FUERZA AÉREA DEL PERÚ
ESCUELA DE OFICIALES

TESIS

TÍTULO:

"USO DE INTERNET SATELITAL EN EL CONTROL CIBERESPACIAL EN DESTACAMENTOS REMOTOS DE LA FUERZA AÉREA DEL PERÚ EN EL AÑO 2025"

Línea De Investigación:

Gestión de Telecomunicaciones

PRESENTADO POR:

TEN FAP JENNY JANET SAONA GARCÍA

CÓDIGO ORCID: 0009-0009-0328-476X

ASESOR TEMÁTICO: COR. FAP (R) MARCO ANTONIO FELIPE MORI

ASESOR METODOLÓGICO: MAG. SONIA ESPINOZA FARÍAS

PARA OPTAR EL TITULO PROFESIONAL DE LICENCIADO
EN CIENCIAS AEROESPACIALES

LIMA - 2025

Dedicatoria

Este trabajo de investigación lo dedico a Dios, a mis padres y a mi esposo, quienes, a lo largo de los años, han cultivado en mí el deseo de superarme constantemente, brindándome su apoyo y guía para alcanzar mis metas.

DECLARACIÓN JURADA
DE ORIGINALIDAD Y DE NO PLAGIO

Tesista

Yo, Jenny Janet Saona García, identificado(a) con DNI 72172635 del Programa de Pregrado en Ciencias Aeroespaciales, autor(a) de la Tesis, titulada:
"Uso del Internet Satelital para el Control Ciberespacial en Destacamentos Remotos de la Fuerza Aérea del Perú, en el año 2025".

DECLARO BAJO JURAMENTO QUE,

El tema y contenido de tesis es original, siendo resultado de mi esfuerzo y trabajo personal, no ha sido copiado, no se han utilizado ideas, formulaciones, citas integrales ni ilustraciones diversas sacadas de otras tesis, obras, artículos, memorias, etc., (en versión digital o impresa), sin mencionar de forma exacta y clara su origen, fuente o autor, tanto en el cuerpo o texto, gráficos o figuras, cuadros, tablas u otro contenido protegido por derechos de autor.

En este sentido, soy consciente de que la falta de respeto a los derechos de autor y plagiar son acciones que serán castigados mediante sanciones universitarias y/o legales.

Me afirmo y me ratifico en lo expresado, en señal de lo cual firmo el presente documento en la ciudad de Piura, 26 de mayo del 2025.

Tesista: Jenny Janet Saona García
D.N.I.: 72172635

Asesora designada por el dpto.
de investigación de la Eofap

INDICE GENERAL

LISTA DE CUADROS

LISTA DE FIGURAS

RESUMEN

La presente investigación evalúa el uso de internet satelital para el control ciberespacial en destacamentos remotos de la Fuerza Aérea del Perú (FAP) en el año 2025. En un contexto de creciente digitalización, donde la seguridad cibernética se ha convertido en un factor esencial para la defensa nacional, la conectividad en zonas remotas del país representa un desafío clave. La geografía peruana, caracterizada por regiones de difícil acceso como la Amazonía y las zonas fronterizas, dificulta el despliegue de infraestructuras terrestres de telecomunicaciones, limitando así la capacidad operativa de la FAP en dichas áreas.

El uso de internet satelital emerge como una solución viable para garantizar la conectividad, permitiendo la transmisión de datos, voz y video necesarios para las operaciones de vigilancia, mando y control en el ciberespacio. No obstante, su implementación enfrenta diversos retos técnicos, operativos, económicos y de seguridad. Este estudio se fundamenta en una investigación cualitativa, exploratoria y descriptiva, centrada en aspectos clave como la velocidad, latencia, cobertura y la capacidad del internet satelital para asegurar un control ciberespacial eficiente y seguro.

La investigación ofrece una perspectiva integral sobre cómo la integración del internet satelital fortalecerá la capacidad operativa de la Fuerza Aérea, mejorando tanto la seguridad como la eficiencia de las operaciones militares en las zonas más aisladas del Perú.

Palabras clave: internet satelital, conectividad, seguridad, operaciones militares.

ABSTRACT

This research evaluates the use of satellite internet for cyberspace control in remote detachments of the Peruvian Air Force (FAP) in 2025. In a context of growing digitalization, where cybersecurity has become a crucial factor for national defense, connectivity in remote areas of the country presents a key challenge. The Peruvian geography, characterized by hard-to-reach regions such as the Amazon and border zones, complicates the deployment of terrestrial telecommunications infrastructure, thus limiting the operational capacity of the FAP in these areas.

Satellite internet emerges as a viable solution to ensure connectivity, enabling the transmission of data, voice, and video necessary for surveillance, command, and control operations in cyberspace. However, its implementation faces various technical, operational, economic, and security challenges. This study is based on a qualitative, exploratory, and descriptive approach, focusing on key aspects such as speed, latency, coverage, and the ability of satellite internet to ensure efficient and secure cyberspace control.

The research offers an integrated perspective on how the integration of satellite internet will strengthen the operational capacity of the Air Force, improving both the security and efficiency of military operations in the most isolated areas of Peru.

Keywords: satellite internet, connectivity, security, military operations.

INTRODUCCIÓN

En la actualidad, el mundo está experimentando una rápida transformación digital que afecta todos los aspectos de la vida cotidiana, incluidas las áreas de defensa y seguridad nacional. Esta digitalización ha dado lugar a la expansión del dominio ciberespacial, un nuevo campo de batalla donde la superioridad tecnológica se ha convertido en un factor clave para la protección de las naciones. El ciberespacio, compuesto por redes de comunicación, sistemas informáticos, bases de datos y aplicaciones, es ahora un entorno estratégico fundamental para las fuerzas armadas. En este contexto, el control ciberespacial se ha vuelto esencial para garantizar la integridad, confidencialidad y disponibilidad de la información crítica, así como para la ejecución de operaciones militares.

Para países como el Perú, con una geografía extremadamente diversa y compleja, la implementación de tecnologías avanzadas en áreas de difícil acceso, como las zonas fronterizas, representa un desafío adicional. Las regiones remotas, donde las infraestructuras terrestres de telecomunicaciones son limitadas o inexistentes, generan una brecha significativa en términos de conectividad y capacidad operativa. Esta falta de infraestructura adecuada afecta negativamente la capacidad de la Fuerza Aérea del Perú (FAP) para llevar a cabo sus funciones de vigilancia, mando y control en el ciberespacio, lo que compromete la eficacia de sus operaciones militares y de defensa.

El internet satelital, como solución tecnológica que permite la transmisión de datos, voz y video a través de satélites en órbita, surge como una opción viable para garantizar la conectividad en zonas remotas donde no existen otras alternativas. Esta tecnología, que ha

avanzado considerablemente en términos de velocidad, cobertura y fiabilidad, podría ofrecer a la FAP la capacidad de mantener un flujo constante de información entre sus destacamentos más aislados y el centro de operaciones. Sin embargo, la implementación del internet satelital en el ámbito militar enfrenta varios retos que deben ser analizados. Entre ellos se incluyen aspectos técnicos, como la latencia y el ancho de banda, así como preocupaciones operativas y de seguridad cibernética.

La presente investigación tiene como objetivo evaluar la factibilidad del uso de internet satelital en el control ciberespacial en destacamentos remotos de la Fuerza Aérea del Perú, en el año 2025. Se pretende analizar aspectos clave de la tecnología, como la velocidad, la cobertura y la latencia, y cómo estos factores afectan la eficiencia de las operaciones militares en el ciberespacio. Además, se explorarán los desafíos económicos, logísticos y de seguridad asociados con la implementación de esta tecnología en áreas de difícil acceso.

Este análisis permitirá identificar tanto las fortalezas como las debilidades de la tecnología satelital en un contexto operativo y estratégico de defensa nacional. Asimismo, proporcionará datos cruciales para la toma de decisiones de la FAP respecto a la expansión de sus capacidades de comunicación y control ciberespacial en el futuro. En última instancia, se espera que esta investigación sirva como base para la mejora de la infraestructura de telecomunicaciones en el Perú, fortaleciendo la seguridad y eficiencia de las operaciones militares en las regiones más vulnerables del país.

CAPÍTULO I: INTRODUCCIÓN

1.1. Situación problemática

En la actualidad, la superioridad en el ámbito aeroespacial y ciberespacial se ha convertido en un factor crítico para la seguridad y defensa nacional de cualquier país. La transformación digital y la dependencia de las tecnologías de la información han extendido el campo de batalla hacia el dominio ciberespacial, donde la rapidez, confiabilidad y seguridad en las comunicaciones determinan la capacidad de un Estado para ejercer control, disuasión y respuesta ante amenazas.

En el caso del Perú, su compleja geografía, que abarca la extensa Amazonía, la cordillera andina y zonas fronterizas dispersas genera un desafío adicional para la implementación de infraestructuras convencionales de telecomunicaciones, lo que limita la conectividad y la comunicación eficiente en muchas regiones. Estos factores geográficos dificultan el despliegue de sistemas terrestres como fibra óptica, enlaces microondas o redes celulares, provocando brechas significativas en la infraestructura tecnológica crítica para la defensa nacional.

La Fuerza Aérea del Perú (FAP), como pilar fundamental del Poder Militar Aeroespacial, mantiene destacamentos en estas zonas remotas con el propósito de ejercer vigilancia, control y protección del espacio aéreo, además de sostener operaciones en el dominio ciberespacial, que según la Doctrina Básica de la FAP (DBFA 1, 2021) es un componente estratégico transversal para garantizar la soberanía, seguridad y eficiencia operativa. La doctrina enfatiza que el control ciberespacial depende de la capacidad para

mantener sistemas de información seguros, integrados y disponibles en tiempo real, requisito que no puede ser satisfecho plenamente con las limitaciones actuales de la infraestructura terrestre.

Ante esta realidad, el internet satelital se presenta como la opción tecnológica más viable para garantizar la conectividad en los destacamentos remotos, permitiendo el flujo continuo de datos, voz y video necesarios para la vigilancia, mando y control en el ambiente ciberespacial. Sin embargo, la implementación y mantenimiento de este servicio enfrentan múltiples desafíos que afectan su factibilidad. Técnicamente, factores como la latencia propia del enlace satelital, la variabilidad en la calidad del servicio, la estabilidad frente a condiciones meteorológicas adversas, así como la capacidad de ancho de banda limitada, influyen directamente en la eficiencia de las operaciones.

Desde el punto de vista económico y logístico, el alto costo asociado con la instalación, operación y mantenimiento de servicios satelitales puede restringir su despliegue masivo o la sostenibilidad a largo plazo. Asimismo, la seguridad cibernética constituye una preocupación fundamental, pues la vulnerabilidad inherente a las comunicaciones vía satélite puede comprometer la integridad, confidencialidad y disponibilidad de la información crítica, afectando la capacidad de control y respuesta frente a amenazas externas.

A pesar de la importancia estratégica y la necesidad manifiesta, actualmente no existen estudios cualitativos que exploren en profundidad la factibilidad del uso del servicio de internet satelital en estos destacamentos, evaluando cómo sus fortalezas y limitaciones impactan la eficiencia operativa en el control ciberespacial. Esta ausencia de información

genera vacíos en la planificación, toma de decisiones y asignación de recursos, condicionando la capacidad de la FAP para mantener una presencia efectiva y resiliente en las zonas más vulnerables del país.

Por ello, resulta imperativo realizar una investigación que analice la factibilidad de este servicio desde una perspectiva integral, que incluya aspectos técnicos, operativos, económicos y de seguridad, con el fin de optimizar la utilización de tecnologías satelitales y fortalecer la capacidad de defensa aeroespacial nacional, alineada con los lineamientos de la doctrina institucional y las exigencias del entorno estratégico actual.

1.2. Objetivo

1.2.1. Objetivo General

Evaluar la factibilidad del uso de internet satelital para el control ciberespacial en los destacamentos remotos de la Fuerza Aérea del Perú, en el año 2025.

1.2.2. Objetivos Específicos

O.E.1: Analizar la eficiencia del uso de internet satelital en las operaciones defensivas del control ciberespacial en los destacamentos remotos de la Fuerza Aérea del Perú, en el año 2025.

O.E.2: Analizar la eficiencia del uso de internet satelital en las operaciones de explotación del control ciberespacial en los destacamentos remotos de la Fuerza Aérea del Perú, en el año 2025.

O.E.3: Analizar la eficiencia del uso de internet satelital en las operaciones de respuesta del control ciberespacial en los destacamentos remotos de la Fuerza Aérea del Perú, en el año 2025.

1.3. Preguntas de Investigación

1.3.1. Pregunta General

¿Cuál es la factibilidad del uso de internet satelital para el control ciberespacial en los destacamentos remotos de la Fuerza Aérea del Perú, en el año 2025?

1.3.2. Preguntas Específicas

P.E.1: ¿Cuál es la factibilidad del uso de internet satelital en las operaciones defensivas del control ciberespacial en los destacamentos remotos de la Fuerza Aérea del Perú, en el año 2025?

P.E.2: ¿Cuál es la factibilidad del uso de internet satelital en las operaciones de explotación del control ciberespacial en los destacamentos remotos de la Fuerza Aérea del Perú, en el año 2025?

P.E.3: ¿Cuál es la factibilidad del uso de internet satelital en las operaciones de respuesta del control ciberespacial en los destacamentos remotos de la Fuerza Aérea del Perú, en el año 2025?

1.4. Hipótesis

1.4.1 Hipótesis general

El uso de internet satelital contribuye positivamente con el control ciberespacial en los destacamentos remotos de la Fuerza Aérea del Perú, en el año 2025.

1.4.2 Hipótesis específicas

H.E.1: El uso de internet satelital contribuye significativamente en las Operaciones Defensivas de los destacamentos remotos de la Fuerza Aérea del Perú, en el año 2025.

H.E.2: El uso de internet satelital contribuye significativa en las Operaciones de Explotación de los destacamentos remotos de la Fuerza Aérea del Perú, en el año 2025.

H.E.3: El uso de internet satelital contribuye significativa en las Operaciones de Respuesta de los destacamentos remotos de la Fuerza Aérea del Perú, en el año 2025.

1.5 Importancia de la Investigación

La presente investigación reviste una importancia estratégica fundamental para la Fuerza Aérea del Perú (FAP), pues aborda un tema crucial en el contexto actual de la defensa nacional: la factibilidad del uso de un servicio de internet satelital para el control ciberespacial en destacamentos remotos. En un entorno donde la superioridad tecnológica y la capacidad de dominio en el espacio ciberespacial se convierten en factores determinantes para la seguridad y soberanía, disponer de una conectividad segura, estable y eficiente es esencial para garantizar el éxito de las operaciones militares.

Este estudio proporciona una base empírica y cualitativa que permitirá comprender, desde una perspectiva integral, cómo el uso del internet satelital impacta en la eficiencia operativa de los destacamentos remotos ubicados en todo el Perú. La evaluación de la factibilidad técnica, operativa y económica del servicio satelital permitirá identificar fortalezas y debilidades, lo que a su vez facilitará la toma de decisiones informadas sobre la inversión, mejora y expansión de las capacidades tecnológicas en zonas donde las condiciones geográficas y logísticas presentan retos significativos.

Además, al alinearse con los principios y lineamientos establecidos en la Doctrina Básica de la FAP (DBFA 1, 2021), esta investigación contribuye a fortalecer el marco doctrinario y operativo de la institución, apoyando la modernización del poder militar aeroespacial y asegurando que la Fuerza Aérea mantenga una ventaja competitiva en un entorno cada vez más digital y dinámico.

En términos prácticos, la investigación aportará insumos relevantes para optimizar la gestión de recursos tecnológicos, el diseño de estrategias de capacitación y la implementación de políticas de seguridad cibernética, elementos indispensables para la continuidad y resiliencia operativa en el dominio ciberespacial. Finalmente, la generación de conocimiento aplicado y contextualizado favorecerá la innovación y la mejora continua, promoviendo una cultura organizacional orientada hacia la excelencia y la adaptación tecnológica en beneficio de la defensa nacional.

1.6 Alcance y limitación

Esta investigación se centrará en evaluar la factibilidad del uso del servicio de internet satelital como herramienta clave para fortalecer el control ciberespacial en destacamentos remotos de la Fuerza Aérea del Perú (FAP), considerando una perspectiva integral que abarque aspectos técnicos, operativos, económicos y de seguridad. El estudio analizará elementos como la cobertura, velocidad, latencia, usabilidad, estabilidad del servicio, así como su incidencia en las operaciones defensivas, de explotación y de respuesta en el ciberespacio.

El ámbito espacial se circunscribe a destacamentos remotos de la FAP ubicados en zonas geográficamente complejas, donde la conectividad terrestre convencional resulta limitada o inexistente.

La población objetivo incluye a oficiales, técnicos y suboficiales especializados en telecomunicaciones, ciberseguridad y sistemas TIC, que tengan participación directa o indirecta en la operación, gestión o supervisión del servicio satelital en dichos destacamentos. Buscando capturar una visión multidimensional de la experiencia operativa en torno al internet satelital.

Desde el punto de vista metodológico, se aplicará un enfoque cualitativo, exploratorio y transversal, utilizando como técnica principal el cuestionario tipo Likert, con el objetivo de recopilar percepciones, valoraciones técnicas y experiencias concretas sobre el fenómeno en estudio. Esta aproximación permitirá una comprensión profunda y contextualizada del funcionamiento del servicio satelital en entornos operacionales reales, donde se cruzan variables tecnológicas y estratégicas.

No obstante, la investigación presenta limitaciones inherentes a su diseño y contexto militar. En primer lugar, el acceso restringido a información clasificada o sensible puede limitar el análisis exhaustivo de algunos aspectos críticos relacionados con la seguridad de las comunicaciones y la arquitectura de red de la FAP. En segundo lugar, las condiciones logísticas y geográficas de los destacamentos remotos podrían dificultar la aplicación de los instrumentos en todos los escenarios previstos.

Adicionalmente, al tratarse de una muestra no probabilística e intencionada, los resultados no podrán ser generalizados estadísticamente al total de la institución, aunque sí permitirán identificar patrones, riesgos, fortalezas y oportunidades estratégicas relevantes. El estudio no busca formular verdades absolutas, sino aportar evidencia exploratoria, práctica y contextualizada que oriente la toma de decisiones institucionales en materia de conectividad y control ciberespacial, sirviendo como base para futuras investigaciones que profundicen los hallazgos obtenidos.

CAPÍTULO II: DEL MARCO TEÓRICO

2.1. Antecedentes de la Investigación

El estudio de la implementación de tecnologías de comunicación en zonas remotas ha sido objeto de interés en diversas áreas de investigación, especialmente en el contexto de la defensa y la seguridad nacional. En los últimos años, se ha incrementado el enfoque en el uso de tecnologías satelitales para resolver los problemas de conectividad en regiones de difícil acceso, tanto en el ámbito civil como en el militar. La creciente dependencia de la información y las comunicaciones ha subrayado la necesidad de garantizar una conectividad eficiente y segura, especialmente en operaciones críticas que requieren un control constante sobre el ciberespacio.

En el ámbito internacional, varios estudios han abordado el uso de internet satelital en contextos de defensa, resaltando sus ventajas y desafíos en términos de cobertura, latencia y seguridad. Las tecnologías de satélites en órbita baja (LEO), por ejemplo, han mostrado un gran potencial para mejorar la velocidad de conexión y reducir la latencia, aspectos clave para las operaciones militares que requieren comunicaciones en tiempo real.

A nivel nacional, el Perú ha iniciado varios proyectos para mejorar la conectividad en áreas remotas, mediante el uso de internet satelital. Estos esfuerzos buscan reducir la brecha digital, fortalecer la capacidad operativa y la seguridad de las fuerzas armadas en regiones de difícil acceso.

A continuación, se presentan los antecedentes internacionales y nacionales que proporcionan el marco necesario para comprender el contexto de la investigación y las tendencias globales y locales en la implementación de internet satelital para la defensa y el control ciberespacial.

2.1.1. Antecedentes Internacionales

Ramírez-Arroyo et al. (2024). Este estudio presenta un análisis integral sobre la integración de tecnologías de redes terrestres 5G y satelitales para brindar conectividad en áreas rurales remotas que carecen de infraestructura tradicional de telecomunicaciones. Los autores examinan el concepto de "multi-conectividad", que combina múltiples tecnologías para asegurar una comunicación estable y de alta capacidad, vital para aplicaciones críticas. En sectores como la teleeducación, monitoreo agrícola y salud remota, esta integración se traduce en mejoras sustanciales en la calidad y continuidad del servicio. Si bien el enfoque principal es civil, las conclusiones del estudio tienen aplicaciones directas en el ámbito militar, donde la necesidad de conectividad robusta y resiliente en destacamentos remotos es crítica para la ejecución efectiva de operaciones de control ciberespacial, vigilancia y defensa. El documento destaca cómo el uso complementario de redes satelitales mejora la cobertura, reduce la latencia y garantiza redundancia, factores que fortalecen la resiliencia de las comunicaciones en entornos hostiles o geográfifcamente aislados.

Lin et al. (2021). En el presente estudio, se evidencia que Lin y colaboradores abordan el papel fundamental de los satélites de órbita baja (Low Earth Orbit - LEO) para la provisión de servicios de internet de baja latencia y alta velocidad en zonas remotas o desprovistas de

infraestructura terrestre. El documento destaca que las redes satelitales basadas en LEO representan una revolución tecnológica que permitirá alcanzar la cobertura global, con mejoras sustanciales en la latencia y ancho de banda respecto a los sistemas satelitales geoestacionarios tradicionales. Esta tecnología es especialmente valiosa para aplicaciones que demandan comunicación en tiempo real, como el control ciberespacial, ya que permite una mejor sincronización y respuesta inmediata ante incidentes o amenazas. El estudio proyecta que la integración de estas tecnologías satelitales con las redes móviles avanzadas potenciará la conectividad en áreas críticas, facilitando operaciones militares en destacamentos remotos, donde la estabilidad y rapidez de la red pueden marcar la diferencia en la eficiencia operativa y la seguridad.

Espinoza, Diego (2021). El estudio “Implementación de Internet Satelital en Zonas Rurales de la Ciudad de Manta, para la continuidad de las Clases Virtuales”, abordó la urgente necesidad de garantizar el acceso a la educación en comunidades rurales afectadas por la brecha digital. Se identificó que solo el 7% de los hogares contaba con acceso a internet y menos del 2% disponía de dispositivos adecuados para la educación virtual. El proyecto implementó un sistema de internet satelital mediante la instalación de antenas y desarrolló un programa de capacitación tecnológica para docentes, estudiantes y padres de familia. Como resultado, se logró conectar al 85% de los hogares, y se redujo del 70% al 15% el porcentaje de personas sin conocimientos básicos en el uso de plataformas virtuales. La intervención, demostró que el internet satelital es una solución viable y efectiva para garantizar la conectividad en zonas geográficamente aisladas. Aunque la finalidad principal del proyecto fue educativa, sus resultados ofrecen implicancias relevantes para el ámbito militar, en

particular en lo que respecta a la viabilidad operativa del internet satelital en entornos remotos**.** Esta experiencia demuestra que, con una adecuada planificación técnica y social, es posible establecer conectividad funcional que respalde actividades críticas, como el control ciberespacial en escenarios rurales o de difícil acceso.

2.1.2. Antecedentes Nacionales

Ministerio de Transportes y Comunicaciones – MTC (2023). El articulo resalta e informa sobre el programa "Conecta Selva" lanzado por el MTC en 2023, que impulsa el Programa Nacional de Telecomunicaciones (Pronatel), esta iniciativa está orientada a reducir la brecha digital en la Amazonía peruana, utilizando tecnología de internet satelital para dotar de conectividad a instituciones claves como escuelas, centros de salud y comisarías ubicadas en zonas aisladas. "El objetivo de la iniciativa es lograr la inclusión digital de alrededor de 264 mil peruanos de las zonas remotas del Amazonas" (MTC, 2023). En este sentido, es importante tener claro que el programa responde a la necesidad urgente de mejorar el acceso a la información y la comunicación en regiones donde las condiciones geográficas dificultan la implementación de infraestructura tradicional de telecomunicaciones, llevando así un avance notorio del 98.5 %. Aunque el enfoque es social y educativo, el impacto del proyecto tiene implicancias claras para la seguridad y defensa, ya que la mejora en la conectividad fortalece la capacidad operativa y coordinación de las fuerzas militares y policiales en estas áreas remotas. El MTC reporto mejoras significativas en la cobertura y calidad del servicio, aunque también reconoce retos en términos de mantenimiento, costos y adaptación tecnológica.

Ushiñahua et al. (2023). El presente estudio, realizado por investigadores de la Universidad ESAN detalla la transición tecnológica y la implementación de soluciones de conectividad satelital para zonas rurales y fronterizas en el Perú, específicamente a través de operadores como Andesat e Intelsat. El trabajo describe el desafío de garantizar un servicio de alta calidad en contextos donde la geografía, la dispersión poblacional y las condiciones climáticas afectan severamente la infraestructura convencional. Los resultados muestran que la conectividad satelital no solo mejora la cobertura, sino que también contribuye a la continuidad y eficiencia operativa en sectores claves, incluyendo la seguridad nacional y la vigilancia territorial. Los autores sugieren que esta tecnología puede ser escalada y adaptada para uso institucional y militar, facilitando operaciones que requieren comunicaciones seguras y estables en destacamentos remotos, contribuyendo así a la reducción de la brecha digital estratégica del país.

Yamakawa (2022). En su artículo Yamakawa, analiza las oportunidades que ofrece el internet satelital para disminuir la brecha digital en el Perú, centrándose en las zonas de la selva, la sierra y las regiones fronterizas. El autor subraya que la conectividad satelital representa una solución estratégica para integrar digitalmente a comunidades aisladas, facilitando el acceso a servicios y mejorando la comunicación institucional. Aunque el enfoque principal es civil, el análisis contempla las implicancias para sectores gubernamentales, incluyendo la defensa y seguridad, donde una infraestructura de comunicaciones robusta y estable es esencial para el desempeño eficiente en el control ciberespacial y operaciones militares remotas. Yamakawa también señala los desafíos

tecnológicos, económicos y de política pública que deben ser superados para maximizar el potencial de estas tecnologías en el Perú.

2.2. Bases teóricas

Para abordar adecuadamente la implementación del internet satelital en el control ciberespacial de los destacamentos remotos de la Fuerza Aérea del Perú, es fundamental establecer un marco conceptual que permita comprender los aspectos técnicos, operativos y estratégicos involucrados en esta tecnología. En esta sección, se desarrollan los conceptos clave que sustentan la investigación, basados en teorías y modelos que explican tanto el funcionamiento del internet satelital como su aplicación en contextos de seguridad y defensa.

El internet satelital, como solución tecnológica para la conectividad en zonas remotas, se basa en principios de comunicaciones por satélite, que permiten superar las limitaciones de infraestructura terrestre, como las redes de fibra óptica o las antenas de microondas. Además, es necesario abordar el concepto de control ciberespacial, que se refiere a la capacidad de las fuerzas armadas para gestionar y proteger las redes de comunicación digital que sustentan sus operaciones.

Esta sección también explora las consideraciones técnicas esenciales para la implementación del internet satelital, como la latencia, el ancho de banda, la resiliencia ante condiciones climáticas adversas y la seguridad de las comunicaciones. Finalmente, se revisan los avances tecnológicos recientes en el campo de los satélites en órbita baja (LEO) y cómo estos avances podrían beneficiar la conectividad en los destacamentos remotos de la FAP.

A continuación, se presentan las teorías y conceptos clave que fundamentan la investigación y su aplicación en el contexto del control ciberespacial y la defensa nacional.

2.2.1 Internet por Satélite

El internet satelital es un sistema de acceso a internet que utiliza satélites artificiales ubicados en órbita alrededor de la Tierra para establecer una conexión entre el usuario y la red global y es importante tener en consideración que “el internet satelital ha ido evolucionando a lo largo del tiempo, de manera significativa, transformando toda la conectividad del mundo en áreas remotas y rurales” (PERUDATA, 2024). Esta tecnología resulta especialmente útil para brindar conectividad en zonas donde las infraestructuras tradicionales, como la fibra óptica o las redes móviles terrestres, no están disponibles o su implementación resulta compleja y costosa.

El funcionamiento del internet satelital se basa en tres elementos principales: la antena del usuario, el satélite en órbita y la estación terrestre o centro de operaciones. En el lugar donde se requiere el servicio, se instala una antena parabólica o terminal satelital que se encarga de enviar y recibir señales de radiofrecuencia hacia y desde un satélite ubicado en órbita geoestacionaria o en órbita baja.

Los satélites geoestacionarios se sitúan aproximadamente a 35,786 kilómetros de altura y mantienen una posición fija relativa a la Tierra, lo que les permite cubrir áreas amplias, aunque con una latencia relativamente alta debido a la gran distancia que recorren las señales. Por otro lado, los satélites en órbita baja están situados a alturas entre 500 y 2,000 kilómetros, lo que reduce significativamente la latencia y mejora la velocidad de conexión, aunque

requieren una constelación más extensa para mantener una cobertura continua. Una vez que el satélite recibe la señal desde la antena del usuario, esta se retransmite a una estación terrestre conectada a la red de internet tradicional. Desde allí, la información viaja a través de la red global y se envía de regreso siguiendo el mismo camino. Este proceso permite que usuarios en lugares remotos puedan acceder a internet sin depender de infraestructuras terrestres complejas.

Figura 1: *¿Cómo funciona el internet satelital?*

Nota: Elaboración propia

Cabe destacar que, entre las principales características del internet satelital destacan su cobertura global, que puede llegar a cualquier punto del planeta, incluyendo zonas rurales, montañosas, marítimas o de difícil acceso. Además, al no depender de cables ni torres terrestres, es menos vulnerable a interrupciones causadas por daños físicos, desastres naturales

o sabotajes. En cuanto a desempeño, las velocidades pueden variar desde algunos megabits por segundo hasta varios cientos, dependiendo del proveedor y la tecnología empleada. Sin embargo, la latencia tiende a ser mayor que en conexiones terrestres, especialmente cuando se utilizan satélites geoestacionarios.

El internet satelital es fundamental para proporcionar acceso a internet en lugares remotos, facilitando el desarrollo social, educativo y económico. También es vital en situaciones de emergencia, cuando otras redes fallan. Además, su aplicación se extiende a sectores que requieren conectividad en lugares remotos o móviles, como la navegación marítima, la aviación, la minería y las operaciones militares.

Cuadro 1: *Evolución del Internet Satelital*

Etapa / Década	Hitos Principales	Aportes y Características
Primeros Inicios (1960-1970) 	-Telstar (1962): primer satélite que permitió transmisiones de TV y abrió el camino a datos. -SATCOM (1970): Satélites de comunicaciones con velocidades muy limitadas.	Inicio de las comunicaciones satelitales. Se usaban sobre todo para TV y telefonía, con capacidades básicas de datos.
Desarrollo de Sistemas (1980) 	- Intelsat y otros: satélites para telecomunicaciones con soporte inicial a datos. - VSAT: terminales pequeñas que permitieron internet satelital en instalaciones reducidas (aunque costosas).	Expansión de la infraestructura y primeras conexiones de datos satelitales en empresas e instituciones.

