civil o militar, en consenso la respuesta fue que pese a los fallos de los servicios, la calidad es buena, en vista que los sistemas informáticos que atraviesan la red facilita muchas de las actividades operativas y administrativas que demanda las actividades de defensa

Un entrevistado mencionó “pese a las caídas de servicio o tráfico común que se experimenta en la red los servicios informáticos siempre están facilitando los trabajos y mejorando la calidad de la información”

Además se consideró la pregunta 9 para cuestionar la percepción de los entrevistados acerca de la calidad del servicio de internet brindado por la empresa, se evidenció, que existe una conformidad con el servicio, en términos generales es rápido y de buena calidad pero volvieron a manifestar que existe un alto número de tráfico de usuarios que comúnmente afectan al servicio, aunque no es común un cliente agregó “la Fuerza Aérea cuenta con internet de alta velocidad y tiene una alta disponibilidad a excepción de situaciones relacionadas con propias actividades de la empresa proveedora o con la seguridad para solventar necesidades”.

Finalmente la pregunta 10 quedó abierta a recibir sugerencias por parte de los entrevistados para poder mejorar los servicios prestados

Una mención consideraba que se debe plantear un mejor sistema de seguridad que permita optimizar las actividades, pero que no disminuya el flujo que se mantiene a través de la red, además también sugirió que todo el personal debería conocer las principales vulnerabilidades.

4.3. Propuesta de mejora

Para mejorar los procesos de la FAE se analizará la gestión de la seguridad de la información para establecer las estrategias del proceso de gestión de infraestructura de red.

4.3.1. Gestión de la seguridad de la información

La implementación de las normas ISO representan mejoras en la gestión de seguridad respecto a las ares vulnerables identificadas, además se dispone de las buenas prácticas y control de seguridad para cada activo informático del objeto de estudio, como por ejemplo:

- Se deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldos adecuada.
- Los procedimientos de operación se deben documentar, mantener y estar disponibles para todos los usuarios que los necesiten.

- Se deben identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no divulgación que reflejan las necesidades de la organización para la protección de la información.

- Las funciones y las áreas de responsabilidad se deben distribuir para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de los activos de información.

- Se deben establecer procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información contra divulgación no autorizada o uso inadecuado.

Para realizar copias de respaldo, siempre el departamento TIC será responsable de esta actividad hasta las últimas dos copias de respaldo de información, esto con el fin de prevenir una pérdida de información ante un colapso del sistema o hackeo de la información esencial de la empresa, es así que a través de la implementación archivística del sistema de gestión documental Chasqui de Fuerzas Armadas, se guarda automáticamente por cada documento su respectiva copia de seguridad. Mencionado sistema se somete a pruebas con regularidad para evaluar su estado.

Cumpliendo con el esquema gubernamental de seguridad de la información, el oficial de seguridad de la información, debe establecer la norma de seguridad informática referente al compromiso del personal militar y civil en mantener la confidencialidad de la información inherente a cualquier tipo de actividad realizada como empresa pública del estado, así como el uso responsable de la información disponible en apoyo a los objetivos organizacionales.

La Fuerza Aérea Ecuatoriana deberá diseñar una guía de implementación para un sistema de gestión de seguridad, que contenga los siguientes pasos:

1. Definir el alcance y política del sistema de gestión de seguridad informática con base en el esquema gubernamental de seguridad de la información (EGSI), para lo cual definirá los procesos respectivos y sus responsables directos.

2. Identificar de manera concreta la estructura de la organización y los sistemas de gestión implementados.

3. Realizar una evaluación de riesgos que identifique vulnerabilidades y proponga mecanismos de control.

4. Generar la documentación necesaria que permita el análisis y aprobación de la directiva.

4.3.2. Planteamiento de estrategias de gestión de la infraestructura de red.

Los diferentes departamentos de toda organización deben comunicarse de manera efectiva entre el cliente y el conjunto de servidores que proporcionan los diferentes sistemas y servicios informáticos, con un sistema de gestión de red óptimo se debe priorizar la seguridad en la misma, y en especial al ser la Fuerza Aérea Ecuatoriana una organización pública del sector de defensa nacional las redes deben estar diseñadas para abarcar todos los problemas de seguridad que puedan existir para garantizar que la comunicación y la información que atraviesa la red sea segura y confiable.

