UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE INFORMACIÓN

La Ciberdefensa y su incidencia en la Gestión de Tecnologías de la Información en la Fuerza Aérea del Perú, Lima 2022

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestro en Ingeniaría de Sistemas con Mención en Tecnologías de Información

AUTOR:

Huertas Espiritu, Pablo Roberto (orcid.org/0000-0002-63824-0167)

ASESOR:

Dr. Visurraga Agüero Joel Martin (orcid.org/0000-0002-0024-668X)

CO-ASESOR:

Dr. Pereyra Acosta, Manuel Antonio (orcid.org/0000-0002-2593-5772)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA – PERÚ

2023

Dedicatoria

A todas las buenas personas que se han cruzado a lo largo de mi vida

Agradecimiento

A mi familia por el apoyo brindado a lo largo de mi vida personal, familiar y profesional

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS Y FIGURAS

Resumen

La presente investigación tiene como objetivo determinar el nivel de incidencia de la ciberdefensa en la gestión de las tecnologías de la Información en la Fuerza Aérea del Perú, Lima 2022.

Por consiguiente, se desarrolló la actual investigación de tipo aplicada, con un diseño no experimental de la misma forma se ha delimitado una población de 180 personas que laboran en el Sistema de Informática de la FAP, desarrollando, administrando y protegiendo la arquitectura de datos que se utilizan para mejorar el ciclo de toma de decisiones, así como de preservar la información que se produce en la institución. Se tomó una muestra de 123 personas y en ellos se ha utilizado la técnica de la encuesta considerando un muestreo probabilístico, se ha empleado el cuestionario como el instrumento que fue validado por profesionales expertos y para el análisis estadístico se emplearon las tablas cruzadas e histogramas.

Como resultado obtenido del presente estudio podemos concluir que la variable ciberdefensa incide significativamente con un 96,9% indicando la relación fuerte y moderada en la variable Gestión de Tecnologías de la Información en la FAP, Lima 2022.

Palabras clave: Ciberdefensa, Gestión de TI, Operaciones, Base de datos.

Abstract

The objective of this investigation is to determine the level of incidence of cyber defense in the management of information technologies in the Peruvian Air Force, Lima 2022.

Therefore, the current applied research was developed, with a non-experimental design, in the same way a population of 180 people who work in the FAP Information System has been delimited, developing, managing and protecting the data architecture that It is used to improve the decision-making cycle, as well as to preserve the information that is produced in the institution. A sample of 123 people was taken and in them the survey technique has been used considering a probabilistic test, the questionnaire has been used as the instrument that was validated by expert professionals and for the statistical analysis cross tables and histograms were used.

As a result obtained from this, we can conclude that the cyber defense variable has a significant incidence with 96.9% indicating the strong and moderate relationship in the Information Technology Management variable in the FAP, Lima 2022.

Keywords: Cyber Defense, IT Management, Operations, Database

I. INTRODUCCIÓN

El territorio durante el siglo XX, era el objetivo militar que buscaban los ejércitos, donde las comunicaciones jugaban un papel crucial para el empleo del mando y control, hasta que alrededor de los siglos XX y XXI aparece un nuevo interés para los ejércitos; el ciberespacio, el quinto ambiente de la guerra (Cubeiro, 2015), actualmente se conoce que debido a la creciente transformación digital la ciberdefensa representa una capacidad esencial de las Fuerzas Armadas en general por el incremento del empleo de las tecnologías de la información (TI) y todos aquellos que la emplean deben de estar muy preparados y encontrarse en una constante actualización; por los avances tecnológicos; así mismo el desarrollo agigantado de los programadores que en muchos casos ellos son reclutados por organizaciones criminales para obtener información confidencial de los países y personajes muy importantes; es así que la ciberdefensa se ha convertido en lo fundamental para los investigadores actuales, coincidentemente su mayor uso se da con el aparición de la nuevas TI, las interconexiones de las LAN y WAN entre equipos de cómputo. Así mismo Al Shahrani et al (2022), nos describe las bondades del empleo del Internet de las cosas pero a la vez recalca los mecanismos de seguridad que se deben tener al emplear los mismos y sobre todo para el uso específico que le damos; todo ello son usos cuyo desarrollo ha significado el nuevo escenario de la guerra actual y viene afectando considerablemente la vida diaria de todos aquellos que emplean las TI a nivel mundial. Siendo, tema de estudio y pasa a ser una prioridad para los gobernantes que se encargar de conducir estratégicamente la política de la soberanía y defensa de los países.

A nivel internacional, según IBM (2022a), en su última edición informa que la constante aparición de los criminales informáticos a nivel mundial ha elevado los desafíos para los que administran las TI, siendo el 39% durante el año 2021 a un 45% en lo que va del presente año, siendo un reto para los encargados de la seguridad en todos los niveles de los estados; siendo el robo de la entidad el que encabeza esta lista con un 65%, seguido de las transferencias bancarias

fraudulentas y el robo de documentos privados con un 61%, estos últimos generan pérdidas a nivel mundial, por lo tanto, esta situación les exige tomar más cuidado y exagerar los niveles y procedimientos de seguridad en los dispositivos informáticos de manera integral en sus tres componentes (sistemas, data y hardware), por otra parte, varios estados extreman medidas de defensa y seguridad de sus equipos informáticos que involucran un riesgo para la seguridad de la nación. Tal es así que, OEA (2021), el Secretario General de la Organización de Estado Americanos, en su informe que realiza todos los años, informa que las actividades de prevención frente a los ataques informáticos se han incrementado en un 45%, siendo 200 000 eventos los analizados en ese año; el cibercrimen le cuesta a los estados y a las organizaciones millones de dólares al año.

A nivel nacional, se aprecia que todos los días existen denuncias de delitos que tienen que ver con la Gestión de las Tecnologías de la Información (GTI) que afectan a nuestro país. ESET (2022) nos dice que durante el presente año nuestro país encabeza la lista con un 18% de cantidad de detecciones a nivel de Latinoamérica seguido por México 17% y Colombia 12%, seguidamente encabeza la lista del país más afectado con el Spyware con un 40% de las detecciones y ocupando el tercer puesto en ataques de Troyanos, con esta información es evidente el nivel de riesgo que existe en el ciberespacio siendo necesario analizar la GTI de cada organización. Cabe mencionar que la protección que se brinda en un primer nivel, se realiza a un usuario a través de la inducción y el conocimiento propio de lo que es seguridad de nuestra información que se encuentra en nuestro equipo, así como el equipo propio, y entendamos por el termino ciberdefensa como el conjunto de acciones que posee un país para ofrecer seguridad a todos sus activos críticos o bienes importantes con el objetivo de brindarle seguridad en la quinta dimensión.

A nivel local, nuestra Fuerza Aérea del Perú (FAP) dirige las acciones para preparar, … y equipar el Componente Aéreo de las Fuerzas Armadas, alineado con varios objetivos y la Política del Gobierno de turno a materia de Defensa y Seguridad de la Nación” en ese sentido como parte de su misión y visión dispuesto en la Ley N°

1139 (2012), debe tener una participación activa en el exterior y tener protagonismo durante las actividades militares en las que se desarrolle y participe mediante el uso de todo los medios asignados, debiendo encontrase en un estado óptimo para el momento de su intervención, en el cual mediante el empleo de las Tecnologías de Información (TI) se podrán tomar decisiones de forma rápida, por lo que le exige a su personal encargado que se encuentre bien capacitado y especializado en sus labores dentro de la organización (Doctrina FAP DBFA 1, 2021).

La Ciberdefensa se encuentra bajo la administración del Grupo de Operaciones del Ciberespacio (GROCE), el cual cumple con la custodia del ciberespacio estipulado en la Ley de Ciberdefensa - Ley N° 30999 (2019), asimismo sus TI que posee la FAP para el cumplimiento de sus labores administrativas y operativas que fueron solicitadas por las unidades de la FAP; según la Ordenanza FAP 20-62 (2016) La Dirección de Telemática por la naturaleza de las actividades que realiza y su dependencia directa de la Comandancia General de la FAP, dirige, controla y supervisa el Sistema de Telemática que consta del Sistema de Comunicaciones y al Sistema de Informática, ejerce autoridad orgánica y funcional sobre el Servicio de Comunicaciones y el Servicio de Informática (SINFA), así como supervisar las actividades de dichas Unidades en el área de su competencia, es el SINFA la unidad que se encarga de su diseño y desarrollo, el cual tiene como misión proporcionar Sistemas de Información (SI), administrando y desarrollando la arquitectura de los sistemas, datos y tecnologías; también, efectúa el desarrollo, implementación, mantenimiento de software, en apoyo a los planes operativos y de administración de la FAP, para contribuir al logro de su misión; esta unidad es liderada por el personal militar calificado en la especialidad de Ingeniería de Sistemas, los cuales trabajan de la mano con ingenieros y técnicos del mismo campo ocupacional especializados y calificados en los diferentes lenguajes de programación establecidos en la normativa interna que son elaborados y actualizados constantemente de acuerdo a los avances tecnológicos, dando como resultado los SI que emplean actualmente (Ordenanza FAP 20-54, 2016).

Por consiguiente de lo descrito en el párrafo anterior, se planteó el presente problema general ¿De qué manera la ciberdefensa incide en la GTI de la FAP en el año 2022?, igualmente, se plantea los problemas específicos: i) ¿Cuál es nivel de incidencia de la dimensión operaciones defensivas en la GTI de la FAP en el año 2022?, ii) ¿Cuál es nivel de incidencia de la dimensión operaciones de explotación en la GTI de la FAP en el año 2022?, y iii) ¿Cuál es nivel de incidencia de la dimensión operaciones de respuesta en la GTI de la FAP en el año 2022? (Doctrina FAP DBFA 1, 2021).

La actual investigación se justificó en los ámbitos siguientes, la justificación epistemológica, se aplicó la ciberdefensa en la GTI de la FAP para reducir los riesgos existentes en el ciberespacio, la justificación teórica, se fundamentó en mejorar el nivel de conocimiento sobre la ciberdefensa en el ámbito militar. Con la finalidad de brindar mejores sapiencias e ilustraciones para próximos estudios, la justificación práctica, es el optimizar procesos para mejorar la seguridad militar en el ciberespacio y finalmente la justificación metodológica, se respaldó que la actual investigación tiene un diseño no experimental esto se debe a que las variables que se estudiaron se mantuvieron iguales para conseguir resultados confiables; además, es significativo porque conservó los datos que se han obtenido empleando un instrumento confiable que fue aceptado y aprobado por expertos.

Ante lo descrito previamente la actual investigación planteó el siguiente objetivo general, Determinar el nivel de incidencia de la Ciberdefensa en la GTI en la FAP en el año 2022 y como objetivos específicos los siguientes : i) Determinar el nivel de incidencia de las operaciones defensivas en la GTI en la FAP en el año 2022, ii) Determinar el nivel de incidencia de las operaciones de explotación en la GTI en la FAP en el año 2022 y iii) Determinar el nivel de incidencia de las operaciones de respuesta en la GTI en la FAP en el año 2022.

En lo que respecta a la hipótesis general se señaló: la Ciberdefensa incide significativamente en la GTI en la FAP, también se plantea las hipótesis específicas: i) Las operaciones defensivas inciden significativamente en la GTI en la FAP, ii) Las

operaciones de explotación inciden significativamente en la GTI en la FAP y iii) Las operaciones de respuesta inciden significativamente en la GTI en la FAP**.**

II. MARCO TEÓRICO.

Con respecto a trabajos nacionales: según Huamán (2021), en su investigación que lleva como título “Análisis de las Capacidades en Ciberseguridad y Ciberdefensa del Centro de Ciberdefensa y Telemática del Ejército del Perú (EPE)” donde su objeto de su investigación fue explicar que competencias de ciberseguridad y ciberdefensa tiene esta dependencia castrense, utilizó para ello metodología cualitativa, llegó a la conclusión de que las fortalezas en el ámbito de ciberdefensa y ciberseguridad de la mencionada entidad son: brindar asistencia y ayuda a las Dependencias del EPE, las cuales aún no son específicas porque actualmente se encuentra en proceso de implementación; finalmente estas competencias están alineadas a dar cumplimiento a lo normado en la Ley N° 30999 “Ley de Ciberdefensa” la cual busca proteger la información para que sea confiable, integra y siempre esté disponible.

A continuación Vilcarromero et al. (2018) en su estudio titulado “Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones de seguridad (SOC) de una empresa de telecomunicaciones”, donde su objeto de su estudio fue “Proporcionar un punto de referencia de ciberseguridad para el área del SOC a fin de crear un procedimiento que le admita realizar actividades para controlar los sistemas más importantes y la información confidencial ante ataques digitales, su finalidad es llegar a convertirse en un SOC modelo y alcanzar un nivel competitivo en el rubro de las Telecomunicaciones” (p. 42), utilizó la metodología cuantitativo, llegó a la conclusión de “al adoptar el Marco NIST para aumentar la ciberseguridad será un elemento de mucha importancia para la creación de valor en las organizaciones, así mismo el marco NIST que se elaboró en esta investigación permite crear planes y políticas de ciberseguridad para empresas de telecomunicaciones”.

Además Zúñiga (2017), en su investigación que lleva como título “Ciberdefensa y su incidencia en la protección de la información del Ejército del Perú (EPE)”, donde

su objeto de su investigación fue el de “Determinar los obstáculos que imposibilitan la mejora de la Ciberdefensa y como afecta en el resguardo de la información del EPE, con el fin de definir las razones que la crean y de esa manera plantear el uso de conocimientos recientes, que ayuden a dar solución y/u optimizar el resguardo de la información del EPE”, utilizó la metodología cuantitativo llegó, llegó a las conclusiones siguientes: La primera, “El personal en general que dirige la infraestructura de TI carecen de un nivel suficiente de preparación concerniente a ciberdefensa así como el conocimiento de la NTP ISO/IEC N°17999 para poner en práctica su aplicación y de esta forma asegurar de una mejor manera la información del EPE (p.188) y la segunda “La carencia de Recursos en lo relacionado a ciberdefensa es lo que no permite asegurar la información del EPE una forma adecuada” (p.191).

También Baretto (2017), en su investigación que lleva como título “La Defensa Nacional y la estrategia militar de seguridad cibernética”, donde su objeto de su investigación fue “establecer los métodos, formas y medios que se emplean a manera de un “sistema de arma cibernético””, utilizó la metodología cualitativa, llegó a estas tres conclusiones: La primera, “es preciso afrontar la réplica de los ataques desde una sola entidad” (p. 136). La segunda, “la elaboración de la estrategia militar se ve afectada por una falta de una Estrategia Nacional de Ciberseguridad” (p. 136). La tercera, “las competencias que se necesitan tener no alcanzan el nivel suficiente para hacer frente a una amenaza” (p.136).

Por otro lado Sotomayor (2015), en su investigación que lleva como título “Cuadro de Indicadores de Seguridad de la Información para la FAP”, donde su objeto de su investigación fue “Proponer de indicadores para la seguridad de la información, los cuales se encuentran en un cuadro alineados a las necesidades de la FAP, el mismo que permita medir la efectividad del modelo de ciberseguridad” utilizó el enfoque cuantitativo dela investigación, llegó a las conclusiones siguientes: La primera, “La FAP realiza las revisiones de seguridad de la información de manera esporádica y en un intervalo de tiempo muy prolongado, lo que dificulta medir de forma correcta

y a tiempo la efectividad de estos", Segundo, "Los indicadores de seguridad propuestos facilitarán al alto mando de la FAP, la toma de decisiones que permitan adoptar medidas que reduzcan el grado de exposición de la data digital de la institución ante los propios riesgos generados por el uso de herramientas tecnológicas.

Finalmente, Villalba (2015), en su investigación que lleva como título "La ciberseguridad en España 2011-2015", donde su objeto de su investigación fue "presentar un estándar apropiado de estructura de ciberseguridad en ese país" utilizó el enfoque cualitativo, llegó a las conclusiones siguientes, la primera, "las estrategias de un país para abordar el tema de confianza en su comunidad se han trasformado en el estándar del que se desglosa la proyección del mismo en una nación; que combinados con los objetivos de la misma nación es uno solo, enfatizando en el poder económico como indicador relacionado a la seguridad; de la misma manera se tiene un estándar organizativo que se basa en un consejo de seguridad nacional; y que las estrategias sectoriales obedecen a las estrategias nacionales de seguridad, por ejemplo la de ciberseguridad" y la segunda: "la ciberseguridad debe formar parte de las agendas de las organizaciones al máximo nivel"

Respectivamente a las teorías del estudio, tenemos que según Cardona (2017), dentro de la Teoría General de Sistemas, define a un sistema de la siguiente manera, es la conjunción de varios elementos entre sí que se relacionan para lograr cumplir un fin determinado, de la misma forma todos los sistemas tienen una entrada, salida y retroalimentación, existiendo en un mismo entorno para interactuar, lo que concuerda con las metas que define Von Bertalanffy (1989), siendo la más importante de ellas la siguiente: La Teoría General de Sistemas conduce a una integración de varias partes (p.38).

Para Lorenzetti (2008), poder entender la teoría del derecho ambiental, tenemos que saber que existen fronteras en los diferentes campos de estudio de la

humanidad así mismo, cada recurso empleado para cada ámbito de estudio genera un valor especial en los mismos y de la misma forma los recursos que se emplean para los estudios se van consumiendo y escaseando, existiendo un detalle muy particular para el caso de la Ciberdefensa porque al definirse de la manera siguiente "es el grupo de medidas que se realizan en la quinta dimensión para contener, prevenir, repeler, identificar, detectar, evitar, impedir, contrarrestar, una amenaza o ataque cibernético", estas se realicen a través de nuevas formas digitales con la finalidad de afirmar el uso del Instrumento Militar de la Nación (Doctrina CCFFAA DFA-CD-03-28, 2018); y para el EPE en su Doctrina TOI 11-113 (2019) la define como la "Competencia Militar que faculta para proceder ante una posible amenaza o al sufrir ataques en y mediante la quinta dimensión siempre que estos perjudiquen la seguridad de la nación" (p.80), por lo tanto es muy difícil definir fronteras así como limitar los recursos, tácticas, métodos y procedimientos dentro de las acciones antes descritas.

Por otra parte según Gutiérrez (2022) considera a la Teoría de la evolución sostenida Charles Darwin, donde las especies tienen que adaptarse a los nuevos ambientes que se generan siendo en este caso y materia de estudio el ciberespacio, un nuevo ambiente generado por el hombre y que según Medina, (2017), la Ciberdefensa, viene a ser el grupo de operaciones o acciones desarrolladas en el ámbito del ciberespacio que comprende el personal especializado, los dispositivos cibernéticos, la red, los software y medios de transmisión de la Defensa, teniendo como finalidad de certificar que se logre el objetivo para los que fueran designados, a la vez que se neutraliza a las Fuerzas enemigas para que no alcancen sus objetivos; asimismo, Vargas et al.(2017), indicó que los estados deben preservar y vigilar a las amenazas, peligros o riesgos que se dan en la quinta dimensión para ello realizan las operaciones de Ciberdefensa, con la finalidad de consentir el empleo del ciberespacio sin anomalías, supervisando y defendiendo los derechos, libertades y garantías de todos aquellos que naveguen en ella, en ayuda y soporte a la protección de la soberanía y la integridad territorial; sin dejar de lado a los nuevos escenarios que existen en la quinta dimensión, que puedan repercutir en el

momento de proponer posibles opciones estratégicas recomendables para el cumplimiento de las diferentes operaciones militares en el ciberespacio.