Comercialización y avances (1990) 	- DirecPC (1996): recepción de datos por satélite, con envío vía línea telefónica. - StarBand (1999): primer servicio bidireccional completo (subida y bajada de datos).	Inicio del internet satelital comercial para hogares, con mejoras en velocidad de descarga.
Mejoras en la Tecnología (2000) 	- Satélites de banda ancha: mayor capacidad y velocidad. - Hughes (2004): servicios más accesibles para consumidores y empresas.	Popularización del internet satelital, expansión de cobertura y reducción relativa de costos.
Nuevas Constelaciones y Orbita Baja (2010) 	- Ka-band: uso de frecuencias más altas para mayor velocidad. - OneWeb y Starlink (2019): constelaciones de satélites en órbita baja (LEO), con baja latencia y cobertura global.	Evolución en la conectividad satelital, con miles de satélites ofreciendo internet de alta velocidad en zonas remotas.
El futuro (2020 en adelante) 	- Conectividad Global: acceso incluso en las regiones más aisladas. - Integración con 5G: redes híbridas satélite + terrestre. - Sostenibilidad: satélites más eficientes y antenas avanzadas.	Internet satelital como complemento clave a otras tecnologías, con foco en rapidez, confiabilidad y sostenibilidad.

Nota: Elaboración propia. Datos tomados de PERUDATA (2024).

2.2.2 Consideraciones técnicas para la implementación del internet satelital

Cabe destacar que, la efectividad del internet satelital como solución de conectividad para el control ciberespacial en destacamentos remotos de la Fuerza Aérea del Perú depende en gran medida de la evaluación, selección e implementación rigurosa de criterios técnicos clave, capaces de garantizar tanto la continuidad operativa como la seguridad de la información transmitida. En contextos militares, donde las comunicaciones deben ser adaptables, rápidas y seguras, el internet satelital no puede concebirse únicamente como un medio de acceso a red, sino como un componente táctico y estratégico de mando, control y vigilancia. A continuación, se detallan las principales consideraciones que deben evaluarse para garantizar un desempeño óptimo y seguro en operaciones militares críticas.

- Velocidad y ancho de banda. - Para el control ciberespacial, que implica la supervisión y gestión en tiempo real de sistemas de defensa, vigilancia y comunicaciones, la velocidad de conexión y el ancho de banda disponible son determinantes. Es necesario que el servicio satelital proporcione velocidades de descarga y subida suficientemente altas para soportar la transmisión continua y simultánea de datos, video en alta resolución, comandos y señales cifradas. Un ancho de banda adecuado también permite la conexión de múltiples dispositivos y sistemas en red dentro del destacamento, favoreciendo la interoperabilidad y la eficiencia operativa. Por tanto, se debe evaluar la capacidad del proveedor de internet satelital para ofrecer planes con ancho de banda escalable que se ajusten a las demandas específicas del control ciberespacial.

- Latencia. - Definida como el tiempo que tarda una señal en viajar desde el punto de origen hasta el destino y regresar, es un factor crítico en operaciones donde la inmediatez de respuesta es vital. En el contexto militar, la demora en las comunicaciones puede comprometer la efectividad de la vigilancia y la toma de decisiones en tiempo real. Los sistemas de internet satelital tradicionales, basados en satélites geoestacionarios ubicados a aproximadamente 36,000 km de altura, presentan una latencia relativamente alta (entre 500 y 600 milisegundos), lo que puede ser un impedimento para aplicaciones sensibles.

  En contraste, las constelaciones de satélites en órbita baja (LEO, por sus siglas en inglés), situadas a menos de 2,000 km, ofrecen latencias significativamente menores (entre 20 y 50 milisegundos), lo que mejora la respuesta y la fluidez de las comunicaciones. Por ello, la selección de tecnología satelital con baja latencia es una prioridad para asegurar la eficiencia en el control ciberespacial.

- Seguridad y soporte técnico: En un entorno militar, la seguridad de la información y la continuidad operativa son innegociables. Por esta razón, la solución de internet satelital debe contar con mecanismos avanzados de protección de datos, incluyendo encriptación robusta, autenticación segura y protocolos que eviten ataques cibernéticos y accesos no autorizados. Además, la confiabilidad del proveedor en cuanto a soporte técnico es esencial para resolver rápidamente cualquier fallo o interrupción que pueda poner en riesgo las operaciones.

El soporte debe incluir monitoreo constante de la red, mantenimiento preventivo, atención 24/7 y capacidad para responder ante contingencias de forma inmediata. Esta combinación garantiza que el servicio sea técnicamente adecuado, seguro y estable, contribuyendo a la integridad y eficacia del control ciberespacial en destacamentos remotos.

Figura 2: *Consideraciones técnicas del Internet Satelital*

Nota: La imagen muestra las consideraciones a tener en cuenta para la óptima implementación del Internet Satelital. Elaboración propia.

2.2.3 Importancia de la conectividad en zonas remotas

En la actualidad, la conectividad a internet se ha convertido en un recurso estratégico fundamental para el desarrollo económico, social y operativo de diversas instituciones. En este contexto, el internet satelital emerge como una solución tecnológica que permite superar estas barreras, ofreciendo cobertura en cualquier ubicación geográfica donde exista visión despejada hacia el cielo, sin requerir una infraestructura terrestre extensa. Este tipo de conexión funciona

mediante la comunicación entre una antena parabólica instalada en el sitio del usuario y satélites en órbita geoestacionaria o de baja altitud, que retransmiten las señales a centros de datos conectados a la red global.

Resulta relevante considerar que la implementación del internet satelital en destacamentos remotos brinda múltiples ventajas que lo hacen viable para aplicaciones críticas como el control ciberespacial militar, entre las principales ventajas resaltan:

- Cobertura global y acceso en zonas aisladas: Permite la conexión en ubicaciones estratégicas donde las redes terrestres no llegan, garantizando la continuidad de las operaciones.

- Rápida instalación y despliegue: La infraestructura requerida es mínima, con antenas y módems que pueden instalarse en corto tiempo, facilitando la pronta activación del servicio.

- Confiabilidad y resistencia: Al no depender de cables físicos, la conexión satelital es menos vulnerable a interrupciones provocadas por desastres naturales o ataques físicos a la infraestructura, aspecto crítico en operaciones militares.

- Adecuada capacidad para actividades en línea: Los avances en tecnología satelital permiten velocidades y estabilidad suficientes para tareas como monitoreo, comunicación segura y gestión remota, esenciales en el control ciberespacial.

2.2.4 Seguridad del Internet Satelital

La seguridad en las comunicaciones a través de internet satelital representa un aspecto fundamental y crítico, particularmente en aplicaciones militares y gubernamentales. En estos contextos, la información manejada puede ser altamente sensible y estratégica, por lo que la integridad, confidencialidad y disponibilidad de los datos transmitidos son esenciales para garantizar el éxito de las operaciones y la protección nacional.

Las fuerzas armadas, al operar en destacamentos remotos y en entornos con posibles amenazas cibernéticas, requieren sistemas de comunicación que no solo sean confiables y estables, sino también altamente seguros. Cualquier vulnerabilidad en la red podría ser aprovechada por adversarios para interceptar información, sabotear operaciones o comprometer la integridad del control ciberespacial. Por ello, la seguridad de las comunicaciones satelitales debe contemplar tanto aspectos tecnológicos como organizativos, integrando medidas preventivas y reactivas.

Una de las principales estrategias para proteger la información transmitida por internet satelital es la encriptación. Este proceso consiste en transformar los datos en un formato codificado que solo puede ser descifrado por quienes poseen las claves o permisos adecuados. En las comunicaciones militares, se emplean protocolos de encriptación robustos que garantizan que la información no sea accesible ni manipulable por actores no autorizados.

- Encriptación de extremo a extremo (E2EE): Este tipo de encriptación asegura que los datos permanezcan cifrados desde el momento en que salen del dispositivo del usuario hasta que llegan al receptor final. Así, incluso si las señales son interceptadas

en cualquier punto del enlace satelital (durante la transmisión al satélite o en la estación terrestre), los datos permanecen ilegibles para terceros. Esta característica es vital para proteger información sensible como órdenes de operación, datos de vigilancia o inteligencia.

- Protocolos de seguridad estándar: Se utilizan protocolos ampliamente reconocidos y probados en el ámbito de la seguridad informática, como IPsec (Internet Protocol Security), que protege la transmisión de datos en la red mediante autenticación y cifrado a nivel de IP; TLS (Transport Layer Security), que asegura la confidencialidad y la integridad de los datos en tránsito; y VPNs (Redes Privadas Virtuales), que crean túneles seguros para el tráfico de información, aislándolo de accesos externos no autorizados. La combinación de estos protocolos contribuye a fortalecer la barrera de defensa contra ataques cibernéticos, tales como espionaje, suplantación de identidad o alteración de datos.

Desde esta perspectiva, otra capa esencial de seguridad, es la implementación de sistemas de autenticación robustos que garantizan que solo el personal autorizado pueda acceder a la red satelital y a los sistemas conectados. Las fuerzas armadas suelen emplear mecanismos de autenticación multifactor (MFA), que requieren no solo una contraseña o clave, sino también un segundo factor adicional como un token físico, un código temporal o la verificación biométrica. Este enfoque reduce significativamente el riesgo de accesos no autorizados y potenciales brechas de seguridad. Asimismo, el control de acceso incluye políticas estrictas sobre permisos y roles, de modo que cada usuario solo pueda interactuar con

la información y los sistemas estrictamente necesarios para su función, minimizando el riesgo de filtraciones internas o errores humanos.

Figura 3: Seguridad del Internet Satelital

Nota: Elaboración propia

Partiendo de lo anterior, la seguridad en internet satelital no se limita únicamente a la protección de la información mediante cifrado y protocolos seguros, sino que también se extiende a la defensa integral de la infraestructura física y lógica que soporta todo el sistema. Esto abarca tanto medidas para asegurar las antenas satelitales, estaciones terrestres y centros de operaciones, como los componentes menos tangibles, entre ellos el software de gestión, los sistemas de control de acceso, evitando sabotajes, interferencias o accesos físicos no autorizados. Mantener la seguridad implica además contar con un soporte técnico especializado y monitoreo continuo de la red para detectar anomalías, intrusiones o fallos.

Los proveedores y operadores de internet satelital suelen ofrecer soporte técnico disponible 24/7, con personal altamente capacitado que puede intervenir de manera inmediata pata restaurar el servicio ante cualquier incidente. Además, se diseñan planes de contingencia y recuperación ante desastres que garantizan la rápida restauración del servicio y canales alternativos de comunicación, minimizando el impacto en las operaciones militares y asegurando la continuidad del control ciberespacial en todo momento.

2.2.5 Avances Tecnológicos en Internet Satelital

En los últimos años, el internet satelital ha experimentado avances tecnológicos significativos impulsados por la innovación en tecnologías espaciales y de comunicación. Estos avances han mejorado sustancialmente la velocidad de transmisión de datos, la reducción de la latencia y la ampliación de la cobertura del servicio, posicionando al internet satelital como una solución cada vez más viable y eficiente para aplicaciones críticas, incluyendo las operaciones militares en zonas remotas.

Tradicionalmente, el internet satelital se ha basado en satélites geoestacionarios (GEO) que permiten una cobertura amplia y estable desde una posición fija respecto a la Tierra. Si bien estos satélites pueden cubrir grandes áreas, presentan una latencia alta debido a la distancia que las señales deben recorrer, lo que limita su uso para aplicaciones que requieren respuestas rápidas. Para superar estas limitaciones, han surgido nuevas constelaciones de satélites en órbita baja (LEO) ubicados entre 500 y 2,000 kilómetros sobre la Tierra, para ofrecer internet satelital de alta calidad en todo el mundo. Estos proyectos buscan resolver las limitaciones de conectividad en áreas rurales, remotas y en desarrollo, donde la infraestructura

terrestre convencional, como cables de fibra óptica y redes celulares, no es viable o es económicamente costosa de implementar.

Uno de los principales objetivos de estos proyectos es ofrecer cobertura global de alta velocidad con baja latencia, permitiendo a usuarios de todo el mundo, incluso en las regiones más aisladas, acceder a internet de calidad similar a las zonas urbanas. Estos satélites están diseñados para trabajar en constelaciones, lo que significa que se lanzan en grupos para garantizar cobertura continua. Además, empresas como SpaceX con su proyecto Starlink, OneWeb y Amazon con Project Kuiper están liderando algunos de los proyectos más ambiciosos de constelaciones de satélites en órbita baja (LEO), con planes de desplegar miles de satélites destinados a ofrecer cobertura global. Estos esfuerzos no solo están orientados a resolver problemas de conectividad en países en desarrollo, sino también mejorar el acceso a internet en zonas urbanas y suburbanas, proporcionando una alternativa tecnológica viable y complementaria a los sistemas terrestres convencionales. La proliferación de estas constelaciones tiene el potencial de generalizar el acceso a la información digital, reducir la dependencia de infraestructuras físicas vulnerables y garantizar una conectividad continua, incluso en escenarios de desastre natural o conflicto.

Para el sector defensa, estas iniciativas abren nuevas posibilidades para el despliegue operativo de comunicaciones seguras, en tiempo real y con cobertura extendida. Asimismo, con el avance sostenido de estas tecnologías, se proyecta que el costo de acceso al internet satelital experimente una reducción progresiva, producto del aumento de constelaciones LEO, la competencia entre proveedores, la optimización de los procesos de fabricación, lanzamiento y operación de satélites. Esta tendencia permitirá que la conectividad satelital deje de ser una

solución costosa y limitada, para convertirse en una alternativa accesible, escalable y sostenible para millones de personas en todo el mundo.

Cuadro 2: Satélites en órbita LEO

Proyecto	**Número de Satélites**	**Objetivo**	**Cobertura**	**Velocidad Estimada**	**Ventajas**
Starlink (SpaceX) 	12000	Proporcionar acceso a internet global de alta velocidad con baja latencia.	Global, con presencia en múltiples partes del mundo.	Hasta 1 Gbps.	Baja latencia, alta velocidad, cobertura global.
OneWeb 	648	Ofrecer internet de alta velocidad en áreas rurales y remotas, especialmente en países en desarrollo.	Inicialmente en mercados emergentes y áreas rurales.	Hasta 100 Mbps.	Concentración en áreas de difícil acceso y países en desarrollo.
Amazon Project Kuiper 	3236	Brindar acceso a internet de alta velocidad a nivel global, especialmente en áreas sin infraestructura terrestre.	Global, con énfasis en regiones sin acceso a infraestructura terrestre.	Hasta 400 Mbps (proyección futura).	Alta velocidad, enfoque en aéreas sin infraestructura terrestre.

Nota: Elaboración propia. Características resaltantes de satélites actuales.

En el ámbito institucional y de defensa, esta reducción de costos no solo representa un alivio presupuestario, sino una palanca estratégica para ampliar las capacidades operativas. Con ello, la Fuerza Aérea del Perú podrá extender su red de comunicaciones seguras a un mayor número de destacamentos remotos, manteniendo un equilibrio entre eficacia y sostenibilidad, dos conceptos que a menudo parecen incompatibles en la gestión de recursos públicos. Lo que antes era visto como un lujo inaccesible para regiones apartadas, hoy se proyecta como una necesidad estratégica.

Estas constelaciones funcionan enviando señales entre satélites en red, que retransmiten la información hacia estaciones terrestres y usuarios finales. La diferencia entre estas nuevas tecnologías y los antiguos sistemas GEO es casi irónica: mientras aquellos satélites GEO con 36 mil kilómetros de distancia, los satélites LEO son mucho más rápidos, gracias a su cercanía orbital, reducen considerablemente la latencia, llegando a valores de entre 20 y 50 milisegundos, comparado con los 500-600 ms de los satélites GEO, permitiendo alcanzar velocidades de descarga y subida comparables o superiores a muchas conexiones terrestres tradicionales. Una diferencia que puede significar el éxito o el fracaso de una operación militar en tiempo real. Dicho de otro modo, la misma distancia que antes convertía la comunicación en un eco tardío, hoy la transforma en un reflejo instantáneo.

La implementación de estas nuevas tecnologías satelitales, especialmente aquellas basadas en constelaciones de satélites en órbita baja (LEO), está transformando de manera acelerada el acceso a internet a nivel global, redefiniendo los modelos de conectividad en zonas remotas, rurales o con infraestructura limitada. Lo que antes se concebía como un

recurso limitado, destinado a usos muy específicos, hoy se perfila como un instrumento democratizador de acceso a la información. Esta transformación incluye aspectos clave como:

Cuadro 3: Aspectos clave del Internet Satelital

Aspecto	Descripción
Reducción de la brecha digital	Facilita el acceso a internet de alta calidad en áreas remotas o con infraestructura limitada.
Mejora en aplicaciones críticas	La baja latencia y alta velocidad permiten un uso eficiente en sectores como defensa, telemedicina, educación a distancia y agricultura de precisión.
Mayor resiliencia y flexibilidad	La red satelital LEO se adapta mejor a cambios en la demanda y es menos vulnerable a desastres o ataques físicos, al no depender de infraestructura fija.
Nuevas oportunidades comerciales	Impulsa el desarrollo de negocios y servicios digitales en mercados emergentes y zonas remotas, fomentando la inclusión digital.

Nota: Elaboración propia.

En el ámbito militar, estas innovaciones representan una oportunidad para mejorar la conectividad en destacamentos remotos y misiones en campo, facilitando un control ciberespacial más efectivo y seguro, con comunicaciones más rápidas y confiables.

2.2.6 Ciberespacio como Dominio de las Operaciones Militares

El reconocimiento del ciberespacio como un nuevo dominio de las operaciones militares ha transformado la concepción tradicional de la guerra. Si antes los ejércitos se disputaban la supremacía en tierra, mar, aire y espacio, hoy el campo de batalla se extiende

también hacia lo intangible, hacia un espacio donde las balas son paquetes de datos y los misiles son líneas de código. Paradójicamente, se trata de un dominio que no se ve ni se toca, pero cuya influencia puede paralizar a un país entero en cuestión de segundos.

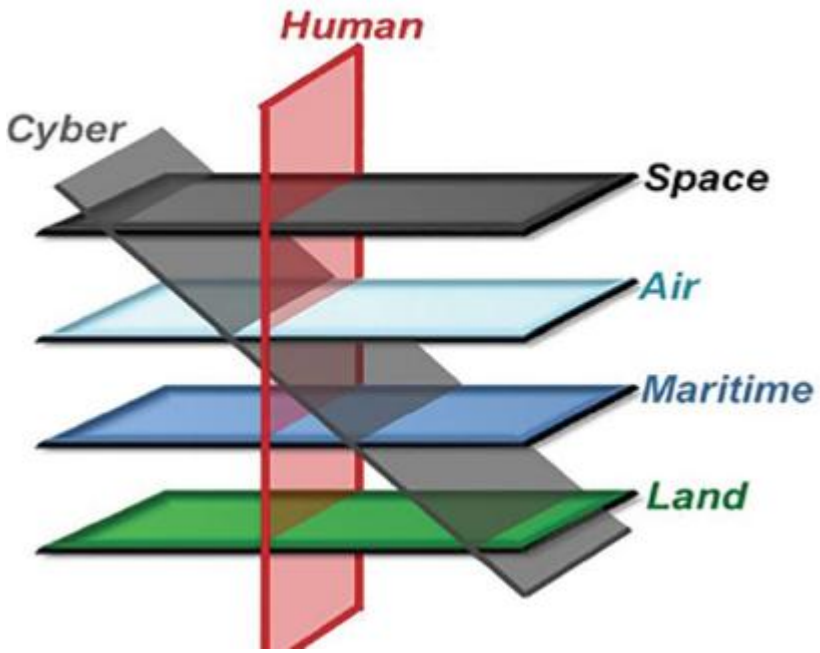
A diferencia de los demás dominios, el ciberespacio es transversal por naturaleza: está presente en cada uno de ellos, los penetra y los conecta, como un tejido nervioso invisible que une al cuerpo. Aquí radica la antítesis central: lo que debería ser un factor de fortaleza y coordinación, se convierte también en un punto crítico de vulnerabilidad. La ironía es evidente: un ejército con aviones supersónicos y tanques de última generación puede quedar inoperativo si un simple ataque digital inhabilita sus sistemas de mando, sus radares o sus cadenas logísticas.

El ciberespacio obliga a un nuevo tipo de coordinación que va más allá de lo que las fuerzas militares estaban acostumbradas en operaciones conjuntas. No se trata de sumar fuerzas, sino de entretejer capacidades en un dominio que se asemeja a un tablero de ajedrez infinito, donde cada movimiento digital tiene repercusiones inmediatas en los demás ámbitos. Así, mientras en el pasado los dominios se representaban uno al lado del otro como compartimentos separados, hoy es imposible negar que se encuentran entrelazados como vasos comunicantes, donde lo que ocurre en uno repercute inevitablemente en los demás.

De ahí la necesidad de una conciencia situacional global y compartida, que permita a los mandos conocer en tiempo real tanto la posición de sus propios activos como los del adversario. No basta con vigilar los cielos, los mares o la tierra; es indispensable vigilar las líneas invisibles de información, porque en ellas se juega la superioridad estratégica. La ironía

final es que, en un mundo cada vez más dependiente de la tecnología, la guerra puede decidirse no por el tamaño de los ejércitos, sino por la capacidad de controlar o desestabilizar un sistema digital.

Figura 4: Dominios en el Ciberespacio



Nota: Mando y Control en el Ciberespacio. Coz, Jose, Pastor, Vicente. (2019)

2.2.7 ¿Qué es el Control Ciberespacial?

El control ciberespacial constituye un conjunto integral de capacidades, procesos, tecnologías y doctrinas operativas orientadas a la **s**upervisión, protección, dominio y gestión efectiva de las actividades que se desarrollan dentro del ciberespacio**.** Este dominio abarca la infraestructura digital global, compuesta por redes de comunicaciones, sistemas informáticos, plataformas tecnológicas, bases de datos, aplicaciones y servicios digitales interconectados, los cuales representan hoy la columna vertebral de las operaciones modernas en los ámbitos civil, gubernamental y militar. En el contexto de la defensa, el control ciberespacial se

configura como un pilar estratégico fundamental para garantizar la seguridad nacional, dado que las fuerzas armadas dependen cada vez más de entornos digitales para ejecutar misiones, coordinar operaciones, procesar inteligencia y ejercer el mando y control. Asegurar el dominio del ciberespacio implica garantizar la integridad, disponibilidad y confidencialidad de los sistemas de información, así como anticiparse, detectar y neutralizar amenazas cibernéticas que puedan comprometer la soberanía, la capacidad operativa o la infraestructura crítica del Estado.

Figura 5: Control ciberespacial en la FAP

Nota: Elaboración propia

2.2.8 Componentes Funcionales del Control Ciberespacial

El control ciberespacial es una disciplina compleja y multifacética que requiere la integración de diversos componentes funcionales para garantizar la seguridad, resiliencia y efectividad de las operaciones en el dominio digital. Cada uno de estos componentes cumple

un rol específico y complementario, que en conjunto permiten a las fuerzas armadas mantener la integridad de sus sistemas, anticipar y responder a amenazas, y asegurar la continuidad operativa en entornos cada vez más hostiles y dinámicos.

- Monitoreo Continuo. - El monitoreo continuo constituye la base para una gestión efectiva del ciberespacio. Consiste en la vigilancia ininterrumpida de todas las actividades y tráfico dentro de las redes y sistemas informáticos, con el objetivo de detectar comportamientos anómalos, accesos no autorizados, intentos de intrusión y posibles vulnerabilidades antes de que sean explotadas. Este proceso utiliza herramientas avanzadas de análisis de datos, inteligencia artificial y aprendizaje automático para identificar patrones sospechosos, alertando en tiempo real a los equipos de seguridad. La capacidad de monitorear continuamente permite anticipar ataques y responder con rapidez, disminuyendo la ventana de exposición y reduciendo el impacto potencial.

- Defensa Cibernética. - La defensa cibernética comprende un conjunto de medidas técnicas, operativas y políticas diseñadas para proteger la infraestructura digital contra una amplia gama de amenazas. Esto incluye la instalación de firewalls, sistemas de detección y prevención de intrusiones (IDS/IPS), tecnologías antivirus, mecanismos de encriptación, segmentación de redes y control de acceso estricto. Además, la defensa cibernética implica el establecimiento de políticas de seguridad, buenas prácticas y normativas internas para minimizar los riesgos.

- Respuesta a Incidentes. - La capacidad para responder a incidentes de seguridad es esencial para mitigar daños y restaurar rápidamente las operaciones afectadas. Este

componente incluye procedimientos y protocolos para identificar, contener, erradicar y recuperar sistemas tras un ataque o fallo de seguridad. Un plan efectivo de respuesta a incidentes contempla la formación de equipos especializados, la comunicación coordinada entre distintas áreas, y la implementación de herramientas que faciliten la investigación para determinar el origen, naturaleza y alcance del ataque.

- Inteligencia Cibernética. - Se refiere a la recolección, análisis y explotación de información relacionada con amenazas y actores maliciosos en el ciberespacio. Esta información permite anticipar ataques, identificar vulnerabilidades propias y ajenas, y diseñar estrategias defensivas y ofensivas basadas en un conocimiento actualizado del panorama de amenazas.
- Coordinación y Colaboración. - El control ciberespacial efectivo requiere una estrecha coordinación y colaboración entre diferentes unidades militares, organismos gubernamentales, proveedores de tecnología y aliados internacionales. Esta integración operativa y estratégica permite optimizar recursos, compartir información crítica, y responder de manera conjunta y coherente a amenazas complejas y de gran escala.

2.2.9 Impacto del Internet Satelital en el Control Ciberespacial

El uso de internet satelital en el control ciberespacial en zonas remotas representa una solución clave para garantizar la conectividad en áreas geográficas complejas, como las regiones fronterizas o la Amazonía peruana. Esta tecnología permite que destacamentos militares, bases aéreas y otras instalaciones aisladas mantengan comunicaciones constantes y

seguras, incluso en lugares donde las infraestructuras terrestres de telecomunicaciones son limitadas o inexistentes.

Uno de los principales impactos positivos del internet satelital es su capacidad para superar las barreras geográficas y garantizar una conexión confiable en condiciones extremas. Al depender de enlaces de comunicación a través de satélites, el internet satelital proporciona cobertura global, lo que facilita la coordinación de operaciones militares en tiempo real, mejorando significativamente la eficiencia operativa y resiliencia de las fuerzas armadas en áreas remotas. Aunque las comunicaciones satelitales pueden ser vulnerables a interferencias e interceptación de señales, los avances tecnológicos en cifrado y autenticación de extremo a extremo han mejorado sustancialmente la seguridad de estas redes. La implementación de protocolos de encriptación avanzados garantiza que las comunicaciones sean seguras, protegiendo la confidencialidad de los datos sensibles durante su transmisión. Estos avances permiten que la información crítica sea protegida incluso en entornos adversos, lo que fortalece la ciberseguridad en misiones de alto valor estratégico.

Otro aspecto clave del internet satelital es la mejora en los tiempos de latencia gracias a las constelaciones de satélites de órbita baja (LEO). Estos satélites operan a altitudes mucho menores, lo que reduce la latencia de las comunicaciones a niveles significativamente más bajos (de 20 a 50 milisegundos), mejorando la velocidad de transmisión de datos y la capacidad de respuesta ante incidentes cibernéticos o situaciones de emergencia. Esta menor latencia es crucial en operaciones de defensa cibernética, donde la rapidez de la respuesta es fundamental para prevenir y mitigar ataques de manera eficaz. Las constelaciones de satélites LEO, al ofrecer cobertura continua, también brindan la capacidad de mantener conexiones

estables y sin interrupciones, lo que optimiza la eficiencia operativa de las fuerzas armadas. Además, estas constelaciones están diseñadas para ofrecer un servicio confiable y redundante, lo que minimiza las posibilidades de fallos en la comunicación, incluso en condiciones meteorológicas adversas o en regiones remotas donde la infraestructura terrestre podría ser susceptible a daños.

Finalmente, el internet satelital, y en particular las mejoras que ofrecen las constelaciones de satélites LEO, no solo resuelven el desafío de la conectividad en áreas remotas, sino que también fortalecen la seguridad y eficacia de las operaciones militares. Esta tecnología representa una ventaja estratégica significativa, permitiendo a la Fuerza Aérea del Perú mejorar su capacidad de respuesta en el control ciberespacial y en la defensa nacional, asegurando que sus destacamentos remotos estén debidamente conectados y protegidos en todo momento.

2.3. Glosario

Con el propósito de facilitar la comprensión de los términos técnicos y especializados utilizados en este estudio, se presenta a continuación definiciones clave relacionadas con el internet satelital, el control ciberespacial y el entorno operativo de la Fuerza Aérea del Perú. Este apartado busca estandarizar el uso del lenguaje técnico y garantizar una interpretación precisa y coherente de los términos empleados.

Cobertura:

Se refiere al área geográfica en la cual un sistema de comunicación o red, como el servicio de internet satelital, puede proporcionar conectividad efectiva y continua.

Área geográfica:

Espacio físico delimitado sobre la superficie terrestre que puede estar comprendido por factores topográficos, políticos o estratégicos, y que determina el ámbito de operación o influencia de un sistema de comunicación o acción militar.

Tiempo de conexión:

Duración por la cual un usuario o sistema mantiene acceso activo y estable a un servicio de comunicación o red. En operaciones ciberespaciales, la continuidad del tiempo de conexión es crítica para asegurar la disponibilidad y eficacia del control y mando.

Calidad:

Conjunto de atributos que determinan la capacidad de un servicio de comunicación para cumplir con los requerimientos operativos, incluyendo estabilidad, integridad de datos, velocidad y latencia.

Velocidad:

Tasa a la cual los datos son transmitidos a través de una red o sistema de comunicación, normalmente medida en megabits por segundo (Mbps). La velocidad afecta directamente la capacidad para procesar información en tiempo real durante operaciones ciberespaciales.

Latencia:

Hace referencia al tiempo que tarda un paquete de datos en viajar desde el origen hasta el destino y viceversa, medido en milisegundos (ms).

Usabilidad:

Se define como el grado en que un sistema o servicio puede ser utilizado por usuarios específicos para lograr objetivos específicos con efectividad, eficiencia y satisfacción en un contexto operativo.

Accesibilidad total:

Capacidad de un sistema o red para ser accesible y utilizable por cualquier usuario o dispositivo autorizado, en cualquier momento y lugar dentro del área de cobertura, sin restricciones técnicas o físicas.

Operaciones Defensivas:

Conjunto de medidas preventivas, proactivas, reactivas y de recuperación destinadas a proteger las redes y sistemas informáticos contra ataques o intrusiones, asegurando la integridad, confidencialidad y disponibilidad de la información crítica.