Importante también es contar con un sistema de gestión de red, esta herramienta permitirá mantener en buen estado la red en general de cualquier organización o los grupos de redes que puedan existir, es así que el personal encargado de la administración de la red debe implementar estrategias efectivas que permitan mantener una escalabilidad de la red de una manera centralizada,

considerando los puntos clave que hemos mencionado el registro fiable de la información y las diferentes comunicaciones a través de la red.

4.3.2.1. Diseño de red

El diseño de una red debe ser elaborado cuidadosamente, que permita un rendimiento continuo entre las conexiones establecidas, el diseño que se proponga representa una parte fundamental en el éxito de la comunicación y transferencia de datos y medios, entre los servidores y el personal que hace uso de los sistemas, el diseño de una red además garantizará una conexión totalmente continua las 24 horas del día los 365 días del año, entregando así una red que permita la personal trabajar de manera eficiente y mejorar su desempeño. Estableciendo un buen diseño de red evitamos tener sistemas con servidores independientes

El diseño de la red es fundamental para el éxito de cualquier organización. La grabación, la comunicación, la transferencia de datos y medios en la red se realizan a diario, y el flujo debe mantenerse constantemente, ya que conecta a las personas que son importantes para nosotros. La comunicación se establece siempre que se envía la solicitud. Siempre hay un logro de conexión del 100 por ciento accesible 24 × 7 para mejorar el servicio al cliente. Una red debe diseñarse cuidadosamente para ofrecer un rendimiento constante en las conexiones que sean confiables y seguras. El diseño de la red ayuda a evitar muchos sistemas de servidores independientes para administrar una red más grande, para lo cual hemos planteado que un diseño de red deberá cumplir con los siguientes componentes:

- Capacidad de adaptarse a muchas redes para implementar nuevos servicios y conexiones sin tener que modificar la estructura vigente.
- Contar con la disponibilidad continua de la red, mediante la instalación de respaldo considerando posibles reemplazos en caso de falla y desconexión.
- Implementar la seguridad necesaria para establecer conexiones entre los sistemas y el personal como por ejemplo: firewalls internos y externos, niveles de autenticación, los que permitirán garantizar la integridad de la información.
- Capacitación calificada para los administradores de red, para que puedan actuar de manera eficiente ante cualquier imprevisto.

4.3.2.2. Topología de red: define la geometría de la red

Para cumplir con los componentes establecidos en el buen diseño de la red, se deberá establecer y elegir el marco geométrico de la red, es decir el diseño como tal de la red, que permita cumplir con las exigencias de la organización, considerando la flexibilidad y la gestión efectiva de los sistemas y servicios proporcionados por la organización, debido a que las Fuerzas Armadas ha implementado varios servicios como son el sistema de gestión documental Chasqui, para la comunicación oficial entre todas sus unidades la FAE requiere que las capas de red: principales, de distribución y acceso brinden un control adecuado con alta seguridad en el cual, cada segmento de la red se pueda administrar de manera efectiva y los posibles cambios en la jerarquía planteada, se puedan realizar de manera ágil y transparente para el usuario.

4.3.2.3. Gestión de red efectivo

Plantear estrategias permitirá que los administradores de red, solventen las fallas que pudieran suscitarse de manera inmediata, para lo cual planteamos:

- Infraestructura de Red

  El o los administradores de la red, establecerán la estrategia de analizar el equipamiento con la tecnología implementada, para establecer si actualmente se obtiene el control sobre la trasferencia de datos o si los sistemas críticos son o no accesibles bajo procesos de autenticación, y bajo este análisis se podrá hacer cambios al sistema central para cerrar brechas de seguridad.

- Tráfico de red

  Una vez analizado la infraestructura central, se debe priorizar las áreas críticas, lugares que demandarán mayor seguridad, diferentes accesos y/o permisos, para evitar al mínimo en estas áreas períodos de desconexión, como se dijo anteriormente el personal debe estar altamente capacitado para que junto a su asesoría técnica y experiencia, inclusive se pueda considerar sistemas de alimentación energética para las áreas que debemos priorizar y disminuir interrupciones a las zonas estratégicas.