Asimismo, la OTAN (2022), nos ofrece a través de su ente acreditado “Centro de Excelencia de Ciberdefensa Cooperativa”, una definición interdisciplinaria para la ciberdefensa, definiéndola como un tema estratégico que forma parte de la defensa colectiva de la OTAN, de otro lado la Escuela Superior de Colombia (2021) define a la misma como la competencia de poder aseverar y asegurar la continuidad de todos los servicios que nos brindan todos los Sistemas de Información bajo los tres cimientos de la seguridad de la información (integridad, confidencialidad y disponibilidad), durante posibles o inminentes acciones malintencionadas originadas en la quinta dimensión. Desde otro punto de vista la Organización Iniciativa Nacional de Carreras y Estudios en Ciberseguridad (2022), describe a la ciberseguridad como el trabajo de seguridad cibernética donde una persona o más personas realizan las actividades para recopilar evidencia sobre entidades de inteligencia criminales o extranjeras para mitigar amenazas posibles o en tiempo real y asegurar contra espionaje o amenazas internas, sabotaje extranjero, actividades terroristas internacionales o para apoyar otras actividades de inteligencia, de la misma manera Kosutic (2012) define la ciberseguridad “como el no tener peligros ni sufrir daños producidos por interrupciones, perdida de continuidad de los servicios o abusos de las TI”, así mismo, el peligro o daño generado por la interrupción de los servicios puede estar constituido por una restricción de la disponibilidad y confiabilidad de Ciberseguridad, una vulneración a la confidencialidad de la información que se guarda en las TI o un daño a la integridad de esa información.

Según Valle et al. (2017) define a la Gestión de TI como un elemento esencial de la organización, como es el caso de algunos negocios que son incapaces de vivir sin ella, así mismo la función de la TI han tenido variaciones a través del tiempo pasando a ser gestionada por áreas especializadas, de la misma forma Matthias Sallé clasifica en tres estados de la función a la TI: Gestión de Infraestructura,

Gestión de Servicios y Gestión del Valor del Negocio, mientras que Eraberritu, (2001), sostiene que las tecnologías que se relacionan con todas aquellas actividades referente al uso de hardware, empleo de software y los servicios informáticos, en conclusión, vienen a ser todas aquellas tecnologías las que tienen el objetivo de tratar o procesar información. Últimamente se ha concretado incluir a las Tecnologías de las Comunicaciones cuyo propósito es publicar y anunciar la información y cooperar en el conocimiento, actualmente hablamos de TIC. Este acrónimo es la denominación genérica que abarca las TI, así como los recursos materiales (el equipamiento) y no materiales (software, configuraciones, etc.), personal capacitado y especializado que en ese ámbito se desenvuelven. El constate empleo de este término ha permitido en gran medida el fenómeno de convergencia entre información y comunicaciones. También Suárez et al. (2007), sostienen que la informática, es una disciplina científica que se encarga de la investigación de las metodologías sistematizadas que ejercen sobre la información y los datos. El vocablo informático viene de las palabras Información y Automático, lo que significa en un origen que se realiza la gestión a través de equipos, actualmente lo vemos presente en nuestro quehacer diario, en todos las actividades y cosas que realizamos en nuestra sociedad, desde la actividad más simple como es el uso de teléfonos móviles para el pago de un servicio o como el empleo de software especializados e integrados para diferentes organizaciones multinacionales.

Finalmente, la GTI es un grupo de conocimientos y métodos que ayudan para asegurar la eficacia de los servicios de TI, el mismo que previamente fue pactado con el cliente y/o usuario final. Eso se aplica a las dimensiones de gestión como por ejemplo la gestión de desarrollo de sistemas, gestión de administración de redes y otras más dimensiones de procesos como son las gestiones de cambio, de activos y problemas de Información (Ordenanza FAP 20-54, 2016).

Referente al enfoque conceptual de la Variable Ciberdefensa, de acuerdo a la Doctrina CCFFCC DFA-CD-03-28 (2018), la ciberdefensa son el conjunto de

actividades que se dan en la quinta dimensión para evitar, contener, identificar, contrarrestar, anular, impedir, evitar un riesgo o probable agresión cibernética, la cual se pueda dar de manera inmediata o potencial, con la finalidad de permitir el uso del arma Militar del país y lo complementa con la definición de la Ciberdefensa Militar, afirmando que es el grupo de tácticas, métodos, recursos, actividades y procedimientos para salvaguardar la integridad de la red de datos y los software de mando, control y comunicaciones (C3) del ámbito que respecta a la defensa de la nación, del mismo modo nos permite explotar y responder en los mismos sistemas que sean necesarios, para asegurar el autónomo acceso al ámbito cibernético de carácter militar y desarrollar eficazmente de las operaciones militares y por lo tanto el empleo eficiente de los recursos; también Álvarez, (2018), la define como el grupo de actividades y operaciones pasivas y activas que se dan en el ámbito de los dispositivos informáticos, la infraestructura de red, software, radioenlaces y recurso humano designado para la defensa a fin de asegurar que se cumplan los procesos, protocolos, ordenes o servicios conceptualizados desde un primer momento, de la misma forma se le niega a los entes enemigos imposibilitar el uso y empleo de los suyos.

También la Junta Interamericana de Defensa (2020). La JID define como la Competencia constituida y capacitada para lidiar en la quinta dimensión. Comprende acciones de defensa, ataques e inteligencia estando alineado con los intereses de un estado mientras que para De Vergara et al. (2017) la definen como las actividades y competencias perfeccionadas por los militares de forma transversal a los diferentes ámbitos operacionales aéreo, terrestre, naval y finalmente en la dimensión ciberespacial". En tal sentido, se requiere un estándar de gobernanza en que incluya ambos conceptos "ciberseguridad" y "ciberdefensa", el mismo que permitirá unir los esfuerzos, recursos, equipos, personal para poder llegar a cumplir el mismo objetivo de la ciberdefensa y ciberseguridad en las naciones. Se tiene presente que, la seguridad se logra con la participación de todos a pesar de que por teoría es tratada individualmente. En término militares el ciberespacio, es el quinto ambiente en donde se dan los enfrentamientos, asimismo se considera el

ciberespacio como un medio donde andan las nuevas tecnologías emergentes y muchas seguirán.

Tomando como referencia la Doctrina FAP DBFA 1 (2021), la FAP considera el ciberespacio tal cual dimensión, la misma que no es natural, la ausencia de un blanco militar físico entorpece la elaboración del plan de operaciones que se realiza contra las amenazas en el quinto dominio y exige a tener una respuesta virtual en la gran cantidad de casos, para ello se establece como dimensiones de esta variable a las siguientes: (a) Dimensión Operaciones Defensivas, (b) Dimensión Operaciones de Explotación y (c) Dimensión Operaciones de Respuesta. Así mismo, la JID (2020), elaboró una Guía de Ciberdefensa, en la cual distingue seis (06) formas de operaciones que pueden darse en el ciberespacio de la cual tomaremos solamente tres (03) para la presente investigación por el objetivo que cumplen las operaciones defensivas, explotación y ofensivas.

En relación a la primera dimensión Operaciones Defensivas, de acuerdo a la Doctrina CCFFCC DFA-CD-03-28 del Comando Conjunto de la Fuerzas Armadas (2018), explica que son acciones preventivas y correctivas, que incluyen medidas de reconocimiento dentro de la organización y sirven para identificar las Ciberamenazas y realizar acciones inmediatas y transversales para asegurar los activos informáticos. Según la Doctrina FAP DBFA 1 (2021), son las operaciones defensivas de nuestro ciberespacio, las que cumplen con el objetivo de ofrecer defensa ante actividades o propósitos opuestos, para garantizar su disponibilidad, confidencialidad e integridad de la información, a través del empleo de actividades preparatorias, proactivas, reactivas y de recuperación. De la misma forma según la Doctrina TOI 11-113 del Ejercito del Perú (2019), son todas las acciones defensa del ciberespacio propio y no propio asignado, a fin de preservarlo de los ataques y posibles amenazas que puedan ocurrir en el ciberespacio, para poder asegurar integridad, disponibilidad y confidencialidad aplicando las medidas proactivas, reactivas y preventivas. Según De Vergara et al. (2017), una operación cibernética defensiva; es aquella operación empleada para salvaguardar la práctica de emplear

el ciberespacio. La defensa activa son acciones que arremeten cualquier operación ofensiva hostil, a fin de salvaguardar la autonomía de maniobra en el ambiente cibernético y la defensa pasiva son las acciones específicas realizadas para minimizar la eficacia de la acción cibernética. Para Scott, K. (2018), las Operaciones Defensivas, se ejecutan para defender el ciberespacio y se han ordenado a las fuerzas para que defiendan nuestros activos de las amenazas que existen en el ciberespacio.

Referente a la segunda dimensión Operaciones de Explotación, de acuerdo a la Doctrina CCFFCC DFA-CD-03-28 (2018), explica que son aquellas operaciones que reúnen un grupo de actividades encaminadas a la colección, revisión y beneficio de información de las competencias cibernéticas de nuestros adversarios. Según la Doctrina FAP DBFA 1 (2021), es una operación que consiste en buscar, detectar e identificar las intenciones del agresor, así mismo la identificación de las debilidades en el ciberespacio, para un correcto desarrollo del plan para futuras operaciones militares en ese campo. Según con la Doctrina TOI 11-113 (2019), son las acciones de búsqueda identificación de amenazas y detección, así también la determinación de las debilidades en el ciberespacio, para un apropiado planeamiento de próximas estrategias militares en ese ámbito. Para De Vergara et al. (2017), una operación de exploración tiene como objetivo producir conocimiento e inteligencia y, en especial, conseguir datos e identificar debilidades y vulnerabilidades. Asimismo, para la JID (2020), Una Operación de Explotación, son aquellas operaciones, ejecutadas en el campo del enemigo en su red o de terceros, para conseguir los datos requeridos para el planeamiento y dirección de las próximas estrategias militares autorizadas.

En cuanto a la tercera dimensión Operaciones de Respuesta, de acuerdo a la Doctrina CCFFCC DFA-CD-03-28 (2018), explica que son aquellas Operaciones que brindan una réplica oportuna, legítima y proporcionada a las amenazas o agresiones en el quinto dominio que alcancen afectarnos en el ámbito de cibernético nacional. Según la Doctrina FAP DBFA 1 (2021), las Operaciones de Respuesta

son aquellas operaciones que consisten en emplear ciberarmas, con el objetivo de denegar, degradar o interrumpir el quinto dominio de los adversarios. Según con la Doctrina TOI 11-113 (2019), el EPE considera a las Operaciones de Respuesta a aquellas que son operaciones que tienen por efectos denegar, degradar o interrumpir del quinto dominio del enemigo. Para De Vergara et al. (2017), Las operaciones cibernéticas ofensivas, vienen a ser todas actividades que proyectan el poder para lograr objetivos militares en o a través del espacio cibernético, es decir la actividad ofensiva puede utilizarse para causar efectos temporales o permanentes y, así, reducir la moral de un adversario en redes o competencias. Asimismo, para la Junta Interamericana de Defensa (2020), las Operaciones de Respuesta, son aquellas operaciones, ejecutadas en las redes de adversarios o de terceros, con la finalidad de prevenir, anticipar o reaccionar ante ciberataques a las redes propias.

Con respecto a la Variable GTI, Según Calatayud et al., (2019), la GTI definen como una agrupación de elementos que facilitan la transformación de datos en información útil y se gestionan para cumplir determinados objetivos de una organización, asimismo las TI se aplican a diversos procesos. Asimismo, Kamble et al., (2020). Considera el alcance del uso de los recursos de TI y sus efectos que causan en las organizaciones. En este sentido, se ha encontrado evidencia sustancial de que cuando las TI se emplean de manera aislada (uso de las TI), no constituye, por sí mismo, una ventaja. (Yu et al., 2017). Sin embargo, cuando las utilizamos con otros elementos y capacidades de la organización, como por ejemplo el personal se desarrollan nuevas competencias que pueden generar una gran ventaja sostenible (Dubey et al., 2019). Finalmente, Ghobakhloo et al. (2018). Sostiene que existen estudios donde al vincular directamente los recursos de TI con la "competencia habilitada por TI", mejora del rendimiento de la organización como el mediador entre los recursos de TI controlados por una empresa y el desempeño comercial.

Por lo expuesto anteriormente, las dimensiones de la variable GTI consideradas para la presente investigación y tomando como referencia la Ordenanza FAP 20-54 (2016) la cual establece las funciones y responsabilidades del SINFA, se consideran: (a) Dimensión Desarrollo de Sistemas, (b) Dimensión Gestión Base de datos y (c) Dimensión Soporte Técnico.

Siendo la primera dimensión Desarrollo de Sistemas y de acuerdo a la Ordenanza FAP 20-54 (2016), el desarrollo de sistemas involucra realizar el análisis, diseño, programación, evaluación, documentación y mantenimiento de los sistemas que se implanten en las Unidades. Según SOFTFLUENT (2022), para el desarrollo un sistema se ha diseñado todo el proceso de construcción de todo tipo de aplicaciones informáticas confiables y de alto rendimiento que va desde el estudio del uso del cliente, pasando por el diseño, implementación hasta el mantenimiento de la app. Estos diversos pasos son posibles gracias a un lenguaje de programación específico o más bien gracias a varios lenguajes… ya los desarrolladores que dominan estos lenguajes. Asimismo, el INACAL (2017), sostiene que el todo de progreso de sistemas contempla las acciones para evaluar el requerimiento, … todo ello relacionado con los sistemas desarrollados. Con respecto a las Metodologías Akbar et al., (2018), se dividen ampliamente en dos categorías, a saber, metodologías de peso pesado y de peso ligero. Ambas metodologías aún no están satisfechas porque las metodologías pesadas están orientadas a procesos, son predecibles y aceptan menos los cambios, mientras que las metodologías livianas están orientadas a las personas, son adoptables y aceptan fácilmente cambios en los requisitos. Sin embargo, las dos metodologías son importantes para las instituciones que trabajan en el rubro de la industria del software. Finalmente, O’brien et al. (2006), Definen al desarrollo de sistemas como el diseñar, conceptualizar e implementar un sistema, así como la construcción de software a través de una serie de pasos los cuales son investigar, analizar, diseñar, implementar y mantener lo que en el mundo de TI se conoce como el ciclo de vida del software.

Referente a la segunda dimensión Gestión Base de datos (BD) y tomando como fuente a la Ordenanza FAP 20-54 (2016), La gestión de BD consiste en administrar el sistema manejador y la estructura de la BD; el acceso a las aplicaciones vía Web, la publicación de información en la intranet, el guardar y recuperación de la BD, el diccionario de datos; así como, la seguridad, control de accesos, auditoria y otras que se requieran. Según IBM (2022b), La administración de una BD, demanda actualmente de un sistema computarizado de mantenimiento de datos, el cual permite ofrecer facilidades al cliente del sistema para cumplir diferentes actividades en los sistemas, ya sea para la acceder a consultar y/o modificar los datos en la BD o gestionar la estructura de la BD en sí. Para ORACLE (2022), Una BD generalmente requiere un programa de software de BD integral conocido como sistema de administración de BD (DBMS). El mismo que a través de una aplicación entre la BD y los clientes finales o programas, lo que nos facilita conocer cómo organizar, optimizar, recuperar, actualizar y administrar la información. Un DBMS contribuye con supervisar y controlar la base de dato, permitiendo un sin número de actividades administrativas, como la vigilancia del rendimiento, el arreglo, el backup de seguridad y su restauración. La Gestión de la BD consiste en vigilar constantemente la BD en busca de eventualidades o situaciones anómalas que se puedan suscitar a fin de considerar en nuestro plan de mantenimiento preventivo, así como aplicar actualizaciones y parches de seguridad, con el tiempo las BD se vuelven más complicadas y la cantidad de datos siguen creciendo. Según Navathe (2011), Gestionar una BD implica detallar los tipos de datos, la arquitectura y loque no debe almacenarse en la BD, también almacena la definición de la BD conocido como la información descriptiva. en forma de catálogo de BD o diccionario; se llama metadatos. También para Deza (2011). Gestión de BD, se define como el grupo de data que pertenecen al mismo ámbito, almacenados de forma ordenada para una próxima consulta.

Finalmente tenemos la tercera dimensión Soporte Técnico de acuerdo a la Ordenanza FAP 20-54 (2016), la dimensión soporte técnico consiste en Proporcionar el soporte técnico requerido para brindar una solución a los problemas

que se generen en el hardware (equipamiento), software (sistemas operativos, lenguajes de programación, utilitarios), conectividad y telecomunicaciones, antivirus, antispam, filtro de contenido, seguridad de internet (perimetral e interna), correo electrónico y otros servicios de nivel Unidad o Institucionales. Según BLUE BEARS IT (2022), El soporte informático es un centro de servicio compuesto por técnicos informáticos calificados, el mismo que brinda respuesta a las solicitudes de incidencias y/o al uso de herramientas informáticas como la mensajería, Internet, el acceso remoto. Asimismo, HUB SPOT (2021), sostiene que el soporte de TI toma la forma de un centro de servicio dirigido por técnicos de TI experimentados. Su objetivo es responder a las solicitudes de soporte enviadas por los clientes. El soporte de TI suele ser el punto de inicio entre una organización de TI y sus usuarios. También llamado helpdesk o service desk, el soporte de TI puede surgir de manera interna o externa de la organización. Manifestaron Montes et al. (2008), que el proporcionar el soporte técnico a los empleados de la organización, es una necesidad a considerar para el cumplimiento de los objetivos de la misma. Finalmente, según Vargas et al. (2016) la Gestión de soporte técnico a los servicios y bienes constituyen una actividad de vital importancia a nivel global.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

3.1.1. Tipo de investigación

La investigación fue de tipo aplicada, el cual según Hernández et al. (2014), sostuvieron que la investigación científica “cumple dos propósitos básicos: a) generar conocimiento y teoría (investigación básica) y b) el resolver problemas (investigación aplicada)” (p.25). De manera similar, Sánchez et al. (2018), indicaron que la investigación aplicada es aquella que “utiliza el conocimiento obtenido de la investigación básica o teórica para comprender y resolver un problema planteado” (p.79). Finalmente, la Ley N° 31250 (2021), Ley del Sistema Nacional de Ciencia, Tecnología e Innovación, estableció que “la investigación aplicada son aquellos estudios originales y planificado que tiene como propósito concebir nuevas aplicaciones a partir del conocimiento disponible e incrementar el volumen de conocimiento (incluida las humanidades, los estudios culturales y los conocimientos sociales)”.

3.1.2. Diseño de investigación

Este estudio fue de diseño no experimental al limitarnos solamente al acopio y acumulación de información de acuerdo a como se encuentra en su estado original para analizarlo posteriormente, y concuerda con lo que sostienen Hernández et al. (2014), sostuvieron que “las investigaciones de diseño no experimental, es “un estudio que se realiza sin manipulación de variables, en el que simplemente se observan los fenómenos en su entorno natural de análisis” (p.152). Este estudio es transversal ya que intenta analizar la precisión de los métodos de clasificación a lo largo del tiempo Sánchez et al. (2018).