Medidas preventivas:

Hace referencia a las acciones orientadas a evitar la ocurrencia de incidentes mediante controles y políticas de seguridad.

Medidas proactivas:

Se describe como las actividades de vigilancia y monitoreo continúo destinadas a la detección anticipada de amenazas antes de que causen daño.

Medidas reactivas:

Hace referencia a las respuestas inmediatas para contener y mitigar ataques detectados.

Medidas de recuperación:

Son los procedimientos para restaurar la operatividad de sistemas y servicios a su estado normal tras un incidente.

Operaciones de Explotación:

Son las actividades destinadas a la búsqueda, detección e identificación de información y amenazas en el ciberespacio para obtener ventaja estratégica. Incluyen técnicas de inteligencia cibernética y monitoreo continuo de sistemas y redes.

Búsqueda:

Se define como el proceso sistemático de localización de información, vulnerabilidades y amenazas.

Detección:

Hace referencia a la identificación de actividad anómala o maliciosa dentro de una red o sistema.

Identificación:

Se refiere al análisis detallado que permite atribuir la amenaza, determinar su naturaleza y establecer su posible origen.

Operaciones de Respuesta:

Son las acciones dirigidas a negar, degradar o interrumpir las capacidades del adversario en el ciberespacio, con el fin de neutralizar amenazas y proteger la infraestructura crítica.

Denegación:

Hace referencia a las acciones que buscan impedir el acceso o el funcionamiento del sistema adversario.

Degradación:

Se define como las acciones para reducir la eficacia operativa del sistema enemigo, afectando su rendimiento o disponibilidad.

Interrupción:

Consiste en provocar fallas temporales o permanentes que imposibilitan el uso de la infraestructura en el sistema objetivo.

CAPÍTULO IV: METODOLÓGIA

3.1 Diseño de la investigación

El diseño es de enfoque cualitativo, de alcance exploratorio y de diseño experimental seleccionado para esta investigación es el más adecuado debido a la naturaleza compleja y multidimensional del fenómeno que se estudia.

En primer lugar, el enfoque cualitativo permite obtener una comprensión profunda y contextualizada de las experiencias, percepciones y valoraciones del personal militar involucrado, así como de los factores técnicos, operativos y de seguridad que influyen en la implementación y uso de esta tecnología. Este enfoque posibilita captar la complejidad y las particularidades del entorno militar y geográfico en que se desarrollan las operaciones, aspectos que difícilmente podrían ser cuantificados o generalizados a través de métodos numéricos.

En segundo lugar, el carácter descriptivo es fundamental para detallar las características específicas del internet satelital en el contexto particular de los destacamentos remotos, permitiendo identificar sus fortalezas, limitaciones y oportunidades. Esta descripción detallada es clave para comprender el grado de factibilidad y los aspectos que requieren mejoras o intervenciones.

Por último, la investigación es exploratoria porque aborda un campo poco estudiado dentro del contexto peruano y militar. Este diseño permite descubrir variables relevantes, relaciones y dinámicas que pueden no estar claramente definidas en la literatura existente,

proporcionando una base sólida para estudios futuros y la formulación de políticas o estrategias adecuadas para la Fuerza Aérea.

Finalmente, este diseño metodológico es coherente con los objetivos de la investigación y responde a la necesidad de generar conocimiento aplicado, pertinente y contextualizado que apoye el fortalecimiento de la capacidad operativa y la soberanía tecnológica de la Fuerza Aérea del Perú en el dominio ciberespacial.

3.2 Población y muestra

La población objetivo de esta investigación está conformada por el personal operativo, técnico y de mando que participa directa o indirectamente en las operaciones de control ciberespacial en los destacamentos remotos de la Fuerza Aérea del Perú. Esta población incluye especialistas en tecnologías de la información y comunicaciones, personal encargado del mantenimiento y operación del servicio de internet satelital, así como oficiales responsables de la supervisión y coordinación de las actividades relacionadas con la vigilancia y control en el ciberespacio. Dado el carácter estratégico y la naturaleza sensible de las actividades, la población se encuentra distribuida en diversas unidades y bases militares localizadas en zonas geográficas con alta complejidad logística y operacional.

Para la recolección de datos se seleccionó una muestra no probabilística, que incluye a miembros con experiencia y conocimiento específico en el uso y gestión del internet satelital y el control ciberespacial. Esta selección busca garantizar la calidad y relevancia de la información, priorizando la participación de individuos con capacidad para aportar perspectivas técnicas, operativas y estratégicas.

Se estimó incluir un número adecuado de participantes para la prueba piloto, aproximadamente de 20 personas, dependiendo de la disponibilidad y acceso facilitado por la institución. La muestra abarcará diferentes niveles jerárquicos y roles funcionales para obtener una visión integral y multidimensional del fenómeno estudiado.

El tamaño y composición de la muestra responderán a criterios de saturación teórica, es decir, se continuará incorporando participantes hasta que la información recopilada sea suficiente para comprender la finalidad del estudio y no se obtengan datos nuevos o relevantes adicionales.

Para una población de 100 individuos, se ha calculado que una muestra de aproximadamente 95 personas, asumiendo un nivel de confianza del 95% y un margen de error del 5%.

$$n = \frac{Z^2 p.qN}{(N-1)e^2 + Z^2 p.q}$$

Dónde:

Z: Es el valor de la abscisa de la curva normal para una probabilidad del 95 % de confianza.

p: Es la proporción de la muestra buscada al 50% de los 95 miembros de la encuesta.

q: Representa la proporción restante de la población, es decir la otra mitad.

e: Este valor representa el margen de error que se presenta en la población el 5 %.

N: Representa la población total del estudio como es 95 miembros de la encuesta.

n: Representa el tamaño muestral que se ha calculado.

3.3 Técnicas e instrumentos de recolección de datos

Para la recolección de datos necesarios para evaluar la factibilidad del uso de internet satelital en el control ciberespacial en destacamentos remotos de la Fuerza Aérea del Perú, se emplearon técnicas e instrumentos orientados a captar no solo la información documental relevante, sino también las experiencias, percepciones y valoraciones del personal directamente involucrado en las operaciones. De esta manera se permitió obtener evidencia sólida, tanto desde el análisis técnico y operativo, como desde la perspectiva crítica de cada personal.

La técnica principal fue la encuesta semiestructurada, diseñada para recopilar datos cualitativos detallados y contextuales de manera flexible. Este método permitió explorar temáticas específicas relacionadas con los aspectos técnicos, operativos, económicos y de seguridad del internet satelital, al mismo tiempo que brindo la posibilidad de profundizar en temas emergentes durante la interacción con los encuestados.

Se diseñó un instrumento conformado de preguntas abiertas y orientativas, agrupadas en seis dimensiones fundamentales: cobertura, calidad, usabilidad y de operaciones defensivas, de explotación y respuesta. Esta guía sirvió como base para dirigir las encuestas asegurando la cobertura de los temas relevantes y permitiendo que al encuestado exprese libremente sus experiencias y opiniones. La guía incluye preguntas directas que profundizan en aspectos clave. De manera complementaria, se diseñó un cuestionario estructurado con escala tipo Likert con cinco puntos, compuesto con una serie de afirmaciones relacionadas con las dimensiones clave del estudio.

Este cuestionario, aplicado como encuesta, facilito la cuantificación de la opinión de los participantes respecto a los diferentes aspectos técnicos, operativos, económicos y de seguridad del servicio de internet satelital. Asimismo, permitió la estandarización de las respuestas, lo que posibilito realizar comparaciones entre participantes y aplicar análisis estadísticos posteriores. Gracias a ello, fue factible identificar tendencias, fortalezas y debilidades percibidas en el servicio.

Cuadro 4: Escala de valoración

ESCALA DE LIKERT	
Totalmente en desacuerdo	1
En desacuerdo	2
Ni de acuerdo ni en desacuerdo	3
De acuerdo	4
Totalmente de acuerdo	5

Nota: Elaboración propia. Valoración de la escala de Likert.

Cuadro 5: Instrumentos de recolección de datos

VARIABLES	DIMENSIONES	INDICADORES	ÍTEMS
Internet Satelital	Cobertura	Área geográfica	1. El servicio de internet satelital cubre adecuadamente las zonas remotas donde opera la Fuerza Aérea del Perú.
			2. La cobertura satelital permite mantener conexión constante en áreas de difícil acceso.
			3. La cobertura actual satisface las necesidades de comunicación en los destacamentos remotos.
		Tiempo de conexión	4. El tiempo de conexión a internet satelital es continuo y sin interrupciones significativas.
			5. El servicio satelital garantiza la disponibilidad de conexión durante las operaciones críticas.
			6. La conexión a internet satelital es estable y confiable en el tiempo necesario para las operaciones.
	Calidad	Velocidad	7. La velocidad de descarga y subida del internet satelital es suficiente para las actividades de control ciberespacial.
			8. El internet satelital permite la transmisión fluida de datos, voz y video sin retrasos importantes.
			9. La velocidad del servicio satelital cumple con los requerimientos operativos de la Fuerza Aérea.
		Latencia	10. La latencia del internet satelital es adecuada para las comunicaciones en tiempo real.
			11. El retraso en la transmisión de datos vía satélite no afecta el desempeño de las operaciones ciberespaciales.
			12. La latencia del servicio satelital permite una respuesta rápida en situaciones críticas.
	Usabilidad	Facilidad de uso	13. El sistema de internet satelital es fácil de operar para el personal técnico y operativo.

			14.El personal recibe capacitación adecuada para el manejo del servicio satelital.
			15.Los equipos y dispositivos del internet satelital son intuitivos y amigables para su uso diario.
		Accesibilidad total	16.El internet satelital está disponible para todos los usuarios autorizados en los destacamentos remotos.
			17.No existen restricciones técnicas que limiten el acceso al servicio satelital en las zonas operativas.
			18.La infraestructura satelital permite un acceso ininterrumpido para las operaciones militares.
Control Ciberespacial	Operaciones Defensivas	Medidas preventivas	19.Existen políticas claras para prevenir ataques cibernéticos en las comunicaciones satelitales.
			20.Se realizan revisiones periódicas para identificar vulnerabilidades en la red satelital.
		Medidas proactivas	21.Se monitorea continuamente el tráfico de datos para detectar posibles amenazas.
			22.El personal está capacitado para anticipar y responder a incidentes cibernéticos.
		Medidas reactivas	23.Existen protocolos claros para responder a incidentes de seguridad en el internet satelital.
			24.El equipo de respuesta actúa rápidamente para contener ataques cibernéticos.
		Medidas de recuperación	25.Se cuenta con planes de contingencia para restaurar el servicio en caso de interrupciones.
			26.La Fuerza Aérea dispone de recursos adecuados para la recuperación ante fallas de seguridad.
	Operaciones de explotación	Búsqueda	27.El personal utiliza herramientas adecuadas para localizar amenazas en el ciberespacio.
			28.La búsqueda de datos contribuye a la anticipación de ataques o vulnerabilidades.

		Detección	29.Se identifican rápidamente posibles intentos de intrusión en la red satelital.
			30.La detección oportuna permite la activación inmediata de medidas defensivas.
		Identificación	31.Se determina el origen de los ataques para diseñar respuestas adecuadas.
			32.La identificación precisa de incidentes fortalece la protección del sistema satelital.
	Operaciones de respuesta	Denegación	33.Se aplican acciones efectivas para impedir ataques que comprometan la comunicación satelital.
			34.Las operaciones de denegación contribuyen a mantener la integridad del sistema.
		Degradación	35.Se implementan medidas para reducir la eficacia de ataques en curso.
			36.El sistema de internet satelital facilita la ejecución de maniobras cibernéticas.
		Interrupción	37.La conectividad satelital garantiza la capacidad de neutralizar temporalmente redes enemigas en el ciberespacio.
			38.El sistema satelital facilita la ejecución de medidas sin comprometer la operatividad de los sistemas propios.

Nota: Elaboración propia

CAPÍTULO IV: INTERPRETACIÓN DE LOS RESULTADOS

4.1 Presentación e interpretación de los resultados

Según Hernández et.al (2014), la presentación de resultados debe realizarse de forma ordenada y objetiva, mientras que la interpretación implica contrastar los hallazgos con la teoría. En mi caso, presenté primero los resultados en tablas y figuras, y luego, siguiendo a Strauss y Corbin (2002), realicé una interpretación cualitativa que permitió identificar las relaciones entre la conectividad satelital y el control ciberespacial en los destacamentos de la Fuerza Aérea del Perú.

En esta sección, se presenta un análisis detallado de los resultados obtenidos a partir de las encuestas realizadas con el fin de evaluar la percepción sobre la cobertura del internet satelital en los destacamentos remotos de la Fuerza Aérea del Perú. Este análisis tiene como objetivo profundizar en la efectividad y confiabilidad del servicio de internet satelital, especialmente en las zonas de difícil acceso, donde la conectividad suele ser limitada. Se ha buscado comprender, a través de las opiniones de los encuestados, el impacto de esta tecnología en su desempeño operativo y en el control ciberespacial.

Según Hernández, Fernández y Baptista (2014), “los cuestionarios son instrumentos estructurados que permiten obtener información específica de los participantes, de acuerdo con los objetivos del estudio, garantizando uniformidad en las respuestas y facilitando su análisis” (p. 206). Por ello, las encuestas aplicadas se dividieron en dos cuestionarios principales: uno enfocado en el uso y la cobertura del internet satelital, y otro relacionado con el control ciberespacial en estos destacamentos. Ambos cuestionarios fueron diseñados para recoger

información clave sobre la calidad del servicio de internet en entornos remotos, proporcionando una visión integral de cómo estos aspectos se relacionan con las necesidades operativas de la Fuerza Aérea del Perú.

A través de los datos recopilados, se busca entender las fortalezas**,** debilidades y las áreas de mejora en el uso de esta tecnología en el contexto de las operaciones militares. Se analizan aspectos como la estabilidad de la conexión, la velocidad de acceso, la capacidad de respuesta en situaciones de alta demanda y la eficiencia general del servicio en condiciones extremas. Además, se exploran las áreas de mejora necesarias para optimizar el rendimiento de esta tecnología en escenarios remotos, donde las condiciones para la conectividad son más adversas.

Según Hernández, Fernández y Baptista (2014), "las investigaciones aplicadas no solo buscan describir o comprender un fenómeno, sino también ofrecer alternativas, propuestas o recomendaciones que contribuyan a resolver problemas reales" (p. 92). En ese sentido, el presente estudio pretende proporcionar una comprensión integral sobre el impacto del internet satelital en las operaciones de la Fuerza Aérea del Perú, identificando sus ventajas, limitaciones y oportunidades de mejora. A partir de los resultados obtenidos, se plantean propuestas orientadas a optimizar la conectividad y la seguridad de los sistemas de comunicación en destacamentos remotos, fortaleciendo así las capacidades operativas y el control ciberespacial en áreas estratégicas del territorio nacional.

Cuadro 6: Distribución de las características sociodemográficas

Variable	Categorías	Cantidad	Porcentaje
Género	Femenino	21	21%
	Masculino	79	79%
Rango de edad	De 25 a 34 años	24	24%
	De 35 a 44 años	36	36%
	De 45 a 54 años	40	40%
Plana Laboral	Oficial	32	32%
	TT.SS.OO	68	68%

Nota: Elaboración propia.

Análisis: El Cuadro 6 presenta la distribución sociodemográfica del personal militar participante en el estudio, compuesto por 100 efectivos de la Fuerza Aérea del Perú. En cuanto al género, se observa una predominancia masculina (79%), lo que refleja la composición tradicional del personal operativo en las unidades militares, especialmente en áreas técnicas como telecomunicaciones, ciberseguridad y sistemas TIC. La presencia femenina (21%) evidencia una participación creciente de mujeres en funciones tecnológicas y de apoyo a las operaciones aeroespaciales, lo cual es un indicador positivo de inclusión institucional. Respecto al rango de edad, el grupo etario más numeroso corresponde al personal entre 45 y 54 años (40%), seguido de los de 35 a 44 años (36%) y 25 a 34 años (24%). Este patrón sugiere que la mayoría de los participantes cuenta con una amplia experiencia profesional, lo cual favorece la calidad de la información proporcionada, al reflejar percepciones basadas en años de servicio y conocimiento técnico-operativo.

Cuadro 7: Resultados Prueba Alfa de Crombach

Variable/Dimensión	N de elementos	Alfa de Cronbach
Internet Satelital	18	0,922
Cobertura	6	0,901
Calidad	6	0,878
Usabilidad	6	0,902
Control Ciberespacial	20	0,944
Operaciones Defensivas	8	0.904
Operaciones de Explotación	6	0,912
Operaciones de Respuesta	6	0,896

Nota: Elaboración propia.

Análisis: El Cuadro 7 presenta los valores del coeficiente Alfa de Cronbach aplicados a las variables e indicadores del instrumento de investigación, con el propósito de determinar la consistencia interna y confiabilidad de los ítems diseñados. Según Hernández, Fernández y Baptista (2014), un instrumento es confiable cuando sus ítems muestran una alta correlación entre sí, indicando que miden de manera coherente el mismo constructo teórico. En general, valores de $\alpha \geq 0.70$ se consideran aceptables; $\alpha \geq 0.80$ son buenos, y $\alpha \geq 0.90$ reflejan una confiabilidad excelente.

En este estudio, los resultados muestran niveles óptimos de confiabilidad en todas las dimensiones. La variable Internet Satelital alcanzó un $\alpha = 0.922$, lo cual evidencia una consistencia interna muy alta en los 18 ítems que evalúan su uso, cobertura, calidad y usabilidad. De manera particular, los indicadores Cobertura ($\alpha = 0.842$), Calidad ($\alpha = 0.855$) y Usabilidad ($\alpha = 0.902$) presentan valores que indican una medición estable y coherente,

asegurando la precisión de las percepciones obtenidas sobre el desempeño del servicio satelital en entornos remotos. Por su parte, la variable Control Ciberespacial alcanzó un $\alpha = 0.944$, considerado excelente, lo que confirma la consistencia del instrumento para medir las percepciones vinculadas a las operaciones defensivas, de explotación y de respuesta. Estos indicadores también registraron niveles de confiabilidad elevados: Operaciones Defensivas ($\alpha = 0.904$), Operaciones de Explotación ($\alpha = 0.912$) y Operaciones de Respuesta ($\alpha = 0.891$).

En conjunto, los valores obtenidos indican que el instrumento aplicado es altamente confiable, lo cual refuerza la validez de los datos recolectados y la solidez de las conclusiones derivadas del estudio.

Cuadro 8. Resultados de las medidas descriptivas de las variables

Variable/Dimensión	Media	Desv. Desviación
Internet Satelital	4,13	,423
Cobertura	4,10	,435
Calidad	4,10	,435
Usabilidad	4,34	,439
Control Ciberespacial	4,41	,452
Operaciones Defensivas	4,13	,423
Operaciones de Explotación	4,34	,439
Operaciones de Respuesta	4,28	,449

Nota: Elaboración propia

El cuadro muestra los valores promedios (media) y la desviación estándar correspondientes a las variables Internet Satelital y Control Ciberespacial, junto con sus

respectivas dimensiones. Estos resultados permiten interpretar el nivel de percepción del personal militar respecto al uso y efectividad del internet satelital en los destacamentos remotos de la FAP. En términos generales, las medias obtenidas son altas (superiores a 4.0), lo que evidencia una percepción favorable por parte de los participantes hacia la tecnología satelital y su contribución al control ciberespacial. Las desviaciones estándar bajas (entre 0.423 y 0.452) indican consistencia y homogeneidad en las respuestas, lo que significa que la mayoría de los encuestados coincidió en su valoración positiva del servicio.

La variable Internet Satelital alcanzó una media general de 4.13, reflejando una buena aceptación de esta tecnología como medio de comunicación confiable en zonas de difícil acceso. Dentro de sus dimensiones, la usabilidad (M = 4.34; DE = 0.439) obtuvo el valor más alto, lo que sugiere que el personal considera el sistema fácil de utilizar y adaptable a las necesidades operativas. Las dimensiones de cobertura (M = 4.10; DE = 0.435) y calidad (M = 4.10; DE = 0.435) también presentan valoraciones positivas, aunque ligeramente inferiores, lo que indica satisfacción general con la estabilidad y alcance del servicio, pero con áreas susceptibles de mejora, especialmente en entornos geográficos adversos.

Respecto a la variable Control Ciberespacial, se obtuvo una media de 4.41 con una desviación estándar de 0.452, lo cual representa una percepción muy favorable del impacto del internet satelital en las operaciones digitales de la FAP. Dentro de esta variable, las operaciones de explotación (M = 4.34; DE = 0.439) fueron las mejor valoradas, seguidas por las operaciones de respuesta (M = 4.28; DE = 0.449) y las operaciones defensivas (M = 4.13; DE = 0.423). Estos valores demuestran que el uso del internet satelital contribuye

significativamente a mejorar la eficiencia en la transmisión de información, la detección de amenazas y la capacidad de respuesta ante incidentes cibernéticos.

En conjunto, los resultados reflejan que el personal militar percibe el internet satelital como una herramienta tecnológica confiable, accesible y estratégica, que fortalece las capacidades de defensa, vigilancia y control ciberespacial en zonas remotas.

4.1.1 *Cuestionario 1 "Internet Satelital"*

4.1.1.1 Dimensión: Cobertura.

- ✓ **Área Geográfica**

Cuadro 9

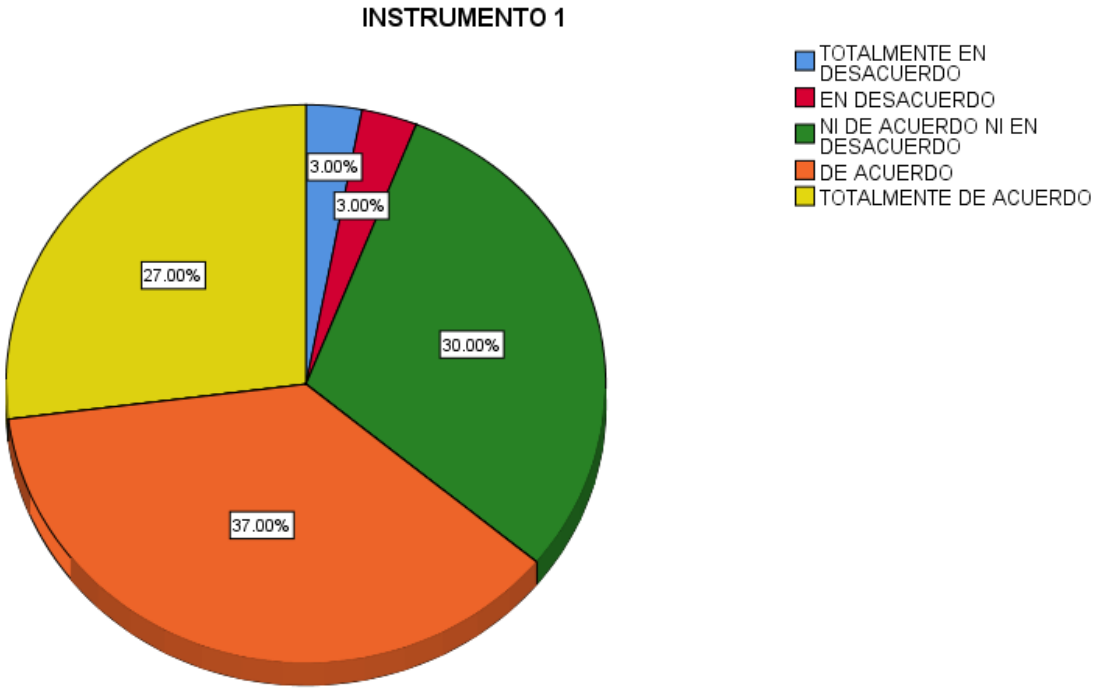
"El servicio de internet satelital cubre adecuadamente las zonas remotas donde opera la Fuerza Aérea del Perú".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en Desacuerdo	3	3.0	3.0	3.0
En Desacuerdo	3	3.0	3.0	6.0
Ni de Acuerdo ni en Desacuerdo	30	30.0	30.0	36.0
De Acuerdo	37	37.0	37.0	73.0
Totalmente de Acuerdo	27	27.0	27.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 6

"El servicio de internet satelital cubre adecuadamente las zonas remotas donde opera la Fuerza Aérea del Perú".



Nota: Elaboración propia. Imagen generada con el software SPSS25.

Análisis: Con respecto al instrumento N°1 el análisis de los datos sugiere que el internet satelital es generalmente bien percibido en cuanto a su cobertura geográfica, con una clara mayoría de 64 encuestados (64%) que considera que el servicio cubre adecuadamente las zonas remotas. Sin embargo, la neutralidad de un 30% de los encuestados resalta la necesidad de proporcionar más información y experiencias que ayuden a aclarar las dudas existentes sobre la calidad de la cobertura. La baja proporción de desacuerdo de 6 encuestados (6%) refuerza la validez de la tecnología satelital como una herramienta útil y eficiente para las operaciones militares en áreas donde otras tecnologías de comunicación no son viables.

Cuadro 10

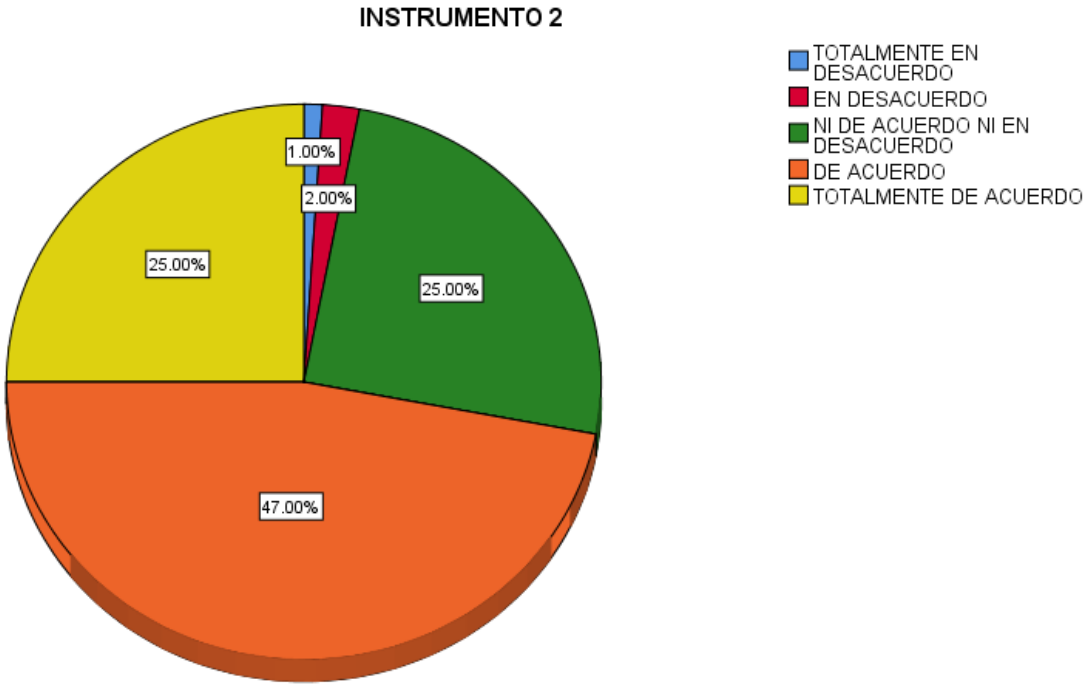
"La cobertura satelital permite mantener conexión constante en áreas de difícil acceso".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en Desacuerdo	1	1.0	1.0	1.0
En Desacuerdo	2	2.0	2.0	3.0
Ni de Acuerdo ni en Desacuerdo	25	25.0	25.0	28.0
De Acuerdo	47	47.0	47.0	75.0
Totalmente de Acuerdo	25	25.0	25.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 7

"La cobertura satelital permite mantener conexión constante en áreas de difícil acceso".



Nota: Elaboración propia. Imagen generada con el software SPSS25.

Análisis: En el instrumento N°2 existe una percepción positiva de un 72 % sobre el tiempo de conexión del internet satelital siendo bastante favorable. Sin embargo, la neutralidad del 25% es un aspecto que debe ser tomado en cuenta, ya que sugiere que aún hay dudas o incertidumbre en algunos sectores sobre la estabilidad del servicio. Por otro lado, el 3% de desacuerdo también indica la posibilidad de que en algunas zonas o condiciones específicas el servicio no sea tan efectivo. Este análisis es útil para identificar tanto las áreas de mejora como la efectividad general del internet satelital en las operaciones en áreas remotas.

Cuadro 11

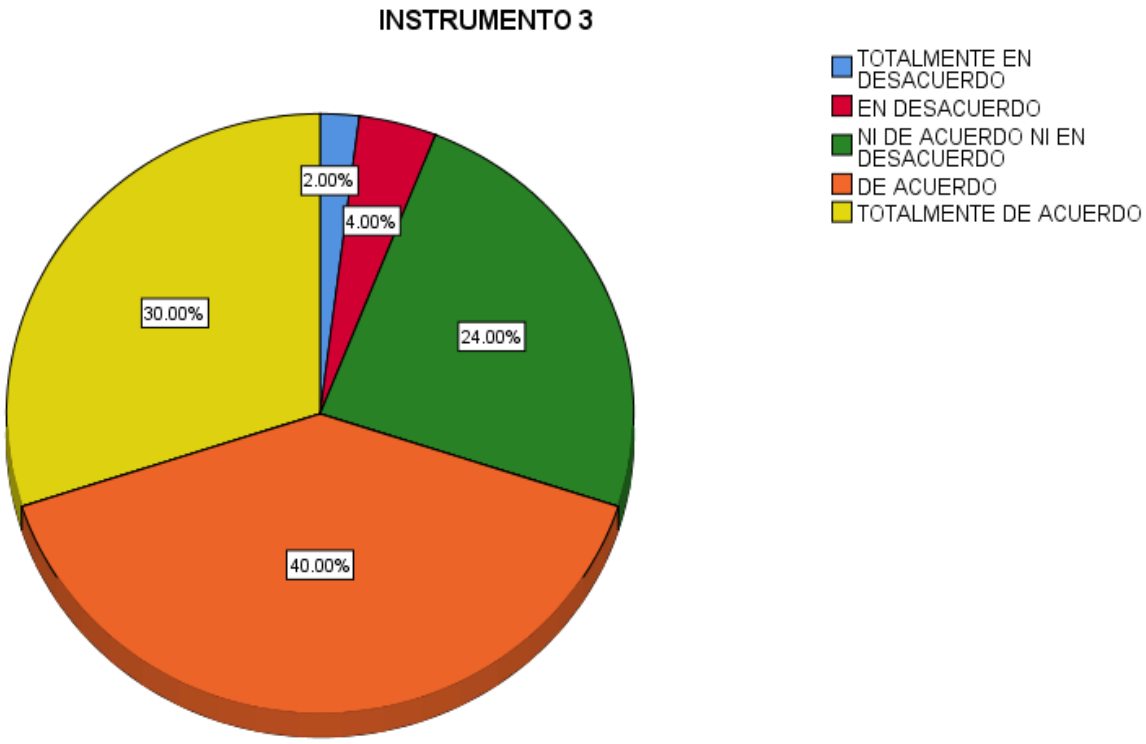
"La cobertura actual satisface las necesidades de comunicación en los destacamentos remotos".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en Desacuerdo	2	2.0	2.0	2.0
En Desacuerdo	4	4.0	4.0	6.0
Ni de Acuerdo ni en Desacuerdo	24	24.0	24.0	30.0
De Acuerdo	40	40.0	40.0	70.0
Totalmente de Acuerdo	30	30.0	30.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 8

"La cobertura actual satisface las necesidades de comunicación en los destacamentos remotos".