- Visualizar la red

  Disponer de un motor de administración de red se debe considerar, para monitorear la red en tiempo real, la representación visual permitirá una mejor administración de los equipos activos de red, o implementar sistemas que vayan desde descubrimiento de dispositivos hasta la visibilidad del sistema, los flujos de tráfico y la gestión de riesgos.

4.3.2.4. Arquitectura de Red

Los Data Center implementados en varias organizaciones generalmente se han construido con una arquitectura de tres niveles; sin embargo, debido a la aparición de la virtualización y de sistemas hiperconvergentes, actualmente se ha desarrollado la arquitectura spine-leaf logrando superar algunas limitaciones de la arquitectura tradicional.

La arquitectura spine-leaf proporciona escalabilidad, fiabilidad y mayor rendimiento al contar con dos capas:

- La capa spine se forma por switches que se encargan de realizar el enrutamiento a manera de columna vertebral de la red
- La capa leaf implementa un switch de acceso que se conecta directamente a los servidores o dispositivos de almacenamiento.

Implementando este diseño cualquier servidor puede comunicarse con cualquier otro servidor usando no más de una ruta de switch de interconexión entre los switch de la capa leaf.

Considerando los sistemas y servicios de uso o implementados por la Fuerza Aérea Ecuatoriana se requiere que el tráfico de la red tenga un tiempo de respuesta eficiente y no pobre cuando existan muchos usuarios finales usando la red, en especial con la modernización de los centros de datos virtuales en dónde se han ubicado servidores de cómputo y almacenamiento en cualquier lugar de la organización.

Es imprescindible que los administradores de la red implementen la arquitectura de dos niveles, para que el Data Center de la organización pueda prosperar y satisfaga todas las necesidades demandadas por los usuarios finales.

4.3.2.5. Capacitación del Personal

El personal encargado de la red deberá estar capacitado en las diferentes áreas para el soporte tanto en la implementación de la nueva tecnología que mejore la gestión de la red de datos siendo asignados por la pericia que tengan en los diferentes niveles que se detallan a continuación:

Nivel 1(Aprendiz): Aprendizaje de las normas básicas que cumple el sistema, identificar posibles fallas, analizar posibles cambios de escalabilidad y revisión constante de vulnerabilidades.

Nivel 2(Técnico): Reparar fallas del sistema, realizar cambios de gestión y administración del sistema, implementar reglas y requerimientos, realizar cambios de escalabilidad y solventar las vulnerabilidades.

Nivel 3(Supervisión): Otorgar permisos a quienes administran la red, supervisar los cambios neurálgicos y solventar problemas tanto software como de hardware.

Todo el personal deberá cumplir con las certificaciones según su grado de pericia las mismas que serán otorgadas por la institución, así como apegarse al plan de carrera para solventar las necesidades que presente la red con una nueva tecnología.

4.4. Mecanismos de control. (Presente las métricas o indicadores para controlar las propuestas y actividades del 4.3.)

4.4.1. Métricas de Gestión

Tabla 5 *Métricas de la organización.*

Lineamiento	Medida Esperada	Medida encontrada	Observaciones
Estándares para unificar el acceso a los elementos de red	1 política de estandarización	0	No se encuentra establecido la forma de estandarizar los elementos de red
Recolección y almacenamiento local de las estadística de actividad de la red	12 informes al año de la estadística de la actividad de la red	2	Al momento sólo se mantiene información estadística de la red una vez cada semestre
Disponer de un centro de control de red	01 centro de control	0	La organización no dispone de un centro de control de red exclusivo
Sistema de gestión de red	01 sistema implementado	0	La organización no dispone de un sistema de gestión de red
Gestión de fallos	01 informe de fallos	01	Únicamente se registra en una bitácora los fallos que se presentan
Gestión de configuración	01 plan de configuración programada	0	Las configuraciones realizada a la red no son planificadas se presentan esporádicamente