Esquema:

VI: Ciberdefensa

VD: Gestión de Tecnologías de la Información

R: Correlación causal entre VI y VD

3.2. Variables y Operacionalización

Variable Independiente Ciberdefensa

La Ciberdefensa, fue una variable de tipo cualitativa, según Baena (2017), menciona que las variables cualitativas expresan características y numéricamente no son medibles. Asimismo, fue una variable de tipo de cualitativa nominal porque sus dimensiones no especifican criterios de ordenación.

Definición Conceptual de la variable Independiente Ciberdefensa

El término ciberdefensa, son el grupo de actividades que emplea un País para poder tener un control de todas aquellas amenazas que tienen por finalidad un mal uso de la cibernética y ponen en riesgo o peligro su ciberespacio, permitiendo posteriormente que se pueda tener acceso con normalidad y a través de un correcto uso, respetando los garantías constitucionales de todas las personas, así mismo contribuye con algunas funciones del estado; sin evitar que en los nuevos escenarios que plantea el ciberespacio, pueden incidir en el momento de diseñar rutas estratégicas recomendable para el acatamiento de las diferentes estrategias en el campo militar de ciberdefensa (Vargas et al., 2017).

Definición Operacional de la variable Ciberdefensa

Con respecto a la variable Ciberdefensa, se operacionalizó mediante tres dimensiones, las cuales son: Operaciones defensivas, Operaciones de Explotación y Operaciones de Respuesta, medidas por un cuestionario en escala Likert de 5 categorías: (1) Totalmente en desacuerdo, (2) En desacuerdo, (3) Ni de acuerdo ni en desacuerdo, (4) De acuerdo, (5) Totalmente de acuerdo (Ver anexo 1).

Variable Dependiente Gestión de las Tecnologías de Información

La Gestión de las Tecnologías de Información, fue una variable de tipo cualitativa, según Baena (2017), menciona que las variables cualitativas expresan características y numéricamente no son medibles. Asimismo, fue una variable tipo de cualitativa nominal, porque sus dimensiones no especifican criterios de ordenación.

Definición Conceptual de la variable Gestión de las Tecnologías de Información

De acuerdo a la Ordenanza FAP 20-54 (2016), la GTI consistió en proporcionar Sistemas de Información, administrando las arquitecturas de sistemas, redes y tecnologías; así como, efectuar el desarrollo, implementación, mantenimiento de software, en apoyo a los planes operativos y de administración de la FAP, para contribuir al logro de su misión.

Definición Operacional de la variable Gestión de las Tecnologías de Información

Con respecto a la variable dependiente GTI, se operacionalizó mediante 3 dimensiones, las cuales son: Dimensión Desarrollo de Sistemas, Dimensión Gestión BD y Dimensión Soporte Técnico, medidas por un cuestionario en escala de Likert, de 5 categorías: Totalmente en desacuerdo, En desacuerdo, Ni de acuerdo ni en desacuerdo, De acuerdo, Totalmente de acuerdo. (Ver anexo 2).

3.3. Población, muestra y muestreo

3.3.1. Población

Según Gómez et al. (2016) “la población, son casos agrupados, limitado, accesible y definido, que constituyen como referencia para la selección de la muestra y cumplen con un conjunto de criterios predeterminados” mientras que, para Hernández et al., (2014) lo define como los elementos agrupados que interesan a

la presente investigación por lo que generalmente tienen características en comunes.

Para este estudio se consideró como la población a los empleados militares y civiles que integra el Sistema de Informática de la FAP, de acuerdo al reporte del sistema de informática de la FAP.

Tabla1

Detalle de la población

Población	Cantidad
Personal Militar	123
Personal Civil	57
Total	180

3.3.2. Muestra

Según Sánchez et al. (2002), una muestra es el grupo de elementos que se van a trabajar, de la cual se van a tomar datos teniendo en cuenta que esta debe ser representativa de la población por lo tanto la muestra será tomada del Sistema del Servicio de Informática. El error de muestreo es del 5% y el rango percentil calculado es del 50%, un grado de confianza de 95% y la población de 180 personas obteniendo como resultado 123 personas.

Tabla 2

Caracterización de la muestra

Población	Cantidad
Personal Militar	84
Personal Civil	39
Total	123

3.3.3. Muestreo

Al respecto, se consideró una muestra probabilística aleatoria simple, la misma que según Hernández et al. (2018) explicaron que dicho muestreo se distingue en que los elementos agrupados que componen la población, poseen igual probabilidad de ser escogidas para establecer la muestra.

3.3.4. Unidad de Análisis

Por consiguiente, esta investigación tomó como unidad de análisis al personal militar y civil que Gestiona las TI en la FAP, considerando la que indicó Ding et al., (2018) Cualquier cambio en la escala o unidad de análisis afectará directamente la incertidumbre de los resultados, y en estudios reales, se debe elegir la unidad de análisis robustas para conseguir resultados razonables.

3.4. Técnicas e instrumentos de recolección de datos

Técnicas de recolección de datos

La presente investigación utilizó la encuesta como la técnica para la obtención de datos. Según Hernández et al (2018) mencionaron que la encuesta se emplea para recoger datos mediante el planteamiento de preguntas respecto a una o más variables, las cuales se someterán a medición.

Instrumentos de recolección de datos

Esta investigación utilizó el cuestionario como el instrumento de obtención de datos. Según Hernández et al. (2018) manifiestan que el cuestionario es el instrumento que está compuesto por una cantidad limitada de preguntas. (Ver anexo 3)

Tabla 3

Ficha técnica del instrumento de medición

Nombre del Instrumento			Cuestionario para el personal militar y civil que Gestiona las TI de la FAP		
Investigador			Pablo Roberto Huertas Espiritu		
Año			2022		
Instrumento			Cuestionario		
Objetivo			Determinar el nivel de incidencia de la Ciberdefensa en la GTI de la FAP en el año 2022		
Población			180 personal militar y civil que Gestiona las TI en la FAP		
Número de Ítems			38 en total, divididos en VI-20 Ítems y VD-18 Ítems		
Aplicación			Virtual		
Tiempo de administración			15 minutos		
Escala			Escala de Likert (1) Totalmente en desacuerdo, (2) En desacuerdo, (3) Ni de acuerdo ni en desacuerdo, (4) De acuerdo, (5) Totalmente de acuerdo		
Variable: Ciberdefensa			Variable: GTI		
Nivel	Valor	Rango	Nivel	Valor	Rango
No óptimo	1	20-46	Bajo	1	18-90
Medio	2	47-73	Medio	2	43-67
Óptimo	3	73-100	Alto	3	68-90

Validez

Para darle la validez de los instrumentos de obtención de datos se empleó el juicio de expertos, de modo que se recurrió a tres profesionales del grado de magister para que emitan su juicio de aplicabilidad como consta en el certificado de validez (Ver anexo 4) Según Hernández et al. (2014) la validez se concibe como el "nivel en que una herramienta incorpora un dominio de contenido específico a medir".

Tabla 4

Validez por juicio de expertos

DNI	Experto	Procedencia	Especialista	Calificación
40425332	Iván Vargas Guevara	Universidad Cesar Vallejo	Temático y Metodólogo	Aplicable
40150542	Fredy Rojas Maguiña	Escuela Superior de Guerra Aérea de la FAP	Metodólogo	Aplicable
40060141	Iván Chávez Marcos	Superior de Guerra Aérea de la FAP	Metodólogo	Aplicable

Nota: Elaboración propia

Como se puede observar se obtuvo un calificativo de APLICABLE para las dos variables lo cual nos garantiza un correcto empleo.

Confiabilidad

Según Sánchez et al. (2020), la confianza es la solidez de las valoraciones obtenidas en diferentes momentos por la misma persona o en dentro del mismo conjunto de ítems. De la misma forma, Tuapanta, et al. (2017) mencionaron que utilizando la herramienta se obtiene el valor del Alfa de Cronbach y luego se obtendrá el valor entre 0 y 1, pudiendo aceptar como valor mínimo el de 0,7, si el resultado es por debajo de este valor, la confiabilidad es baja. Para determinar la confiabilidad se les realizó una prueba piloto de la herramienta de recolección de datos con 20 personas al azar y una muestra de 123 personas conocedoras de Ciberdefensa y GTI.

Tabla 5

Confiabilidad del instrumento

Variable	N° encuestas	N° elementos	Alfa de Cronbach
Piloto	20	38	0.931
Muestra	123	38	0.966

3.5. Procedimientos

Respecto la captura de la información se realizará la encuesta mediante la plataforma de Google a través de formulario, allí se colocarán las preguntas del cuestionario, posteriormente, se enviará por correo electrónico a cada uno de las muestras seleccionadas, una vez que hayan sido resueltas las preguntas de las encuestas se procederán a recolectar los datos para luego ser exportados a un Excel se deberán dividir en dimensiones y variables determinando los valores para luego insertarlo a un SPSS V25.

3.6. Método de análisis de datos

En esta investigación se utilizó el análisis descriptivo e inferencial para cada indicador mediante el software IBM SPSS V25.

En la elaboración del análisis descriptivo se utilizó tablas de contingencia y apoyándose para la interpretación de los datos a través de tablas e histogramas.

En la realización del análisis inferencial se aplicará la regresión logística ordinal, para demostrar el grado de correlación causal existente de la variable ciberdefensa sobre la variable GTI.

3.7. Aspectos éticos

En suma, la ética expuesta en la investigación se ajustó a los principios éticos, considerando los siguientes principios establecidos por los códigos de ética de la Universidad Cesar Vallejo dispuestos en la Resolución de Consejo Universitario N°034-2021-UCV:

Principio de autenticidad: La información que se ha mostrado es legítima, tenga en cuenta la privacidad de esta investigación.

Principio de originalidad: Se citó en las fuentes bibliográficas de la información presentada para indicar el repudio a la copia.

Principio de confidencialidad: La información que se recabó en calidad de la institución y en calidad de las personas implicadas como informantes de la investigación.

IV. RESULTADOS

Análisis descriptivos

Análisis descriptivo de la variable ciberdefensa y la variable GTI

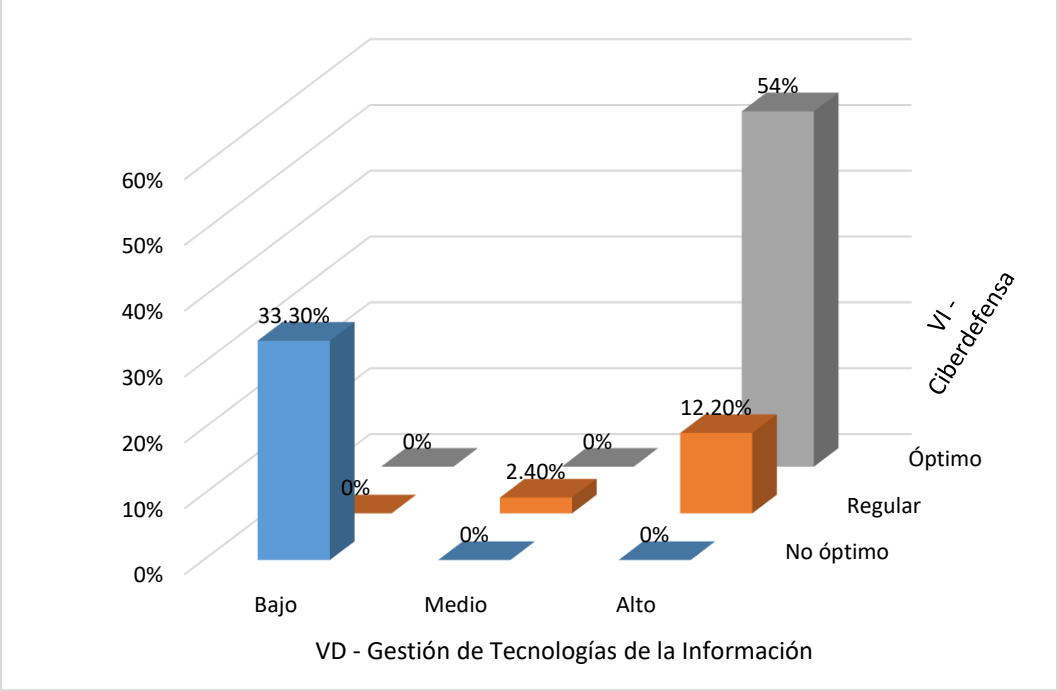
Tabla 6

*Tabla cruzada VI – ciberdefensa * VD – GTI*

		VD -GTI			Total
		Bajo	Medio	Alto	
VI - Ciberdefensa	No óptimo	41 (33,3%)	0 (0%)	0 (0%)	41 (33,3%)
	Regular	0 (0%)	3 (2,4%)	15 (12,2%)	18 14,6%)
	Óptimo	0 (0%)	0 (0%)	64 (54%)	64 (52,0%)
	Total	41 (33,3%)	3 (2,4%)	79 (64,2%)	123 (100%)

Figura 1

Histograma VI – ciberdefensa VD – GTI*



Respecto a la tabla 6 y a la figura 1, se puede discriminar que la gran aglomeración ocurre en la intersección del límite “óptimo” de la variable Ciberdefensa y el nivel “alto” de la variable GTI, siendo las 64 respuestas lo que representa un 54%; por otra parte, la frecuencia menor se encuentra ubicada en la unión del límite “No óptimo”, “Regular” y ”Óptimo” de la variable Ciberdefensa con el eje “Alta”, “Medio” y “Bajo” respectivamente de la variable GTI, registrando “0” observaciones las cuales representan el 0,0% definitivamente se describe que el nivel “Alto” de la variable GTI es aquel que demuestra la mayor proporción con 79 repeticiones que corresponde al 57,9%.

Análisis descriptivo de la dimensión operaciones defensivas de la variable ciberdefensa y la variable GTI

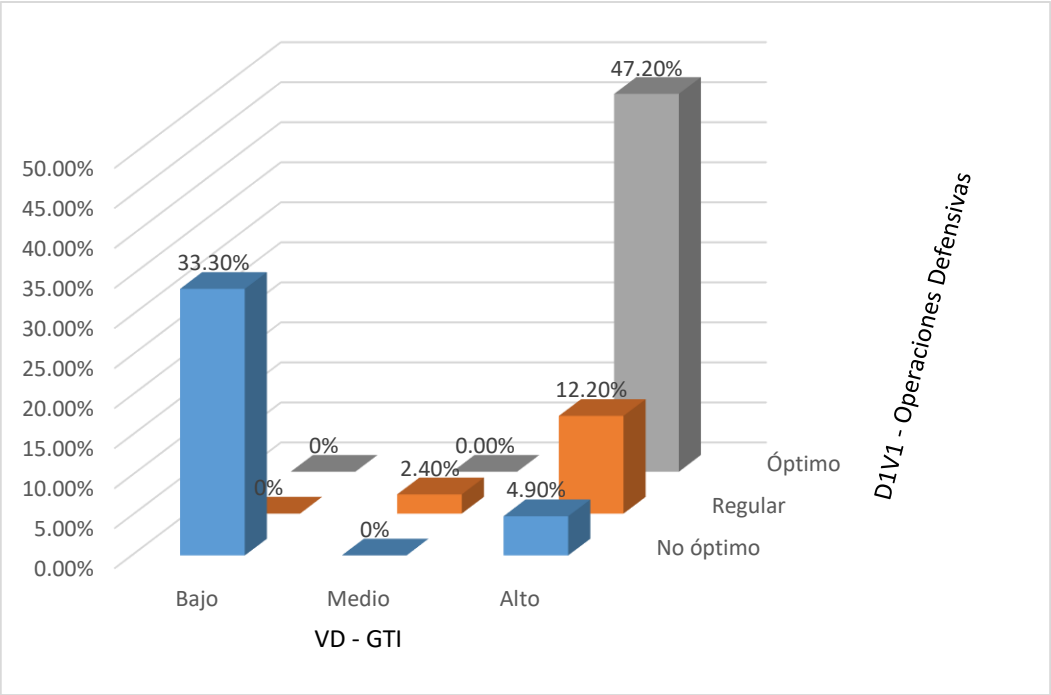
Tabla 7

*Tabla cruzada D1VI – operaciones defensivas * VD – GTI*

		VD -GTI			Total
		Bajo	Medio	Alto	
D1VI – Operaciones Defensivas	No óptimo	41 (33,3%)	0 (0%)	6 (4,9%)	47 (38,2%)
	Regular	0 (0,0%)	3 (2,4%)	15 (12,2%)	18 (14,6%)
	Óptimo	0 (0,0%)	0 (0,0%)	58 (47,2%)	58 (47,2%)
	Total	41 (33,3%)	3 (2,4%)	79 (64,2%)	123 (100%)

Figura 2

*Histograma D1VI – operaciones defensivas * VD – GTI*



Respecto a la tabla 7 y a la figura 2, se discrimina que la gran aglomeración se da en la intersección del límite “óptimo” de la dimensión Operaciones Defensivas de la variable Ciberdefensa y el nivel “alto de la variable GTI, siendo las 58 respuestas lo que representa un 47,2%; por otra parte, la frecuencia más baja se encuentra ubicada en la unión del límite “No óptimo”, “Regular” y ”Óptimo” de la dimensión Operaciones Defensivas de la variable Ciberdefensa con el eje “Alta” y “Medio” respectivamente de la variable GTI, contabilizando “0” observaciones las cuales representan el 0,0% definitivamente se describe que el rango “Alto” de la variable GTI es aquel que demuestra la gran proporción con 79 repeticiones equivalente a 64,2%.