Nota: Elaboración propia. Imagen generada con el software SPSS25.

Análisis: En el instrumentoN°3, el internet satelital es percibido de manera positiva en términos de velocidad, con un 70% de los encuestados de acuerdo con que la cobertura satisface las necesidades de comunicación en los destacamentos remotos. Sin embargo, el 24% neutral indica que algunas personas no tienen una evaluación clara sobre la calidad del servicio, lo que podría deberse a una falta de experiencia o conocimiento directo. El 6% en desacuerdo señala que, aunque el servicio es generalmente eficaz, en algunos casos no está cumpliendo con las expectativas o necesidades.

- ✓ **Tiempo de Conexión**

Cuadro 12

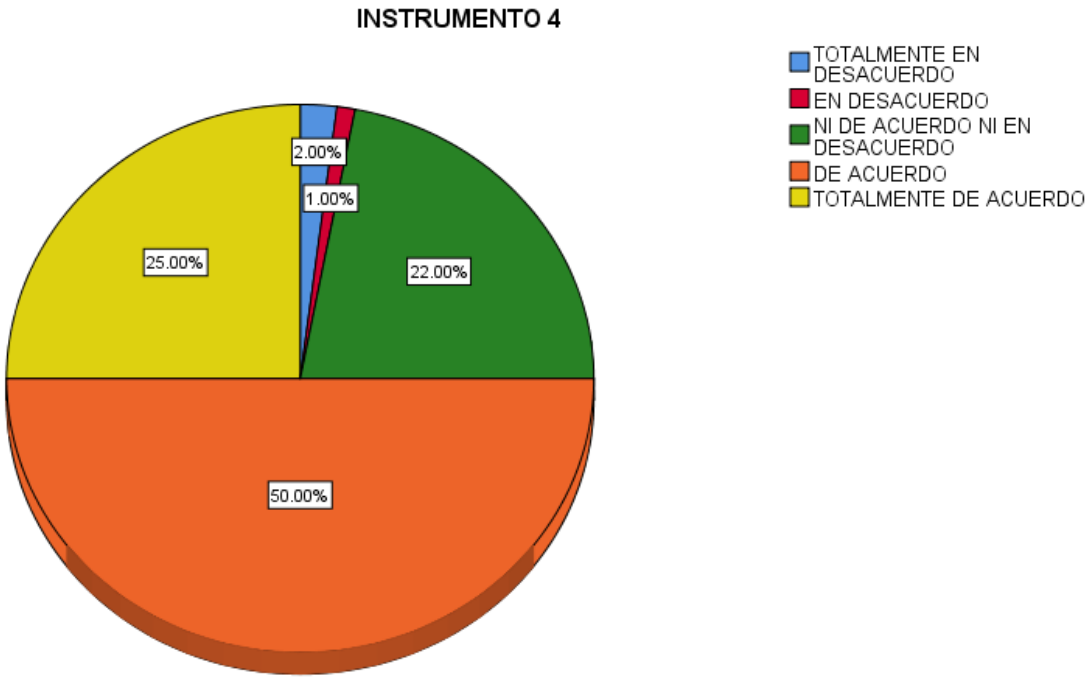
"El tiempo de conexión a internet satelital es continuo y sin interrupciones significativas".

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
Totalmente en Desacuerdo	2	2.0	2.0	2.0
En Desacuerdo	1	1.0	1.0	3.0
Ni de Acuerdo ni en Desacuerdo	22	22.0	22.0	25.0
De Acuerdo	50	50.0	50.0	75.0
Totalmente de Acuerdo	25	25.0	25.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 9

"El tiempo de conexión a internet satelital es continuo y sin interrupciones significativas".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumentoN°4, la percepción sobre el tiempo de conexión a internet satelital es mayormente positiva, con un 75% de los encuestados (50% de acuerdo y 25% totalmente de acuerdo) indicando que el servicio es continuo y sin interrupciones significativas. Sin embargo, 22% de los encuestados permanece neutral, lo que puede reflejar dudas o falta de experiencia en la evaluación del servicio. Solo un 3% de los encuestados considera que la conexión no es continua, lo que sugiere que, pueden haber experimentado interrupciones o inconsistencias en su experiencia.

Cuadro 13

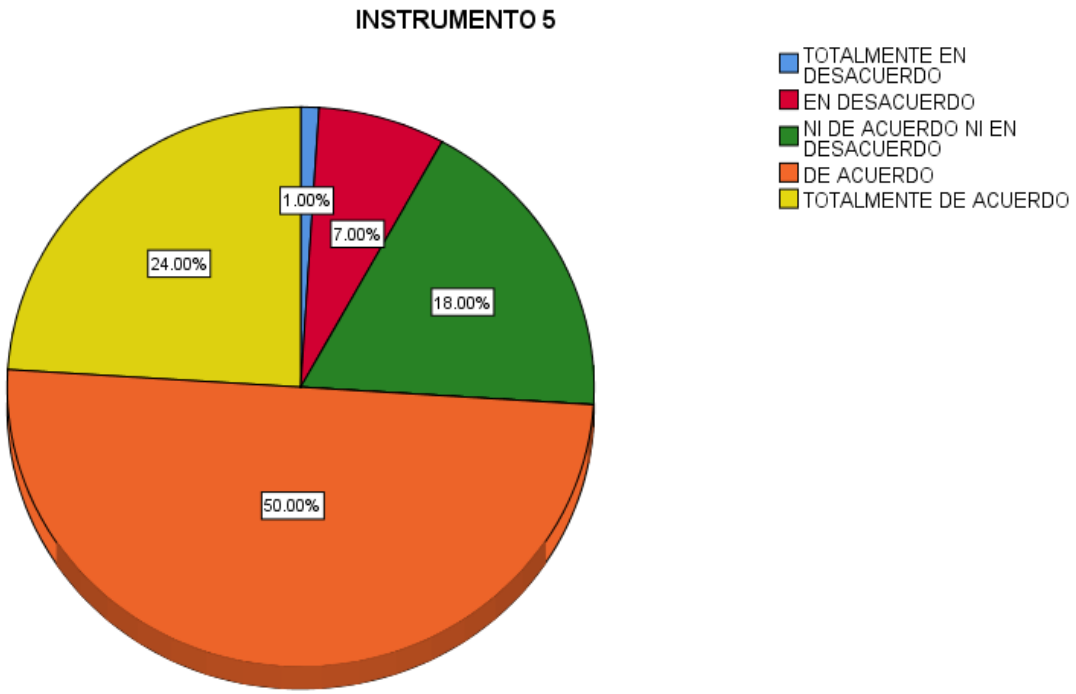
"El servicio satelital garantiza la disponibilidad de conexión durante las operaciones críticas".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en Desacuerdo	1	1.0	1.0	1.0
En Desacuerdo	7	7.0	7.0	8.0
Ni de Acuerdo ni en Desacuerdo	18	18.0	18.0	26.0
De Acuerdo	50	50.0	50.0	76.0
Totalmente de Acuerdo	24	24.0	24.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 10

"El servicio satelital garantiza la disponibilidad de conexión durante las operaciones críticas".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumentoN°5, el servicio satelital es percibido positivamente en términos de facilidad de uso, con un 76% de los encuestados (50% de acuerdo y 24% totalmente de acuerdo) indicando que el sistema es fácil de operar. Sin embargo, un 26% permanece neutral o en desacuerdo, lo que sugiere que una pequeña proporción de usuarios encuentra dificultades en el uso o manejo del servicio. Este dato podría reflejar la necesidad de proporcionar asistencia técnica adicional para aquellos que no perciben el sistema como intuitivo o fácil de usar.

Cuadro 14

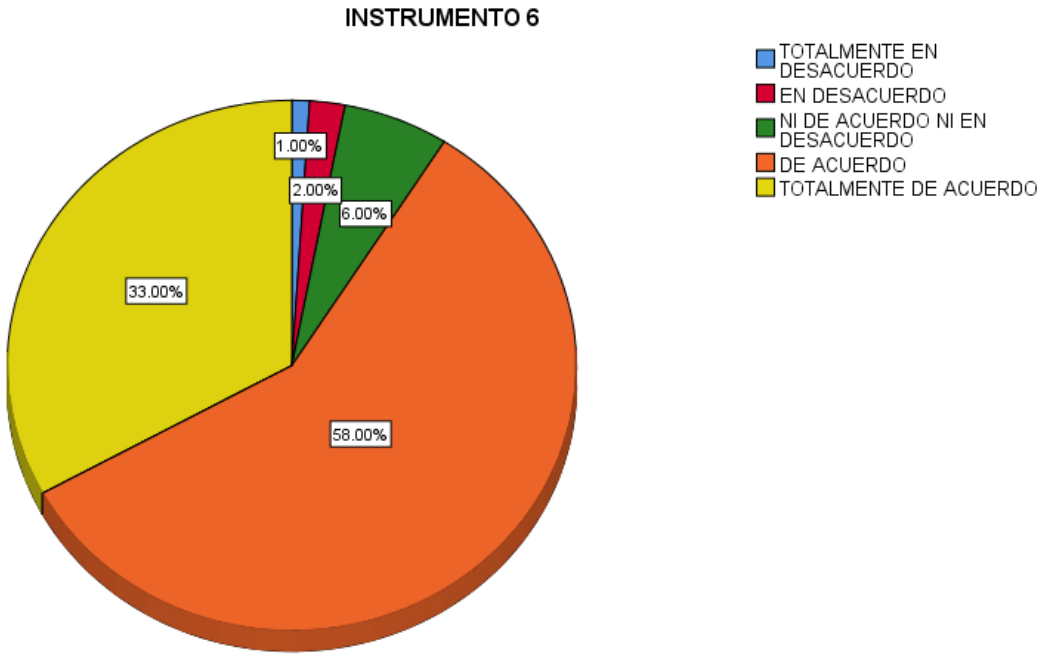
"La conexión a internet satelital es estable y confiable en el tiempo necesario para las operaciones".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en Desacuerdo	1	1.0	1.0	1.0
En Desacuerdo	2	2.0	2.0	3.0
Ni de Acuerdo ni en Desacuerdo	6	6.0	6.0	9.0
De Acuerdo	58	58.0	58.0	67.0
Totalmente de Acuerdo	33	33.0	33.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 11

"La conexión a internet satelital es estable y confiable en el tiempo necesario para las operaciones".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumento N° 6, se evidencia que la conexión a internet satelital es generalmente considerada estable y confiable, con un 91% de los encuestados (58% de acuerdo y 33% totalmente de acuerdo) afirmando que cumple con los requisitos de estabilidad necesarios para las operaciones. Solo un 9% se muestra neutral o en desacuerdo, lo que indica que, en general, el servicio es confiable para las operaciones, aunque un pequeño porcentaje de usuarios podría haber experimentado dificultades ocasionales con la accesibilidad o estabilidad del servicio.

4.1.1.2 Dimensión: Calidad

- ✓ **Velocidad**

Cuadro 15

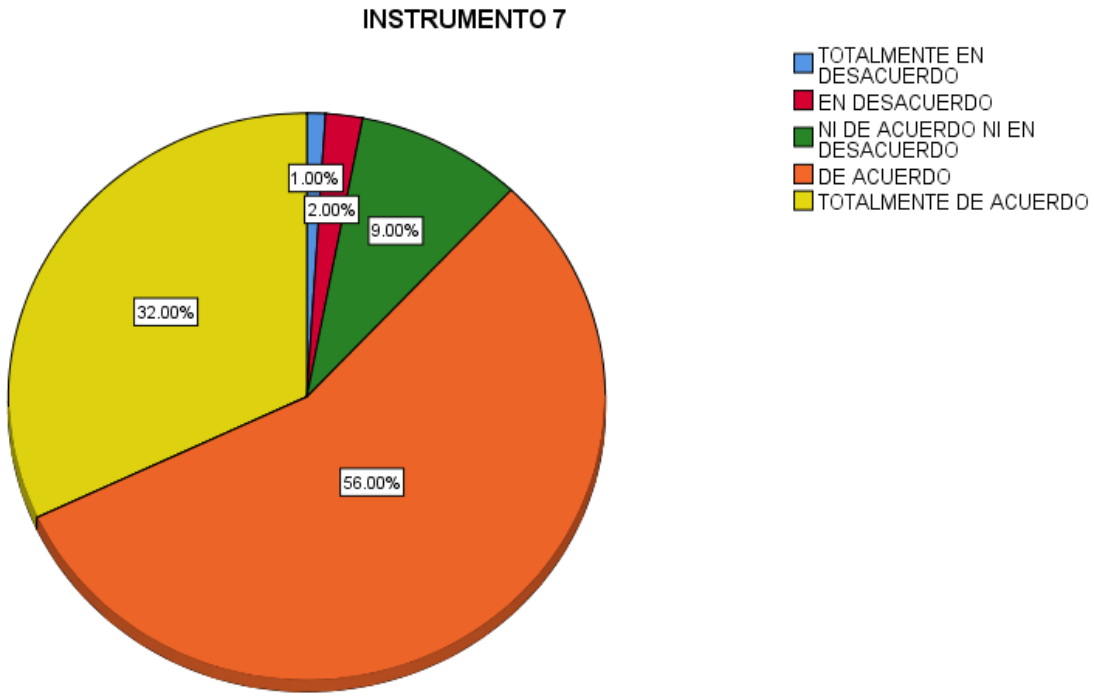
"La velocidad de descarga y subida del internet satelital es suficiente para las actividades de control ciberespacial".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en Desacuerdo	1	1.0	1.0	1.0
En Desacuerdo	2	2.0	2.0	3.0
Ni de Acuerdo ni en Desacuerdo	9	9.0	9.0	12.0
De Acuerdo	56	56.0	56.0	68.0
Totalmente de Acuerdo	32	32.0	32.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 12

"La velocidad de descarga y subida del internet satelital es suficiente para las actividades de control ciberespacial".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumentoN°7 la velocidad de descarga y subida del internet satelital es percibida como adecuada para las actividades de control ciberespacial, con un 88% de los encuestados (56% de acuerdo y 32% totalmente de acuerdo) indicando que cumple con los requisitos operativos. Solo un 12% permanece neutral o en desacuerdo, lo que sugiere que, en general, la velocidad del servicio es adecuada para las medidas preventivas del control ciberespacial, aunque podría haber casos específicos donde la velocidad no sea suficiente para ciertos requerimientos o actividades.

Cuadro 16

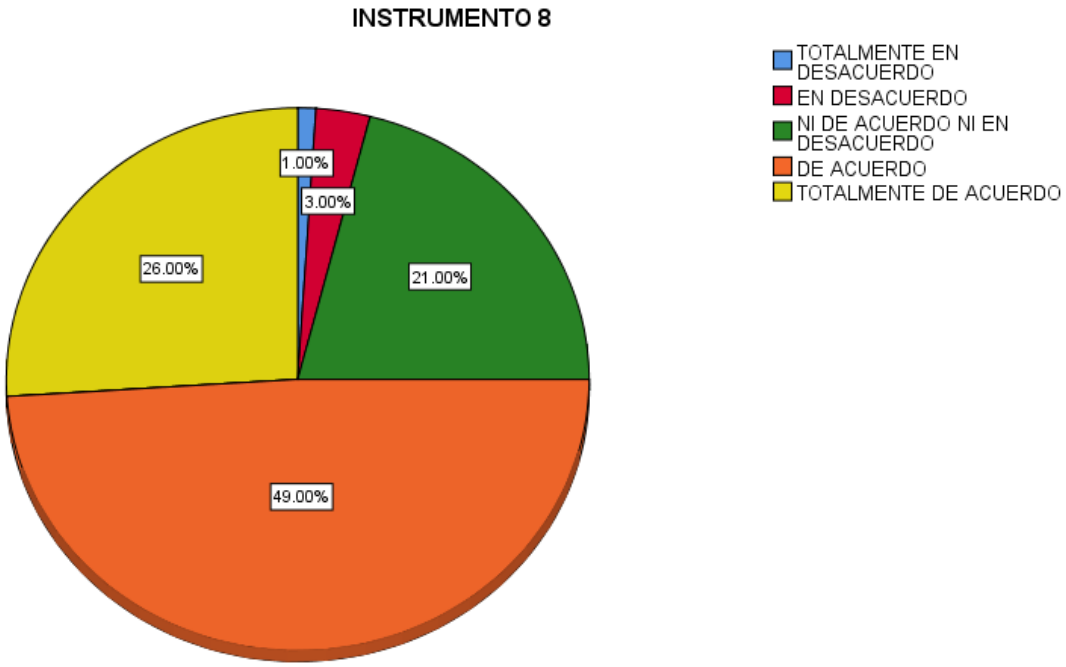
"El internet satelital permite la transmisión fluida de datos, voz y video sin retrasos importantes".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en Desacuerdo	1	1.0	1.0	1.0
En Desacuerdo	3	3.0	3.0	4.0
Ni de Acuerdo ni en Desacuerdo	21	21.0	21.0	25.0
De Acuerdo	49	49.0	49.0	74.0
Totalmente de Acuerdo	26	26.0	26.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 13

"El internet satelital permite la transmisión fluida de datos, voz y video sin retrasos importantes".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumentoN°8, indica que el internet satelital es percibido de manera positiva en cuanto a la transmisión fluida de datos, voz y video**,** con un 74% de los encuestados (49% de acuerdo y 26% totalmente de acuerdo) considerando que el servicio cumple con los requisitos para las operaciones de control ciberespacial. Sin embargo, un 25% permanece neutral o en desacuerdo, lo que podría indicar que, en algunas situaciones específicas, la transmisión no es tan fluida como se esperaría.

Cuadro 17

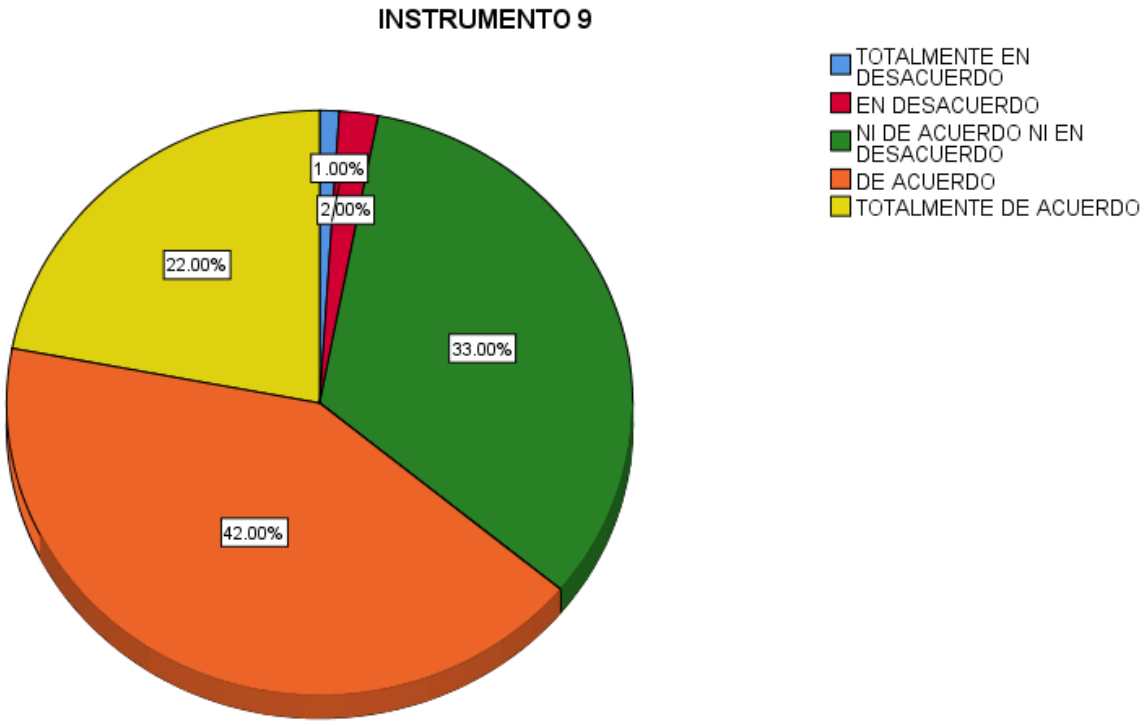
"La velocidad del servicio satelital cumple con los requerimientos operativos de la Fuerza Aérea".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en Desacuerdo	1	1.0	1.0	1.0
En Desacuerdo	2	2.0	2.0	3.0
Ni de Acuerdo ni en Desacuerdo	33	33.0	33.0	36.0
De Acuerdo	42	42.0	42.0	78.0
Totalmente de Acuerdo	22	22.0	22.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 14

"La velocidad del servicio satelital cumple con los requerimientos operativos de la Fuerza Aérea".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumentoN° 9, la velocidad del servicio satelital es percibida como adecuada para cumplir con los requerimientos operativos de la Fuerza Aérea, con un 78% de los encuestados (42% de acuerdo y 22% totalmente de acuerdo) indicando que la velocidad es suficiente para las operaciones. Sin embargo, un 36% permanece neutral, lo que sugiere que hay incertidumbre o experiencias variadas respecto a la velocidad en ciertas operaciones. Solo un pequeño porcentaje (3% en desacuerdo) considera que la velocidad no es adecuada, lo que destaca que, aunque la mayoría percibe el servicio como suficiente, todavía hay aspectos que podrían mejorar.

- ✓ **Latencia**

Cuadro 18

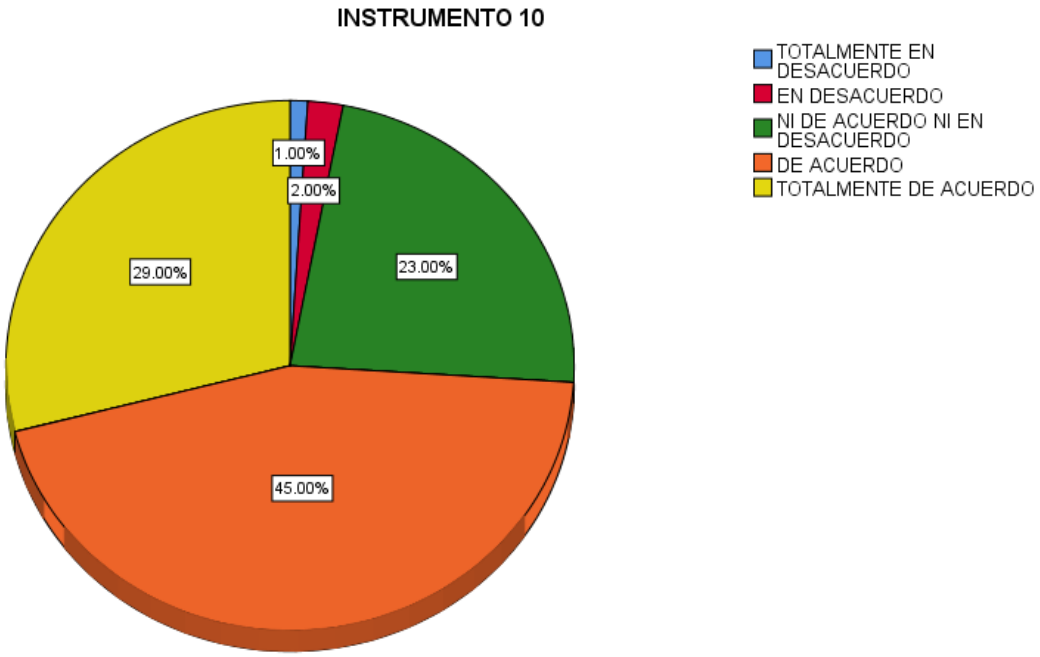
"La latencia del internet satelital es adecuada para las comunicaciones en tiempo real".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en Desacuerdo	1	1.0	1.0	1.0
En Desacuerdo	2	2.0	2.0	3.0
Ni de Acuerdo ni en Desacuerdo	23	23.0	23.0	26.0
De Acuerdo	45	45.0	45.0	71.0
Totalmente De Acuerdo	29	29.0	29.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 15

"La latencia del internet satelital es adecuada para las comunicaciones en tiempo real".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumentoN°10, la latencia del internet satelital es percibida como adecuada para las comunicaciones en tiempo real, con un 74% de los encuestados (45% de acuerdo y 29% totalmente de acuerdo) considerando que cumple con los requisitos operativos. Sin embargo, un 26% permanece neutral o en desacuerdo, lo que sugiere que, aunque la mayoría percibe la latencia como adecuada, aún existe un porcentaje significativo que podría estar experimentando retrasos o inconsistencias en la comunicación en tiempo real. Este dato resalta la oportunidad de mejorar la latencia en ciertos casos para garantizar comunicaciones más fluidas y oportunas en las operaciones de recuperación.

Cuadro 19

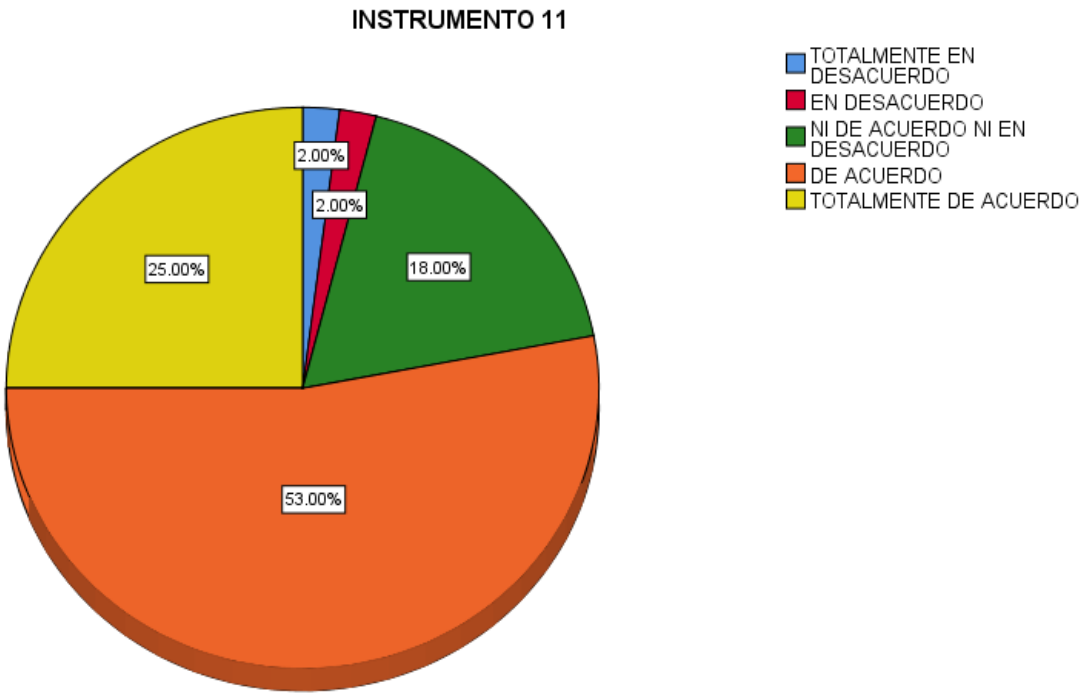
"El retraso en la transmisión de datos vía satélite no afecta el desempeño de las operaciones ciberespaciales".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en Desacuerdo	2	2.0	2.0	2.0
En Desacuerdo	2	2.0	2.0	4.0
Ni de Acuerdo ni en Desacuerdo	18	18.0	18.0	22.0
De Acuerdo	53	53.0	53.0	75.0
Totalmente de Acuerdo	25	25.0	25.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 16

"El retraso en la transmisión de datos vía satélite no afecta el desempeño de las operaciones ciberespaciales".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumentoN°11, el retraso en la transmisión de datos vía satélite no se percibe como un factor significativo que afecte el desempeño de las operaciones ciberespaciales, con un 78% de los encuestados (53% de acuerdo y 25% totalmente de acuerdo) indicando que el retraso no impacta negativamente las operaciones. Sin embargo, un 22% permanece neutral o en desacuerdo, lo que podría reflejar casos específicos en los que el retraso sí afecta la eficiencia de la búsqueda y las operaciones relacionadas. Esto sugiere que, en general, la transmisión de datos es adecuada para las actividades ciberespaciales.

Cuadro 20

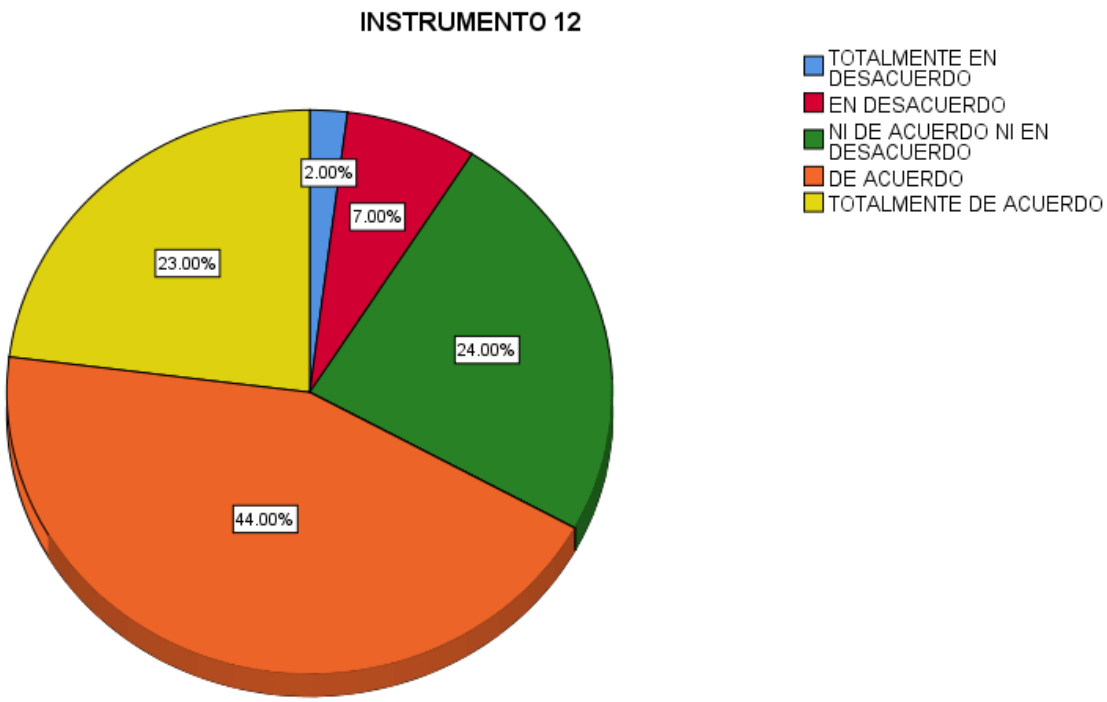
"La latencia del servicio satelital permite una respuesta rápida en situaciones críticas".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en Desacuerdo	2	2.0	2.0	2.0
En Desacuerdo	7	7.0	7.0	9.0
Ni de Acuerdo ni en Desacuerdo	24	24.0	24.0	33.0
De Acuerdo	44	44.0	44.0	77.0
Totalmente de Acuerdo	23	23.0	23.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 17

"La latencia del servicio satelital permite una respuesta rápida en situaciones críticas".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: Con respecto a el instrumentoN°12, la latencia del servicio satelital es vista positivamente en términos de permitir una respuesta rápida en situaciones críticas, con un 67% de los encuestados (44% de acuerdo y 23% totalmente de acuerdo) indicando que el servicio es adecuado. Sin embargo, se observa que 24% se muestra neutral, lo que sugiere que este grupo no tiene una evaluación clara sobre la latencia o no ha experimentado situaciones en las que la latencia sea un factor determinante. Además, 9% de los encuestados están en, lo que indica que en algunos casos la latencia podría afectar negativamente la rapidez de la respuesta en situaciones críticas.