Lineamiento	Medida Esperada	Medida encontrada	Observaciones
Gestión de calidad de funcionamiento	02 informes al año de la calidad de funcionamiento	0	La organización no genera información exacta de la calidad del funcionamiento
Gestión de seguridad	01 política de gestión de seguridad	0	No existen documentos que planteen políticas exclusivas de seguridad a la red

Con los lineamientos establecidos se deberán cumplir para obtener un sistema de gestión distribuido, en el que existan varios administradores de red con acceso limitado e implementar un centro de control de red con acceso global capaz de controlar todos los recursos de la red, obteniendo así beneficios como:

- Mantener la capacidad de respuesta centralizado
- Minimizar el tráfico de gestión
- Brinda mayor escalabilidad
- Se minimiza los fallos

4.5. Mecanismos de implementación

La Fuerza Aérea Ecuatoriana por ser una organización pública, plantea sus diferentes necesidades a través de los mecanismos y directrices establecidas por los ministerios

4.5.1. Plan Anual de Planificación PAP

Una vez realizado el estudio de mercado con las diferentes empresas tecnológica que sustentan, se solicita a través del gasto público el monto requerido, en el que se considerará que la propuesta de mejora tanto a nivel físico como lógico será considerado dentro del presupuesto de gasto no permanente sin proyecto de inversión en vista que es un gasto adecuado al año vigente.

4.5.2. Plan Anual de Inversiones PAI

A través de la formulación de un proyecto de inversión, la propuesta de mejora puede ser financiada, en donde se deberá sustentar la vigencia tecnológica del proyecto, los montos plurianuales que requiere el proyecto para mantenimiento y demás respaldos que garanticen un proyecto de inversión, además que de plantear dentro del PAI deberá sustentar el aporte y logro a los objetivos estratégicos de Fuerzas Armadas que actualmente comprende los años 2020 al 2030.

4.5.3. Otras fuentes de financiamiento

La parte tecnológica de la Fuerza Aérea Ecuatoriana, brinda un apoyo directo al cumplimiento de su misión, al pertenecer al sector de la defensa se crean coyunturas con otras organizaciones de sectores estratégicos y de interés nacional, es así que para garantizar la confidencialidad, confiabilidad e integridad de la información que se genera con las organizaciones mencionadas, éstas organizaciones a través de los recursos propios de su actividad financian los proyectos de interés y de relación directa con a la Fuerza Aérea Ecuatoriana, considerando que este mecanismo de financiamiento está establecido dentro del

catálogo de fuentes de financiamiento del Ministerio de Economía y Finanzas, en tal virtud este mecanismo sería el más viable para la propuesta de mejor.

Capítulo V

Sugerencias

5.1. Motivaciones para las sugerencias

La propuesta de mejora planteada puede abrir varios campos para que las instituciones públicas del sector defensa gestionen de mejor manera la infraestructura de red que disponen, en especial para garantizar los pilares fundamentales de la información, como es la confidencialidad, integridad y disponibilidad de la misma, actualmente una infraestructura de red debe ser considerada de gran importancia dentro de una organización a fin de cumplir con los objetivos propios de la empresa a través de todos los datos que fluyen por la red implementada.

Mediante la propuesta planteada, se podrá a futuro implementar una estandarización de conocimiento e infraestructura, que permita al personal militar involucrado desempeñar su mismo nivel de conocimiento en cualquier parte del país, en vista que constantemente se encuentra activa la rotación del personal.

5.2. Sugerencias de estudios complementarios

El deseo de modernizar una infraestructura puede significar cosas diferentes desde el punto de vista de varias personas, es decir no existen dos infraestructuras de red que han sido implementadas con el mismo objetivo; sin embargo, las nuevas infraestructuras son más similares de lo que se piensa, plantearemos algunas sugerencias que permitirán a las organizaciones actualizar la infraestructura de TI, considerando las últimas tecnologías o

herramientas a fin de que la propuesta de mejora planteada, permita abrir el campo de estudio para obtener mayor información de cómo gestionar la red de manera eficaz y eficiente ante el avance continuo de la tecnología y que la gerencia considere a las TI algo sumamente importante en las organizaciones.