Análisis descriptivo de la dimensión operaciones de explotación de la variable ciberdefensa y la variable GTI

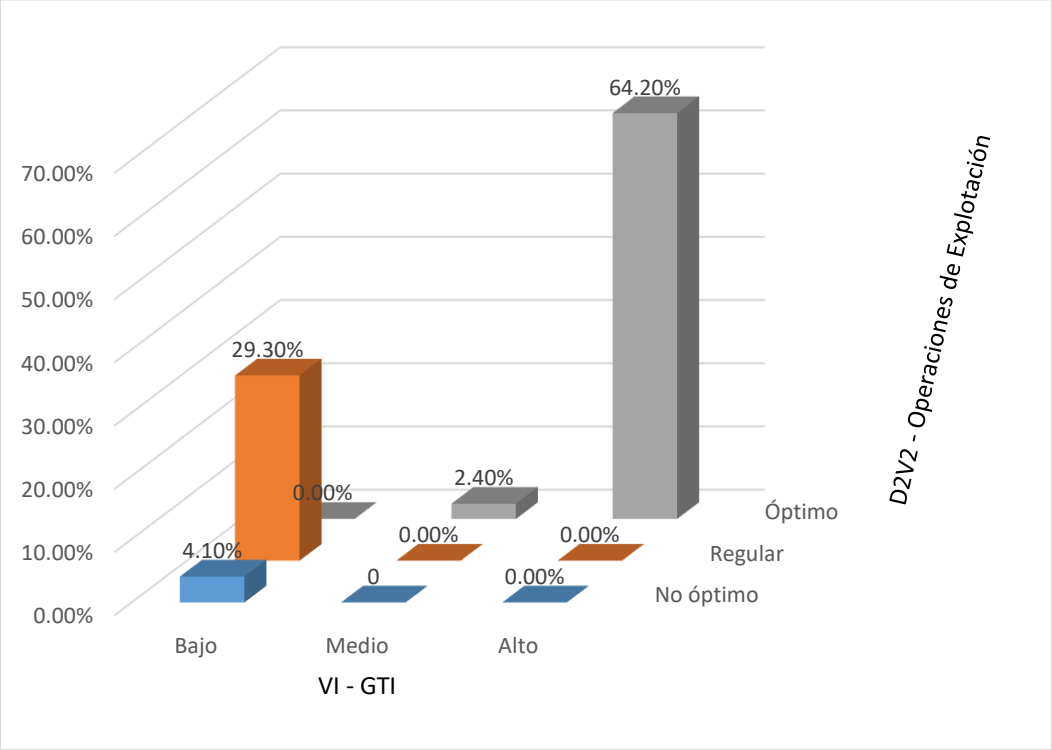
Tabla 8

Tabla cruzada D2VI – operaciones de explotación * *VD – GTI*

		VD -GTI			Total
		Bajo	Medio	Alto	
D2VI – Operaciones Defensivas	No óptimo	5 (4,1%)	0 (0,0%)	0 (0,0%)	5 (4,1%)
	Regular	36 (29,3%)	0 (0,0%)	0 (0,0%)	36 (29,3%)
	Óptimo	0 (0,0%)	3(2,4%)	79 (64,2%)	82 (66,7%)
	Total	41 (33,3%)	3 (2,4%)	79 (64,2%)	123 (100%)

Figura 3

*Histograma D2VI – operaciones de explotación * VD – GTI*



Respecto a la tabla 8 y a la figura 3, se discrimina que la gran aglomeración se da en la intersección del límite “óptimo” de la dimensión Operaciones de Explotación de la variable Ciberdefensa y el nivel “alto de la variable GTI, siendo las 79 respuestas lo que representa un 64,2%; por otra parte, la frecuencia más baja se encuentra ubicada en la unión del límite “No óptimo”, “Regular” y ”Óptimo” de la dimensión Operaciones de Explotación de la variable Ciberdefensa con el eje ”Bajo”, “Alta” y “Medio” respectivamente de la variable GTI, contabilizando “0” observaciones las cuales representan el 0,0% definitivamente se describe que el rango “Alto” de la variable GTI es aquel que demuestra la gran proporción con 79 repeticiones equivalente a 64,2%.

Análisis descriptivo de la dimensión operaciones de respuesta de la variable ciberdefensa y la variable GTI

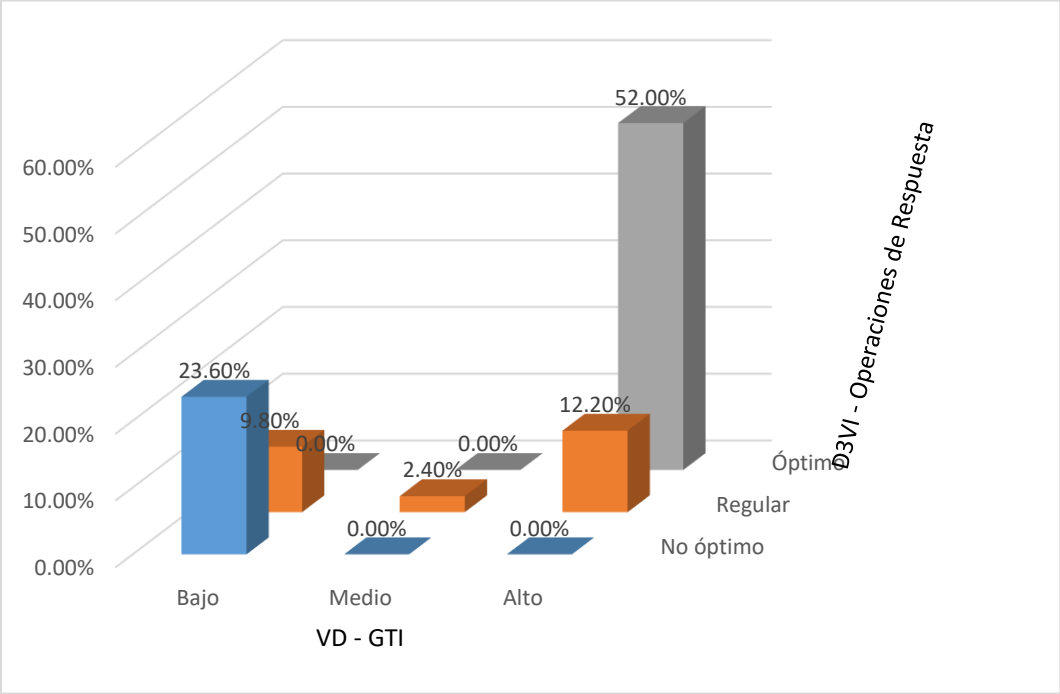
Tabla 9

Tabla cruzada D3VI – operaciones de respuesta * *VD – GTI*

		VD -GTI			Total
		Bajo	Medio	Alto	
D3VI – Operaciones Defensivas	No óptimo	29 (23,6%)	0 (0,0%)	0 (0,0%)	29 (23,6%)
	Regular	12(9,8%)	3 (2,4%)	15 (12,2%)	30 (24,4%)
	Óptimo	0 (0,0%)	0 (0,0%)	64 (52,0)	64 (52,0%)
	Total	41 (33,3%)	3 (2,4%)	79 (64,2%)	123 (100%)

Figura 4

*Histograma D3VI – operaciones de respuesta * VD – GTI*



Respecto a la tabla 9 y a la figura 4, se discrimina que la gran aglomeración se da en la intersección del límite “óptimo” de la dimensión Operaciones de Respuesta de la variable Ciberdefensa y el nivel “alto de la variable GTI, siendo las 64 respuestas lo que representa un 52%; por otra parte, la frecuencia más baja se encuentra ubicada en la unión del límite “No óptimo” y ”Óptimo” de la dimensión Operaciones de Respuesta de la variable Ciberdefensa con el eje ”Bajo”, “Alta” y “Medio” respectivamente de la variable GTI, contabilizando “0” observaciones las cuales representan el 0,0% definitivamente se refiere que el rango “Alto” de la variable GTI es aquel que demuestra la gran proporción con 79 repeticiones equivalente a 64,2%.

Análisis Inferencial

Se empleó la regresión logística ordinal que según Heredia (2014), es el modelo estadístico que relaciona linealmente 2 variables en busca que se evalúe el efecto de la variable independiente sobre la variable dependiente y se utiliza para variable

dependiente de tipo cualitativa. También, las funciones de uso común son Logit y Cloglog; la función Logit se utilizó para el estudio actual porque las variables son ordenadas y normalmente distribuidas. De esta manera se fijó la incidencia de las variables con las dimensiones, consiguientemente se tomó la consideración indicada por Liang et al. (2020) Menciona que al usar un estimador de máxima verosimilitud como el logit multinomial, el exponente proporciona un ajuste entre variables que incluye 4 tipos de consideraciones de escala, tales como: si 0 de 0.25 es igual a faltante o nulo; de 0,26 a 0,50: denota débil; 0,51 a 0,75: equivalente a resistencia media; y valores entre 0.76 y 1.00: equivalente a fuerte y perfecto usando regresión logística ordinaria..

Prueba de Hipótesis

Formulación de la hipótesis estadística:

H_0: La Ciberdefensa no incide significativamente en la GTI de la FAP, Lima 2022
H_1: La Ciberdefensa incide significativamente en la GTI de la FAP, Lima 2022
Contrastación de Hipótesis estadística:

Tabla 10

Información de ajuste de los modelos para la variable GTI

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	168,911			
Final	0,000	168,911	2	,000

En la tabla 10 se demuestra la significación estadística donde el valor es (p=0,000), siendo inferior a 0.05, es significativo para confirmar si la variable ciberdefensa tiene efecto sobre la variable GTI, de la misma forma se puede ratificar que se encuentra dentro del análisis de regresión ordinal y por lo tanto la hipótesis nula es rechazada.

Tabla 11

Bondad de ajuste del impacto de la variable ciberdefensa en la variable GTI

	Chi-cuadrado	gl	Sig.
Pearson	,000	2	1,000
Desvianza	,000	2	1,000

En la tabla 11 podemos advertir como valor de Chi-cuadrado a 1.000 y como es superior a 0.05 significa que la muestra es consistente con la población.

Tabla 12

Prueba Pseudo R cuadrado para la variable GTI

Pseudo R	**Valor**
Cox y Snell	0,747
Nagelkerke	0,966
McFadden	0,926

En la tabla 12 apreciamos que en los tres coeficientes de R cuadrado tienen valores altos Nagelkerke ya que representa un valor preciso de 0,966 en porcentaje 96.6% esto significa que repercuten la variable ciberdefensa en la variable GTI, al mismo tiempo se observa que R cuadrado de Nagelkerke obtiene una posición entre 0,76 y 1,00. Por razón se aparta la hipótesis nula (H0) y se admite alternativa (H1).

Tabla 13

Prueba paramétrica de la estimación de la incidencia de la variable ciberdefensa en la variable GTI

		Estimación	Desv Error	Wald	gl	Sig.	Intervalo de confianza al 95%	
							Límite inferior	Límite superior
Umbral	[V2R=1]	-38,714	6107,802	,000	1	,995	-12009,785	11932,358
	[V2R=2]	-21,261	5172,706	,000	1	,997	-10159,579	10117,057
Ubicación	[V1R=1]	-60,018	8994,682	,000	1	,995	-17689,271	17569,235
	[V1R=2]	-19,652	5172,706	,000	1	,997	-10157,970	10118,666
	[V1R=3]	0[a]			0			

Sobre la Tabla 13 se desprende que el cálculo (coeficiente de regresión) evaluado de la variable independiente ciberdefensa -19,652, se aprecia que la variable independiente ciberdefensa obtiene p=0,000con con relación considerado el conjunto (wald) superior a 0,000, por lo que la efectividad de la variable ciberdefensa en la variable GTI.

Por consiguiente, la regresión logística ordinal de valor p=0,000el cual es inferior a la estimación del error 0,05 el cual refleja la existencia estadística suficiente para descartar la hipótesis nula (H0) y del mismo modo aseverar que la variable independiente ciberdefensa incide en la variable dependiente GTI.

Prueba de Hipótesis específica 1:

Formulación de la hipótesis estadística:

H_0: La dimensión operaciones defensivas no incide significativamente en la GTI de la FAP, Lima 2022

H_1: La dimensión operaciones defensivas incide significativamente en la GTI de la FAP, Lima 2022

Contrastación de Hipótesis estadística:

Tabla 14

Información de ajuste de los modelos para la variable GTI

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	136,533			
Final	17,919	118,614	2	,000

En la tabla 14 se demuestra la significación estadística cuyo valor es (p=0,000), siendo inferior a 0.05, es significativo para confirmar, si la dimensión operaciones defensivas de la variable ciberdefensa tiene efecto sobre la variable GTI, de la misma manera se puede confirmar que se encuentra dentro del análisis de regresión ordinal y por lo tanto la hipótesis nula es rechazada.

Tabla 15

Bondad de ajuste del impacto de la dimensión operaciones defensivas *de la variable ciberdefensa en la variable GTI*

	Chi-cuadrado	gl	Sig.
Pearson	9,699	2	,008
Desvianza	11,586	2	,003

En la tabla 15 podemos advertir como valor de Chi-cuadrado a 0.008 y como es superior a 0.05 significa que la muestra es consistente con la población.

Tabla 16

Prueba Pseudo R cuadrado para la variable GTI

Pseudo R	**Valor**
Cox y Snell	0,619
Nagelkerke	0,801
McFadden	0,651

En la tabla 16 observamos que en los tres coeficientes de R cuadrado tuvieron valores altos Nagelkerke ya que representa un valor preciso de 0,801 en porcentaje 80.1% esto significa que repercuten la dimensión operaciones defensivas de la variable ciberdefensa en la variable GTI, al mismo tiempo se observa que R cuadrado de Nagelkerke obtiene una posición entre 0,76 y 1,00. Por razón se aparta la hipótesis nula (H0) y se admite alternativa (H1).

Tabla 17

Prueba paramétrica de la estimación de la incidencia de la dimensión operaciones defensivas *de la variable ciberdefensa en la variable GTI*

		Estimación	Desv Error	Wald	gl	Sig.	Intervalo de confianza al 95%	
							Límite inferior	Límite superior
Umbral	[V2R=1]	-22,741	,698	1060,177	1	,000	-24,109	-21,372
	[V2R=2]	-22,283	,659	1143,772	1	,000	-23,574	-20,991
Ubicación	[D1V1R=1]	-24,612	,813	917,368	1	,000	-26,205	-23,0195
	[D1V1R=2]	-20,548	,000		1		-20,548	-20,548
	[D1V1R=3]	0[a]			0			

Sobre la Tabla 17 se desprende que el cálculo (coeficiente de regresión) evaluado de la dimensión operaciones defensivas de la variable independiente ciberdefensa -24,612, se aprecia que la variable independiente ciberdefensa obtiene p=0,000con con relación considerado el conjunto (wald) superior a 917,000, por lo que la efectividad de la variable ciberdefensa en la variable GTI.

En definitiva, la regresión logística ordinal de valor p=0,000 el cual es inferior a la estimación del error 0,05 el cual refleja la existencia estadística suficiente para descartar la hipótesis nula (H0) y del mismo modo aseverar que la dimensión operaciones defensivas de la variable independiente ciberdefensa incide en la variable dependiente GTI.

Prueba de Hipótesis específica 2:

Formulación de la hipótesis estadística:

H_0: La dimensión operaciones de explotación no incide significativamente en la GTI de la FAP, Lima 2022

H_1: La dimensión operaciones de explotación incide significativamente en la GTI de la FAP, Lima 2022

Contrastación de Hipótesis estadística:

Tabla 18

Información de ajuste de los modelos para la variable GTI

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	159,537			
Final	,000	159.537	2	,000

En la tabla 18 se demuestra la significación estadística donde el valor es (p=0,000), siendo inferior a 0.05, es significativo para confirmar si la dimensión operaciones explotación de la variable ciberdefensa tiene efecto sobre la variable GTI, de la

misma manera se puede confirmar que se encuentra dentro del análisis de regresión ordinal y por lo tanto la hipótesis nula es rechazada.

Tabla 19

Bondad de ajuste del impacto de la dimensión operaciones de explotación de la variable ciberdefensa en la variable GTI

	Chi-cuadrado	gl	Sig.
Pearson	,000	2	1,000
Desvianza	,000	2	1,000

En la tabla 19 podemos advertir como valor de Chi-cuadrado a 0.008 y como es superior a 0.05 significa que la muestra es consistente con la población.

Tabla 20

Prueba Pseudo R cuadrado para la variable GTI

Pseudo R	**Valor**
Cox y Snell	0,727
Nagelkerke	0,940
McFadden	0,875

En la tabla 16 observamos que en los tres coeficientes de R cuadrado tuvieron valores altos Nagelkerke ya que representa un valor preciso de 0,801 en porcentaje 80.1% esto significa que repercuten la dimensión operaciones explotación de la variable ciberdefensa en la variable GTI, al mismo tiempo se observa que R cuadrado de Nagelkerke obtiene una posición entre 0,76 y 1,00. Por razón se aparta la hipótesis nula (H0) y se admite alternativa (H1).

Tabla 21

Prueba paramétrica de la estimación de la incidencia de la dimensión operaciones de explotación de la variable ciberdefensa en la variable GTI

		Estimación	Desv Error	Wald	gl	Sig.	Intervalo de confianza al 95%	
							Límite inferior	Límite superior
Umbral	[V2R=1]	-19,824	2187,146	,000	1	,993	-4306,553	4266,904
	[V2R=2]	-3,271	,588	30,921	1	,000	-4,424	-2,118
Ubicación	[D2V1R=1]	-40,128	,000		1		-40,128	-40,128
	[D2V1R=2]	-40,128	4800,188	,000	1	,993	-9448,324	9368,068
	[D2V1R=3]	0[a]			0			

Sobre la Tabla 21 se desprende que el cálculo (coeficiente de regresión) evaluado de la dimensión operaciones de explotación de la variable independiente ciberdefensa -40,128, se aprecia que la dimensión operaciones de explotación de la variable independiente ciberdefensa obtiene p= ,993 con relación considerado el conjunto (wald) superior a ,000, por lo que la efectividad de la dimensión operaciones de explotación de la variable ciberdefensa en la variable GTI.

En definitiva, la regresión logística ordinal de valor p=0,000 el cual es inferior a la estimación del error 0,05 el cual refleja la existencia estadística suficiente para descartar la hipótesis nula (H0) y del mismo modo aseverar que la dimensión operaciones de explotación de la variable independiente ciberdefensa incide en la variable dependiente GTI.

Prueba de Hipótesis específica 3:

Formulación de la hipótesis estadística:

H_0: La dimensión operaciones de respuesta no incide significativamente en la GTI de la FAP, Lima 2022

H_1: La dimensión operaciones de respuesta incide significativamente en la GTI de la FAP, Lima 2022

Contrastación de Hipótesis estadística:

Tabla 22

Información de ajuste de los modelos para la variable GTI

Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	132,360			
Final	6,641	125,719	2	,000

En la tabla 22 se demuestra la significación estadística donde el valor es (p=0,000), siendo inferior a 0.05, es significativo para confirmar si la dimensión operaciones respuesta de la variable ciberdefensa tiene efecto sobre la variable GTI, de la misma manera se puede confirmar que se encuentra dentro del análisis de regresión ordinal y por lo tanto la hipótesis nula es rechazada.

Tabla 23

Bondad de ajuste del impacto de la dimensión operaciones de respuesta de la variable ciberdefensa en la variable GTI

	Chi-cuadrado	gl	Sig.
Pearson	0,000	2	1,000
Desvianza	0,000	2	1,000

En la tabla 23 podemos advertir como valor de Chi-cuadrado a 1.000 y como es superior a 0.05 significa que la muestra es consistente con la población.

Tabla 24

Prueba Pseudo R cuadrado para la variable GTI

Pseudo R	**Valor**
Cox y Snell	0,640
Nagelkerke	0,828
McFadden	0,690

En la tabla 24 observamos que en los tres coeficientes de R cuadrado tuvieron valores altos Nagelkerke ya que representa un valor preciso de 0,828 en porcentaje

82.8% esto significa que repercuten la dimensión operaciones de respuesta de la variable ciberdefensa en la variable GTI, al mismo tiempo se observa que R cuadrado de Nagelkerke obtiene una posición entre 0,76 y 1,00. Por razón se aparta la hipótesis nula (H0) y se admite alternativa (H1).

Tabla 25

Prueba paramétrica de la estimación de la incidencia de la dimensión operaciones de respuesta de la variable ciberdefensa en la variable GTI

		Estimación	Desv Error	Wald	gl	Sig.	Intervalo de confianza al 95%	
							Límite inferior	Límite superior
Umbral	[V2R=1]	-21,691	,373	3387,639	1	,000	-22,422	-20,961
	[V2R=2]	-21,286	,365	3398,098	1	,000	-22,001	-20,570
Ubicación	[V1R=1]	-43,019	7943,720	,000	1	,996	-15612,424	15526,387
	[V1R=2]	-21,286	,000		1		-21,286	-21,286
	[V1R=3]	0[a]			0			

Sobre la Tabla 25 se desprende que el cálculo (coeficiente de regresión) evaluado de la dimensión operaciones de respuesta de la variable independiente ciberdefensa -43,019, se aprecia que la dimensión operaciones de respuesta de la variable independiente ciberdefensa obtiene p=0,000con con relación considerado el conjunto (wald) superior a 0,000, por lo que la efectividad de la dimensión operaciones de respuesta de la variable ciberdefensa en la variable GTI.