4.1.1.3 Dimensión: Usabilidad

- ✓ **Facilidad de uso**

Cuadro 21

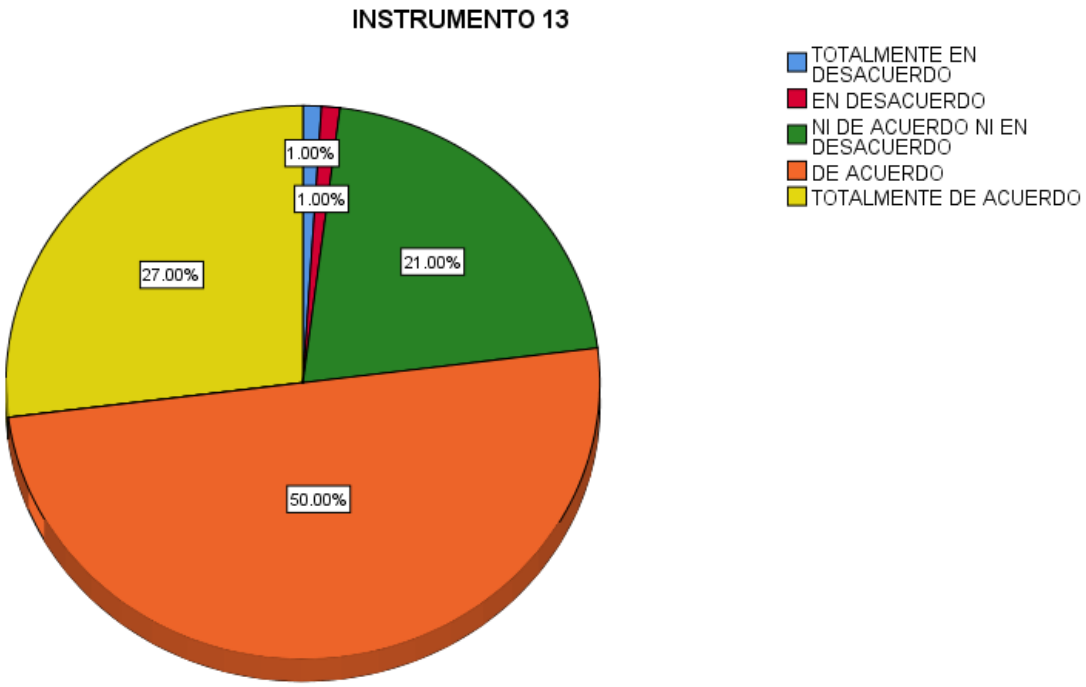
"El sistema de internet satelital es fácil de operar para el personal técnico y operativo".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en Desacuerdo	1	1.0	1.0	1.0
En Desacuerdo	1	1.0	1.0	2.0
Ni de Acuerdo ni en Desacuerdo	21	21.0	21.0	23.0
De Acuerdo	50	50.0	50.0	73.0
Totalmente de Acuerdo	27	27.0	27.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 18

"El sistema de internet satelital es fácil de operar para el personal técnico y operativo".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumento N°13 el sistema de internet satelital es percibido como fácil de operar por el personal técnico y operativo, con un 77% de los encuestados (50% de acuerdo y 27% totalmente de acuerdo) mostrando una evaluación positiva. Un 21% se mantiene neutral, lo que puede reflejar falta de experiencia práctica o una percepción aún no definida. Solo un 2% está en desacuerdo, lo que indica una mínima insatisfacción con la facilidad de uso del sistema. Los resultados respaldan que el servicio es accesible y funcional para el personal encargado de las tareas operativas en el control ciberespacial.

Cuadro 22

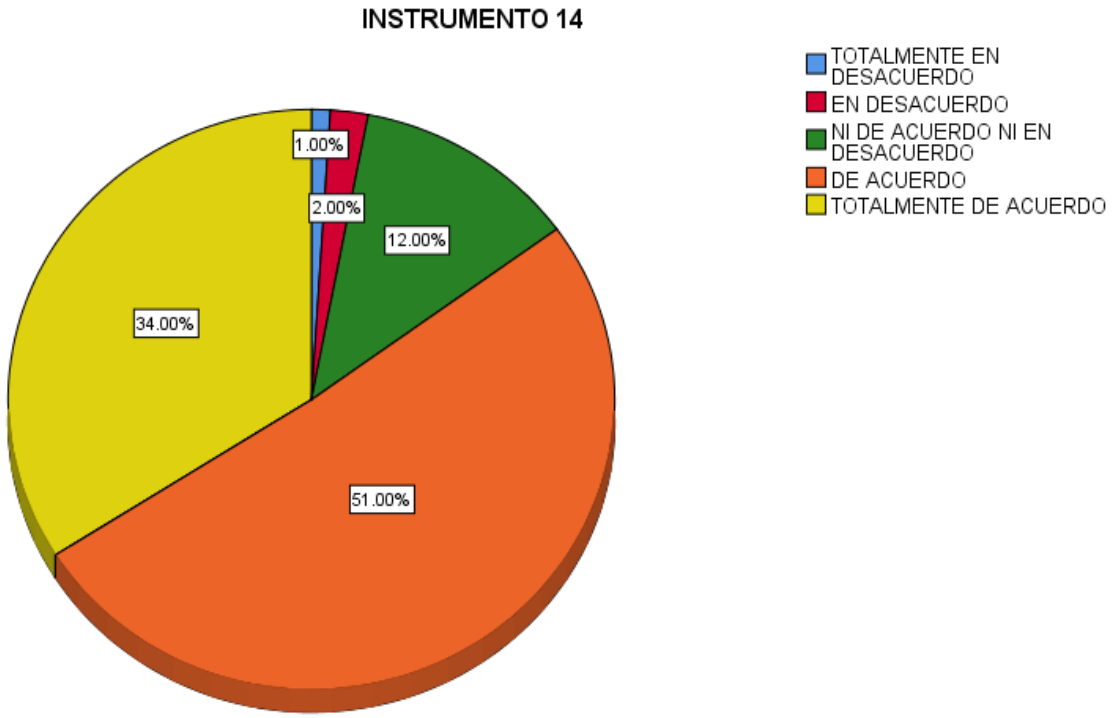
"El personal recibe capacitación adecuada para el manejo del servicio satelital".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en Desacuerdo	1	1.0	1.0	1.0
En Desacuerdo	2	2.0	2.0	3.0
Ni de Acuerdo ni en Desacuerdo	12	12.0	12.0	15.0
De Acuerdo	51	51.0	51.0	66.0
Totalmente de Acuerdo	34	34.0	34.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 19

"El personal recibe capacitación adecuada para el manejo del servicio satelital".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumento N° 14, el personal parece recibir capacitación adecuada para el manejo del servicio satelital, con un 85% de los encuestados (51% de acuerdo y 34% totalmente de acuerdo) confirmando que la capacitación es suficiente. Sin embargo, un 12% se mantiene neutral, lo que podría indicar dudas o falta de claridad sobre el nivel de preparación. Un pequeño 3% está en desacuerdo, lo que sugiere que en algunas áreas puede haber deficiencias en la capacitación, y se podría considerar reforzar los programas de formación.

Cuadro 23

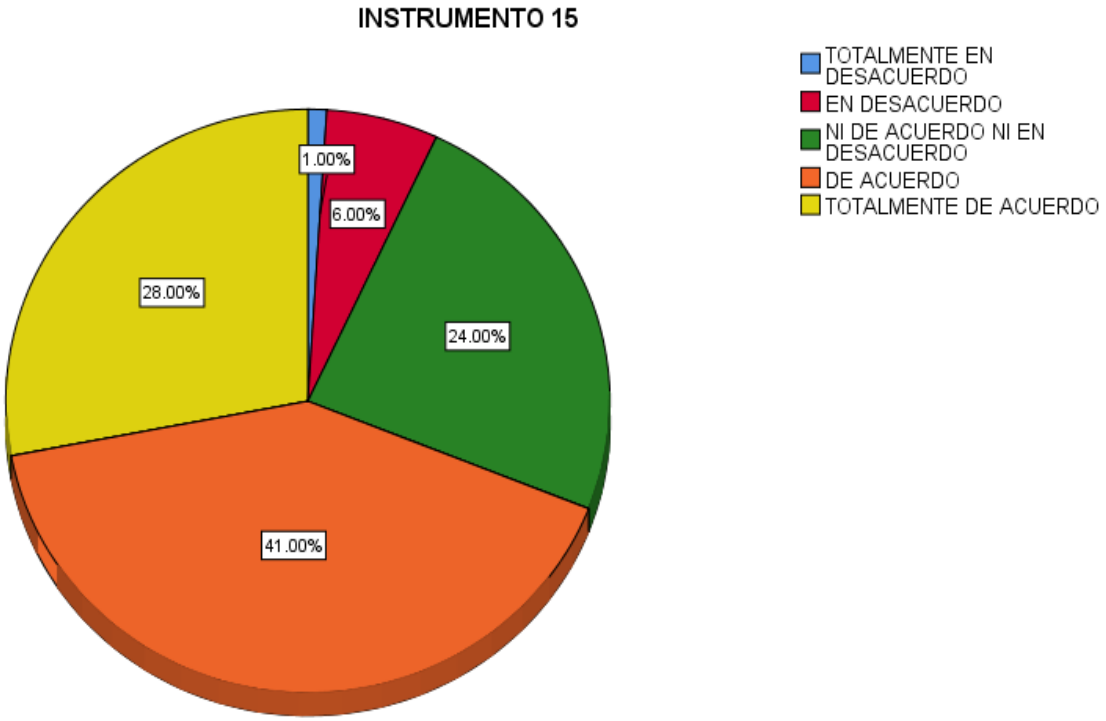
"Los equipos y dispositivos del internet satelital son intuitivos y amigables para su uso diario".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en Desacuerdo	1	1.0	1.0	1.0
En Desacuerdo	6	6.0	6.0	7.0
Ni de Acuerdo ni en Desacuerdo	24	24.0	24.0	31.0
De Acuerdo	41	41.0	41.0	72.0
Totalmente de Acuerdo	28	28.0	28.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 20

"Los equipos y dispositivos del internet satelital son intuitivos y amigables para su uso diario".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumento N° 15, los equipos y dispositivos del internet satelital son generalmente percibidos como intuitivos y amigables para su uso diario, con un 72% de los encuestados (41% de acuerdo y 28% totalmente de acuerdo) consideran que los equipos cumplen con estas características. Sin embargo, un 31% se mantiene neutral, lo que podría indicar que algunos usuarios no han tenido suficiente experiencia para evaluar la facilidad de uso o no han percibido una diferencia significativa. Un pequeño 7% está en desacuerdo, sugiriendo que en algunas ocasiones los dispositivos pueden no ser tan fáciles de operar, lo que podría requerir mejoras en la interfaz o capacitación adicional.

- ✓ **Accesibilidad total**

Cuadro 24

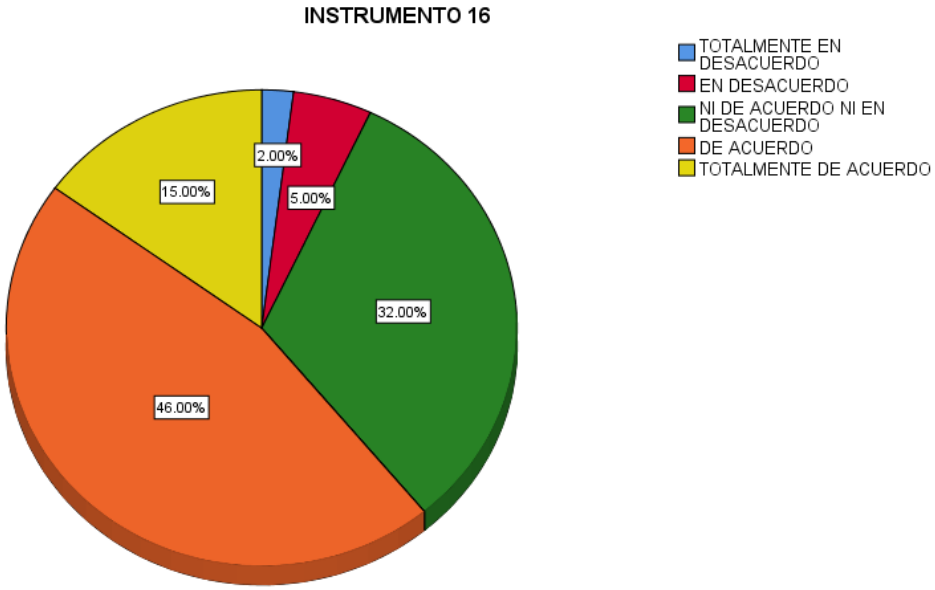
"El internet satelital está disponible para todos los usuarios autorizados en los destacamentos remotos".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en Desacuerdo	2	2.0	2.0	2.0
En Desacuerdo	5	5.0	5.0	7.0
Ni de Acuerdo ni en Desacuerdo	32	32.0	32.0	39.0
De Acuerdo	46	46.0	46.0	85.0
Totalmente de Acuerdo	15	15.0	15.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 21

"El internet satelital está disponible para todos los usuarios autorizados en los destacamentos remotos".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumento N° 16, el internet satelital es generalmente considerado disponible para todos los usuarios autorizados en los destacamentos remotos, con un 61% de los encuestados (46% de acuerdo y 15% totalmente de acuerdo) confirmando que el servicio es accesible. Sin embargo, un 32% se mantiene neutral, lo que podría indicar que algunos usuarios no tienen una experiencia clara o consistente con la disponibilidad del servicio. Un 7% está en desacuerdo.

Cuadro 25

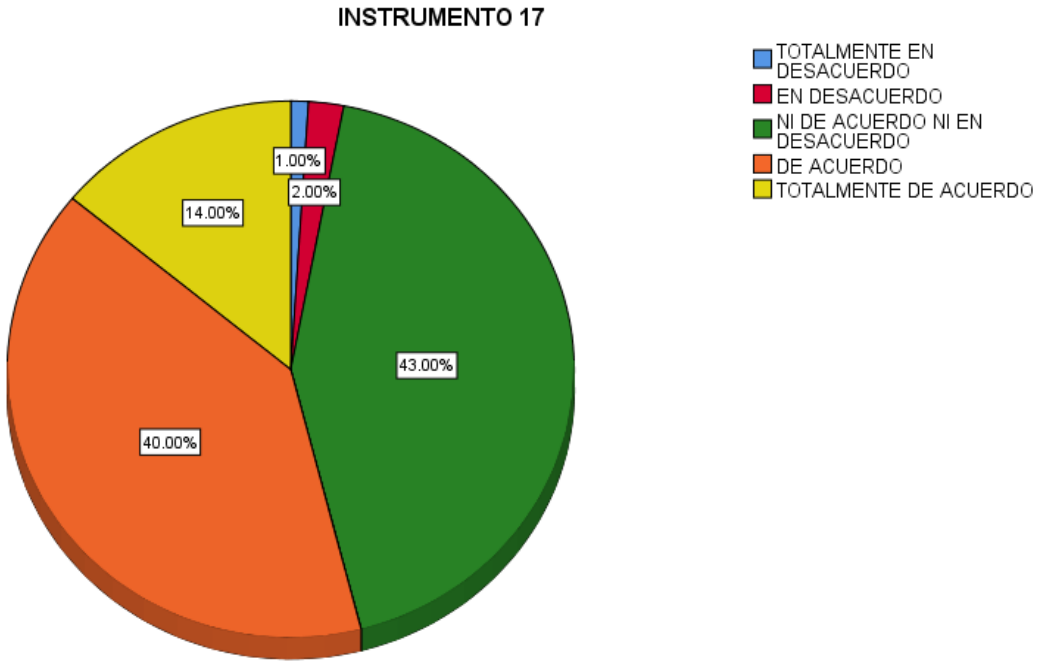
"No existen restricciones técnicas que limiten el acceso al servicio satelital en las zonas operativas".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en Desacuerdo	1	1.0	1.0	1.0
En Desacuerdo	2	2.0	2.0	3.0
Ni de Acuerdo ni en Desacuerdo	43	43.0	43.0	46.0
De Acuerdo	40	40.0	40.0	86.0
Totalmente de Acuerdo	14	14.0	14.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 22

"No existen restricciones técnicas que limiten el acceso al servicio satelital en las zonas operativas".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumento N° 17, el acceso al servicio satelital es percibido en su mayoría como libre de restricciones técnicas en las zonas operativas, con un 54% de los encuestados (40% de acuerdo y 14% totalmente de acuerdo) afirmando que no existen limitaciones técnicas importantes. Sin embargo, un 43% se mantiene neutral, lo que podría indicar que estos usuarios no han experimentado restricciones claras o no tienen suficiente información sobre posibles limitaciones. Un pequeño 3% está en desacuerdo, lo que sugiere que, en algunas ocasiones, puede haber restricciones técnicas que afectan el acceso al servicio en ciertas zonas operativas.

Cuadro 26

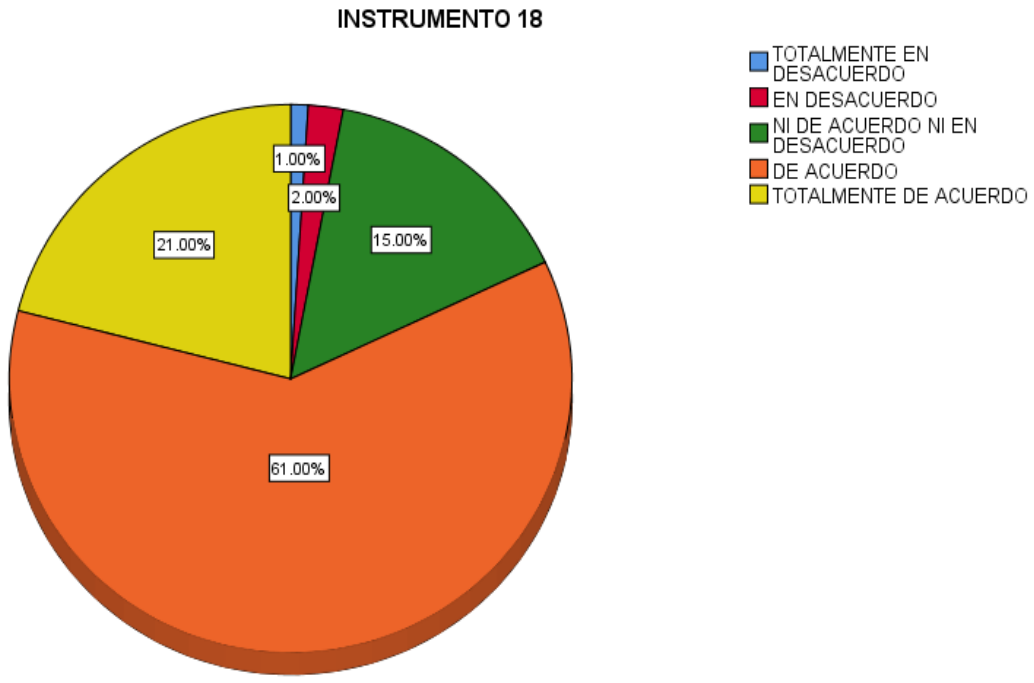
"La infraestructura satelital permite un acceso ininterrumpido para las operaciones militares".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en Desacuerdo	1	1.0	1.0	1.0
En Desacuerdo	2	2.0	2.0	3.0
Ni de Acuerdo ni en Desacuerdo	15	15.0	15.0	18.0
De Acuerdo	61	61.0	61.0	79.0
Totalmente de Acuerdo	21	21.0	21.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 23

"La infraestructura satelital permite un acceso ininterrumpido para las operaciones militares".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumento N° 18, la infraestructura satelital es vista en su mayoría como capaz de proporcionar un acceso ininterrumpido para las operaciones militares, con un 82% de los encuestados (61% de acuerdo y 21% totalmente de acuerdo) indicando que el servicio cumple con esta expectativa. Sin embargo, un 15% permanece neutral, lo que podría sugerir falta de experiencia directa o duda sobre la consistencia del servicio. Un pequeño 3% está en desacuerdo, lo que señala que, en algunos casos, podría haber interrupciones que afectan la continuidad de las operaciones.

4.1.2 Cuestionario 2 "Control Ciberespacial".

4.1.2.1 Dimensión: Operaciones Defensivas

- ✓ **Medidas Preventivas**

Cuadro 27

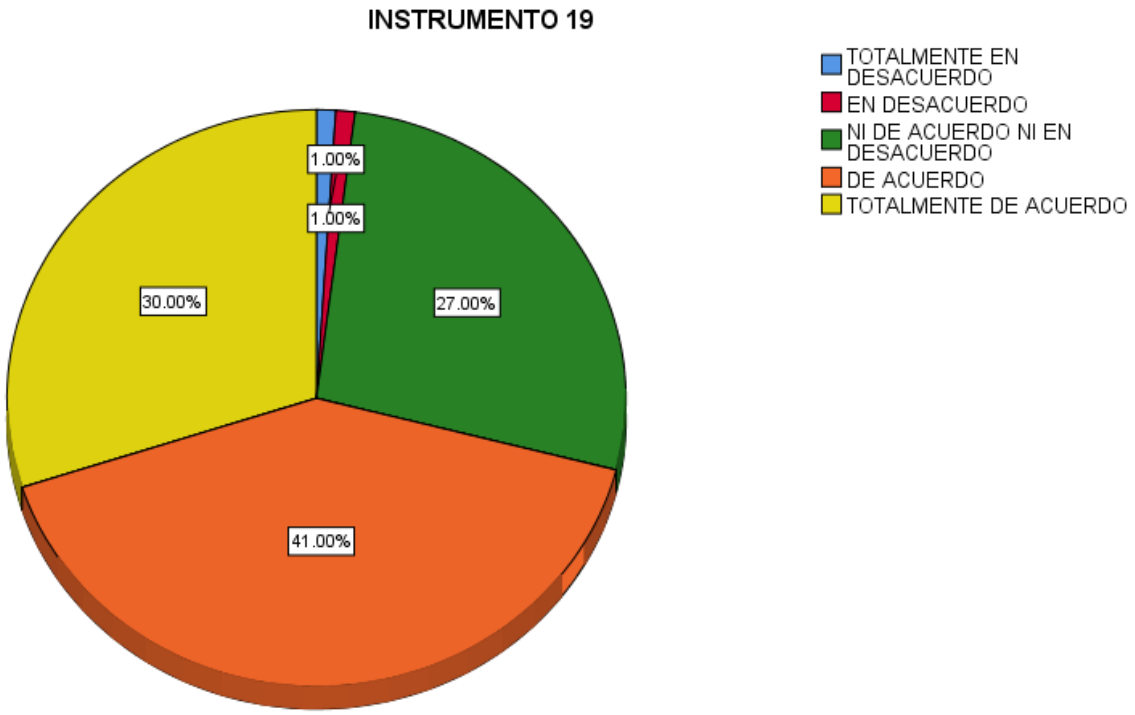
"Existen políticas claras para prevenir ataques cibernéticos en las comunicaciones satelitales".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en Desacuerdo	1	1.0	1.0	1.0
En Desacuerdo	1	1.0	1.0	2.0
Ni de Acuerdo ni en Desacuerdo	27	27.0	27.0	29.0
De Acuerdo	41	41.0	41.0	70.0
Totalmente de Acuerdo	30	30.0	30.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 24

"Existen políticas claras para prevenir ataques cibernéticos en las comunicaciones satelitales".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumento N° 19, la mayoría de los encuestados considera que existen políticas claras para prevenir ataques cibernéticos en las comunicaciones satelitales, con un 71% (41% de acuerdo y 30% totalmente de acuerdo) afirmando que las políticas son adecuadas. Sin embargo, un 27% permanece neutral, lo que podría indicar que no tienen una opinión definida o que no tienen suficiente información sobre las políticas existentes. Un 2% está en desacuerdo, lo que sugiere que algunos podrían sentir que las políticas son insuficientes o no claras en su implementación.

Cuadro 28

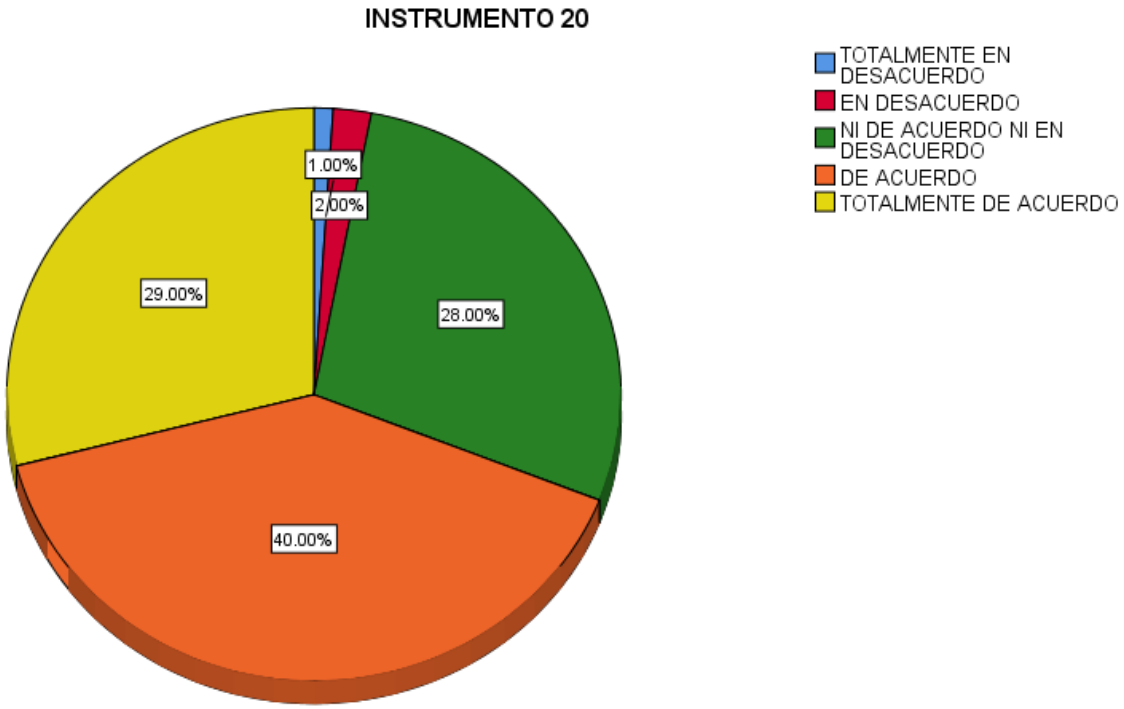
"Se realizan revisiones periódicas para identificar vulnerabilidades en la red satelital".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en Desacuerdo	1	1.0	1.0	1.0
En Desacuerdo	2	2.0	2.0	3.0
Ni de Acuerdo ni en Desacuerdo	28	28.0	28.0	31.0
De Acuerdo	40	40.0	40.0	71.0
Totalmente de Acuerdo	29	29.0	29.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 25

"Se realizan revisiones periódicas para identificar vulnerabilidades en la red satelital".



Nota: Tabla generada con el software SPSS25.

Análisis: En el instrumento N° 20, la mayoría de los encuestados cree que se realizan revisiones periódicas para identificar vulnerabilidades en la red satelital, con un 69% (40% de acuerdo y 29% totalmente de acuerdo) indicando que este proceso se lleva a cabo de manera adecuada. Sin embargo, un 31% permanece neutral, lo que podría sugerir que algunos usuarios no tienen claridad sobre si se realizan estas revisiones de forma regular o no. Solo un 3% está en desacuerdo, lo que sugiere que existe una mínima preocupación sobre la falta de estas revisiones en algunas áreas.