Aspectos de la infraestructura moderna

Como primera parte se debe entender la manera en que las TI han evolucionado durante los últimos años o en la última década, anteriormente de manera general la infraestructura de red tenía una red LAN, una red WAN y un Data center privado con las seguridades necesarias, actualmente la infraestructura disponible se ha extendido más allá de los límites físicos de las organizaciones, los administradores de TI hoy en día analizan que una infraestructura más eficiente sería migrar los datos y otros servicios de TI a una o más nubes públicas utilizando un modelo de nube híbrida, además las infraestructuras modernas amplían la red para proporcionar los niveles necesarios de rendimiento, escalabilidad y agilidad que exigen las aplicaciones modernas implementadas o que se desean implementar.

Infraestructura actual evaluada

Es imperante evaluar todos los componentes actuales de LAN, WAN, internet y la nube, si lo que se requiere es tener una infraestructura moderna que pueda satisfacer las demandas actuales y futuras de la organización, generalmente puede primero evaluar las aplicaciones disponibles y posterior ir bajando de nivel hasta la red implementada detrás de los datos y aplicaciones finales.

Con una evaluación detallada de las aplicaciones o servicios críticos de la organización, de los datos y los flujos de red, podrá determinar que partes necesitan o pueden ganar rendimiento, además que se puede plantear una eficiencia de costos y un análisis de los servicios, aplicaciones o procesos que posiblemente podrán ser reemplazados con alternativas modernas que aporten mayor eficiencia.

Carencias de la infraestructura actual propia

Una vez evaluada la infraestructura actual podemos plantear si un nuevo hardware, software o mejores plataformas y servicios podrán reforzar el rendimiento de ciertas áreas de la organización e incrementar la eficiencia de costos.

Un breve ejemplo planteado, podemos decir que tras una evaluación se decide trasladar ciertos servicios y/o aplicaciones críticas para la organización de la intranet hacia una nube pública, para los empleados que trabajan desde casa; sin embargo, este cambio puede generar una brecha de seguridad, sugiriendo que se realice un estudio adicional de seguridad en la nube y mitigando la brecha reformulando las políticas de seguridad de TI existentes tanto en la nube como al usuario final, con el uso de herramientas modernas para proteger los datos sensibles y demás información reservada contra posibles pérdidas o robo.

5.3. Sugerencias de implementación

La propuesta de mejora sugiere primero establecer, hacia qué tipo de organización está destinada la implementación, de manera general dividimos a las organizaciones en dos grandes sectores, el sector privado y público, en ambos sectores dependerá del nivel de detalle de la evaluación que se realice a la infraestructura tecnológica, para así destacar el nivel de importancia.

Sector Privado

La implementación dependerá de los recursos propios de la empresa considerando la eficiencia de costos.

Sector Público

Las organizaciones públicas, planteas sus diferentes necesidades a través de los mecanismos y directrices establecidas por los ministerios, pudiendo destacar, el Plan Anual de Planificación (PAP), Plan Anual de Inversiones PAI, Otras fuentes de financiamiento de acuerdo al catálogo de fuentes de financiamiento.

5.3.1. Formular una versión de la modernización de la infraestructura

Como se mencionó anteriormente, no existen dos infraestructuras que sean construidas de manera igual debido a que cada empresa tiene planteados objetivos diferentes. Cuando se realice un rediseño de la infraestructura, los responsables de TI deberán entender la manera en que operarán los líderes de

las organizaciones en el futuro, a fin de mitigar imprevistos a grande escala como por ejemplo la pandemia de COVID-19.

Si la organización planea extender mucho más las políticas de teletrabajo, la infraestructura propia se deberá acoplar a que los empleados requieran de los servicios informáticos de la empresa desde cualquier parte geográfica en un futuro previsible, los Data centers podrían reducirse en favor de infraestructura basada en la nube pública, pero si se espera que oportunamente el trabajo sea completamente presencial al momento, un modelo de infraestructura de nube híbrida sería la opción más viable.

5.3.2. Calcular el costo de modernización

Tomando como base la visión de la organización, y la evaluación detallada de cómo debería ser la infraestructura moderna, es momento de plantear las opciones de hardware, software y servicios que podrían utilizarse para alcanzar los objetivos de la organización.