En definitiva, la regresión logística ordinal de valor p=0,000 el cual es inferior a la estimación del error 0,05 el cual refleja la existencia estadística suficiente para descartar la hipótesis nula (H0) y del mismo modo aseverar que la dimensión operaciones de respuesta de la variable independiente ciberdefensa incide en la variable dependiente GTI.

V. DISCUSIÓN

En relación al objetivo general, empezamos a debatir lo que se ha conseguido como resultados en el presente estudio con relación a la incidencia de la Ciberdefensa en la GTI de la FAP en el año 2022.

En cuanto al análisis descriptivo, se comprobó que el grado “Óptimo” de la variable ciberdefensa se relaciona con el grado “alto” de la variable GTI simbolizando el 54%, mientras que el grado “No óptimo” de la variable ciberdefensa se afecta con el grado “Bajo” de la variable GTI, simbolizando el 33,3%, el grado “Regular” de la variable ciberdefensa se afecta con el grado “alto” de la variable GTI simbolizando el 12,2% y finalmente se describe que el grado “Regular” de la variable ciberdefensa se afecta con el grado “alto” de la variable GTI simbolizando el 2,4% rango “Medio” de la variable GTI.

Por lo que se refiere al análisis inferencial se empleó el producto de R cuadrado de Nagelkerke de 0,966, el cual alcanzó el grado fuerte y perfecto, por lo que fue posible probar la alta ocurrencia de la variable independiente ciberdefensa en la variable dependiente GTI. De igual forma, para la escala de significancia de p=0,000, siendo menor al 0.05% determinante para reafirmar el efecto significativo de repercusión de la variable independiente ciberdefensa en la variable dependiente GTI.

Los resultados señalados líneas arriba concuerdan en cierto sentido con lo descrito por Villalba (2015), que nos indica lo siguiente, los ciberterroristas pueden emplear las TIC para realizar ataques en contra de algún estado;

Por otra parte, Huamán (2021), nos describe que la seguridad de las TIC se ven amenazadas por cualquier actividad desarrollada por algún ente malintencionado que busca vulnerar la confidencialidad, integridad o disponibilidad de la información que se maneja en ellas.

Del mismo modo, Vilcarromero (2018), señala que la ciberseguridad protege los activos digitales que son empleados a través de las TIC que se encuentran en las entidades.

Así también, Zúñiga (2017), nos explica que a medida que las TIC crecen en alguna entidad sus mecanismos de defensa o entiéndase como protección deben ser implementados con la finalidad de evitar ataques de virus, aplicaciones o programas maliciosos a la red.

En relación al objetivo específico 1 del análisis descriptivo, se concluyó que la magnitud “Óptimo” de la dimensión Operaciones Defensivas de la variable Ciberdefensa está enlazado con el nivel “alto” de la variable GTI con el 47,2%, mientras que la magnitud “No óptimo” de la dimensión Operaciones Defensivas de la variable Ciberdefensa está enlazado con el nivel “Bajo” de la variable GTI con el 33,3%, asimismo la magnitud “Regular” de la dimensión Operaciones Defensivas de la variable Ciberdefensa está enlazado con el nivel “Bajo” de la variable GTI con el 12,2% finalmente la magnitud “No óptimo” de la dimensión Operaciones Defensivas de la variable Ciberdefensa está relacionado con el nivel “Alto” de la variable GTI con el 4,9%.

Para el análisis inferencial se utilizó el producto de R cuadrado de Nagelkerke de 0,801, el cual se sitúa en el grado fuerte y perfecto, es por ello se puede constatar la notable ocurrencia de la variable independiente ciberdefensa en la variable dependiente GTI. De igual forma, para la escala de significancia de p=0,000, siendo menor al 0.05% determinante para confirmar el efecto significativo de repercusión de la variable independiente ciberdefensa en la variable dependiente GTI.

Los resultados señalados líneas arriba concuerdan en cierto sentido con lo descrito por Villalba (2015) que nos indica lo siguiente, las naciones y/o estados deben elaborar planes para saber defenderse ante un futuro ciberataques en contra de ellos;

Por otra parte, Huamán (2021), nos describe a través de la teoría de la defensa que se debe tener una capacidad desarrollada para poder defender el ciberespacio, así como la protección de los SI de forma rápida en caso nos realicen un ciberataque.

Conforme a Calatayud et al., (2019), la GTI ayuda a reducir los riesgos existentes en el ciberespacio puesto que facilitan la transformación de datos en información útil con la finalidad de cumplir determinados objetivos y así asegurar la eficacia de los servicios de TI.

Así también, Zúñiga (2017), nos explica que a medida que las TIC crecen en alguna entidad sus mecanismos de defensa o entiéndase como protección deben ser implementados con la finalidad de evitar ataques de virus, aplicaciones o programas maliciosos a la red.

En relación al objetivo específico 2 del análisis descriptivo, se concluyó que la magnitud “Óptimo” de la dimensión Operaciones de Explotación de la variable Ciberdefensa está enlazado con el nivel “alto” de la variable GTI con el 64,2%, mientras que la magnitud “Regular” de la dimensión Operaciones de Explotación de la variable Ciberdefensa está enlazado con el nivel “Bajo” de la variable GTI con el 29,3%, asimismo la magnitud “No óptimo” de la dimensión Operaciones de Explotación de la variable Ciberdefensa está enlazado con el nivel “Bajo” de la variable GTI con el 12,2% finalmente la magnitud “No óptimo” de la dimensión Operaciones de Explotación de la variable Ciberdefensa está enlazado con el nivel “Alto” de la variable GTI con el 4,1%.

Para el análisis inferencial se utilizó el producto de R cuadrado de Nagelkerke de 0,940, el cual se sitúa en el grado fuerte y perfecto, es por ello se puede constatar la notable ocurrencia de la dimensión Operaciones de Explotación de la variable independiente ciberdefensa en la variable dependiente GTI. De igual forma, para la escala de significancia de p=0,000, siendo menor al 0.05% determinante para confirmar el efecto significativo de repercusión de la dimensión Operaciones de

Explotación de la variable independiente ciberdefensa en la variable dependiente GTI.

Los resultados señalados líneas arriba concuerdan en cierto sentido con lo descrito por Villalba (2015) que nos indica que los países deben promover el análisis y detección de posibles ataques a los sistemas de información de los estados cooperando entre estados a fin de contrarrestar ciberataques que vayan afectar a algún país.

Por otra parte, Huamán (2021), nos describe a través de la teoría de la ciberdefensa que se deben emplear toda la información y conocimientos para resguardar los datos empleando alianzas con otras Fuerzas Amigas.

Así también, Zúñiga (2017), nos explica que las medidas defensivas internas se realizan en nuestras redes para defender nuestras redes a través de procedimientos y herramientas.

En relación al objetivo específico 3 del análisis descriptivo, se concluyó que la magnitud “Óptimo” de la dimensión Operaciones de Respuesta de la variable Ciberdefensa está enlazado con el nivel “alto” de la variable GTI con el 52%, mientras que la magnitud “No óptimo” de la dimensión Operaciones de Respuesta de la variable Ciberdefensa está enlazado con el nivel “Bajo” de la variable GTI con el 23,6%, asimismo la magnitud “Regular” de la dimensión Operaciones de Respuesta de la variable Ciberdefensa está relacionado con el nivel “Alto” de la variable GTI con el 12,2% finalmente la magnitud “Regular” de la dimensión Operaciones de Respuesta de la variable Ciberdefensa está enlazado con el nivel “Bajo” de la variable GTI con el 9,8%.

Para el análisis inferencial, se utilizó el R cuadrado de Nagelkerke de 0,828, ubicado en el grado fuerte y perfecto, por lo que fue posible verificar la presencia significativa de la variable independiente dimensión Operaciones de Respuesta de la variable

independiente ciberdefensa en la variable dependiente GTI. Asimismo, para la escala de significancia de p=0,000, el factor determinante de menos de 0.05% confirma la influencia significativa de la variable independiente dimensión Operaciones de Respuesta de la variable independiente ciberdefensa en la variable dependiente GTI.

Los resultados señalados líneas arriba concuerdan en cierto sentido con lo descrito por Villalba (2015) que nos recuerda que las entidades de un estado deben generar capacidades para poder recuperarse ante un posible ciberataque de ente ajeno a la OTAN.

Por otra parte, Huamán (2021), nos describe que debemos configurar una frontera para gestar defensas para combatir aquellos ataques a nuestros SI.

Del mismo modo, Vilcarromero (2018), señala que de acuerdo a la norma ISO/IEC 27032, está orientada a ayudar a responder ataques y preparase para luchar frente a ellos que realicen actividades como ingeniería social, malwares, spyware, etc.

Así también, Zúñiga (2017), concuerda en que las operaciones de respuesta son un tipo de operación que se realizan empleando software en contra de las TIC del adversario, es decir que se encuentran fuera de nuestra red y afectan los SI de ellos.

En cuanto al método utilizado, este estudio sustenta el aspecto que, al ser utilizado ayuda a incrementar el volumen de conocimiento y nuevas aplicaciones como aporte al conocimiento universal. Como fue una investigación de diseño no experimental anotamos y analizamos nuestras dos variables y su relación sin realizar ningún cambio. Nuestra herramienta, el cuestionario online recogido, ya ha sido resuelto por 123 personas, lo cual nos ha permitido obtener los datos necesarios. Gracias a la diversificación de las encuestas virtuales ha permitido que las personas encuestadas puedan colaborar y aportar de esta manera sin interferir con los que haceres y con sus labores personales, laborales y otros. Finalmente, la

creación de una muestra probabilística se suma a nuestra ventaja al extraer de personas en una variedad de situaciones, que pueden ser empleados militares y/o civiles que trabajan en la FAP, lo que nos permite generar más respuestas a nuestra herramienta de recopilación de datos.

VII. CONCLUSIONES

Primero Se concluye que la ciberdefensa incide significativamente en la GTI de la FAP, Lima 2022. De acuerdo al valor obtenido de R cuadrado de Nagelkerke de 96,9% indicando la correlación fuerte y moderada de la variable ciberdefensa sobre la variable GTI.

Segundo La primera dimensión operaciones defensivas incide significativamente en la GTI en la FAP, Lima 2022. De acuerdo al valor que obtuvimos de R cuadrado de Nagelkerke de 80,1% revelando la correlación fuerte y moderada de la dimensión operaciones defensivas sobre la variable GTI.

Tercero La segunda dimensión operaciones de explotación incide significativamente en la GTI en la FAP, Lima 2022. De acuerdo al valor que obtuvimos de R cuadrado de Nagelkerke de 94,0% revelando la correlación fuerte y moderada de la dimensión operaciones de explotación sobre la variable GTI.

Cuarto La tercera dimensión operaciones de respuesta inciden significativamente en la GTI en la FAP, Lima 2022. De acuerdo al valor que obtuvimos de R cuadrado de Nagelkerke de 82,8% revelando la correlación fuerte y moderada de la dimensión operaciones de respuesta sobre la variable GTI.

VIII. RECOMENDACIONES

Primero Continuar con el empleo de la ciberdefensa en la GTI de la FAP, Se recomienda al Comando del GROCE continuar con las metodologías empleadas al personal que se encarga de las GTI con la finalidad de mantener el nivel alcanzado hasta el momento.

Segundo Continuar con las operaciones defensivas en la GTI de la FAP, Se recomienda al Comando del GROCE desarrollar una continua capacitación de las nuevas herramientas para lograr buenos resultados.

Tercero Mantener las operaciones de explotación en la GTI de la FAP. Se recomienda al Comando del GROCE continuar con las técnicas de explotación de acuerdo a los avances tecnológicos.

Cuarto Conservar las operaciones de respuesta en la GTI de la FAP, Se recomienda al Comando del GROCE que conserve el nivel alcanzado hasta el momento para hacer frente ante posibles situaciones.

REFERENCIAS

Al Shahrani, AM, Rizwan, A., Sánchez Chero, M., Rosas-Prado, CE, Salazar, EB, Awad, NA (2022). An Internet of Things (IoT)-Based Optimization to Enhance Security in Healthcare Applications. https://www.scopus.com/record/display.uri?eid=2-s2.0-85139551180&doi=10.1155%2f2022%2f6802967&origin=inward&txGid=6ba70be2de59900425b0844f2b39349b

Akbar, M., Sang, J., Khan, A., Fazal-E-Amin, Nasrullah, Shafiq, M., Hussain, S. y Hu, H., Elahi, M., Xiang, H. (2018). "Improving the Quality of Software Development Process by Introducing a New Methodology–AZ-Model," in IEEE Access. Https://ieeexplore.ieee.org/document/8241771

Álvarez, A. (2018). Ciberseguridad y ciberdefensa, ¿Estamos preparados?. Revista ESGE. pp. 20-33. Http://esge.edu.pe/wpcontent/uploads/2020/05/Revista-ESGE-3ra-Edicio%CC%81n-2018.pdf

Baena, G. (2017). Metodología de la investigación (3ra edición ed.). Ciudad de México: Editorial Patria. ISBN ebook: 978-607-744-748-1

Baretto, J. (2017). La Defensa Nacional y la estrategia militar de seguridad cibernética (Tesis). Escuela Superior de Guerra Conjunta, La Plata, Argentina. Http://cefadigital.edu.ar/bitstream/1847939/1061/1/TFM%2004-2018%20BARETTO.pdf

BLUE BEARS IT (2022). Qu'est-ce qu'un support informatique? – [¿Qué es el soporte informático?]. Https://bluebearsit.com/support-informatique/#:~:text=Un%20support%20informatique%20est%20avant,%2C%20l'acc%C3%A8s%20%C3%A0%20distance%E2%80%A6

Calatayud, A., Mangan, J. and Christopher, M. (2019), "The self-thinking supply chain", *Supply Chain Management*, Vol. 24 No. 1, pp. 22-38. Https://org/10.1108/SCM-03-2018-0136

Cardona, C. (2017) Teoría General de Sistemas. Fondo editorial Areandino.

Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (2022). Perspectiva Estratégica del Ciberespacio 2030. Https://ccdcoe.org/library/publications/cyberspace-strategic-outlook-2030-horizon-scanning-and-analysis/

Cubeiro, E. (2015). Ciberdefensa, Capacidad esencial de las Fuerzas Armadas. *Pensamiento Conjunto*, 116, 30-38.

Deza, J. P., Yuen, R. T., & Quispe, E. B. (2011). Gestión de base de datos con SCADA para el control automatizado de una válvula de control proporcional. *Industrial data*. Https://www.redalyc.org/pdf/816/81622585004.pdf

Ding H, Na JM, Huang XL, et al. (2018). Stability analysis unit and spatial distribution pattern of the terrain texture in the northern Shaanxi Loess Plateau. Journal of Mountain Science 15(3). Https://.org/10.1007/s11629-017-4551-4

De Vergara, E. y Trama, G. (2017). *Operaciones Militares Cibernéticas.* https://esgcffaa.edu.ar/pdf/ESGCFFAA-2016_pdf-49.pdf

Doctrina CCFFAA DFA-CD-03-28. (2018). *Doctrina de Operaciones en el Ciberespacio*

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

Doctrina TOI 11-113 (2019). *Doctrina General del Ejército del Perú.*

Dubey, R., Gunasekaran, A., & Childe, S. J. (2019). Big data analytics capability in supply chain agility: The moderating effect of organizational flexibility. *Management Decision*. https://org/10.1108/MD-01-2018-0119

Escuela Superior de Guerra de Colombia (20 de setiembre del 2022*). Diplomado en Ciberseguridad y Ciberdefensa – Introducción a la Ciberdefensa*. Https://esdegue.edu.co/index.php/es/maestria-en-seguridad-y-defensa-nacionales.

ESET (2021). Informe Latinoamérica 2022. Security Report. Https://www.eset.com/ve/security-report/.

Ghobakhloo, M., & Azar, A. (2018). Information Technology Resources, the Organizational Capability of Lean-Agile Manufacturing, and Business Performance. *Information Resources Management Journa.* http://org/10.4018/IRMJ.2018040103

Gutiérrez-O. (2022). Charles Darwin y la teoría de la evolucion. *Logos Boletín Científico de La Escuela Preparatoria No. 2*.https://repository.uaeh.edu.mx/revistas/index.php/prepa2/article/view/8290

Hernández S., Fernández C. y Baptista L. (2014). Metodología de la investigación. México: Editorial Mc Graw Hill.

Huaman, J. (2021) Análisis de las Capacidades en Ciberseguridad y Ciberdefensa que realizó en el Centro de Ciberdefensa y Telemática del Ejército", Lima, 2020. Http://repositorio.esge.edu.pe/handle/20.500.14141/692.

HUB SPOT (2021**),** Support informatique: définition et conseils pour le mettre en place - [Soporte TI: definición y consejos para su puesta en marcha]. Https://blog.hubspot.fr/service/support-informatique

IBM (2022a). Documentation – What is a database managemet system? [Documentación - ¿Qué es un Sistema de Gestión de Base de Datos]? https://www.ibm.com/docs/en/zos-basic-skills?topic=zos-what-is-database-management-system

IBM (2022b). Informe Cost of a Data Breach 2022. https://www.ibm.com/downloads/cas/7G14X1W4.

INACAL (2016). Norma Técnica Peruana 12207 Ingenieria de Sistemas *Ciclo de Vida del Software*. 3ra edición

Iniciativa Nacional de Carreras y Estudios en Ciberseguridad (2022). About NICSS. https://niccs.cisa.gov/cybersecurity-career-resources/glossary#C.

Junta Interamericana de Defensa (2020). Guía de ciberdefensa - *Orientaciones para el diseño, planeamiento, implantación y desarrollo de una Ciberdefensa Militar*. Https://www.iadfoundation.org/wp-content/uploads/2020/08/Ciberdefensa10.pdf

Kamble, S., Gunasekaran, A., & Dhone, N. C. (2020). Industry 4.0 and lean manufacturing practices for sustainable organisational performance in Indian manufacturing companies. *International Journal of Production Research,* Https://org/10.1080/00207543.2019.1630772.

Kosutic, D, (2022). 9 *Steps to Cybersecurity* [Ciberseguridad en 9 pasos]. Http://www.iso27001standard.com/.

Ley N° 1139. Ley de la Fuerza Aérea del Perú. *Diario Oficial El Peruano*. 10 de diciembre de 2012

Ley N° 30999. Ley de Ciberdefensa. *Diario Oficial El Peruano*. 27 de agosto de 2019

Ley N° 31250. Ley del Sistema Nacional de Ciencia, Tecnología e Innovación. *Diario Oficial El Peruano.* 2 de julio de 2021

Lorenzetti, R. (2008) Teoría de Derecho Ambiental. Argentina. 1ra edición. Https://aulavirtual4.unl.edu.ar/pluginfile.php/6962/mod_resource/content/1/Teor%C3%ADa%20del%20Derecho%20Ambiental%20-%20Lorenzetti%2C%20Ricardo%20Luis.pdf

Medina, G. (2020). La Seguridad en el Ciberespacio: Un desafio para Colombia (2ª ed. Editorial Planeta.

