ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO

ESCUELA DE POSTGRADO

TESIS

LA CIBERSEGURIDAD ENFOCADA A LOS SISTEMAS INFORMÁTICOS EN LA 5ª BRIGADA DE MONTAÑA, 2022

AUTOR

Bach. José Luis BURGOS VIEYRA
0000-0002-5830-5793

Para optar el Grado Académico de

MAESTRO EN CIENCIAS MILITARES
Con mención en Planeamiento Estratégico y Toma de Decisiones

ASESOR TEMÁTICO
Mg. Adrián CAMACHO SORIANO
0000-0003-1961-9666

ASESOR METODOLOGICO
Dr. Hugo Ricardo PRADO LOPEZ
0000-0003-4010-3517

2023

ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO
ESCUELA DE POSTGRADO

DEPARTAMENTO GESTIÓN DE INVESTIGACIÓN

ACTA DE SUSTENTACIÓN DE TESIS No 001 – 2023/ DGI

En la Escuela Superior de Guerra del Ejército - Escuela de Postgrado, a los diecisiete días del mes de abril del año dos mil veintitrés, siendo las ..10:05.. horas, se reunió el jurado evaluador conformado por los docentes:

❖	**Doctora**	**BERTHA MILAGROS VILLALOBOS MENESES**	**Presidente**
❖	**Maestro**	**ROBERTO JOAQUIN VIVANCO BURGOS**	**Secretario**
❖	**Maestro**	**GABRIELA KATHERINE GALLEGOS CHIARELLA**	**Vocal**

Designados según Resolución de Expedito para Sustentación de Tesis **N° 001-2023/SIE/DGI/ESGE-EPG** del 13 de marzo del 2023, para evaluar la sustentación presencial y defensa de la Tesis de Grado titulada **"LA CIBERSEGURIDAD ENFOCADA A LOS SISTEMAS INFORMÁTICOS EN LA 5ª BRIGADA DE MONTAÑA, 2022"**, presentado por los Bachiller **JOSE LUIS BURGOS VIEYRA**, para optar el Grado Académico de Maestro en Ciencias Militares con mención en Planeamiento Estratégico y Toma de decisiones, de acuerdo a lo establecido en el artículo 45° de la Ley Universitaria N° 30220.

Luego de atender la sustentación presencial, defensa de la tesis de grado y realizadas las preguntas de rigor, el jurado acordó concederle la calificación de ..APROBADO POR MAYORÍA..

En mérito del cual, el jurado ..APRUEBA.. (aprueba / no aprueba) que se le otorgue el Grado Académico de Maestro en Ciencias Militares con mención en Planeamiento Estratégico y Toma de decisiones.

Firmado, en Chorrillos a los diecisiete días del mes de abril del 2023.

DRA. BERTHA MILAGROS VILLALOBOS MENESES	**MG. ROBERTO JOAQUIN VIVANCO BURGOS**	**MG. GABRIELA KATHERINE GALLEGOS CHIARELLA**
PRESIDENTE	**SECRETARIO**	**VOCAL**

Dedicatoria

Esta tesis es dedicada a mi amada esposa Lorena Gomez, por el soporte que siempre me ha brindado para poder concluir con éxito mis estudios.

A mis hijas Alondra y Lucianna, que siempre me han inspirado a ser mejor persona y a ser perseverante en esta carrera de servir a nuestra Patria.

Agradecimientos

A Dios por permitirme cumplir unas de mis anheladas metas, también a mis asesores de tesis, por el apoyo que me ha permitido el desarrollo y culminación de mi trabajo de investigación.

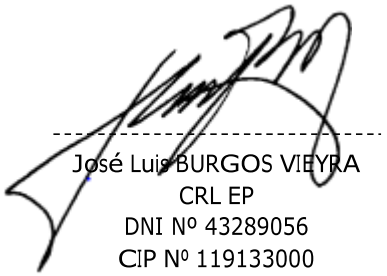
A mi familia por la paciencia y confianza puesta en mí.

Autorización de publicación y uso

A través del presente documento autorizo a la Escuela Superior de Guerra del Ejercito, la publicación del texto completo o parcial de la tesis de grado titulada: La Ciberseguridad Enfocada a los Sistemas Informáticos en la 5ª Brigada de Montaña 2022, presentada para optar el grado académico de Maestro en Ciencias Militares, con mención en Planeamiento Estratégico y Toma de Decisiones en el Repositorio Institucional y en el Repositorio Nacional de Tesis (RENATI) de la SUNEDU, de conformidad al marco legal y normativo vigente. La tesis se mantendrá permanente e indefinidamente en el Repositorio para beneficio de la comunidad académica y de la sociedad. En tal sentido autorizo gratuitamente y en régimen de no exclusividad los derechos estrictamente necesarios para hacer efectiva la publicación, de tal forma que el acceso al mismo sea libre y gratuito, permitiendo su consulta e impresión, pero no su modificación. La tesis puede ser distribuida, copiada, exhibida y usada también con fines académicos siempre que se indique la autoría y no se podrán realizar obras derivadas de la misma.