Al momento de calcular el costo de la modernización de la infraestructura, según la propuesta o basándose en estudios complementarios, no se debe limitar incluir gastos relacionados con la compra e implantación de tecnologías y servicios de vanguardia que se acoplen a la organización y estén dentro de la eficiencia de costos, además es importante incluir planes de mantenimiento continuo tanto preventivo como correctivo y la transferencia de conocimientos con el personal involucrado de las TI dentro de la organización.

Conclusiones

La mejora de la gestión de la red de datos de la Fuerza Aérea, permitirá que muchas instituciones estandaricen o implementen varias políticas planteadas, a fin que la red establecida pueda trabajar de manera mucho más funcional, además que permitirá una escalabilidad de tecnologías, se concluye que para un óptimo desempeño de las TIC dentro de una organización debemos contar con varios parámetros como son las políticas y equipamiento acorde a las necesidades.

Una vez que se determinan las necesidades críticas de la red, podemos concluir, que la seguridad de la información es un pilar fundamental dentro de cualquier empresa, es necesario realizar adaptaciones de la red funcional, para que esta cumpla no solo con políticas o protocolos internacionales de seguridad, sino también para que se adapte a los diferentes escenarios, que como sabemos en el ámbito de la seguridad cambian constantemente, siendo necesario explorar nuevas tecnologías que aporten a mantener una correcta gestión de la misma por eso se puede inferir que si bien la tecnología es global no siempre es necesario cambiar todo el aparataje de soporte, debido a que existen terminales que se los debe gestionar bajo políticas más estrictas para que funcionen con similitud a un equipo vanguardista.

Analizar la obsolescencia tecnológica de los puntos neuronales que conmutan toda la información, permitirán contar con políticas de actualización que no necesariamente demandarán de grandes recursos económicos, las funciones de estos puntos se encargan del tránsito en general, sin embargo al cambiar a una estructura vanguardista se podría reconsiderar que conexiones se podrían prescindir

y cuales estarían en otros nivel de prioridad, los recursos económicos no permiten una renovación de alto impacto dentro de la red, pero ya determinado el nuevo modelo a utilizarse para mejoramiento tanto de las políticas de gestión y el funcionamiento de la red, se podría gestionar los recursos de forma focalizada para realizar inversiones en tecnología vanguardista de forma puntual e inteligente, y permitir que la red se adapte a una escalabilidad de forma progresiva evitando totalmente la obsolescencia.

Al tener una red convencional el personal técnico entra en una zona de confort en el que se visualizan solo los errores comunes, y la actualización a redes de mejor desempeño requiere que la autoeducación, así como, las destrezas que se adquieran por medio del conocimiento impartido por expertos se apeguen a un plan de actualización de conocimientos y también cumplan con su difusión, en conclusión no solo disponer de recursos económicos o del mejor equipamiento permitirá una optima gestión de la red, el recurso humano responsable de las TIC deberá disponer de la capacitación adecuada que permita implementar más y mejores soluciones de las que se ha planteado para la red de datos.

BIBLIOGRAFÍA

Merchán, F., Bohórquez, D., (2019). Diseño para la renovación de una infraestructura de red LAN Aplicando el estándar CCNA – Cisco. https://repository.ucc.edu.co/bitstream/20.500.12494/11051/1/2019-infraestructura-Promotec-Colombia.pdf

Sampieri, H. (2000). Metodología de la Investigación. 6ta edicion.

Bedoya, V. H. (17 de JULIO de 2020). Espiritu Emprendedor TES. https://doi.org/10.33970/eetes.v4.n3.2020.207

Fuerza Aérea Ecuatoriana (2018). MANUAL DE INSTRUCCIÓN DE COMUNICACIONES

Vega, O. A. (2012). Efectos colaterales de la obsolescencia tecnológica. Revista Facultad de Ingeniería, UPTC, 32.