MICROSOFT (2022). https://www.microsoft.com/en-us/research/publication/database-management-systems/

Montes Soldado, R., Hornos Barranco, M. J., Abad Grau, M., & Hurtado Torres, M. V. (2008). HELP DESK: SOPORTE TÉCNICO PARA LA EMPRESA DEL SIGLO XXI. *III Encuentro Iberoamericano de Finanzas y Sistemas de la Información (EFSI'02)*.

Navathe, E. (2011). Fundamentals of Database Systems [Fundamentos de los Sistemas de Base de Datos]. 6ta Edición. https://docs.ccsu.edu/curriculumsheets/ChadTest.pdf

NTP-ISO/IEC 1779. (2007, 22 de enero). “Norma Técnica Peruana NTP-ISO/IEC 1779:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2da Edición”. Comisión de Reglamentos Técnicos y Comerciales – INACAL.

O’brien y Marakas (2006). Sistemas de Información Gerencial. 7ma edición.

ORACLE (2022). Oracle Cloud Infrastructure (OCI) – Infraestructura en la nube de Oracle [Desafíos de la Base de datos]. https://www.oracle.com/es/manageability/database-management/

Ordenanza FAP 20-54. (2016, 13 de setiembre). “Organización – Servicio de Informática”. Publicación de la Red Interna Institucional de la Fuerza Aérea del Perú

Ordenanza FAP 20-62 (2016, 6 de diciembre). “Organización – Dirección de Telemática”. Publicación de la Red Interna Institucional de la Fuerza Aérea del Perú

Organización de los Estados Americanos (2021). Informe anual 2021. Fomentando y fortaleciendo la confianza y la seguridad hemisférica. Http://scm.oas.org/pdfs/2022/CP45984SCP.pdf.

Pressman, R. (2010). Ingeniería de Software – Un enfoque práctico 7ma edición. Https://www.academia.edu/24308956/Ingenieria_del_Software_Un_Enfoque_Practico_7ma_edici%C3%B3n

Robotiker (2001). Guía Básica para la aplicación de las TIC’s en Pymes

Sánchez, H., Reyes, C. y Mejía, K. (2018) Manual de términos en Investigación Científica, Tecnológica y Humanística. 1era Edición. Editorial: Universidad Ricardo Palma.

Scott, K (2018). Cyberspace Operations [Operaciones Ciberespaciales]. Https://dl.acm.org/doi/book/10.5555/3285221

SOFTFLUENT, (2022). Qu’est-ce que le développement logiciel? - [¿Qué es el desarrollo de software?]. Https://www.softfluent.fr/blog/developpement-logiciel-quand-quoi-comment/

Sotomayor, R. (2021). Cuadro de Indicadores de Seguridad de la Información para la Fuerza Aérea del Perú. Colombia

Suarez y Alonso, R. (2007). Tecnologías de la Información y la Comunicación. España: Editorial Ideaspropias

Valle A., Puerta A. y Núñez R. (2017) Curso de Consultoría TIC. Gestión, Software ERP y CRM (2.ª ed.). Editorial IT Campus Academy. Vigo. ISBN: 978-1542964517.

Vargas, Y., & Chávez, A. (2016). La Gestión de Servicios de soporte técnico en el ciclo de vida del desarrollo de software Management Support Services in the

life cycle software development. Http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=s2227-18992016000600004

Vargas, R., Reclade, L. y Reyes, R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. URVIO, Revista Latinoamericana de Estudios de Seguridad. Ecuador.

Vilcarromero y Vilchez (2018). Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones de seguridad (SOC) de una empresa de telecomunicaciones. Http://hdl.handle.net/10757/624832

Villalba, D. (2015). “La ciberseguridad en España 2011-2015”, realizada en la Universidad Nacional de Educación en Madrid – España. Http://e-spacio.uned.es/fez/eserv/tesisuned:CiencPolSoc-Avillalba/VILLALBA_FERNANDEZ_Anibal_Tesis.pdf

Von Bertalanffy L. (1989). Teoría General de los Sistemas. Fondo de Cultura Económica.

Yu, W., Jacobs, M. A., Chavez, R., & Feng, M. (2017). The impacts of IT capability and marketing capability on supply chain integration: A resource-based perspective. *International Journal of Production Research.* Https://org/10.1080/00207543.2016.1275874

Zúñiga, R. (2017). Ciberdefensa y su incidencia en la protección de la Información del Ejército del Perú. Caso COPERE 2013-2014 (Tesis Maestría) Instituto Científico y Tecnológico del Ejército, Perú. Http://repositorio.icte.ejercito.mil.pe/bitstream/123456789/183/1/Tesis%20Bach.%20Zu%c3%b1iga%20Figueroa%2c%20Jesus%20Rolando.pdf

ANEXOS

Anexo 1: Matriz de Consistencia

TÍTULO: La Ciberdefensa y su incidencia en la Gestión de Tecnologías de la Información en la Fuerza Aérea del Perú, Lima 2022

AUTOR: Pablo Roberto Huertas Espiritu

<table>
<tr><th>PROBLEMA</th><th>OBJETIVOS</th><th>HIPÓTESIS</th><th colspan="4">VARIABLES E INDICADORES</th></tr>
<tr><td rowspan="2">Problema principal:
¿Cuál es nivel de incidencia de la Ciberdefensa en la Gestión de las tecnologías de información de la FAP, Lima 2022?

Problemas específicos:
¿Cuál es nivel de incidencia de las operaciones defensivas en la Gestión de las tecnologías de información de la FAP, Lima 2022?

¿Cuál es nivel de incidencia de las operaciones de explotación en la Gestión</td><td rowspan="2">Objetivo principal:
Determinar el nivel de incidencia de la Ciberdefensa en la Gestión de las tecnologías de información de la FAP en el año 2022

Objetivos Específicos
Determinar el nivel de incidencia de las operaciones defensivas en la Gestión de las tecnologías de información de la FAP en el año 2022

Determinar el nivel de incidencia de las operaciones de explotación en la Gestión de las</td><td rowspan="2">Hipótesis principal:
La Ciberdefensa incide de manera significativa y positiva en la Gestión de las tecnologías de información.

Hipótesis específica
Las operaciones defensivas inciden de manera significativa y positiva en la Gestión de las tecnologías de información.

Las operaciones de explotación inciden de manera significativa y</td><td colspan="4">Variable - 1: Ciberdefensa</td></tr>
<tr><td>Dimensiones</td><td>Indicadores</td><td>Ítems</td><td>Niveles</td></tr>
<tr><td rowspan="4">Operaciones defensivas</td><td>Medidas preventivas</td><td>1-2</td><td rowspan="6">(1) Totalmente en desacuerdo
(2) En desacuerdo
(3) Ni de acuerdo ni en desacuerdo
(4) De acuerdo
(5) Totalmente de acuerdo.</td></tr>
<tr><td>Medidas proactivas</td><td>3-4</td></tr>
<tr><td>Medidas reactivas</td><td>5-6</td></tr>
<tr><td>Medidas de recuperación</td><td>7-8</td></tr>
<tr><td rowspan="3">Operaciones de Explotación</td><td>Búsqueda</td><td>9-10</td></tr>
<tr><td>Detección</td><td>11-12</td></tr>
<tr><td>Identificación</td><td>13-14</td></tr>
<tr><td></td><td>Denegación</td><td>15-16</td></tr>
</table>

TÍTULO: La Ciberdefensa y su incidencia en la Gestión de Tecnologías de la Información en la Fuerza Aérea del Perú, Lima 2022

AUTOR: Pablo Roberto Huertas Espiritu

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES			
de las tecnologías de información de la FAP, Lima 2022?	tecnologías de información de la FAP en el año 2022	positiva en la Gestión de las tecnologías de información.	Operaciones de Respuesta	Degradación	17-18	
				Interrupción	19-20	
¿Cuál es nivel de incidencia de las operaciones de respuesta en la Gestión de las tecnologías de información de la FAP, Lima 2022?	Determinar el nivel de incidencia de las operaciones de respuesta en la Gestión de las tecnologías de información de la FAP en el año 2022	Las operaciones de respuesta inciden de manera significativa y positiva en la Gestión de las tecnologías de información.	**Variable - 2: Gestión de Tecnologías de la Información**			
			Dimensiones	**Indicadores**	**Ítems**	**Niveles**
			Desarrollo de Sistemas	Monitorear el desempeño de las funciones de base de datos	21-22	(1) Totalmente en desacuerdo (2) En desacuerdo (3) Ni de acuerdo ni en desacuerdo (4) De acuerdo (5) Totalmente de acuerdo.
				Controlar las versiones de software	23-24	
				Establecer los estándares	25-26	
			Gestión Base de datos	Monitorear el desempeño de las funciones de base de datos	27-28	
				Estándares en las estructuras lógicas	29-30	
				Estándares en las estructuras físicas	31-32	

TÍTULO: La Ciberdefensa y su incidencia en la Gestión de Tecnologías de la Información en la Fuerza Aérea del Perú, Lima 2022 **AUTOR:** Pablo Roberto Huertas Espiritu						
PROBLEMA	**OBJETIVOS**	**HIPÓTESIS**	**VARIABLES E INDICADORES**			
			Soporte Técnico	Planificar la renovación periódica de la infraestructura de TI	33-34	
				Planear el programa de mantenimiento preventivo	35-36	
				Planear el programa de mantenimiento correctivo	37-38	

Metodología

TIPO Y DISEÑO	POBLACIÓN Y MUESTRA	TÉCNICAS E INSTRUMENTOS	ESTADÍSTICA POR UTILIZAR
Tipo: Aplicada **Diseño:** No experimental	**Población:** 180 **Tamaño de muestra:** **123** **Muestreo: No probabilístico de tipo por conveniencia**	**Técnicas:** Encuesta **Instrumentos:** Cuestionario	**Descriptiva:** Se utilizarán tablas de contingencia con la que efectuará el análisis descriptivo e histogramas, estos irán junto a su propia interpretación de resultados de las variables, así como de las dimensiones definidas para la variable dependiente. **Inferencial:** Se considerará el análisis no paramétrico y su estadística de regresión logística ordinal para así determinar la incidencia que existe de la variable Ciberdefensa sobre la variable Gestión de las TI

Anexo 2: Matriz de Operacionalización de Variables

TÍTULO: La Ciberdefensa y su incidencia en la Gestión de Tecnologías de la Información en la Fuerza Aérea del Perú, Lima 2022

AUTOR: Pablo Roberto Huertas Espiritu

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
Ciberdefensa Según Doctrina CCFFAA DFA-CD-03-28 (2018) La Ciberdefensa es el grupo de acciones que se desarrollan en el ciberespacio para prevenir, detectar, identificar, anular, impedir, evitar, contrarrestar, contener o repeler una amenaza o agresión cibernética, sea ésta inmediata, latente o potencial, a fin de permitir el empleo del Instrumento Militar de la Nación	**Operaciones defensivas** De acuerdo a la Doctrina CCFFCC DFA-CD-03-28 (2018), son operaciones de defensa del ciberespacio propio y asignado, con la finalidad de brindar protección ante actos o intenciones Hostiles, para asegurar su disponibilidad, confidencialidad e integridad del ciberespacio, mediante la aplicación de medidas preventivas, proactivas, reactivas y de recuperación**.**	Medidas preventivas	1	¿Las Medidas preventivas, de las Operaciones Ciberespaciales Defensivas, han cambiado los métodos empleados para el desarrollo de sistemas?	(1) Totalmente en desacuerdo (2) En desacuerdo (3) Ni de acuerdo ni en desacuerdo (4) De acuerdo (5) Totalmente de acuerdo.
			2	¿Las Medidas preventivas, de las Operaciones Ciberespaciales Defensivas, han incidido en los protocolos establecidos para la gestión de TI?	
		Medidas proactivas	3	¿Las Medidas proactivas de las Operaciones Ciberespaciales defensivas, contribuye con la gestión de los de TI?	
			4	¿Las Medidas proactivas de las Operaciones Ciberespaciales defensivas, mejoran la gestión de base de datos?	
		Medidas reactivas	5	¿Las Medidas reactivas de las Operaciones Ciberespaciales defensivas, mejoran el soporte técnico de las TI?	
			6	¿Las Medidas reactivas de las Operaciones Ciberespaciales defensivas, inciden gestión de TI?	
		Medidas de recuperación	7	¿Las Medidas de recuperación de las Operaciones Ciberespaciales defensivas, ayudan al desarrollo de sistemas en la gestión de TI?	

TÍTULO: La Ciberdefensa y su incidencia en la Gestión de Tecnologías de la Información en la Fuerza Aérea del Perú, Lima 2022

AUTOR: Pablo Roberto Huertas Espiritu

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
			8	¿Las Medidas de recuperación de las Operaciones Ciberespaciales defensivas, ayudan al Soporte Técnico de la Gestión de TI?	
	Operaciones de Explotación De acuerdo a la Doctrina CCFFCC DFA-CD-03-28 (2018), son operaciones de búsqueda, detección e identificación de intenciones hostiles, así como la determinación de las vulnerabilidades en el ciberespacio, para un adecuado planeamiento para futuras operaciones militares en ese ámbito	Búsqueda	9	¿La búsqueda de vulnerabilidades a través de las Operaciones de Explotación contribuyen a la gestión base de datos?	
			10	¿La búsqueda de vulnerabilidades a través de las Operaciones de Explotación contribuyen al desarrollo de sistemas?	
		Detección	11	¿Se detecta a través de las Operaciones de Explotación las vulnerabilidades de la gestión de TI?	
			12	¿Se detecta a través de las Operaciones de Explotación riesgos de la gestión de Base de datos?	
		Identificación	13	¿Se identifica a través de las Operaciones de Explotación mejoras en el monitoreo del desempeño de las funciones de base de datos?	
			14	¿Se identifica a través de las Operaciones de Explotación mejoras en la Gestión de Base de datos?	
	Operaciones de Respuesta	Denegación	15	¿Se deniega a través de las Operaciones de Respuesta el acceso a la Base de datos?	

TÍTULO: La Ciberdefensa y su incidencia en la Gestión de Tecnologías de la Información en la Fuerza Aérea del Perú, Lima 2022

AUTOR: Pablo Roberto Huertas Espiritu

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
	De acuerdo a la Doctrina CCFFCC DFA-CD-03-28 (2018), son operaciones destinadas a crear efectos de denegación, degradación o interrupción del ciberespacio de los adversarios, mediante el empleo de ciberarmas		16	¿Se deniega a través de las Operaciones de Respuesta el acceso al desarrollo de Sistemas de Información?	
		Degradación	17	¿Se degrada a través de las Operaciones de Respuesta el acceso a la gestión de Base de datos?	
			18	¿Se degrada a través de las Operaciones de Respuesta el acceso al desarrollo de Sistemas de Información?	
		Interrupción	19	¿Se interrumpe a través de las Operaciones de Respuesta el acceso al desarrollo de Sistemas de Información?	
			20	¿Se interrumpe a través de las Operaciones de Respuesta el acceso a la gestión de Base de datos?	
Gestión de Tecnologías de la Información Según Valle et al. (2017) definen a la gestión de TI como un elemento esencial de la organización que administra las TI, y esta función ha	**Desarrollo de Sistemas** De acuerdo a la Ordenanza FAP 20-54 (2016), el desarrollo de sistemas involucra Realizar el análisis, diseño, programación, evaluación, documentación y mantenimiento de los sistemas que se implanten en las Unidades	Diseño de los sistemas de información	21	¿Se considera las medidas de ciberdefensa durante el diseño de los sistemas de información?	(1) Totalmente en desacuerdo (2) En desacuerdo (3) Ni de acuerdo ni en desacuerdo
			22	¿La ciberdefensa permite diseñar los sistemas de información con mayor seguridad?	
		Controlar las versiones de software	23	¿Se controla las versiones de software de acuerdo a las medidas de ciberdefensa?	
			24	¿Las versiones de software son controlados por el personal que conoce la ciberdefensa?	
		Establecer los estándares	25	¿Los estándares de desarrollo de sistemas están alineados a las medidas ciberdefensa?	

TÍTULO: La Ciberdefensa y su incidencia en la Gestión de Tecnologías de la Información en la Fuerza Aérea del Perú, Lima 2022

AUTOR: Pablo Roberto Huertas Espiritu

Variables	Dimensiones	Indicadores	No.	Ítems (Preguntas)	Niveles
sufrido cambios a lo largo de la historia pasando a ser gestionada por áreas altamente especializadas			26	¿El establecer los estándares de desarrollo de sistemas contribuyen con las medidas de ciberdefensa?	(4) De acuerdo (5) Totalmente de acuerdo.
	Gestión de Base de datos De acuerdo a la Ordenanza FAP 20-54 (2016), La gestión de base de datos consiste en administrar el sistema manejador y la estructura de la base de datos; el acceso a las aplicaciones vía Web, la publicación de información en la intranet, el respaldo y recuperación de la base de datos, el diccionario de datos; así como, la seguridad, control de accesos, auditoria y otras que se requieran	Monitorear el desempeño de las funciones de base de datos	27	¿El personal que monitorea el desempeño de las funciones de base de datos aplica los conocimientos de ciberdefensa?	
			28	¿La gestión de base de datos es monitoreada continuamente con personal de ciberdefensa?	
		Estándares en las estructuras lógicas	29	¿Establecen los estándares en las estructuras lógicas de la base de datos de acuerdo a lo normativa de ciberdefensa?	
			30	¿Se analiza con frecuencia los estándares en las funciones lógicas de la base de datos?	
		Estándares en las estructuras físicas	31	¿Establecen los estándares en las estructuras físicas de la base de datos de acuerdo a lo normativa de ciberdefensa?	
			32	¿Se analiza con frecuencia los estándares en las funciones físicas de la base de datos?	
	Soporte Técnico De acuerdo a la Ordenanza FAP 20-54 (2016), la dimensión soporte técnico consiste en Proporcionar el soporte técnico requerido para la solución de los problemas que se	Planificar la renovación periódica de la infraestructura de TI	33	¿Se orienta la renovación de infraestructura de TI con la finalidad de cumplir las medidas de ciberdefensa?	
			34	¿La planificación de la renovación de infraestructura de TI cumple con la normatividad de ciberdefensa?	

TÍTULO: La Ciberdefensa y su incidencia en la Gestión de Tecnologías de la Información en la Fuerza Aérea del Perú, Lima 2022 **AUTOR:** Pablo Roberto Huertas Espiritu					
Variables	**Dimensiones**	**Indicadores**	**No.**	**Ítems (Preguntas)**	**Niveles**
	presenten en el hardware (equipamiento), software (sistemas operativos, lenguajes de programación, utilitarios), conectividad y telecomunicaciones, antivirus, antispam, filtro de contenido, seguridad de internet (perimetral e interna), correo electrónico y otros servicios de nivel Unidad o Institucionales	Planear el programa de mantenimiento preventivo	35	¿Se realiza el mantenimiento preventivo considerando las medidas de ciberdefensa?	
			36	¿La planificación del mantenimiento preventivo esta alineada a las actividades de ciberdefensa?	
		Planear el programa de mantenimiento correctivo	37	¿Se realiza el mantenimiento correctivo considerando las medidas de ciberdefensa? ¿La planificación del mantenimiento preventivo esta alineada a las actividades de ciberdefensa?	
			38	¿La planificación del mantenimiento correctivo esta alineada a las actividades de ciberdefensa?	