Dicha investigación no ha sido presentada ni publicada anteriormente por ningún otro investigador ni por el suscrito, para optar otro grado académico ni título profesional alguno. Declaro que se ha citado debidamente toda idea, texto, figura, fórmulas, tablas u otros que corresponde al suscrito u a otro en respeto irrestricto a los derechos del autor. Declaro conocer y me someto al marco legal y normativo vigente relacionado a dicha responsabilidad.

Chorrillos, 28 de noviembre del 2022.



José Luis BURGOS VIEYRA
CRL EP
DNI Nº 43289056
CIP Nº 119133000

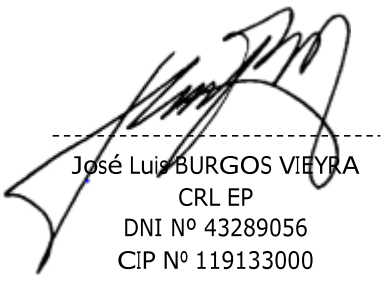
Declaración Jurada de Autoría

Mediante el presente documento, yo José Luis BURGOS VIEYRA, identificado con Documento Nacional de Identidad N° 43289056 con domicilio real Av. Ejercito Nº 214, Santiago – Cusco, egresado de la VI MCM de la Escuela Superior de Guerra-Escuela de Postgrado (ESGE-EPG), declaro bajo juramento que:

Soy el autor de la investigación titulada “LA CIBERSEGURIDAD ENFOCADA A LOS SISTEMAS INFORMÁTICOS EN LA 5ª BRIGADA DE MONTAÑA 2022, que presento a los veintiocho días del mes de noviembre del año 2022, ante esta institución con fines de optar el grado académico de Maestro en Ciencias Militares.

Dicha investigación no ha sido presentada ni publicada anteriormente por ningún otro investigador ni por el suscrito, para optar otro grado académico ni título profesional alguno. Declaro que se ha citado debidamente toda idea, texto, figura, fórmulas, tablas u otros que corresponde al suscrito u a otro en respeto irrestricto a los derechos del autor. Declaro conocer y me someto al marco legal y normativo vigente relacionado a dicha responsabilidad.

Declaro bajo juramento que los datos e información presentada pertenecen a la realidad estudiada, que no han sido falseados, adulterados, duplicadas ni copiados. Que no he cometido fraude científico, plagio o vicios de autoría; en caso contrario, eximo de toda responsabilidad a la Escuela Superior de Guerra – Escuela de Postgrado y me declaro como el único responsable.



José Luis BURGOS VIEYRA
CRL EP
DNI Nº 43289056
CIP Nº 119133000

Índice

Índice de tablas

Índice figuras

Resumen

En la investigación: “La ciberseguridad enfocada a los sistemas informáticos en la 5ª Brigada de Montaña 2022”, el objetivo general consta de analizar la ciberseguridad enfocada a los sistemas informáticos en la 5ª Brigada de Montaña, de igual forma, la Unión Internacional de Telecomunicaciones (2013) define a la ciberseguridad, como los conceptos sobre seguridad, protecciones de seguridad, normas, métodos de gestión de riesgos, ejercicios, prácticas habilidosas y tecnologías que son empleados para proteger los activos de las instituciones y a los usuarios del ciberentorno. Los activos de las instituciones, son los servicios, las aplicaciones, los sistemas de comunicaciones y todas las informaciones gestionadas y almacenada en el ciberentorno. El tipo de esta investigación fue cualitativa, los sujetos de estudio están conformados por los expertos en sistemas informáticos de la 5ª Brigada de Montaña. Como resultado principal, se muestra concordancia en la forma de gestionar los recursos tecnológicos para generar ciberseguridad, dentro de los sistemas informáticos de la 5ª Brigada de Montaña. Donde coinciden las medidas de protección para el empleo del internet, con relación a las que son adoptadas en los sistemas y por los usuarios. Se concluye que los recursos tecnológicos que posee la 5ª Brigada de Montaña ofrecen un alto nivel de ciberseguridad, el cual dispone de componentes seguros para realizar las comunicaciones empleando las conexiones a internet.

PALABRAS CLAVES: *Ciberseguridad, sistemas informáticos, organización.*

Abstract

In the investigation: "Cybersecurity Focused on Computer Systems in the 5th Mountain Brigade 2022", the general objective is to analyze cybersecurity focused on computer systems in the 5th Mountain Brigade, likewise, the International Telecommunications Union (2013) approved a definition of cybersecurity, security concepts, security safeguards, guidelines, risk management methods, actions, training, best practices, insurance, and technologies that can be used to protect organizational assets and users in the cyber environment. The assets of the organization and users are the connected computing devices, users, services/applications, communication systems, multimedia communications, and all the information transmitted and/or stored in the cyber environment. The type of this research was qualitative, the study subjects are made up of the Members of the 5th Mountain Brigade. As a main result, agreement is shown in the way of managing technological resources to generate cybersecurity within the systems of the 5th Mountain Brigade, where they coincide in the assignment of communication components through the Internet and the relationship with users. It is concluded that the technological resources that the 5th Mountain Brigade possesses offer a high level of cybersecurity, which has communication components through an Internet connection, as well as computer systems capable of managing the data they collect, equipment such as Laptops, Servers, Printers, Switch's, Routers and Access Point.