- ✓ **Medidas Proactivas**

Cuadro 29

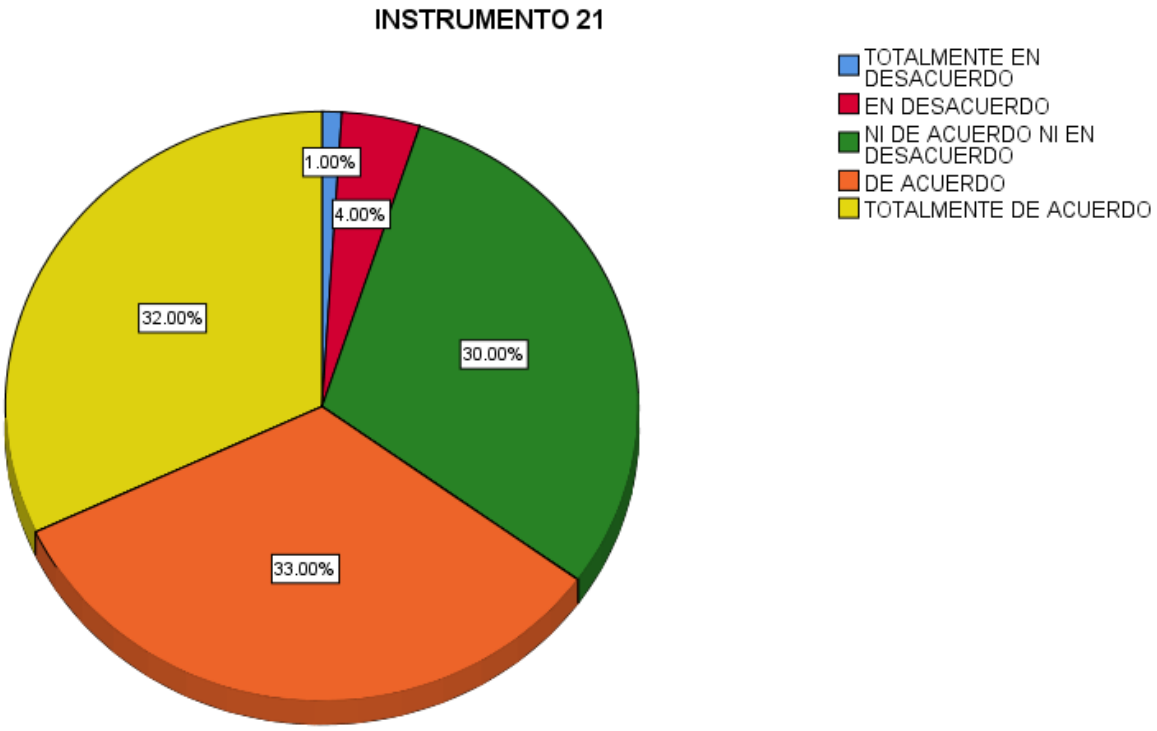
"Se monitorea continuamente el tráfico de datos para detectar posibles amenazas".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en Desacuerdo	1	1.0	1.0	1.0
En Desacuerdo	4	4.0	4.0	5.0
Ni de Acuerdo ni en Desacuerdo	30	30.0	30.0	35.0
De Acuerdo	33	33.0	33.0	68.0
Totalmente de Acuerdo	32	32.0	32.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 26

"Se monitorea continuamente el tráfico de datos para detectar posibles amenazas".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumento N° 21, el monitoreo continuo del tráfico de datos para detectar posibles amenazas es percibido como adecuado por un 65% de los encuestados (33% de acuerdo y 32% totalmente de acuerdo). Sin embargo, un 30% permanece neutral, lo que podría indicar falta de información o de experiencia directa sobre la efectividad del monitoreo. Un pequeño 5% está en desacuerdo, lo que sugiere que algunos usuarios consideran que el monitoreo no es tan efectivo o no se realiza con la frecuencia necesaria.

Cuadro 30

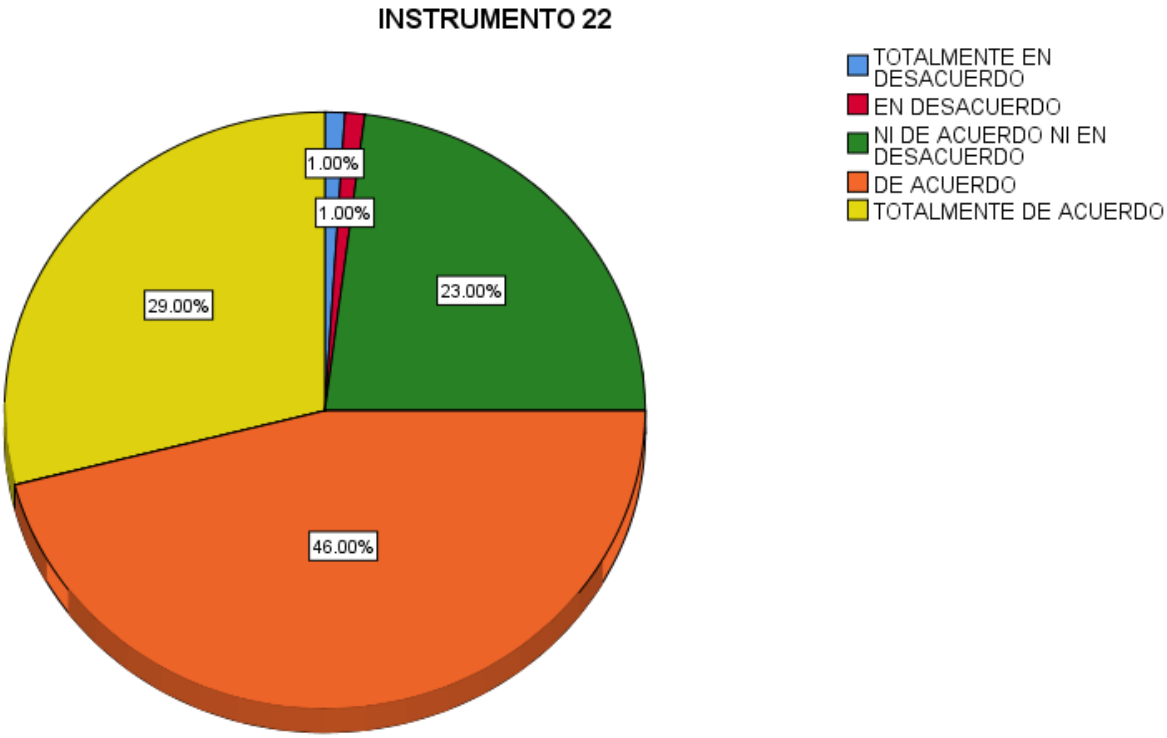
"El personal está capacitado para anticipar y responder a incidentes cibernéticos".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en Desacuerdo	1	1.0	1.0	1.0
En Desacuerdo	1	1.0	1.0	2.0
Ni de Acuerdo ni en Desacuerdo	23	23.0	23.0	25.0
De Acuerdo	46	46.0	46.0	71.0
Totalmente de Acuerdo	29	29.0	29.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 27

"El personal está capacitado para anticipar y responder a incidentes cibernéticos".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumento N° 22, el personal es percibido en su mayoría como adecuadamente capacitado para anticipar y responder a incidentes cibernéticos, con un 75% de los encuestados (46% de acuerdo y 29% totalmente de acuerdo) indicando que tienen la formación necesaria. Sin embargo, un 23% permanece neutral, lo que podría sugerir falta de claridad o experiencia directa en este aspecto. Un 2% está en desacuerdo, lo que señala que hay áreas donde la capacitación podría necesitar fortalecerse.

- ✓ **Medidas Reactivas**

Cuadro 31

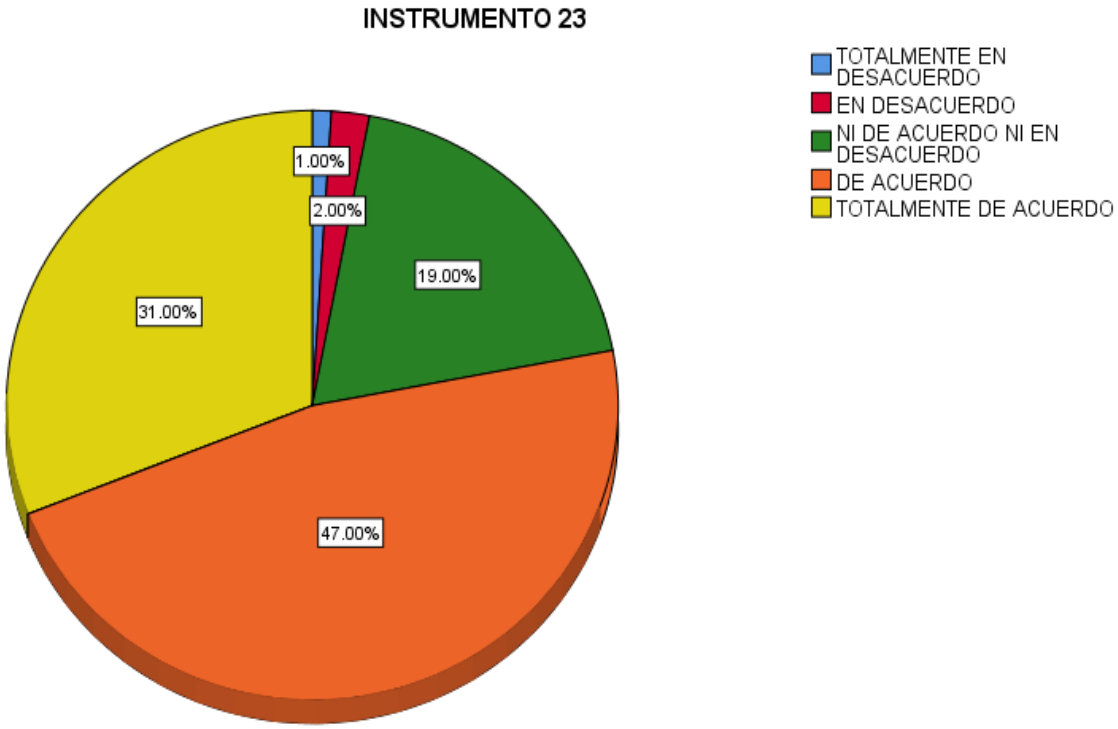
"Existen protocolos claros para responder a incidentes de seguridad en el internet satelital".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en Desacuerdo	1	1.0	1.0	1.0
En Desacuerdo	2	2.0	2.0	3.0
Ni de Acuerdo ni en Desacuerdo	19	19.0	19.0	22.0
De Acuerdo	47	47.0	47.0	69.0
Totalmente de Acuerdo	31	31.0	31.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 28

"Existen protocolos claros para responder a incidentes de seguridad en el internet satelital".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumento N° 23, la mayoría de los encuestados considera que existen protocolos claros para responder a incidentes de seguridad en el internet satelital, con un 78% (47% de acuerdo y 31% totalmente de acuerdo) afirmando que los protocolos son adecuados. Sin embargo, un 19% se mantiene neutral, lo que podría indicar que algunos no tienen suficiente información o experiencia sobre los protocolos existentes.

Un 3% está en desacuerdo, lo que sugiere que algunos consideran que los protocolos no son lo suficientemente claros o efectivos.

Cuadro 32

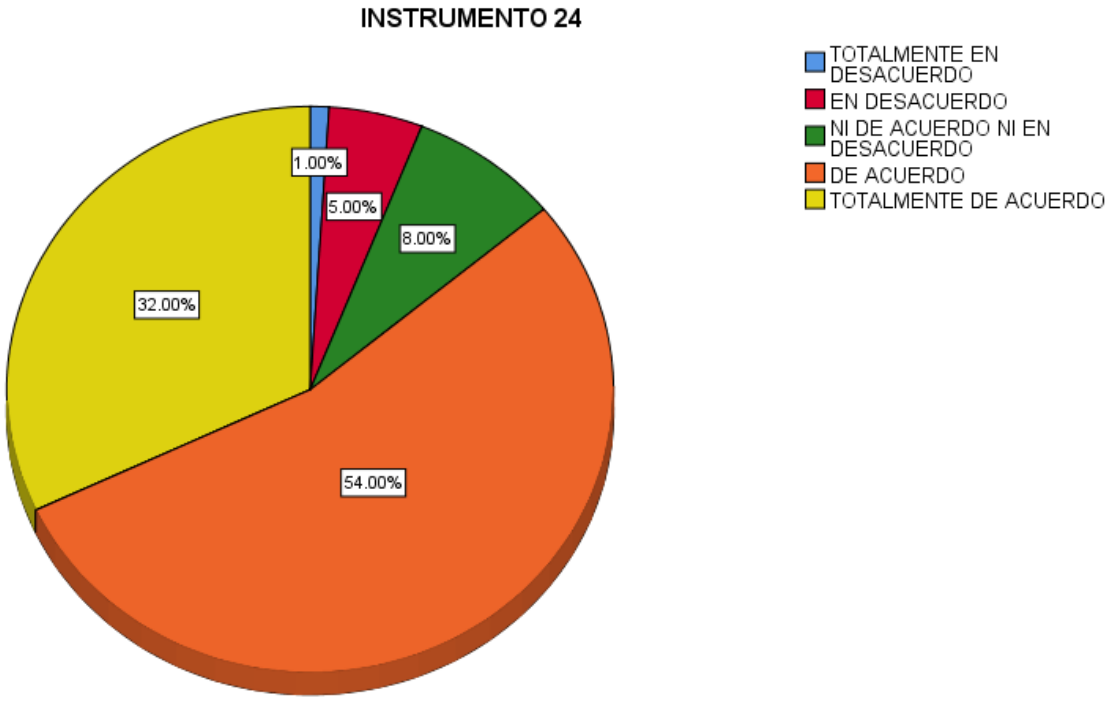
"El equipo de respuesta actúa rápidamente para contener ataques cibernéticos".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en Desacuerdo	1	1.0	1.0	1.0
En Desacuerdo	5	5.0	5.0	6.0
Ni de Acuerdo ni en Desacuerdo	8	8.0	8.0	14.0
De Acuerdo	54	54.0	54.0	68.0
Totalmente de Acuerdo	32	32.0	32.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 29

"El equipo de respuesta actúa rápidamente para contener ataques cibernéticos".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumento N° 24, el equipo de respuesta es percibido como rápido y eficaz para contener ataques cibernéticos, con un 86% de los encuestados (54% de acuerdo y 32% totalmente de acuerdo) afirmando que el equipo actúa con rapidez.

Sin embargo, un 14% permanece neutral o en desacuerdo, lo que sugiere que algunos usuarios pueden no haber experimentado la misma eficacia o rapidez en la respuesta, o bien tienen dudas sobre la capacidad de respuesta ante incidentes.

- ✓ **Medidas de Recuperación**

Cuadro 33

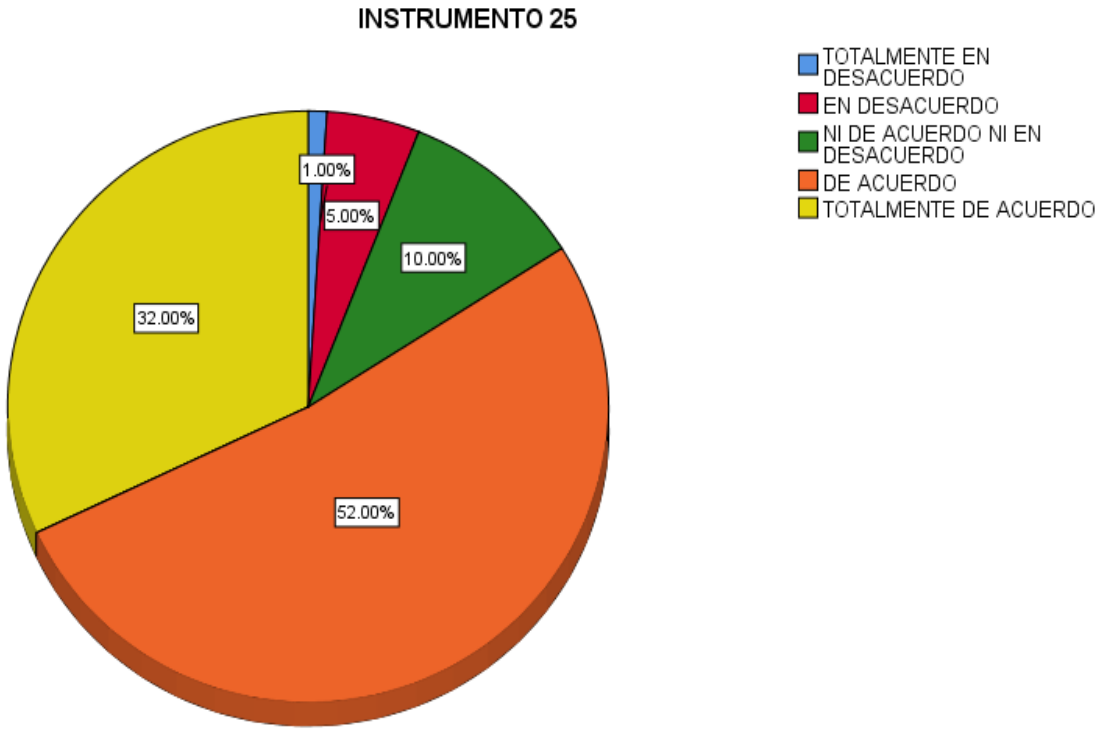
"Se cuenta con planes de contingencia para restaurar el servicio en caso de interrupciones".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en Desacuerdo	1	1.0	1.0	1.0
En Desacuerdo	5	5.0	5.0	6.0
Ni de Acuerdo ni en Desacuerdo	10	10.0	10.0	16.0
De Acuerdo	52	52.0	52.0	68.0
Totalmente de Acuerdo	32	32.0	32.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 30

"Se cuenta con planes de contingencia para restaurar el servicio en caso de interrupciones".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumento N° 25, la mayoría de los encuestados considera que existen planes de contingencia adecuados para restaurar el servicio en caso de interrupciones, con un 84% (52% de acuerdo y 32% totalmente de acuerdo) afirmando que los planes son efectivos. Sin embargo, un 16% se mantiene neutral o en desacuerdo, lo que sugiere que algunos usuarios no están completamente informados o no han experimentado la eficacia de estos planes de contingencia. Esto podría indicar la necesidad de mejorar la comunicación o las pruebas de los planes para garantizar que todos los involucrados estén completamente preparados.

Cuadro 34

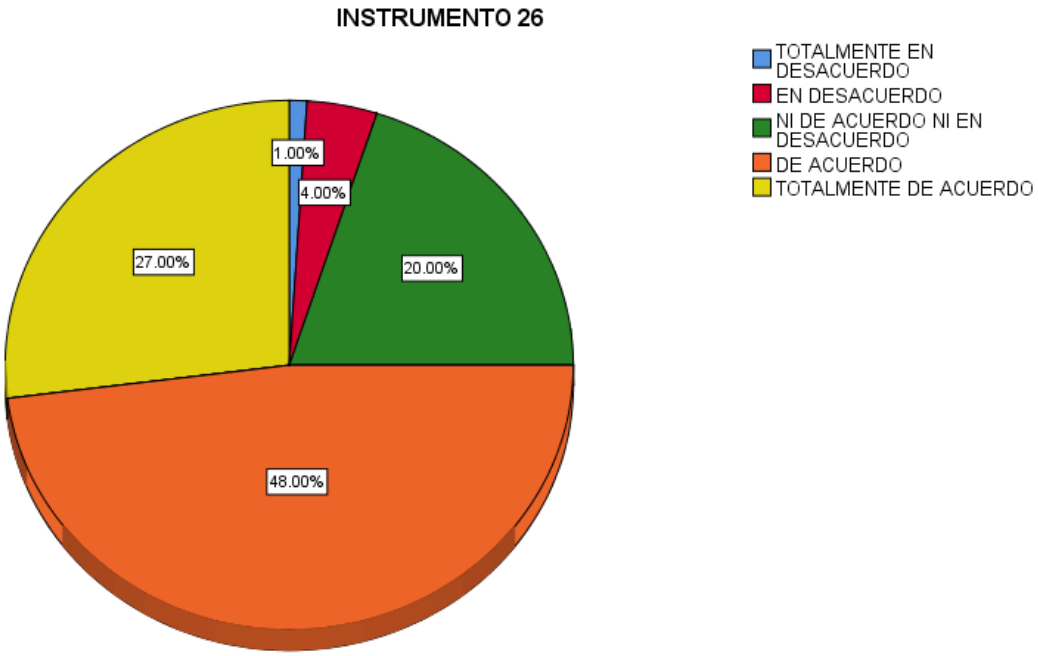
"La Fuerza Aérea dispone de recursos adecuados para la recuperación ante fallas de seguridad".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en Desacuerdo	1	1.0	1.0	1.0
En Desacuerdo	4	4.0	4.0	5.0
Ni de Acuerdo ni en Desacuerdo	20	20.0	20.0	25.0
De Acuerdo	48	48.0	48.0	73.0
Totalmente de Acuerdo	27	27.0	27.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 31

"La Fuerza Aérea dispone de recursos adecuados para la recuperación ante fallas de seguridad".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumento N° 26, la mayoría de los encuestados considera que la Fuerza Aérea dispone de recursos adecuados para la recuperación ante fallas de seguridad, con un 75% (48% de acuerdo y 27% totalmente de acuerdo) confirmando que los recursos son suficientes. Sin embargo, un 25% se mantiene neutral o en desacuerdo, lo que sugiere que algunos usuarios pueden no estar completamente informados sobre los recursos disponibles o pueden haber experimentado limitaciones en su implementación.

4.1.2.2 Dimensión: Operaciones de explotación

- ✓ **Búsqueda**

Cuadro 35

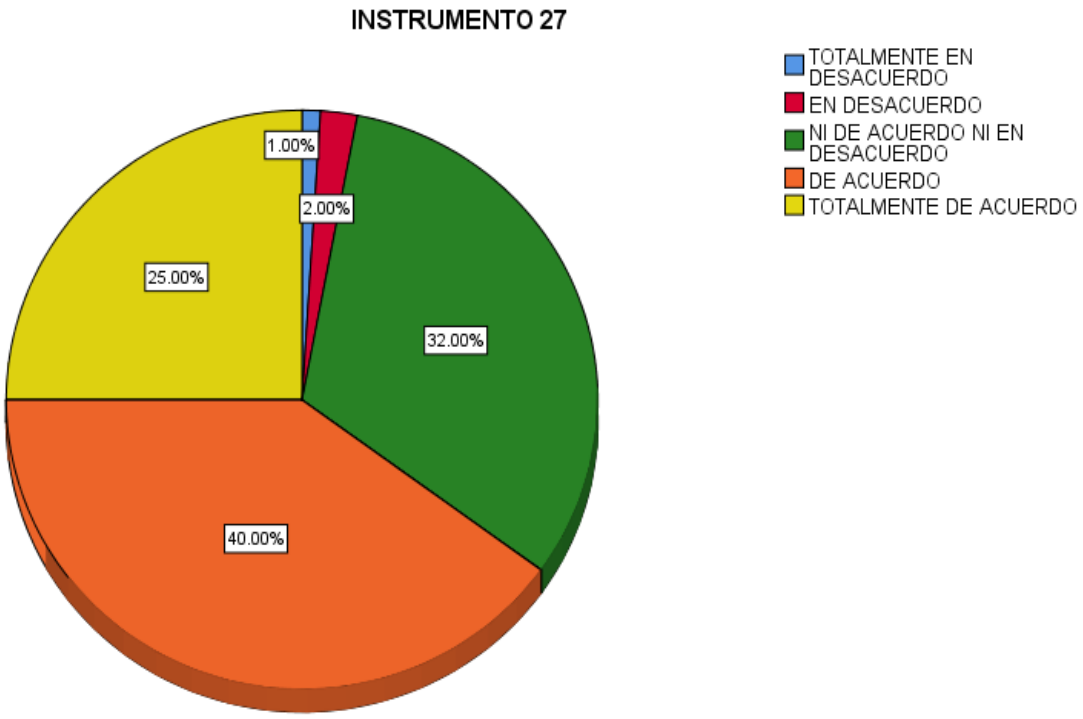
"El personal utiliza herramientas adecuadas para localizar amenazas en el ciberespacio".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en Desacuerdo	1	1.0	1.0	1.0
En Desacuerdo	2	2.0	2.0	3.0
Ni de Acuerdo ni en Desacuerdo	32	32.0	32.0	35.0
De Acuerdo	40	40.0	40.0	75.0
Totalmente de Acuerdo	25	25.0	25.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 32

"El personal utiliza herramientas adecuadas para localizar amenazas en el ciberespacio".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumento N° 27, el personal es percibido en su mayoría como utilizando herramientas adecuadas para localizar amenazas en el ciberespacio, con un 65% (40% de acuerdo y 25% totalmente de acuerdo) afirmando que las herramientas son suficientes. Sin embargo, un 32% permanece neutral, lo que podría indicar que estos usuarios no tienen una opinión clara sobre la efectividad de las herramientas o no han tenido suficiente experiencia para evaluarlas y finalmente un 3% está en desacuerdo, lo que señala que las herramientas no son adecuadas.

Cuadro 36

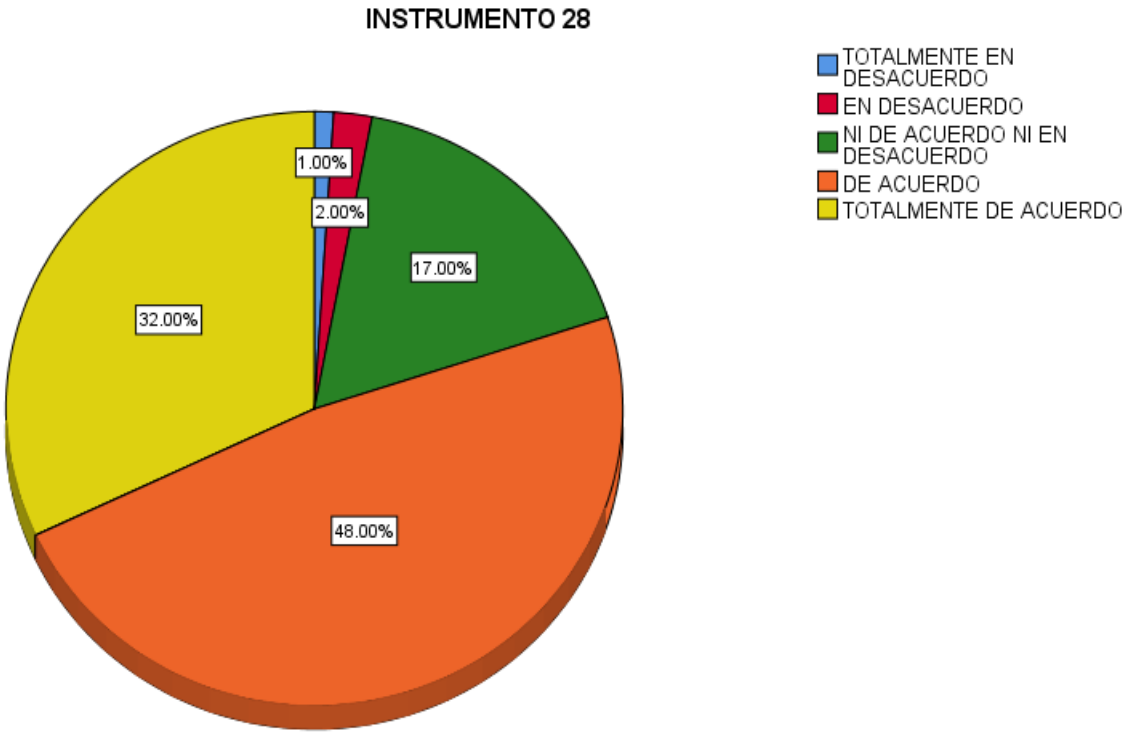
"La búsqueda de datos contribuye a la anticipación de ataques o vulnerabilidades".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Totalmente en Desacuerdo	1	1.0	1.0	1.0
En Desacuerdo	2	2.0	2.0	3.0
Ni de Acuerdo ni en Desacuerdo	17	17.0	17.0	20.0
De Acuerdo	48	48.0	48.0	68.0
Totalmente de Acuerdo	32	32.0	32.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 33

"La búsqueda de datos contribuye a la anticipación de ataques o vulnerabilidades".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumento N° 28, la búsqueda de datos es percibida como una herramienta eficaz para anticipar ataques o vulnerabilidades, con un 80% (48% de acuerdo y 32% totalmente de acuerdo) indicando que esta actividad contribuye significativamente a la prevención.

Un 17% permanece neutral, lo que sugiere que algunos usuarios no tienen una opinión clara sobre su impacto o no tienen suficiente experiencia con la búsqueda de datos. Un pequeño 3% está en desacuerdo, lo que indica que una mínima proporción de usuarios considera que la búsqueda de datos no es útil para anticipar amenazas o vulnerabilidades.

- ✓ **Detección**

Cuadro 37

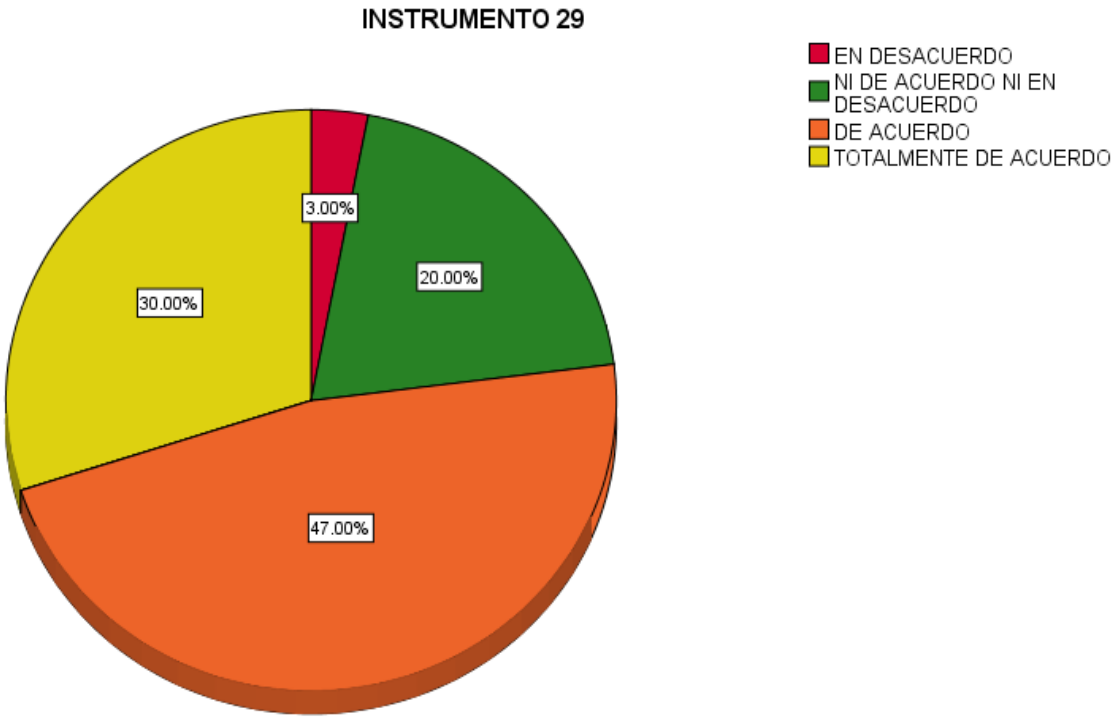
"Se identifican rápidamente posibles intentos de intrusión en la red satelital".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
En Desacuerdo	3	3.0	3.0	3.0
Ni de Acuerdo ni en Desacuerdo	20	20.0	20.0	23.0
De Acuerdo	47	47.0	47.0	70.0
Totalmente de Acuerdo	30	30.0	30.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 34

"Se identifican rápidamente posibles intentos de intrusión en la red satelital".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumento N° 29, la capacidad para identificar rápidamente posibles intentos de intrusión en la red satelital es generalmente percibida como adecuada, con un 77% (47% de acuerdo y 30% totalmente de acuerdo) indicando que los intentos de intrusión se identifican de manera eficiente.

Un 20% permanece neutral, lo que podría sugerir que algunos usuarios no tienen una experiencia definida con este aspecto o no están completamente seguros de su efectividad. Solo un 3% está en desacuerdo, lo que señala que un pequeño porcentaje considera que la identificación de intrusiones no es lo suficientemente rápida o eficiente.