Anexo 3: Instrumento de Recolección de Datos

Cuestionario para usuarios del Sistema de Informática de la FAP

Fecha: [/ /] **Edad:** [ ]

Sexo: Femenino[ ] Masculino[ ]

Personal: Militar [ ] Civil [ ]

Instrucciones: Marque con un aspa la respuesta que crea conveniente teniendo en consideración el puntaje que corresponda de acuerdo al siguiente **ejemplo**: Totalmente en desacuerdo (1), En desacuerdo (2), Ni de acuerdo ni en desacuerdo (3), De acuerdo (4) y Totalmente de acuerdo (5).

No	Pregunta	Valoración				
		1	2	3	4	5
	Sobre la Ciberdefensa					
1	¿Las Medidas preventivas, de las Operaciones Ciberespaciales Defensivas, han cambiado los métodos empleados para el desarrollo de sistemas?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
2	¿Las Medidas preventivas, de las Operaciones Ciberespaciales Defensivas, han incidido en los protocolos establecidos para la gestión de TI?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
3	¿Las Medidas proactivas de las Operaciones Ciberespaciales defensivas, contribuye con la gestión de los de TI?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
4	¿Las Medidas proactivas de las Operaciones Ciberespaciales defensivas, mejoran la gestión de base de datos?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
5	¿Las Medidas reactivas de las Operaciones Ciberespaciales defensivas, mejoran el soporte técnico de las TI?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
6	¿Las Medidas reactivas de las Operaciones Ciberespaciales defensivas, inciden gestión de TI?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
7	¿Las Medidas de recuperación de las Operaciones Ciberespaciales defensivas, ayudan al desarrollo de sistemas en la gestión de TI?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
8	¿Las Medidas de recuperación de las Operaciones Ciberespaciales defensivas, ayudan al Soporte Técnico de la Gestión de TI?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
9	¿La búsqueda de vulnerabilidades a través de las Operaciones de Explotación contribuyen a la gestión base de datos?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
10	¿La búsqueda de vulnerabilidades a través de las Operaciones de Explotación contribuyen al desarrollo de sistemas?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo

No	Pregunta	Valoración				
		1	2	3	4	5
11	¿Se detecta a través de las Operaciones de Explotación las vulnerabilidades de la gestión de TI?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
12	¿Se detecta a través de las Operaciones de Explotación riesgos de la gestión de Base de datos?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
13	¿Se identifica a través de las Operaciones de Explotación mejoras en el monitoreo del desempeño de las funciones de base de datos?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
14	¿Se identifica a través de las Operaciones de Explotación mejoras en la Gestión de Base de datos?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
15	¿Se deniega a través de las Operaciones de Respuesta el acceso a la Base de datos?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
16	¿Se deniega a través de las Operaciones de Respuesta el acceso al desarrollo de Sistemas de Información?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
17	¿Se degrada a través de las Operaciones de Respuesta el acceso a la gestión de Base de datos?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
18	¿Se degrada a través de las Operaciones de Respuesta el acceso al desarrollo de Sistemas de Información?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
19	¿Se interrumpe a través de las Operaciones de Respuesta el acceso al desarrollo de Sistemas de Información?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
20	¿Se interrumpe a través de las Operaciones de Respuesta el acceso a la gestión de Base de datos?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
	Sobre la Gestión de las Tecnologías de la Información					
21	¿Se considera las medidas de ciberdefensa durante el diseño de los sistemas de información?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
22	¿La ciberdefensa permite diseñar los sistemas de información con mayor seguridad?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
23	¿Se controla las versiones de software de acuerdo a las medidas de ciberdefensa?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
24	¿Las versiones de software son controlados por el personal que conoce la ciberdefensa?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo

No	Pregunta	Valoración				
		1	2	3	4	5
25	¿Los estándares de desarrollo de sistemas están alineados a las medidas ciberdefensa?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
26	¿El establecer los estándares de desarrollo de sistemas contribuyen con las medidas de ciberdefensa?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
27	¿El personal que monitorea el desempeño de las funciones de base de datos aplica los conocimientos de ciberdefensa?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
28	¿La gestión de base de datos es monitoreada continuamente con personal de ciberdefensa?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
29	¿Establecen los estándares en las estructuras lógicas de la base de datos de acuerdo a lo normativa de ciberdefensa?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
30	¿Se analiza con frecuencia los estándares en las funciones lógicas de la base de datos?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
31	¿Establecen los estándares en las estructuras físicas de la base de datos de acuerdo a lo normativa de ciberdefensa?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
32	¿Se analiza con frecuencia los estándares en las funciones físicas de la base de datos?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
33	¿Se orienta la renovación de infraestructura de TI con la finalidad de cumplir las medidas de ciberdefensa?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
34	¿La planificación de la renovación de infraestructura de TI cumple con la normatividad de ciberdefensa?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
35	¿Se realiza el mantenimiento preventivo considerando las medidas de ciberdefensa?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
36	¿La planificación del mantenimiento preventivo esta alineada a las actividades de ciberdefensa?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
37	¿Se realiza el mantenimiento correctivo considerando las medidas de ciberdefensa?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
38	¿La planificación del mantenimiento correctivo esta alineada a las actividades de ciberdefensa?	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo

Anexo 4: Certificado de Validación del Instrumento de Recolección de Datos

Validación del Experto N°1

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO

VARIABLE: Ciberdefensa

Nº	DIMENSIONES / items	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Operaciones defensivas	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Las Medidas preventivas, de las Operaciones Ciberespaciales Defensivas, han cambiado los métodos empleados para el desarrollo de sistemas?	x		x		x		
2	¿Las Medidas preventivas, de las Operaciones Ciberespaciales Defensivas, han incidido en los protocolos establecidos para la gestión de TI?	x		x		x		
3	¿Las Medidas proactivas de las Operaciones Ciberespaciales defensivas, contribuye con la gestión de los de TI?	x		x		x		
4	¿Las Medidas proactivas de las Operaciones Ciberespaciales defensivas, mejoran la gestión de base de datos?	x		x		x		
5	¿Las Medidas reactivas de las Operaciones Ciberespaciales defensivas, mejoran el soporte técnico de las TI?	x		x		x		
6	¿Las Medidas reactivas de las Operaciones Ciberespaciales defensivas, inciden gestión de TI?	x		x		x		
7	¿Las Medidas de recuperación de las Operaciones Ciberespaciales defensivas, ayudan al desarrollo de sistemas en la gestión de TI?	x		x		x		
8	¿Las Medidas de recuperación de las Operaciones Ciberespaciales defensivas, ayudan al Soporte Técnico de la Gestión de TI?	x		x		x		
	Operaciones de Explotación	**Si**	**No**	**Si**	**No**	**Si**	**No**	
9	¿La búsqueda de vulnerabilidades a través de las Operaciones de Explotación contribuyen a la gestión base de datos?	x		x		x		
10	¿La búsqueda de vulnerabilidades a través de las Operaciones de Explotación contribuyen al desarrollo de sistemas?	x		x		x		
11	¿Se detecta a través de las Operaciones de Explotación las vulnerabilidades de la gestión de TI?	x		x		x		
12	¿Se detecta a través de las Operaciones de Explotación riesgos de la gestión de Base de datos?	x		x		x		
13	¿Se identifica a través de las Operaciones de Explotación mejoras en el monitoreo del desempeño de las funciones de base de datos?	x		x		x		
14	¿Se identifica a través de las Operaciones de Explotación mejoras en la Gestión de Base de datos?	x		x		x		
	Operaciones de Respuesta	**Si**	**No**	**Si**	**No**	**Si**	**No**	
15	¿Se deniega a través de las Operaciones de Respuesta el acceso a la Base de datos?	x		x		x		
16	¿Se deniega a través de las Operaciones de Respuesta el acceso al desarrollo de Sistemas de Información?	x		x		x		
17	¿Se degrada a través de las Operaciones de Respuesta el acceso a la gestión de Base de datos?	x		x		x		
18	¿Se degrada a través de las Operaciones de Respuesta el acceso al desarrollo de Sistemas de Información?	x		x		x		
19	¿Se interrumpe a través de las Operaciones de Respuesta el acceso al desarrollo de Sistemas de Información?	x		x		x		

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
20	¿Se interrumpe a través de las Operaciones de Respuesta el acceso a la gestión de Base de datos?	x		x		x		

VARIABLE: Gestión de Tecnologías de la Información

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Desarrollo de Sistemas	**Si**	**No**	**Si**	**No**	**Si**	**No**	
21	¿Se considera las medidas de ciberdefensa durante el diseño de los sistemas de información?	x		x		x		
22	¿La ciberdefensa permite diseñar los sistemas de información con mayor seguridad?	x		x		x		
23	¿Se controla las versiones de software de acuerdo a las medidas de ciberdefensa?	x		x		x		
24	¿Las versiones de software son controlados por el personal que conoce la ciberdefensa?	x		x		x		
25	¿Los estándares de desarrollo de sistemas están alineados a las medidas ciberdefensa?	x		x		x		
26	¿El establecer los estándares de desarrollo de sistemas contribuyen con las medidas de ciberdefensa?	x		x		x		
	Gestión de Base de datos	**Si**	**No**	**Si**	**No**	**Si**	**No**	
27	¿El personal que monitorea el desempeño de las funciones de base de datos aplica los conocimientos de ciberdefensa?	x		x		x		
28	¿La gestión de base de datos es monitoreada continuamente con personal de ciberdefensa?	x		x		x		
29	¿Establecen los estándares en las estructuras lógicas de la base de datos de acuerdo a lo normativa de ciberdefensa?	x		x		x		
30	¿Se analiza con frecuencia los estándares en las funciones lógicas de la base de datos?	x		x		x		
31	¿Establecen los estándares en las estructuras físicas de la base de datos de acuerdo a lo normativa de ciberdefensa?	x		x		x		
32	¿Se analiza con frecuencia los estándares en las funciones físicas de la base de datos?	x		x		x		
	Soporte Técnico	**Si**	**No**	**Si**	**No**	**Si**	**No**	
33	¿Se orienta la renovación de infraestructura de TI con la finalidad de cumplir las medidas de ciberdefensa?	x		x		x		
34	¿La planificación de la renovación de infraestructura de TI cumple con la normatividad de ciberdefensa?	x		x		x		
35	¿Se realiza el mantenimiento preventivo considerando las medidas de ciberdefensa?	x		x		x		
36	¿La planificación del mantenimiento preventivo esta alineada a las actividades de ciberdefensa?	x		x		x		
37	¿Se realiza el mantenimiento correctivo considerando las medidas de ciberdefensa?	x		x		x		
38	¿La planificación del mantenimiento correctivo esta alineada a las actividades de ciberdefensa?	x		x		x		

Observaciones (precisar si hay suficiencia):___ _____**SUFICIENTE**_____

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

26 de octubre del 2022

Apellidos y nombre s del juez evaluador: Vargas Guevara Magno Iván **DNI:** 40425332

Especialista: Metodólogo [X] **Temático [X]**

Grado: Maestro [X] **Doctor [ ]**

[1] **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo
[2] **Pertinencia:** Si el ítem pertenece a la dimensión.
[3] **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante

Validación del Experto N°2

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO

VARIABLE: Ciberdefensa

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Operaciones defensivas	Sí	No	Sí	No	Sí	No	
1	¿Las Medidas preventivas, de las Operaciones Ciberespaciales Defensivas, han cambiado los métodos empleados para el desarrollo de sistemas?	x		x		x		
2	¿Las Medidas preventivas, de las Operaciones Ciberespaciales Defensivas, han incidido en los protocolos establecidos para la gestión de TI?	x		x		x		
3	¿Las Medidas proactivas de las Operaciones Ciberespaciales defensivas, contribuye con la gestión de los de TI?	x		x		x		
4	¿Las Medidas proactivas de las Operaciones Ciberespaciales defensivas, mejoran la gestión de base de datos?	x		x		x		
5	¿Las Medidas reactivas de las Operaciones Ciberespaciales defensivas, mejoran el soporte técnico de las TI?	x		x		x		
6	¿Las Medidas reactivas de las Operaciones Ciberespaciales defensivas, inciden gestión de TI?	x		x		x		
7	¿Las Medidas de recuperación de las Operaciones Ciberespaciales defensivas, ayudan al desarrollo de sistemas en la gestión de TI?							
8	¿Las Medidas de recuperación de las Operaciones Ciberespaciales defensivas, ayudan al Soporte Técnico de la Gestión de TI?							
	Operaciones de Explotación	Sí	No	Sí	No	Sí	No	
9	¿La búsqueda de vulnerabilidades a través de las Operaciones de Explotación contribuyen a la gestión base de datos?	x		x		x		
10	¿La búsqueda de vulnerabilidades a través de las Operaciones de Explotación contribuyen al desarrollo de sistemas?	x		x		x		
11	¿Se detecta a través de las Operaciones de Explotación las vulnerabilidades de la gestión de TI?	x		x		x		
12	¿Se detecta a través de las Operaciones de Explotación riesgos de la gestión de Base de datos?	x		x		x		
13	¿Se identifica a través de las Operaciones de Explotación mejoras en el monitoreo del desempeño de las funciones de base de datos?	x		x		x		
14	¿Se identifica a través de las Operaciones de Explotación mejoras en la Gestión de Base de datos?	x		x		x		
	Operaciones de Respuesta	Sí	No	Sí	No	Sí	No	
15	¿Se deniega a través de las Operaciones de Respuesta el acceso a la Base de datos?	x		x		x		
16	¿Se deniega a través de las Operaciones de Respuesta el acceso al desarrollo de Sistemas de Información?	x		x		x		
17	¿Se degrada a través de las Operaciones de Respuesta el acceso a la gestión de Base de datos?	x		x		x		
18	¿Se degrada a través de las Operaciones de Respuesta el acceso al desarrollo de Sistemas de Información?	x		x		x		
19	¿Se interrumpe a través de las Operaciones de Respuesta el acceso al desarrollo de Sistemas de Información?	x		x		x		

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
20	¿Se interrumpe a través de las Operaciones de Respuesta el acceso a la gestión de Base de datos?	x		x		x		

VARIABLE: Gestión de Tecnologías de la Información

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Desarrollo de Sistemas	Si	No	Si	No	Si	No	
21	¿Se considera las medidas de ciberdefensa durante el diseño de los sistemas de información?	x		x		x		
22	¿La ciberdefensa permite diseñar los sistemas de información con mayor seguridad?	x		x		x		
23	¿Se controla las versiones de software de acuerdo a las medidas de ciberdefensa?	x		x		x		
24	¿Las versiones de software son controlados por el personal que conoce la ciberdefensa?	x		x		x		
25	¿Los estándares de desarrollo de sistemas están alineados a las medidas ciberdefensa?	x		x		x		
26	¿El establecer los estándares de desarrollo de sistemas contribuyen con las medidas de ciberdefensa?	x		x		x		
	Gestión de Base de datos	Si	No	Si	No	Si	No	
27	¿El personal que monitorea el desempeño de las funciones de base de datos aplica los conocimientos de ciberdefensa?	x		x		x		
28	¿La gestión de base de datos es monitoreada continuamente con personal de ciberdefensa?	x		x		x		
29	¿Establecen los estándares en las estructuras lógicas de la base de datos de acuerdo a lo normativa de ciberdefensa?	x		x		x		
30	¿Se analiza con frecuencia los estándares en las funciones lógicas de la base de datos?	x		x		x		
31	¿Establecen los estándares en las estructuras físicas de la base de datos de acuerdo a lo normativa de ciberdefensa?	x		x		x		
32	¿Se analiza con frecuencia los estándares en las funciones físicas de la base de datos?	x		x		x		
	Soporte Técnico	Si	No	Si	No	Si	No	
33	¿Se orienta la renovación de infraestructura de TI con la finalidad de cumplir las medidas de ciberdefensa?	x		x		x		
34	¿La planificación de la renovación de infraestructura de TI cumple con la normatividad de ciberdefensa?	x		x		x		
35	¿Se realiza el mantenimiento preventivo considerando las medidas de ciberdefensa?	x		x		x		
36	¿La planificación del mantenimiento preventivo esta alineada a las actividades de ciberdefensa?	x		x		x		
37	¿Se realiza el mantenimiento correctivo considerando las medidas de ciberdefensa?	x		x		x		

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
38	¿La planificación del mantenimiento correctivo esta alineada a las actividades de ciberdefensa?	x		x		x		

Observaciones (precisar si hay suficiencia): ___ ____SUFICIENTE_____

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombre s del juez evaluador: Rojas Maguiña Fredy **DNI:** 40150542

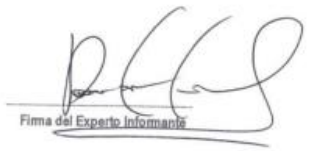
27.de octubre.del 2022

Especialista: Metodólogo [X] **Temático [ ]**

Grado: Maestro [X] **Doctor [ ]**

[1] **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo
[2] **Pertinencia:** Si el ítem pertenece a la dimensión.
[3] **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión



Firma del Experto Informante

Validación del Experto N°3

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO

VARIABLE: Ciberdefensa

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Operaciones defensivas	Si	No	Si	No	Si	No	
1	¿Las Medidas preventivas, de las Operaciones Ciberespaciales Defensivas, han cambiado los métodos empleados para el desarrollo de sistemas?	x		x		x		
2	¿Las Medidas preventivas, de las Operaciones Ciberespaciales Defensivas, han incidido en los protocolos establecidos para la gestión de TI?	x		x		x		
3	¿Las Medidas proactivas de las Operaciones Ciberespaciales defensivas, contribuye con la gestión de los de TI?	x		x		x		
4	¿Las Medidas proactivas de las Operaciones Ciberespaciales defensivas, mejoran la gestión de base de datos?	x		x		x		
5	¿Las Medidas reactivas de las Operaciones Ciberespaciales defensivas, mejoran el soporte técnico de las TI?	x		x		x		
6	¿Las Medidas reactivas de las Operaciones Ciberespaciales defensivas, inciden gestión de TI?	x		x		x		
7	¿Las Medidas de recuperación de las Operaciones Ciberespaciales defensivas, ayudan al desarrollo de sistemas en la gestión de TI?							
8	¿Las Medidas de recuperación de las Operaciones Ciberespaciales defensivas, ayudan al Soporte Técnico de la Gestión de TI?							
	Operaciones de Explotación	Si	No	Si	No	Si	No	
9	¿La búsqueda de vulnerabilidades a través de las Operaciones de Explotación contribuyen a la gestión base de datos?	x		x		x		
10	¿La búsqueda de vulnerabilidades a través de las Operaciones de Explotación contribuyen al desarrollo de sistemas?	x		x		x		
11	¿Se detecta a través de las Operaciones de Explotación las vulnerabilidades de la gestión de TI?	x		x		x		
12	¿Se detecta a través de las Operaciones de Explotación riesgos de la gestión de Base de datos?	x		x		x		
13	¿Se identifica a través de las Operaciones de Explotación mejoras en el monitoreo del desempeño de las funciones de base de datos?	x		x		x		
14	¿Se identifica a través de las Operaciones de Explotación mejoras en la Gestión de Base de datos?	x		x		x		
	Operaciones de Respuesta	Si	No	Si	No	Si	No	
15	¿Se deniega a través de las Operaciones de Respuesta el acceso a la Base de datos?	x		x		x		
16	¿Se deniega a través de las Operaciones de Respuesta el acceso al desarrollo de Sistemas de Información?	x		x		x		
17	¿Se degrada a través de las Operaciones de Respuesta el acceso a la gestión de Base de datos?	x		x		x		
18	¿Se degrada a través de las Operaciones de Respuesta el acceso al desarrollo de Sistemas de Información?	x		x		x		
19	¿Se interrumpe a través de las Operaciones de Respuesta el acceso al desarrollo de Sistemas de Información?	x		x		x		