Peña, M. & Anías, C. (2019). Modelo para la gestión de infraestructuras de tecnologías de la información. https://doi.org/10.22430/22565337.1449

Kerravala, Z. (2014, Octubre). La infraestructura para sucursales de Cisco impulsa la WAN híbrida. https://www.cisco.com/c/dam/global/es_es/assets/pdf/en_06_zk_hybrid_wan_3 party_wp_pt e_cte_es.pdf

GESTIÓN | Definición de GESTIÓN por Oxford Dictionary en Lexico.com y también el significado de GESTIÓN. (n.d.). Retrieved April 2, 2022, from https://www.lexico.com/es/definicion/gestion

Beltrán Pardo, M., & Sevillano Jaén, F. (2013). Cloud Computing, tecnología y negocio. Ediciones Paraninfo, SA.

Trott, P. (2005), Innovation management and new product development, 3rd edition, Harlow, Pearson Education Limited, England.

González, M. (2021). GESTIÓN DE LA INFRAESTRUCTURA DE TI, http://www.ties.unam.mx/

Altamirano, C. A. V. (2003). Un modelo funcional para la administración de redes. línea]. Disponible: http://www. itescam. edu. mx/principal/sylabus/fpdb/recursos/r51037. DOC

Ladino, M. I., Villa, P. A., & López, A. M. (2011). Fundamentos de iso 27001 y su aplicación en las empresas. Scientia et technica, 17(47), 334-339.

Villaroel Salvatierra, J. (Marzo de 2011). Virtualización de Servidores. http://www.cb.udabol.edu.bo/cicc/archivos /villarroel.pdf

De la Fuente, J. (2003, July 13). Cableado estructurado: ¿De qué nos habla la Norma 606 A? | CanalAR. https://www.canal-ar.com.ar/Nota.asp?Id=294

Cestari, F., Alexandre, F., Motta, C., Dimmit, J., Piccolini, B., & Adaptada Al Ecuador, V. (n.d.). ITIL Information Technology Infrastructure Library. Retrieved April 2, 2022, from www.renata.edu.co

Plan Estratégico Institucional de Defensa. (2017). Elaborado por el Ministerio de Defensa Nacional

Estatuto Orgánico de Gestión Organizacional por Procesos del Comando Conjunto de las Fuerzas Armadas. (2018, Marzo) por Acuerdo Ministerial No. 049.

Estatuto Orgánico de Gestión Organizacional por Procesos de la Fuerza Aérea Ecuatoriana. (2018, Marzo) por Acuerdo Ministerial No. 052.

Talancón, H. P. (2007). La matriz foda: alternativa de diagnóstico y determinación de estrategias de intervención en diversas organizaciones. Enseñanza e investigación en psicología, 12(1), 113-130.

FORMATO DE ENTREVISTA

GUÍA DE ENTREVISTA
OBJETIVO: Determinar cómo se gestiona la red de datos de la FAE.
SUJETO DE ESTUDIO: Fuerza Aérea Ecuatoriana
TIPO DE ENTIDAD: Entidad pública sector de la Defensa
ENTREVISTADO:
CARGO QUE OCUPA:
ENTREVISTADOR: Jonathan Gamboa y Jefferson Gamboa
FECHA Y HORA DE LA ENTREVISTA:
1. ¿Considera haber recibido ataques cibernéticos de cualquier índole que afecten la gestión de la red actualmente?
2. Mencione cuantas veces se han realizado ataques a la red de datos de la FAE
3. ¿Conoce cómo se administra la red de datos de FAE y si está estandarizada bajo alguna norma?
4. ¿Se inclinaría por alguna marca específica para mejorar el funcionamiento de la red?
5. ¿Cuál es su percepción de la calidad de la actual tecnología usada en la infraestructura de red con la que cuenta la FAE?
6. ¿Considera que se debe trabajar con las topologías de redes convencionales o explorar nuevas tecnologías y por qué?
7. ¿La existencia de problemas en la red es común o se da en casos específicos?
8. Evalúe la calidad de los servicios en términos generales que presta la red de Fuerza Aérea en el parámetro de excelente, bueno o regular.

9. ¿Cómo considera la calidad de servicio de internet que se presta a través de la red?(excelente, buena, regular)
10. Escriba una sugerencia orientada a mejorar los servicios que se ofrece por la red.