Cuadro 38

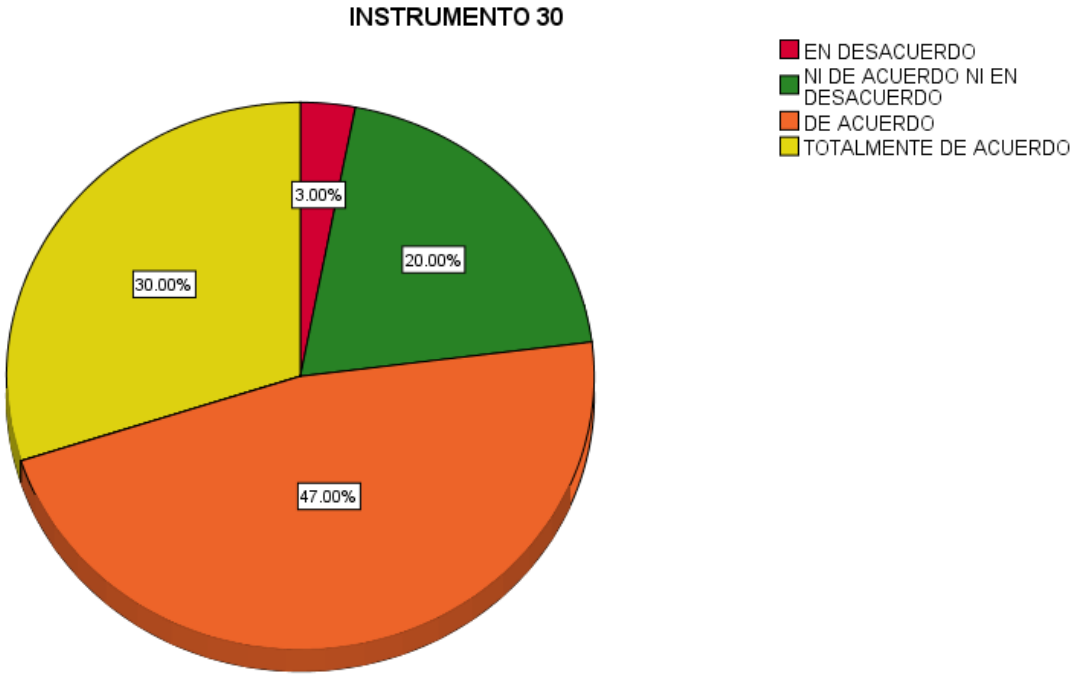
"La detección oportuna permite la activación inmediata de medidas defensivas".

	Frecuencia	Porcentaje	Porcentaje Válido	Porcentaje Acumulado
En Desacuerdo	3	3.0	3.0	3.0
Ni de Acuerdo ni en Desacuerdo	20	20.0	20.0	23.0
De Acuerdo	48	48.0	48.0	71.0
Totalmente de Acuerdo	29	29.0	29.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 35

"La detección oportuna permite la activación inmediata de medidas defensivas".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumento N° 30, la detección oportuna es percibida como efectiva para permitir la activación inmediata de medidas defensivas, con un 77% (48% de acuerdo y 29% totalmente de acuerdo) afirmando que la detección se realiza de manera eficiente. Un 20% permanece neutral, lo que sugiere que algunos usuarios no tienen una experiencia definida o no han notado la rapidez en la activación de medidas defensivas.

Un pequeño 3% está en desacuerdo, lo que indica que algunos consideran que la detección no es lo suficientemente rápida o efectiva para activar las medidas necesarias a tiempo.

- ✓ **Identificación**

Cuadro 39

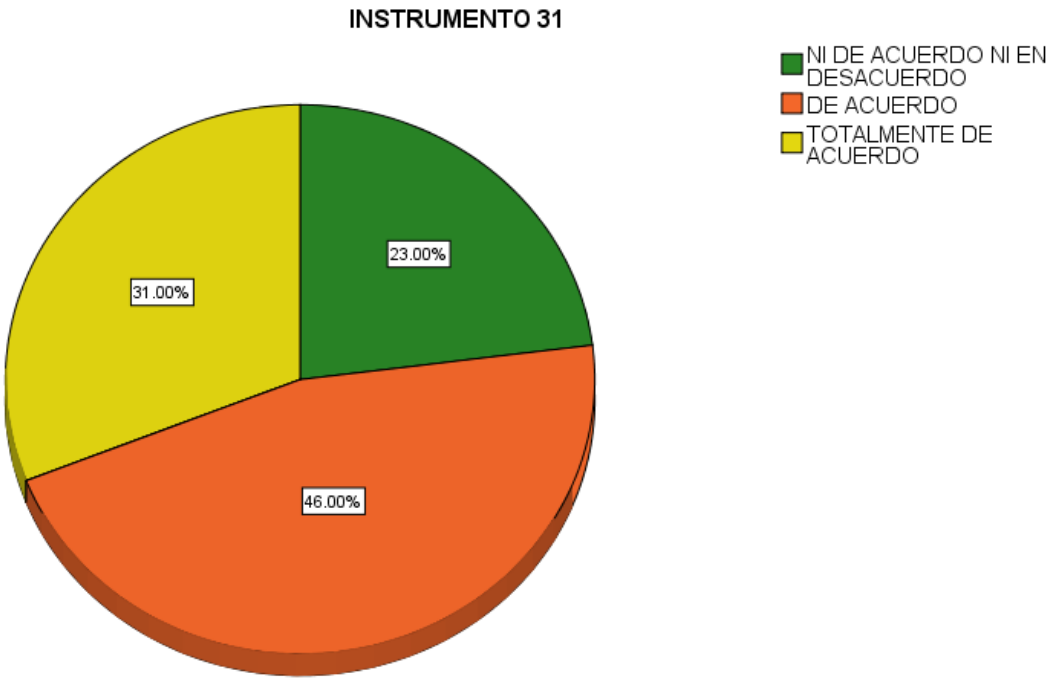
"Se determina el origen de los ataques para diseñar respuestas adecuadas".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Ni de Acuerdo ni en Desacuerdo	23	23.0	23.0	23.0
De Acuerdo	46	46.0	46.0	69.0
Totalmente de Acuerdo	31	31.0	31.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 36

"Se determina el origen de los ataques para diseñar respuestas adecuadas".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumento N° 31, la mayoría de los encuestados considera que se determina adecuadamente el origen de los ataques para diseñar respuestas adecuadas, con un 77% (46% de acuerdo y 31% totalmente de acuerdo) indicando que el proceso es efectivo. Sin embargo, un 23% permanece neutral, lo que sugiere que algunos usuarios no tienen una evaluación clara sobre la efectividad de este proceso. Esto podría reflejar falta de experiencia directa o de claridad en la comunicación sobre cómo se lleva a cabo esta tarea.

Cuadro 40

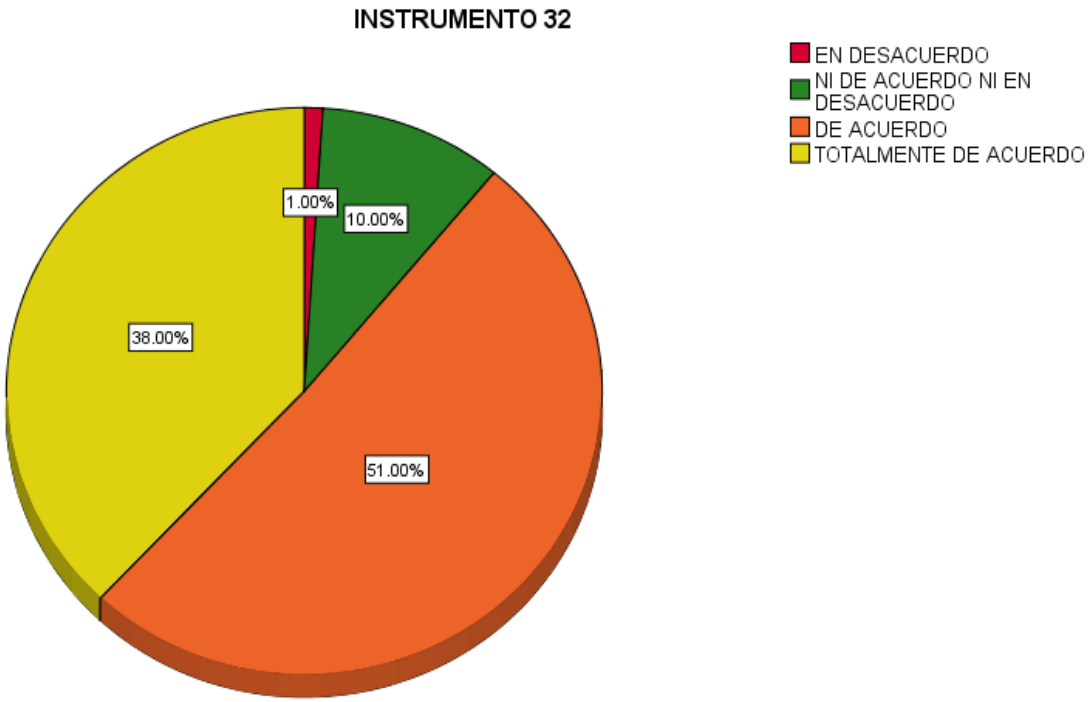
"La identificación precisa de incidentes fortalece la protección del sistema satelital".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
En Desacuerdo	1	1.0	1.0	1.0
Ni de Acuerdo ni en Desacuerdo	10	10.0	10.0	11.0
De Acuerdo	51	51.0	51.0	62.0
Totalmente de Acuerdo	38	38.0	38.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 37

"La identificación precisa de incidentes fortalece la protección del sistema satelital".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumento N° 32, la identificación precisa de incidentes es considerada clave para fortalecer la protección del sistema satelital, con un 89% (51% de acuerdo y 38% totalmente de acuerdo) afirmando que este proceso contribuye significativamente a la seguridad del sistema. Sin embargo, un 10% permanece neutral, lo que podría indicar falta de experiencia o conocimiento sobre cómo la identificación precisa impacta la protección. Un pequeño 1% está en desacuerdo, sugiriendo que, en algunas situaciones, los incidentes pueden no ser identificados con suficiente precisión, lo que podría debilitar la protección.

4.1.2.3 Dimensión: Operaciones de respuesta

- ✓ **Denegación**

Cuadro 41

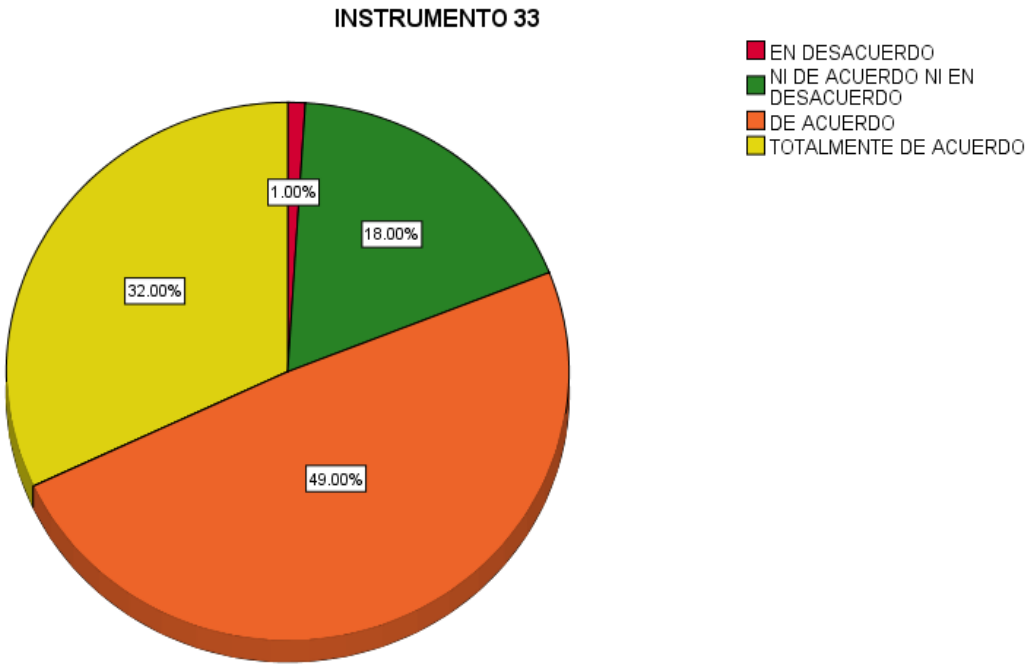
"Se aplican acciones efectivas para impedir ataques que comprometan la comunicación satelital".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
En Desacuerdo	1	1.0	1.0	1.0
Ni de Acuerdo ni en Desacuerdo	18	18.0	18.0	19.0
De Acuerdo	49	49.0	49.0	68.0
Totalmente de Acuerdo	32	32.0	32.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 38

"Se aplican acciones efectivas para impedir ataques que comprometan la comunicación satelital".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumento N° 33, se percibe que se aplican acciones efectivas para impedir ataques que comprometan la comunicación satelital, con un 81% (49% de acuerdo y 32% totalmente de acuerdo) afirmando que las medidas son adecuadas. Sin embargo, un 18% permanece neutral, lo que podría indicar que algunos usuarios no tienen una experiencia clara sobre la efectividad de estas acciones. Un pequeño 1% está en desacuerdo, lo que sugiere que en algunas situaciones las acciones podrían no ser tan eficaces para prevenir ataques.

Cuadro 42

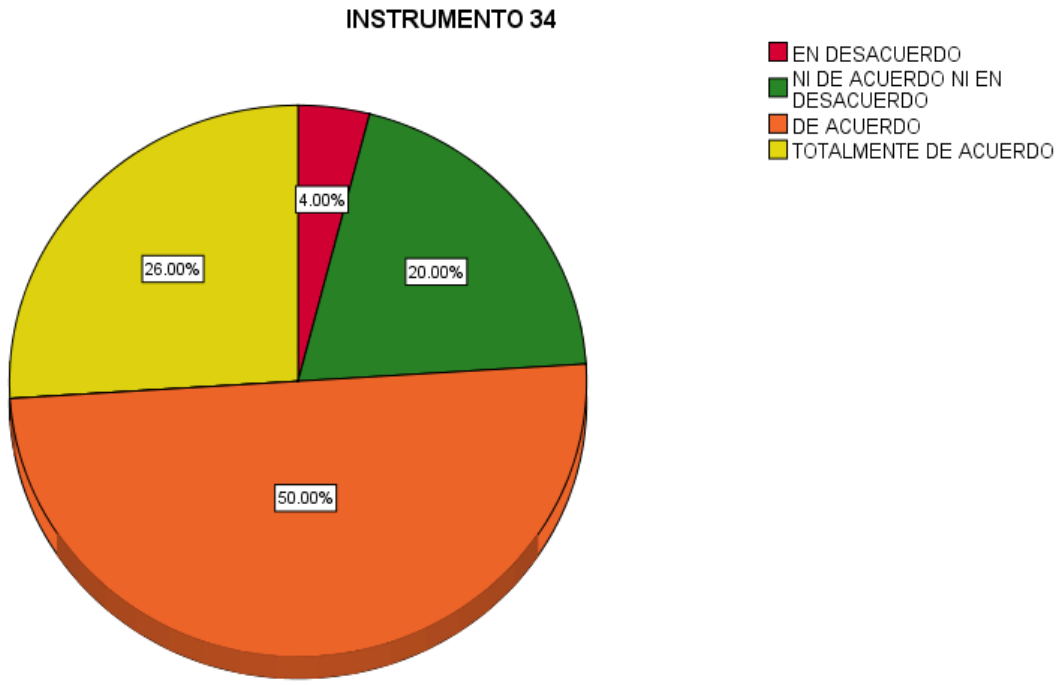
"Las operaciones de denegación contribuyen a mantener la integridad del sistema".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
En Desacuerdo	4	4.0	4.0	4.0
Ni de Acuerdo ni en Desacuerdo	20	20.0	20.0	24.0
De Acuerdo	50	50.0	50.0	74.0
Totalmente de Acuerdo	26	26.0	26.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 39

"Las operaciones de denegación contribuyen a mantener la integridad del sistema".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumento N° 34, las operaciones de denegación son vistas como contribuyentes importantes para mantener la integridad del sistema, con un 74% (50% de acuerdo y 26% totalmente de acuerdo) considerando que estas operaciones son eficaces. Un 20% permanece neutral, lo que podría indicar que algunos usuarios no tienen una evaluación clara o no han tenido suficientes experiencias para evaluar el impacto de estas operaciones.

Un pequeño 4% está en desacuerdo, sugiriendo que en algunos casos las operaciones de denegación pueden no ser percibidas como suficientemente efectivas para proteger la integridad del sistema.

- ✓ **Degradación**

Cuadro 43

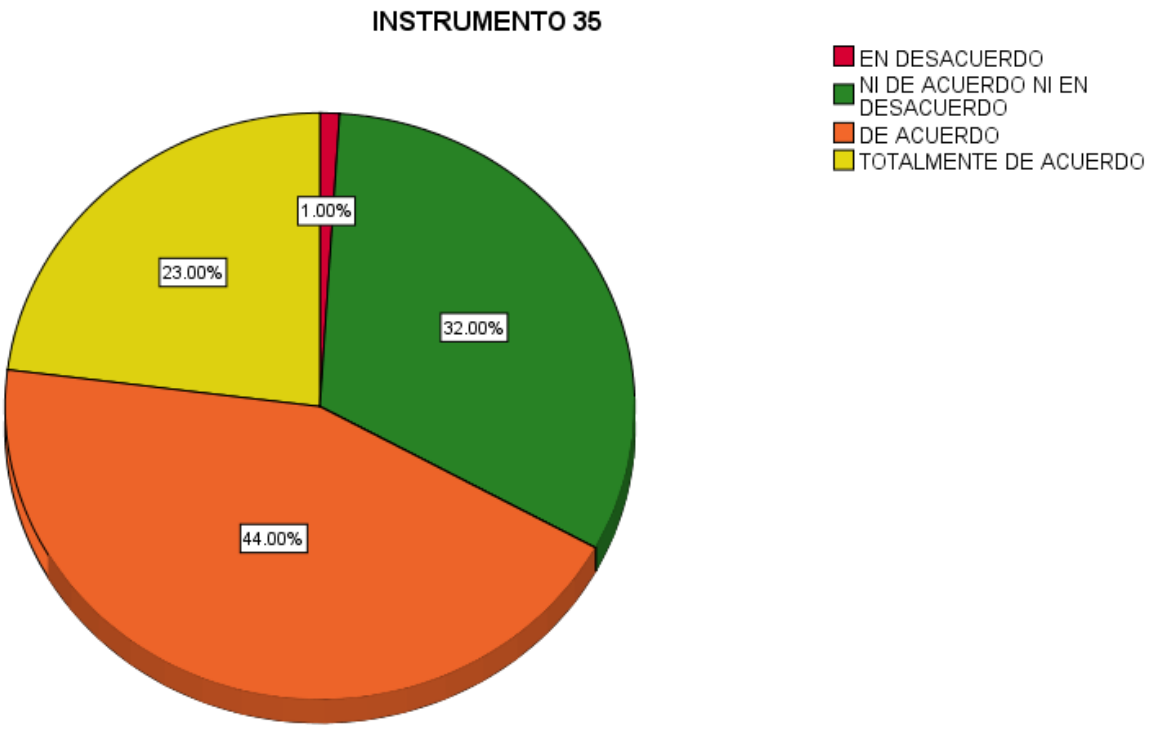
"Se implementan medidas para reducir la eficacia de ataques en curso".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
En Desacuerdo	1	1.0	1.0	1.0
Ni de Acuerdo ni en Desacuerdo	32	32.0	32.0	33.0
De Acuerdo	44	44.0	44.0	77.0
Totalmente de Acuerdo	23	23.0	23.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 40

"Se implementan medidas para reducir la eficacia de ataques en curso".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumento N° 35, se considera que se implementan medidas efectivas para reducir la eficacia de los ataques en curso, con un 67% (44% de acuerdo y 23% totalmente de acuerdo) afirmando que las acciones son eficaces. Un 32% permanece neutral, lo que podría indicar que algunos usuarios no tienen suficiente claridad sobre la efectividad de estas medidas. Un 1% está en desacuerdo, lo que sugiere que en ciertos casos las medidas implementadas podrían no ser suficientes para reducir la eficacia de los ataques.

Cuadro 44

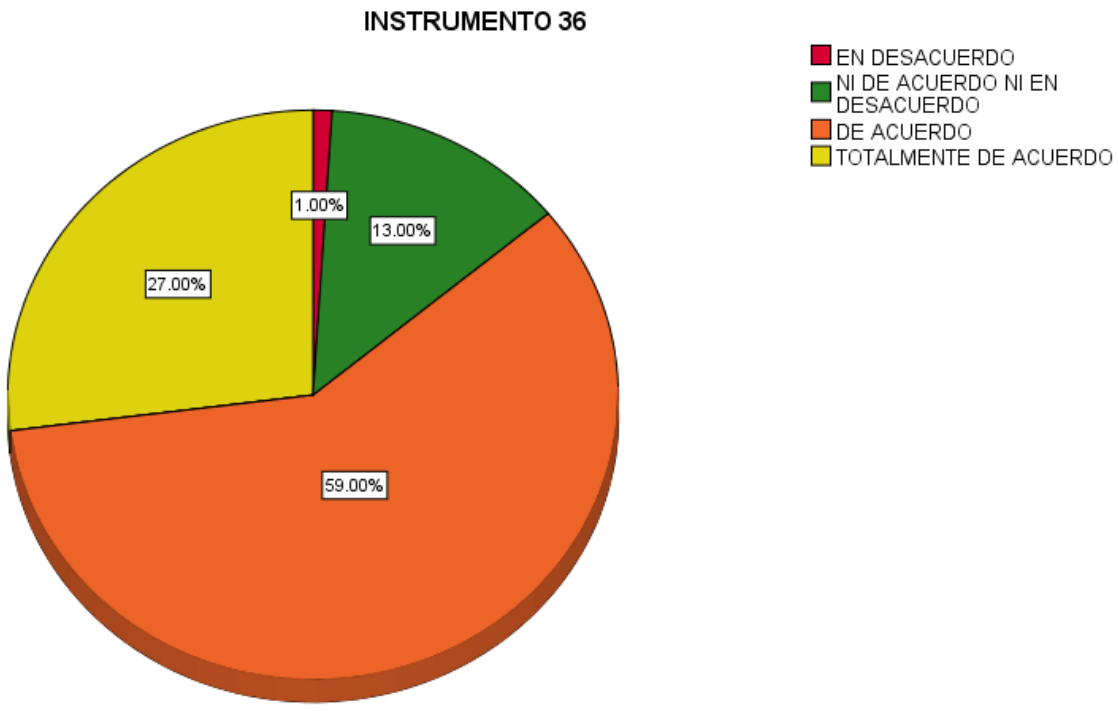
"La degradación controlada de ataques ayuda a proteger la continuidad operativa".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
En Desacuerdo	1	1.0	1.0	1.0
Ni de Acuerdo ni en Desacuerdo	13	13.0	13.0	14.0
De Acuerdo	59	59.0	59.0	73.0
Totalmente de Acuerdo	27	27.0	27.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 41

"La degradación controlada de ataques ayuda a proteger la continuidad operativa".



Nota: Elaboración propia. Tabla generada con el software SPSS25.

Análisis: En el instrumento N° 36, la degradación controlada de ataques es considerada útil para proteger la continuidad operativa, con un 86% (59% de acuerdo y 27% totalmente de acuerdo) indicando que esta medida es eficaz. Sin embargo, un 13% permanece neutral, lo que sugiere que algunos usuarios no tienen una evaluación clara sobre el impacto de esta estrategia en la continuidad operativa.

Un pequeño 1% está en desacuerdo, lo que señala que, en algunos casos, la degradación controlada podría no ser suficiente para garantizar la protección total de las operaciones.

- ✓ **Interrupción**

Cuadro 45

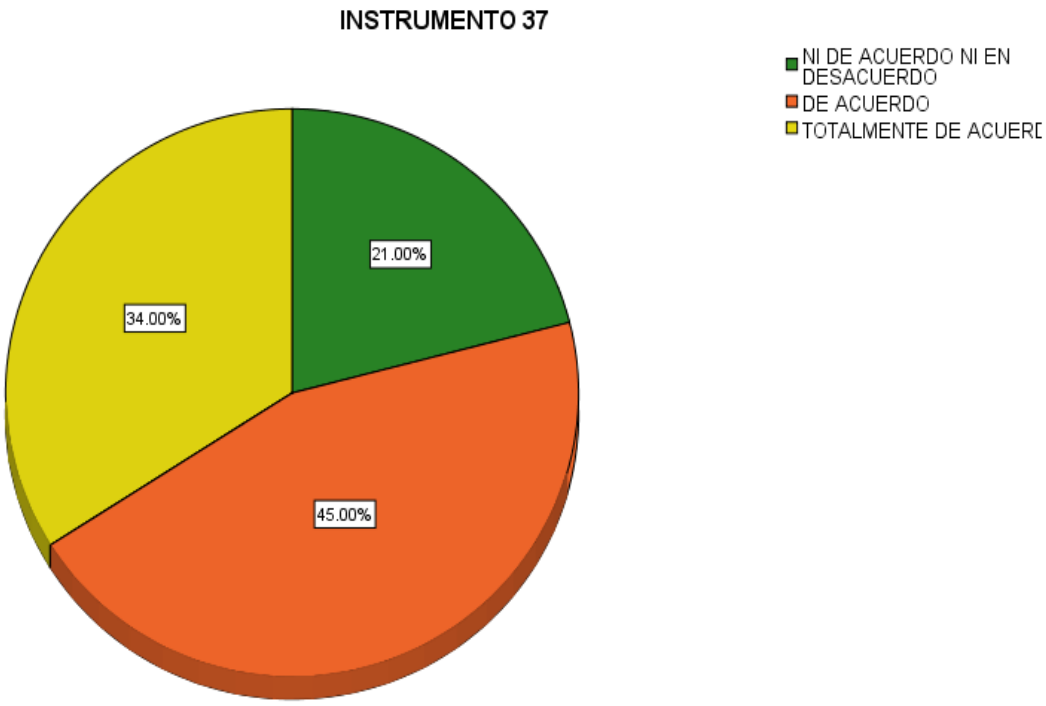
"Se dispone de protocolos para detener ataques que buscan interrumpir el servicio".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Ni de Acuerdo ni en Desacuerdo	21	21.0	21.0	21.0
De Acuerdo	45	45.0	45.0	66.0
Totalmente de Acuerdo	34	34.0	34.0	100.0
Total	100	100.0	100.0	

Nota: Elaboración propia. Tabla generada con el software SPSS25.

Figura 42

"Se dispone de protocolos para detener ataques que buscan interrumpir el servicio".



Nota: Tabla generada con el software SPSS25.

Análisis: En el instrumento N° 37, la mayoría de los encuestados considera que existen protocolos adecuados para detener ataques que buscan interrumpir el servicio, con un 79% (45% de acuerdo y 34% totalmente de acuerdo) afirmando que estos protocolos son efectivos. Sin embargo, un 21% permanece neutral, lo que podría sugerir que algunos usuarios no tienen una experiencia clara sobre la efectividad de estos protocolos o no están completamente informados.

Cuadro 46

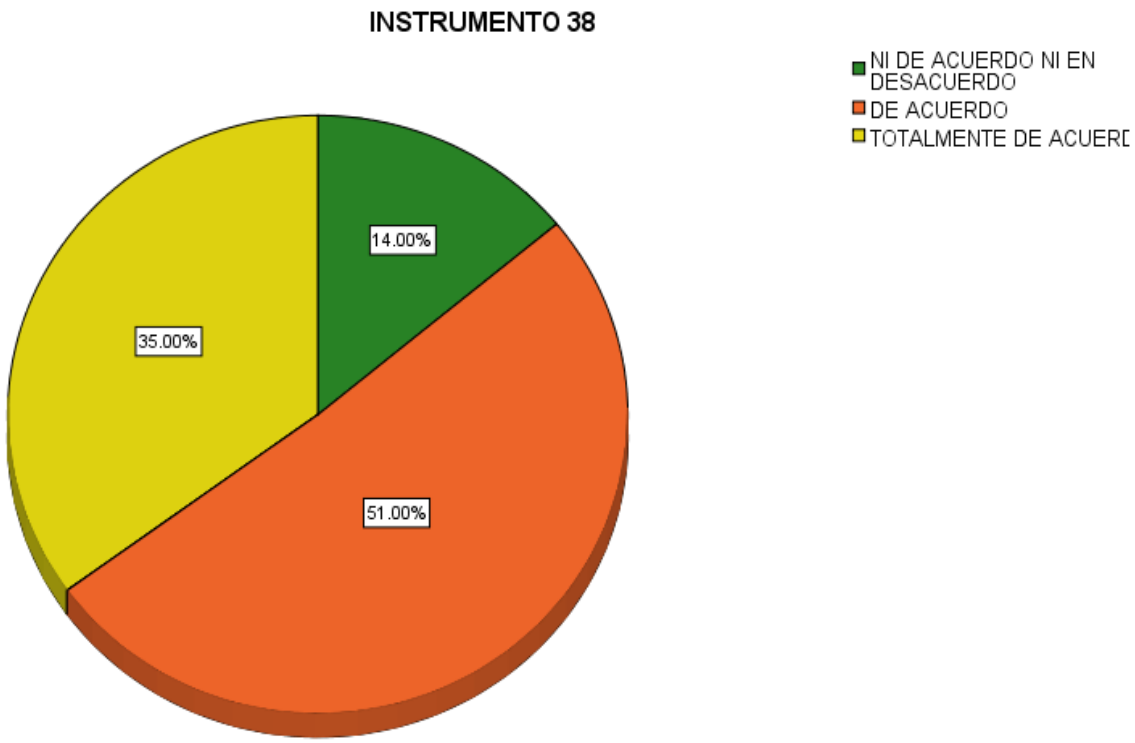
"Las acciones de interrupción neutralizan eficazmente las amenazas críticas".

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Ni de Acuerdo ni en Desacuerdo	14	14.0	14.0	14.0
De Acuerdo	51	51.0	51.0	65.0
Totalmente de Acuerdo	35	35.0	35.0	100.0
Total	100	100.0	100.0	

Nota: Tabla generada con el software SPSS25.

Figura 43

"Las acciones de interrupción neutralizan eficazmente las amenazas críticas".



Nota: Tabla generada con el software SPSS25.

Análisis: En el instrumento N° 38, las acciones de interrupción son consideradas efectivas para neutralizar amenazas críticas, con un 86% (51% de acuerdo y 35% totalmente de acuerdo) indicando que las acciones son eficaces. Sin embargo, un 14% permanece neutral, lo que podría sugerir que algunos usuarios no han tenido suficiente experiencia directa con estas acciones o no están completamente seguros de su efectividad.

CAPÍTULO V: PROPUESTA

5.1 Propuesta para la solución del problema

En concordancia con los resultados obtenidos en la presente investigación y en atención al cumplimiento del objetivo general, que es evaluar la factibilidad del uso del internet satelital en el control ciberespacial de los destacamentos remotos de la Fuerza Aérea del Perú, se plantea una propuesta estratégica de solución que permita superar las limitaciones identificadas en materia de conectividad, vigilancia digital y capacidad operativa en entornos remotos.