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
20	¿Se interrumpe a través de las Operaciones de Respuesta el acceso a la gestión de Base de datos?	x		x		x		

VARIABLE: Gestión de Tecnologías de la Información

Nº	DIMENSIONES / ítems	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Desarrollo de Sistemas	Si	No	Si	No	Si	No	
21	¿Se considera las medidas de ciberdefensa durante el diseño de los sistemas de información?	x		x		x		
22	¿La ciberdefensa permite diseñar los sistemas de información con mayor seguridad?	x		x		x		
23	¿Se controla las versiones de software de acuerdo a las medidas de ciberdefensa?	x		x		x		
24	¿Las versiones de software son controlados por el personal que conoce la ciberdefensa?	x		x		x		
25	¿Los estándares de desarrollo de sistemas están alineados a las medidas ciberdefensa?	x		x		x		
26	¿El establecer los estándares de desarrollo de sistemas contribuyen con las medidas de ciberdefensa?	x		x		x		
	Gestión de Base de datos	Si	No	Si	No	Si	No	
27	¿El personal que monitorea el desempeño de las funciones de base de datos aplica los conocimientos de ciberdefensa?	x		x		x		
28	¿La gestión de base de datos es monitoreada continuamente con personal de ciberdefensa?	x		x		x		
29	¿Establecen los estándares en las estructuras lógicas de la base de datos de acuerdo a lo normativa de ciberdefensa?	x		x		x		
30	¿Se analiza con frecuencia los estándares en las funciones lógicas de la base de datos?	x		x		x		
31	¿Establecen los estándares en las estructuras físicas de la base de datos de acuerdo a lo normativa de ciberdefensa?	x		x		x		
32	¿Se analiza con frecuencia los estándares en las funciones físicas de la base de datos?	x		x		x		
	Soporte Técnico	Si	No	Si	No	Si	No	
33	¿Se orienta la renovación de infraestructura de TI con la finalidad de cumplir las medidas de ciberdefensa?	x		x		x		
34	¿La planificación de la renovación de infraestructura de TI cumple con la normatividad de ciberdefensa?	x		x		x		
35	¿Se realiza el mantenimiento preventivo considerando las medidas de ciberdefensa?	x		x		x		
36	¿La planificación del mantenimiento preventivo esta alineada a las actividades de ciberdefensa?	x		x		x		
37	¿Se realiza el mantenimiento correctivo considerando las medidas de ciberdefensa?	x		x		x		

Nº	DIMENSIONES / items	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
38	¿La planificación del mantenimiento correctivo esta alineada a las actividades de ciberdefensa?	x		x		x		

Observaciones (precisar si hay suficiencia): ___ ____**SUFICIENTE**_____

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

28.de octubre.del 2022

Apellidos y nombre s del juez evaluador: Chávez Marcos Ivan **DNI:** 40060141

Especialista: Metodólogo [X] **Temático [ ]**

Grado: Maestro [X] **Doctor [ ]**

[1] **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo
[2] **Pertinencia:** Si el ítem pertenece a la dimensión.
[3] **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Anexo 5: Base de datos

Encuestado	Sexo	Personal	V1: Ciberseguridad																				V2: Gestión de Tecnologías de la Información																	
								D1			D2						D3						D1						D2						D3					
			I1		I2		I3	I4		I4	I5		I6		I7		I8		I9		I1		I2		I3	I4		I5		I6		I7		I8		I9			
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38
1	2	1	4	4	4	4	5	5	4	4	5	5	4	4	4	4	4	4	5	5	4	4	4	4	4	4	4	4	4	4	5	5	4	4	4	4	4	4	5	5
2	1	2	5	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	4
3	2	2	4	4	5	4	4	4	4	4	4	5	4	5	4	4	5	4	4	4	4	5	4	4	4	4	5	4	4	4	4	5	4	5	4	4	5	4	4	5
4	1	2	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	4
5	1	1	4	4	4	4	4	5	4	4	4	5	4	5	4	4	4	4	4	5	4	5	4	4	4	4	4	4	4	4	4	5	4	5	4	4	4	4	4	5
6	2	1	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
7	1	1	4	4	5	4	4	5	4	4	4	5	4	5	4	4	4	4	4	5	4	5	4	4	4	4	5	4	4	4	4	5	4	5	4	4	4	4	4	4
8	2	2	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5
9	1	2	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4	5	5	4	4	4	4	4	4	5	4
10	2	2	5	5	5	5	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	5
11	1	1	4	4	5	4	4	4	4	5	4	5	4	5	4	4	4	4	4	4	4	5	4	4	4	4	5	4	4	4	4	5	4	5	4	4	5	4	4	5
12	2	2	4	4	4	4	5	5	4	4	5	5	5	4	5	5	4	4	5	5	5	4	5	5	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	4
13	1	1	4	4	4	4	5	4	4	4	5	5	4	4	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4	5	4	5	4	4	4	4	4	5
14	1	1	5	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
15	2	1	4	4	5	4	4	4	4	4	4	5	4	5	4	4	5	4	4	4	4	5	4	4	4	4	5	4	4	4	4	5	4	5	4	4	4	4	4	4
16	1	1	4	4	4	5	5	4	5	5	5	5	5	5	5	5	5	5	5	4	4	4	5	5	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5
17	2	2	4	4	4	4	4	4	4	4	4	5	4	5	4	4	4	4	4	4	4	4	4	4	4	4	5	4	5	4	4	4	4	4	4	5	5	5	5	4
18	1	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	4	5
19	2	2	4	4	5	4	4	4	4	4	4	5	4	5	4	4	4	4	4	4	4	5	4	4	4	4	5	4	5	4	4	4	4	4	4	5	5	5	5	5
20	1	1	4	4	4	5	5	4	5	5	5	5	5	5	5	5	5	5	5	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4	4	4	5
21	1	1	5	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	4
22	2	1	5	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	4
23	2	2	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	4	5
24	2	2	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	4
25	2	2	4	4	4	4	4	5	4	4	4	5	4	5	4	4	4	4	4	5	4	5	4	4	4	4	4	4	4	4	4	5	4	5	4	4	4	4	4	5
26	2	1	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
27	1	2	4	4	5	4	4	5	4	4	4	5	4	5	4	4	4	4	4	5	4	5	4	4	4	4	5	4	4	4	4	5	4	5	4	4	4	4	4	4
28	2	1	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5
29	2	1	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4	5	5	4	4	4	4	4	4	5	4
30	2	1	5	5	5	5	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	5
31	2	1	4	4	5	4	4	4	4	5	4	5	4	5	4	4	4	4	4	4	4	5	4	4	4	4	5	4	4	4	4	5	4	5	4	4	5	4	4	5
32	2	1	5	5	5	5	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	5
33	2	1	4	4	5	4	4	4	4	5	4	5	4	5	4	4	4	4	4	4	4	5	4	4	4	4	5	4	5	4	4	4	4	5	4	4	5	4	4	5
34	2	2	4	4	4	4	5	5	4	4	5	5	5	4	5	5	4	4	5	5	5	4	5	5	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	4
35	2	1	4	4	4	4	5	4	4	4	5	5	4	4	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4	5	4	5	4	4	4	4	4	5
36	2	1	5	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
37	2	1	4	4	5	4	4	4	4	4	4	5	4	5	4	4	5	4	4	4	4	5	4	4	4	4	5	4	4	4	4	5	4	5	4	4	4	4	4	4
38	2	1	4	4	4	5	5	4	5	5	5	5	5	5	5	5	5	5	5	4	4	4	5	5	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5
39	1	1	4	4	4	4	4	4	4	4	4	5	4	5	4	4	4	4	4	4	4	4	4	4	4	4	5	4	5	4	4	4	4	4	4	5	5	5	5	4
40	2	1	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	4	5
41	1	2	4	4	5	4	4	4	4	4	4	5	4	5	4	4	4	4	4	4	4	5	4	4	4	4	5	4	5	4	4	4	4	4	4	5	5	5	5	5
42	1	1	4	4	4	5	5	4	5	5	5	5	5	5	5	5	5	5	5	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4	4	4	5
43	2	1	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	4	5
44	1	1	5	5	5	5	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	5

Encuestado	Sexo	Personal	V1: Ciberseguridad																				V2: Gestión de Tecnologías de la Información																	
							D1			D2						D3							D1						D2						D3					
			I1		I2		I3		I4	I4		I5		I6		I7		I8		I9			I1		I2		I3		I4		I5		I6		I7		I8		I9	
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38
45	2	1	4	4	5	4	4	4	4	5	4	5	4	5	4	4	4	4	4	4	4	5	4	4	4	4	5	4	4	4	4	5	4	5	4	4	5	4	4	5
46	1	1	5	5	5	5	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	5
47	2	1	5	5	5	5	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	5
48	1	1	4	4	5	4	4	4	4	5	4	5	4	5	4	4	4	4	4	4	4	5	4	4	4	4	5	4	4	4	4	5	4	5	4	4	5	4	4	5
49	1	1	5	5	5	5	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	5
50	2	1	5	5	5	5	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	5
51	2	1	4	4	5	4	4	4	4	5	4	5	4	5	4	4	4	4	4	4	4	5	4	4	4	4	5	4	4	4	4	5	4	5	4	4	5	4	4	5
52	2	1	5	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	4
53	2	1	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	4	5
54	2	1	4	4	4	5	5	4	5	5	5	5	5	5	5	5	5	5	5	4	4	4	5	5	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5
55	2	1	5	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	4
56	1	1	5	5	5	5	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	5
57	2	1	4	4	5	4	4	4	4	5	4	5	4	5	4	4	4	4	4	4	4	5	4	4	4	4	5	4	4	4	4	5	4	5	4	4	5	4	4	5
58	1	1	4	4	4	4	5	5	4	4	5	5	5	4	5	5	4	4	5	5	5	4	5	5	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	4
59	1	1	4	4	4	4	5	4	4	4	5	5	4	4	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4	5	4	5	4	4	4	4	4	5
60	2	1	5	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
61	1	1	4	4	5	4	4	4	4	4	4	5	4	5	4	4	5	4	4	4	4	5	4	4	4	4	5	4	4	4	4	5	4	5	4	4	4	4	4	4
62	2	2	4	4	4	5	5	4	5	5	5	5	5	5	5	5	5	5	5	4	4	4	5	5	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5
63	1	1	4	4	4	4	4	4	4	4	4	5	4	5	4	4	4	4	4	4	4	4	4	4	4	4	5	4	5	4	4	4	4	4	4	5	5	5	5	4
64	2	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	4	5
65	1	2	4	4	5	4	4	4	4	4	4	5	4	5	4	4	4	4	4	4	4	5	4	4	4	4	5	4	5	4	4	4	4	4	4	5	5	5	5	5
66	1	2	4	4	4	5	5	4	5	5	5	5	5	5	5	5	5	5	5	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4	4	4	5
67	2	1	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	4	5
68	2	1	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	4	5
69	2	1	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	4	5
70	2	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	4	5
71	2	2	4	4	4	5	5	4	5	5	5	5	5	5	5	5	5	5	5	4	4	4	5	5	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5
72	2	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	4	5
73	1	2	4	4	4	5	5	4	5	5	5	5	5	5	5	5	5	5	5	4	4	4	5	5	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5
74	2	2	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	4	5
75	1	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	4	5
76	1	1	5	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	4
77	2	1	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	4	5
78	1	1	5	5	5	5	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	5
79	2	2	4	4	5	4	4	4	4	5	4	5	4	5	4	4	4	4	4	4	4	5	4	4	4	4	5	4	4	4	4	5	4	5	4	4	5	4	4	5
80	1	2	5	5	5	5	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	5
81	2	2	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	4	5
82	1	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	4	5
83	1	2	4	4	4	5	5	4	5	5	5	5	5	5	5	5	5	5	5	4	4	4	5	5	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5
84	2	1	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	4	5
85	1	1	4	4	4	5	5	4	5	5	5	5	5	5	5	5	5	5	5	4	4	4	5	5	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5
86	2	1	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	4
87	1	2	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	4	5
88	1	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	4	5
89	2	2	5	5	5	5	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	5

Encuestado	Sexo	Personal	V1: Ciberseguridad																				V2: Gestión de Tecnologías de la Información																	
							D1		D2						D3						D1				D2				D3											
			I1		I2		I3		I4		I4		I5		I6		I7		I8		I9		I1		I2		I3		I4		I5		I6		I7		I8		I9	
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38
90	1	2	4	4	5	4	4	4	4	5	4	5	4	5	4	4	4	4	4	4	4	5	4	4	4	4	5	4	4	4	4	5	4	5	4	4	5	4	4	5
91	2	2	4	4	4	4	5	5	4	4	5	5	5	4	5	5	4	4	5	5	5	4	5	5	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	4
92	1	1	4	4	4	4	5	4	4	4	5	5	4	4	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4	5	4	5	4	4	4	4	4	5
93	2	1	5	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
94	1	1	5	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	4
95	1	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
96	2	2	4	4	5	4	4	5	4	4	4	5	4	5	4	4	4	4	4	5	4	5	4	4	4	4	5	4	4	4	4	5	4	5	4	4	4	4	4	4
97	2	2	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5
98	2	2	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4	5	5	4	4	4	4	4	4	5	4
99	2	2	5	5	5	5	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	5
100	2	1	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4	5	5	4	4	4	4	4	4	5	4
101	1	1	5	5	5	5	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	5
102	2	1	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	4	5
103	2	2	5	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	4
104	1	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	4	5
105	2	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
106	1	2	4	4	5	4	4	5	4	4	4	5	4	5	4	4	4	4	4	5	4	5	4	4	4	4	5	4	4	4	4	5	4	5	4	4	4	4	4	4
107	1	2	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5
108	2	2	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4	5	5	4	4	4	4	4	4	5	4
109	1	1	5	5	5	5	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	5
110	2	1	5	5	5	5	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	5
111	1	1	4	4	5	4	4	4	4	5	4	5	4	5	4	4	4	4	4	4	4	5	4	4	4	4	5	4	4	4	4	5	4	5	4	4	5	4	4	5
112	1	2	4	4	4	4	5	5	4	4	5	5	5	4	5	5	4	4	5	5	5	4	5	5	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	4
113	2	2	5	5	5	5	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	5
114	1	2	4	4	5	4	4	4	4	5	4	5	4	5	4	4	4	4	4	4	4	5	4	4	4	4	5	4	4	4	4	5	4	5	4	4	5	4	4	5
115	2	2	5	5	5	5	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	4	5
116	1	2	4	4	5	4	4	4	4	5	4	5	4	5	4	4	4	4	4	4	4	5	4	4	4	4	5	4	4	4	4	5	4	5	4	4	5	4	4	5
117	2	2	4	4	4	4	5	5	4	4	5	5	5	4	5	5	4	4	5	5	5	4	5	5	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	4
118	1	2	4	4	4	4	5	4	4	4	5	5	4	4	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4	5	4	5	4	4	4	4	4	5
119	1	2	5	5	5	5	4	5	5	5	4	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
120	2	1	4	4	5	4	4	4	4	4	4	5	4	5	4	4	5	4	4	4	4	5	4	4	4	4	5	4	4	4	4	5	4	5	4	4	4	4	4	4
121	2	1	4	4	4	5	5	4	5	5	5	5	5	5	5	5	5	5	5	4	4	4	5	5	4	4	4	5	5	5	5	5	5	5	5	5	5	5	5	5
122	2	1	4	4	4	4	4	4	4	4	4	5	4	5	4	4	4	4	4	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	4	5	5	5	5	4
123	2	2	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	4	5	5	4	5

Anexo 6: Autorización de la investigación

UNIVERSIDAD CÉSAR VALLEJO

AUTORIZACIÓN DE LA ORGANIZACIÓN PARA PUBLICAR SU IDENTIDAD EN LOS RESULTADOS DE LAS INVESTIGACIONES

Datos Generales

Nombre de la Organización:	RUC: 20144364059
FUERZA AÉREA DEL PERÚ	
Nombre del Titular o Representante legal:	
Nombres y Apellidos PABLO ROBERTO HUERTAS ESPIRITU	DNI: 43374731

Consentimiento:

De conformidad con lo establecido en el artículo 7º, literal "f" del Código de Ética en Investigación de la Universidad César Vallejo (*), autorizo [x], no autorizo [ ] publicar LA IDENTIDAD DE LA ORGANIZACIÓN, en la cual se lleva a cabo la investigación:

Nombre del Trabajo de Investigación	
LA CIBERDEFENSA Y SU INCIDENCIA EN LA GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN EN LA FUERZA AÉREA DEL PERÚ	
Nombre del Programa Académico: MAESTRÍA DE INGENIERIA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN.	
Autor: Nombres y Apellidos PABLO ROBERTO HUERTAS ESPIRITU	DNI: 43374731

En caso de autorizarse, soy consciente que la investigación será alojada en el Repositorio Institucional de la UCV, la misma que será de acceso abierto para los usuarios y podrá ser referenciada en futuras investigaciones, dejando en claro que los derechos de propiedad intelectual corresponden exclusivamente al autor (a) del estudio.

Lugar y Fecha: Santiago de Surco, 09 de Noviembre del 2022

Firma: _____

P/O del Director General de Educación y Doctrina
El Sub Director General de Educación y Doctrina
Mayor General FAP
TONINO ANNICCHIARICO ONGARO
G-9516185-O

(Titular o Representante legal de la Institución)

(*) Código de Ética en Investigación de la Universidad César Vallejo, artículo 7º, literal "f" Para difundir o publicar los resultados de un trabajo de investigación es necesario mantener bajo anonimato el nombre de la institución donde se llevó a cabo el estudio, salvo el caso en que haya un acuerdo formal con el gerente o director de la organización, para que se difunda la identidad de la institución. Por ello, tanto en los proyectos de investigación como en los informes o tesis, no se deberá incluir la denominación de la organización, pero sí será

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Declaratoria de Autenticidad del Asesor

Yo, VISURRAGA AGUERO JOEL MARTIN, docente de la ESCUELA DE POSGRADO MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "La Ciberdefensa y su incidencia en la Gestión de Tecnologías de la Información en la Fuerza Aérea del Perú, Lima 2022", cuyo autor es HUERTAS ESPIRITU PABLO ROBERTO, constato que la investigación tiene un índice de similitud de 25.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

LIMA, 24 de Enero del 2023

Apellidos y Nombres del Asesor:	**Firma**
VISURRAGA AGUERO JOEL MARTIN **DNI:** 10192325 **ORCID:** 0000-0002-0024-668X	Firmado electrónicamente por: JMVISURRAGA el 24-01-2023 18:46:28

Código documento Trilce: TRI - 0527449

INVESTIGA UCV