La propuesta consiste en el diseño e implementación progresiva de un sistema de internet satelital de órbita baja (LEO) en destacamentos seleccionados, como solución tecnológica destinada a optimizar las operaciones de monitoreo, comando y control digital, fortaleciendo la capacidad de respuesta de la FAP dentro del ciberespacio. Esta solución responde directamente a los objetivos específicos de la investigación, los cuales se relacionan de la siguiente manera:

- **Objetivo específico 1: Analizar las características técnicas, operativas, económicas y de seguridad del servicio de internet satelital.** La propuesta contempla una selección tecnológica adecuada basada en estándares de eficiencia, seguridad y sostenibilidad presupuestaria. Se sugiere priorizar sistemas como Starlink u otras constelaciones LEO que ofrecen baja latencia, alta cobertura y compatibilidad con entornos militares, lo cual garantiza una implementación técnicamente viable.

- **Objetivo específico 2: Identificar las capacidades actuales de control ciberespacial en destacamentos remotos.** La solución parte del diagnóstico de las limitaciones actuales en cuanto a infraestructura digital, proponiendo una plataforma de comunicaciones satelitales que cierre las brechas existentes y potencie el alcance del sistema de defensa cibernética, incorporando vigilancia, detección de amenazas y comunicaciones seguras.
- **Objetivo específico 3: Determinar la viabilidad del uso del internet satelital como recurso para el control ciberespacial.** La propuesta integra criterios de viabilidad técnica, operativa y económica, además de considerar factores logísticos y recursos humanos capacitados, permitiendo evaluar su sostenibilidad en el tiempo como recurso estratégico de defensa.

Los componentes clave de la propuesta son:

1. Implementación de sistemas de conectividad satelital LEO en destacamentos con bajo o nulo acceso a redes terrestres, con equipos de recepción compactos, móviles y de fácil instalación. Este componente consiste en la adquisición, instalación y configuración de sistemas de internet satelital basados en constelaciones de órbita baja (LEO)**,** como Starlink, OneWeb u otros que cumplan con estándares de eficiencia operativa y seguridad militar. Estos sistemas permiten una conectividad de alta velocidad y baja latencia. El equipamiento debe incluir antenas receptoras con capacidad de autoalineación, terminales de usuario resistentes a condiciones climáticas extremas y fuentes de energía autónomas (como paneles solares), a fin de garantizar la continuidad del servicio.

2. Capacitación del personal técnico-operativo en gestión del servicio satelital para asegurar la operatividad autónoma y sostenida del sistema, se propone un programa de capacitación especializada para el personal militar y técnico destinado en los destacamentos remotos. Esta formación incluirá conocimientos en:

    - ✓ Instalación y alineación de antenas satelitales.
    - ✓ Diagnóstico de fallas y mantenimiento preventivo.
    - ✓ Configuración de redes internas seguras y encriptadas.
    - ✓ Manejo de incidentes técnicos y ciberataques básicos.
    - ✓ Integración del sistema con redes de mando y control existentes.

3. Integración de los sistemas satelitales con los entornos de comando y control de la FAP, este componente busca garantizar que la conectividad satelital no funcione de forma aislada, sino que se integre plenamente con los sistemas de mando, control y vigilancia existentes**,** cumpliendo con los protocolos de interoperabilidad técnica y doctrinal de la institución.

    - ✓ Compatibilidad con sistemas de gestión de información táctica (C2/C4ISR).
    - ✓ Enlace seguro con bases de datos institucionales, flujos de inteligencia y videovigilancia en tiempo real.
    - ✓ Implementación de protocolos de encriptación militar (como AES-256 o equivalentes) para evitar interceptaciones o intrusiones.
    - ✓ Segmentación lógica de redes para separar canales administrativos, operativos y de mando.

4. Fortalecimiento de las operaciones de control ciberespacial, especialmente en los componentes de vigilancia, interrupción, degradación y respuesta táctica, gracias a la conectividad estable y constante proporcionada por el sistema satelital. Gracias a la conectividad satelital confiable, será posible implementar capacidades específicas como:

    - ✓ Monitoreo continuo de amenazas digitales mediante sensores y sistemas IDS/IPS integrados a la red satelital.
    - ✓ Ejecución de operaciones de interrupción y degradación selectiva frente a ataques cibernéticos o redes enemigas.
    - ✓ Coordinación en tiempo real de respuestas tácticas cibernéticas, incluyendo el aislamiento de segmentos comprometidos o el despliegue de contramedidas.
    - ✓ Participación activa en simulacros de defensa cibernética (cyber range), fortaleciendo la preparación del personal.

5. Evaluación periódica del servicio mediante indicadores operativos que permitan medir el impacto real sobre la eficacia del control ciberespacial en cada destacamento.

    - ✓ Latencia promedio (en milisegundos).
    - ✓ Velocidad de subida y bajada (en Mbps).
    - ✓ Porcentaje de disponibilidad mensual (uptime).
    - ✓ Número de interrupciones no programadas.
    - ✓ Tiempo medio de recuperación (MTTR) ante fallas.
    - ✓ Grado de satisfacción del usuario operativo.

La presente propuesta representa una solución técnica y estratégica alineada con los objetivos de la investigación, al ofrecer una alternativa factible, adaptable y sostenible para fortalecer la presencia operativa de la Fuerza Aérea del Perú en el entorno ciberespacial, con especial énfasis en contextos geográficos de difícil acceso.

5.2 Beneficios que aporta la propuesta

La presente propuesta tiene como finalidad principal fortalecer el control ciberespacial en los destacamentos remotos de la Fuerza Aérea del Perú (FAP) mediante la implementación de un sistema de internet satelital basado en tecnología de órbita baja (LEO). Esta medida no solo busca resolver la problemática de conectividad en zonas de difícil acceso, sino también mejorar la capacidad operativa, táctica y estratégica de la institución en el entorno digital. A través de un enfoque multidimensional, la propuesta aporta beneficios que impactan en lo tecnológico, lo organizacional, lo operativo y lo estratégico, contribuyendo a la modernización institucional y a la consolidación de una postura nacional robusta en materia de defensa cibernética.

Uno de los principales beneficios que se espera obtener es la mejora sustancial en la conectividad de los destacamentos ubicados en zonas geográficamente aisladas**,** donde actualmente la infraestructura de telecomunicaciones es inexistente o insuficiente. La incorporación de internet satelital permitirá garantizar acceso continuo, estable y seguro a redes digitales, lo que es fundamental para el cumplimiento de misiones operativas, vigilancia del espacio aéreo y la ejecución de protocolos de defensa cibernética. Esta conectividad confiable no solo reducirá las brechas tecnológicas internas, sino que también permitirá una presencia más efectiva de la FAP en áreas de interés estratégico.

Asimismo, la propuesta contribuye directamente al fortalecimiento del control ciberespacial como capacidad operativa prioritaria. La posibilidad de contar con acceso en tiempo real a los sistemas institucionales, plataformas de vigilancia, flujos de inteligencia y comunicaciones cifradas, permite que los destacamentos remotos actúen como nodos activos dentro de la red nacional de defensa cibernética. De esta manera, se potencia la capacidad de monitoreo, detección temprana, análisis de amenazas, y ejecución de respuestas cibernéticas desde regiones que, anteriormente, no participaban plenamente de este dominio.

Otro beneficio sustantivo es la continuidad operativa y la autonomía táctica que la conectividad satelital proporciona. En escenarios de emergencia, conflicto o desastres naturales, donde las comunicaciones tradicionales pueden colapsar, el internet satelital garantiza la persistencia de las operaciones, permitiendo mantener la cadena de mando y control, así como la transferencia segura de datos críticos. Esto asegura que las unidades desplegadas puedan operar de manera autónoma sin interrupciones, aumentando su capacidad de respuesta y resistencia frente a situaciones adversas. La autonomía táctica que se genera es especialmente relevante para la defensa nacional en zonas de frontera o alto valor geoestratégico.

Desde una perspectiva institucional, la propuesta favorece la modernización tecnológica de la FAP y la incorporación de nuevas competencias digitales en su personal. La implementación de sistemas satelitales exige el desarrollo de habilidades técnicas en instalación, mantenimiento, operación y seguridad informática, lo cual se traduce en formación especializada y profesionalización del recurso humano militar y técnico. Esta evolución genera capacidades sostenibles dentro de la institución, reduciendo la dependencia de proveedores externos y permitiendo un crecimiento autónomo de las competencias

tecnológicas. Además, contribuye al fortalecimiento de una cultura organizacional orientada a la innovación, la ciberseguridad y el dominio de tecnologías de punta.

A mediano y largo plazo, también se espera una optimización de los recursos logísticos y operativos. Aunque la inversión inicial en tecnología satelital pueda ser considerable, su portabilidad, escalabilidad y bajo requerimiento de infraestructura terrestre permitirán reducir los costos asociados al traslado físico de personal, al mantenimiento de sistemas analógicos y a las interrupciones en la cadena de comunicaciones. Esto se traduce en una mayor eficiencia en el uso de recursos presupuestales, así como en una mejor planificación de operaciones en entornos remotos o variables.

Finalmente, los beneficios derivados de esta propuesta trascienden la simple mejora en la conectividad. Se trata de una solución integral que impacta positivamente en la operatividad, seguridad, capacitación y modernización de la Fuerza Aérea del Perú, a la vez que contribuye a la consolidación de una infraestructura digital defensiva soberana, resiliente y articulada con los desafíos del ciberespacio contemporáneo. Su implementación permitirá que los destacamentos remotos dejen de ser puntos vulnerables y pasen a ser activos estratégicos dentro de una red nacional de defensa digital cohesionada y eficiente.

CONCLUSIONES

- Los resultados del estudio permiten confirmar que el uso del internet satelital representa una solución tecnológicamente viable y operativamente efectiva para mejorar el control ciberespacial en destacamentos remotos de la Fuerza Aérea del Perú. La disponibilidad de conectividad satelital de baja latencia y alta cobertura en zonas geográficamente aisladas permite asegurar la continuidad de las operaciones, el enlace con los sistemas de mando y control, y el ejercicio oportuno de respuestas cibernéticas ante amenazas digitales, validando así la hipótesis de investigación.
- El análisis de las características técnicas, operativas, económicas y de seguridad del internet satelital, en especial de las constelaciones en órbita baja (LEO), demuestra que esta tecnología cumple con los estándares necesarios para ser utilizada en contextos militares. Su capacidad de adaptarse a entornos complejos sin requerir infraestructura terrestre fija, junto con su compatibilidad con sistemas de cifrado y gestión de red, confirma su pertinencia como solución estratégica para la defensa digital del país.
- En relación con las capacidades actuales de control ciberespacial en los destacamentos, la investigación evidenció limitaciones significativas vinculadas a la ausencia de conectividad estable, lo que afecta negativamente la vigilancia, el monitoreo y la respuesta digital en tiempo real. En este sentido, la implementación del internet satelital contribuye directamente a superar estas limitaciones, convirtiéndose en un facilitador clave para la integración de estas unidades periféricas al sistema nacional de defensa cibernética.

- El internet satelital no solo mejora las condiciones de conectividad técnica, sino que también impulsa procesos complementarios como la capacitación del personal, la modernización institucional, la optimización logística y la mejora en la soberanía tecnológica. Estos efectos colaterales fortalecen el impacto positivo del servicio en el conjunto del sistema de defensa digital, proyectando beneficios sostenibles a largo plazo. Es así que el uso del internet satelital tiene un impacto positivo, significativo y multifactorial en el control ciberespacial de los destacamentos remotos de la Fuerza Aérea del Perú, al mejorar su capacidad de operación, respuesta, monitoreo y seguridad en entornos digitales exigentes.

RECOMENDACIONES

- Se recomienda un plan piloto de implementación de internet satelital en destacamentos remotos, como primera fase de despliegue institucional, orientado a validar en condiciones reales la operatividad, seguridad y sostenibilidad del servicio satelital basado en tecnología de órbita baja (LEO), evaluando su impacto directo en las funciones de vigilancia, comando, respuesta cibernética y continuidad operativa. Este plan permitirá evaluar en condiciones reales la operatividad del sistema, identificar oportunidades de mejora y validar su impacto en el control ciberespacial antes de una expansión institucional.
- Para asegurar el éxito de la implementación y operación del sistema de internet satelital, se recomienda establecer un programa permanente de capacitación y especialización en tecnologías satelitales y control ciberespacial, dirigido al personal técnico y operativo desplegado en los destacamentos remotos. Este debe abarcar conocimientos sobre instalación y mantenimiento de sistemas satelitales, gestión de redes seguras, respuesta a incidentes cibernéticos y operación de plataformas de comando y control en entornos conectados vía satélite. La capacitación debe ser progresiva, adaptada al nivel técnico de los participantes y desarrollada en alianza con instituciones especializadas, tanto militares como académicas. Esta inversión en talento humano garantiza la sostenibilidad del sistema, reduce la dependencia externa y fortalece la autonomía táctica del personal destacado.
- Es necesario que se implemente un sistema de monitoreo y evaluación continua del desempeño técnico y operativo del internet satelital instalado en los destacamentos.

Este sistema debe incluir indicadores clave como latencia, estabilidad de la conexión, disponibilidad mensual, velocidad de transmisión, incidencia de fallos, tiempo medio de recuperación y nivel de satisfacción del usuario. Además, deben incorporarse indicadores específicos para medir su impacto en el control ciberespacial, como la capacidad de detección de amenazas, eficacia en la respuesta cibernética y fluidez del comando remoto. La información recogida debe alimentar un sistema de mejora continua, que permita ajustar configuraciones, capacitar al personal según nuevas necesidades y tomar decisiones estratégicas con base en evidencia real.

REFERENCIAS

Agencia Órbita (2024) *Internet satelital: Seis años conectando las zonas más alejadas del Perú* https://agenciaorbita.org/internet-satelital-seis-anos-conectando-las-zonas-mas-alejadas-del-peru/

Aguilar, J. (2021). Realidad y retos entorno a la capacidad de las FF.AA. para neutralizar ciberataques que atenten contra la Seguridad Natural. https://www.recide.caen.edu.pe/index.php/recide/article/view/99/121

Arce, J & Maguin, . (2024). Cobertura de Internet Satelital y Acciones Militares. https://repositorio.esge.edu.pe/items/962ae7ea-8a9f-4751-9df0-664be5630d38

Arellano, I (2024) Acceso a Internet Satelital sobre redes de mega constelaciones LEO. http://cicese.repositorioinstitucional.mx/jspui/handle/1007/4201

Brito, J (2019). Evolución de las redes Móviles. https://redtis.webaccess.mx/index.php/Redtis/article/view/36

Burns. W& Taylor J. (2020). Internet Satelital y Conectividad Global.

Cardenas, S (2022) El Impacto del Internet Global "Starlink" https://revistas.unesum.edu.ec/index.php/unesumciencias/article/view/461

CircleID Editorial (2024) ¿Qué es el Internet Satelital? https://circleid.com/guides/what-is-satellite-internet

Comparaiso Perú (2025) *Internet satelital en Perú: todos los proveedores y precios.* https://comparaiso.com.pe/hogar/internet-satelital

Cui, J., et al. (2023). *Cybersecurity Threats and Countermeasures in Satellite Communication Systems. Computers & Security.* https://www.sciencedirect.com/science/article/abs/pii/S0167404823000652?via%3Dihub

Edward. S (2025). Implementación de soluciones de ciberseguridad para la protección de la red. https://csiac.dtic.mil/articles/implementing-cybersecurity-solutions-for-space-network-protection/

Fuerza Aérea del Perú (FAP). (2021). *Doctrina básica de la Fuerza Aérea del Perú (DBFA 1)*. Fuerza Aérea del Perú

Hernández, R., Fernández, C., & Baptista, P. (2014). *Metodología de la investigación* (6.ª ed.). México D.F.: McGraw-Hill.

Internet Satelital: La solución para conectar zonas remotas https://fiberlux.pe/internet-satelital-la-solucion-para-conectar-zonas-remotas/

Fernández, Y (2019) - Internet Satelital https://www.xataka.com/basics/internet-satelite-que-como-funciona-mejores-tarifas

Gobierno del Perú – PRONATEL (2023). *Conecta Selva: Internet satelital para zonas aisladas de la Amazonía.* https://www.gob.pe/institucion/pronatel/noticias/498079

Gobierno del Perú – MTC (2023). MTC y MINDEF suscriben convenio para fortalecer la ciberseguridad y conectividad del sector Defensa. https://www.gob.pe/institucion/mtc/noticias/1177993

International Telecommunication Union – ITU (2023). *Satellite communications for remote and defense connectivity.* https://www.itu.int/en/ITU-R/space/Pages/default.aspx

Jaramillo, O (2024). La apropiación de la órbita terrestre baja (LEO) por Starlink y Amazon: Retos del derecho internacional en materia del acceso equitativo a los recursos del servicio de Internet satelital https://repository.urosario.edu.co/items/c7d4a970-d22d-41fa-8cba-f1e2e0ef992f

La República (2024). *Se implementó un millonario sistema satelital en Perú de última generación: aumentará la capacidad militar y llevará internet a zonas Rurales*

https://larepublica.pe/sociedad/2024/12/23/se-implemento-un-millonario-sistema-satelital-en-peru-de-ultima-generacion-aumentara-la-capacidad-militar-y-llevara-internet-a-zona

Lin, X., et al. (2021). *On the path to 6G: Embracing the next wave of Low Earth Orbit satellite access*. arXiv. https://doi.org/10.48550/arXiv.2104.10533

Ministerio de Defensa del Perú (2024). *Fuerza Aérea moderniza su sistema de comunicación satelital para fortalecer capacidades de Defensa.* https://www.gob.pe/institucion/mindef/noticias/1072650

Ministerio de Defensa del Perú. *Fuerza Aérea del Perú fortalecerá su capacidad de ciberseguridad gracias a convenio firmado por Mindef*. https://www.gob.pe/institucion/mindef/noticias/946290-fuerza-aerea-del-peru-fortalecera-su-capacidad-de-ciberseguridad-gracias-a-convenio-firmado-por-mindef

Ministerio de Transportes y Comunicaciones (2023). *MTC lanzó "Conecta Selva" para beneficiar con internet satelital a 200 mil peruanos en zonas aisladas de la Amazonía*. Gobierno del Perú. Recuperado de: https://www.gob.pe/institucion/pronatel/noticias/498079

Ramírez-Arroyo, et al. (2024). *Multi-connectivity solutions for rural areas: Integrating terrestrial 5G and satellite networks to support innovative IoT use cases*. *arXiv*. https://doi.org/10.48550/arXiv.2411.06979

Ts2.space (2024). *Tecnología satelital en la milicia y defensa: una visión global.* https://ts2.tech/es/tecnologia-satelital-en-la-milicia-y-defensa-una-vision-global/

PeruData (2025) *Internet para Áreas Remotas: ¿Cuál Elegir?* https://perudata.net/cual-es-la-mejor-opcion-de-internet-para-areas-remotas-satelital-o-radio-enlace/

Proyecto de Implementación de Internet Satelital en Zonas Rurales de la Ciudad de Manta. (2021). *Implementación de Internet Satelital en Zonas Rurales de la Ciudad de Manta, para la continuidad de las Clases Virtuales durante el año 2021* https://ciencialatina.org/index.php/cienciala/article/view/15767

Rasis, J. (2012). Las Comunicaciones Satelitales en apoyo a la conducción en un Teatro de Operaciones.

Reta, I & Ibarra, A (2022) Evolución del costo beneficio del Internet Satelital para áreas rurales.

Selectra Perú (2025) *Internet satelital en Perú: Precios y planes 2025.* https://selectra.com.pe/internet/satelital

Yamakawa, P. (2022). *Internet satelital: ¿Se reducirá la brecha digital en el Perú?* Universidad ESAN. https://www.esan.edu.pe/conexion-esan/internet-satelital-se-reducira-la-brecha-digital-en-el-peru

Zhang, X., et al. (2023). *Security Challenges of LEO Satellite Internet for Military Applications. IEEE Communications Surveys & Tutorials.*

ANEXOS

Anexo N.º 01: Matriz de consistencia

Anexo N.º 02: Matriz de Conceptualización

Anexo N.º 02: Matriz de instrumento de Investigación

Anexo N.º 03: Instrumentos de recolección de datos

ANEXO N.º 1: Matriz de consistencia

"USO DEL INTERNET SATELITAL EN EL CONTROL CIBERESPACIAL EN DESTACAMENTOS REMOTOS DE LA FUERZA AÉREA DEL PERÚ, EN EL AÑO 2025"

PREGUNTA GENERAL	OBJETIVO PRINCIPAL	HIPÓTESIS PRINCIPAL	VARIABLES	DIMENSIONES E INDICADORES	METODOLOGÍA
¿Cuál es la factibilidad del uso de internet satelital para el control ciberespacial en los destacamentos remotos de la Fuerza Aérea del Perú?	Evaluar la factibilidad del uso de internet satelital para el control ciberespacial en los destacamentos remotos de la Fuerza Aérea del Perú, en el año 2025.	El uso de internet satelital contribuye positivamente con el control ciberespacial en los destacamentos remotos de la Fuerza Aérea del Perú, en el año 2025.	**Independiente X:** INTERNET SATELITAL	**Variable Independiente** **D1 Cobertura** • Área geográfica • Tiempo de conexión **D2 Calidad** • Velocidad • Latencia **D3 Usabilidad** • Facilidad de uso • Accesibilidad total **Variable Dependiente** **D1 Operaciones Defensivas** • Medidas preventivas • Medidas proactivas	**Enfoque de investigación:** Cualitativa **Tipo de investigación:** Aplicada **Alcance de Investigación:** Exploratoria **Técnicas de recolección datos:** Encuesta
ESPECIFICOS	**ESPECIFICOS**	**ESPECIFICOS**			
¿Cuál es la factibilidad del uso de internet satelital en las operaciones defensivas del control ciberespacial en los destacamentos remotos de la Fuerza Aérea del Perú, en el año 2025?	Determinar la relación entre el liderazgo y el desempeño del personal de Comunicaciones y Electrónica del Ala Aérea Nº1 en el año 2025.	El uso de internet satelital contribuye significativamente en las Operaciones Defensivas de los destacamentos remotos de la Fuerza Aérea del Perú, en el año 2025.			

¿Cuál es la factibilidad del uso de internet satelital en las operaciones de explotación del control ciberespacial en los destacamentos remotos de la Fuerza Aérea del Perú, en el año 2025? ¿Cuál es la factibilidad del uso de internet satelital en las operaciones de respuesta del control ciberespacial en los destacamentos remotos de la Fuerza Aérea del Perú, en el año 2025?	Analizar la eficiencia del uso de internet satelital en las operaciones de explotación del control ciberespacial en los destacamentos remotos de la Fuerza Aérea del Perú, en el año 2025. Analizar la eficiencia del uso de internet satelital en las operaciones de respuesta del control ciberespacial en los destacamentos remotos de la Fuerza Aérea del Perú, en el año 2025.	El uso de internet satelital contribuye significativa en las Operaciones de Explotación de los destacamentos remotos de la Fuerza Aérea del Perú, en el año 2025. El uso de internet satelital contribuye significativa en las Operaciones de Respuesta de los destacamentos remotos de la Fuerza Aérea del Perú, en el año 2025.	**Dependiente Y:** CONTROL CIBERESPACIAL	• Medidas reactivas • Medidas de recuperación **D2 Operaciones de explotación** • Búsqueda • Detección • Identificación **D3 Operaciones de respuesta** • Denegación • Degradación • Interrupción	**Instrumento:** Cuestionario **Población:** 100 militares **Muestra:** 100

ANEXO N.º 2: Matriz de Conceptualización. Dimensiones. Indicadores

VARIABLES	DEFINICIÓN	DIMENSIONES	INDICADORES
INTERNET SATELITAL (Variable independiente)	Tecnología que permite el acceso a internet mediante satélites artificiales en órbita baja, facilitando la conexión en zonas remotas o de difícil acceso.	Cobertura	Área geográfica
			Tiempo de conexión
		Calidad	Velocidad
			Latencia
		Usabilidad	Facilidad de uso
			Accesibilidad total
CONTROL CIBERESPACIAL (Variable dependiente)	Conjunto de procesos, tecnologías y capacidades que permiten supervisar, proteger y gestionar el dominio digital, asegurando la integridad, disponibilidad y seguridad de los sistemas de información en operaciones militares y estratégica	Operaciones Defensivas	Medidas preventivas
			Medidas proactivas
			Medidas reactivas
			Medidas de recuperación
		Operaciones de explotación	Búsqueda
			Detección
			Identificación
		Operaciones de respuesta	Denegación
			Degradación
			Interrupción

Nota. Elaboración propia

ANEXO N.º 3: Matriz de Instrumentos de Investigación

VARIABLE	DIMENSIONES	INDICADORES	ITEMS	ESCALA
Internet Satelital	- Cobertura	- Área geográfica	1,2,3	Escala de Likert
		- Tiempo de conexión	4,5,6	
	- Calidad	- Velocidad	7,8,9	
		- Latencia	10,11,12	
	- Usabilidad	- Facilidad de uso	13,14,15	
		- Accesibilidad total	16,17,18	
Control Ciberespacial	- Operaciones Defensivas	- Medidas preventivas	1,2	Escala de Likert
		- Medidas proactivas	3,4	
		- Medidas reactivas	5,6	
		- Medidas de recuperación	7,8	
	- Operaciones de explotación	- Búsqueda	9,10	
		- Detección	11,12	
		- Identificación	13,14	
	- Operaciones de respuesta	- Denegación	15,16	
		- Degradación	17,18	
		- Interrupción	19,20	

ANEXO N.º 04: Instrumento de Recolección De Datos

“USO DE INTERNET SATELITAL EN EL CONTROL CIBERESPACIAL EN DESTACAMENTOS REMOTOS DE LA FUERZA AÉREA DEL PERÚ, EN EL AÑO 2025”

Le invitamos a participar en esta encuesta que forma parte de un estudio sobre el uso de internet satelital en los destacamentos remotos de la Fuerza Aérea del Perú, enfocado en aspectos técnicos, operativos, económicos y de seguridad relacionados con el control ciberespacial.

La información recopilada será utilizada de manera confidencial y con fines exclusivamente investigativos, con el propósito de identificar áreas de mejora y fortalecer las políticas de la institución. Su participación es fundamental para contribuir al desarrollo de la Fuerza Aérea del Perú. ¡Gracias por su tiempo y colaboración!

Escala de valoración:
1 = TOTALMENTE EN DESACUERDO
2 = EN DESACUERDO
3 = NI DE ACUERDO NI EN DESACUERDO
4 = DE ACUERDO
5 = TOTALMENTE DE ACUERDO

VARIABLE	OPCIONES
Edad	De 25-34 años ( ) / - 35-44 años ( ) / - 45-54 años ( )/ - 55 años o más ( )
Género	- Masculino ( ) / - Femenino ( )
Plana Laboral	- Oficial ( ) / - TTSSOO ( )
Años de Servicio	- De 1-5 años ( ) / - 6-10 años ( ) / - 11-15 años ( ) / - Más de 15 años ( )

ENCUESTA 1: INTERNET SATELITAL

N.º	COBERTURA	1	2	3	4	5
01	El servicio de internet satelital cubre adecuadamente las zonas remotas donde opera la Fuerza Aérea del Perú.					
02	La cobertura satelital permite mantener conexión constante en áreas de difícil acceso.					
03	La cobertura actual satisface las necesidades de comunicación en los destacamentos remotos.					
04	El tiempo de conexión a internet satelital es continuo y sin interrupciones significativas.					
05	El servicio satelital garantiza la disponibilidad de conexión durante las operaciones críticas.					
06	La conexión a internet satelital es estable y confiable en el tiempo necesario para las operaciones.					
CALIDAD						
07	La velocidad de descarga y subida del internet satelital es suficiente para las actividades de control ciberespacial.					
08	El internet satelital permite la transmisión fluida de datos, voz y video sin retrasos importantes.					
09	La velocidad del servicio satelital cumple con los requerimientos operativos de la Fuerza Aérea.					
10	La latencia del internet satelital es adecuada para las comunicaciones en tiempo real.					
11	El retraso en la transmisión de datos vía satélite no afecta el desempeño de las operaciones ciberespaciales.					
12	La latencia del servicio satelital permite una respuesta rápida en situaciones críticas.					
USABILIDAD						
13	El sistema de internet satelital es fácil de operar para el personal técnico y operativo.					
14	El personal recibe capacitación adecuada para el manejo del servicio satelital.					
15	Los equipos y dispositivos del internet satelital son intuitivos y amigables para su uso diario.					
16	El internet satelital está disponible para todos los usuarios autorizados en los destacamentos remotos.					
17	No existen restricciones técnicas que limiten el acceso al servicio satelital en las zonas operativas.					
18	La infraestructura satelital permite un acceso ininterrumpido para las operaciones militares.					

ENCUESTA 2: CONTROL CIBERESPACIAL

N.º	OPERACIONES DEFENSIVAS	1	2	3	4	5
01	Existen políticas claras para prevenir ataques cibernéticos en las comunicaciones satelitales.					
02	Se realizan revisiones periódicas para identificar vulnerabilidades en la red satelital.					
03	Se monitorea continuamente el tráfico de datos para detectar posibles amenazas.					
04	El personal está capacitado para anticipar y responder a incidentes cibernéticos.					
05	Existen protocolos claros para responder a incidentes de seguridad en el internet satelital.					
06	El equipo de respuesta actúa rápidamente para contener ataques cibernéticos.					
07	Se cuenta con planes de contingencia para restaurar el servicio en caso de interrupciones.					
08	La Fuerza Aérea dispone de recursos adecuados para la recuperación ante fallas de seguridad.					
OPERACIONES DE EXPLOTACIÓN						
09	El personal utiliza herramientas adecuadas para localizar amenazas en el ciberespacio.					
10	La búsqueda de datos contribuye a la anticipación de ataques o vulnerabilidades.					
11	Se identifican rápidamente posibles intentos de intrusión en la red satelital.					
12	La detección oportuna permite la activación inmediata de medidas defensivas.					
13	Se determina el origen de los ataques para diseñar respuestas adecuadas.					
14	La identificación precisa de incidentes fortalece la protección del sistema satelital.					
OPERACIONES DE RESPUESTA						
15	Se aplican acciones efectivas para impedir ataques que comprometan la comunicación satelital.					
16	Las operaciones de denegación contribuyen a mantener la integridad del sistema.					
17	Se implementan medidas para reducir la eficacia de ataques en curso.					

18	La degradación controlada de ataques ayuda a proteger la continuidad operativa.					
19	Se dispone de protocolos para detener ataques que buscan interrumpir el servicio.					
20	Las acciones de interrupción neutralizan eficazmente las amenazas críticas.					