KEY WORDS: *Cybersecurity, computer systems, organization.*

Introducción

El Estado Peruano para vigilar y defender la soberanía nacional, cuenta con las Fuerzas Armadas que tienen el compromiso de proteger la soberanía de nuesta nación, la defensa, integridad e independencia del Estado peruano y garantizar su ordenamiento jurídico.

Para Viollier et al. (2013) la ciberseguridad se ha transformado en un aspecto muy importante en los planes de los gobiernos e instituciones del estado y autónomas, ahora es una política pública que concierne a académicos, compañías, periodistas, políticos y civiles. En la actualidad los ataques informáticos han evolucionado y son más sofisticados y frecuentes. Por lo que, en la actualidad la ciberseguridad pasó a ser un tema relevante para toda la sociedad y tienen un lugar primordial en los modelos de negocios que utilizan la red.

Acurio (2016) sostiene que la rápida evolución de la tecnología, han permitido el incremento de los medios digitales, producto de esta evolución se han ido desarrollando diferentes sistemas interactivos en línea y en tiempo real. Por este motivo, se ha visto la necesidad de añadir y mejorar los elementos de seguridad en los sistemas informáticos, como las contraseñas de identificación de usuarios, con la finalidad de mejorar la seguridad al acceder a los datos.

Es por ello que se presenta esta investigación, con la finalidad de analizar la ciberseguridad enfocada a los sistemas informáticos en la 5ª Brigada de Montaña 2022. Esta investigación tiene como objetivos específicos: Estudiar las vulnerabilidades, amenazas y delitos informáticos que pueden presentarse en la 5ª Brigada de Montaña 2022. Identificar las políticas y normas de ciberseguridad que ha implementado la 5ª Brigada de Montaña 2022. Proponer acciones que se deben realizar en la ciberseguridad enfocada a los sistemas informáticos en la 5ª Brigada de Montaña 2022.

Asimismo, el análisis de los resultados tiene el fin de presentar una propuesta moderna sobre la ciberseguridad enfocada a los sistemas informáticos. Esto implica, observar el actual funcionamiento de los sistemas informáticos, recursos humanos, y otros elementos tecnológicos en la 5ª Brigada de Montaña.

CAPÍTULO I
EL PROBLEMA DE INVESTIGACIÓN

1.1 Planteamiento del problema

En los últimos años, los ataques cibernéticos no solo se centran en motivaciones intelectuales o económicos, sino también en la desestabilización de la seguridad de los países, a fin de generar conflictos armados entre ellos o guerras internas; uno de los primeros ciberataques se presentó en el 2007, cuando estalló la primera guerra cibernética mundial en Estonia, atacando a su parlamento, ministerios, bancos y periódicos; mediante el ataque a sus servidores. El segundo ataque fue en Irán el gusano STUXnet, que fue un programa malicioso que creó copias de sí mismo y se propagó para infectar programas específicos, fue diseñado con la finalidad de poder sabotear el programa nuclear de Irán. Incluso logró infiltrarse en dispositivos protegidos y fuera de línea, que le permitió controlar las centrifugadoras utilizadas para enriquecer el uranio. Este hecho permitió que el desarrollo del programa nuclear de Irán se retrase dos años. Con este ataque se observó por primera vez en la historia, el surgimiento de un malware que fue utilizado como un arma cibernética, que fue capaz de atacar un objetivo industrial.

La 5ª Brigada de Montaña es una organización que también hace uso diario de tecnologías con acceso a internet, las mismas que permiten su empleo en un gran abanico de posibilidades, pues admiten conectar distintos equipos entre sí, que proporcionan información en tiempo real, posibilitando la elaboración de estrategias que reducen los riesgos y aminoran el tiempo de respuesta. Sin embargo, con la expansión de las redes inalámbricas, el almacenamiento, el procesamiento digital, el mejoramiento de las estructuras informáticas, el crecimiento de aplicaciones y análisis de software innovadores; también se incrementan los riesgos de sufrir ciberataques, poniendo en peligro los datos que son gestionados por las redes.

Es preciso mencionar que, aunque los sistemas informáticos incluyan funciones de seguridad, las personas no siempre dedican el tiempo necesario para configurarlos adecuadamente. Las personas dejan para más adelante la configuración de las funciones de seguridad y no son conscientes del riesgo que puede originar desde el punto de vista informático. El caso es que nunca llegan a hacerlo, permitiendo que la seguridad de los dispositivos con acceso a internet pueda ser vulnerable.

En este contexto, la 5ª Brigada de Montaña tiene el potencial de adquirir enormes beneficios al incorporar masivamente la ciberseguridad, adoptar prácticas modernas habilitadas para estas tecnologías. En la actualidad la 5ª Brigada de Montaña, dispone aproximadamente de quinientos sesenta (560) personas, entre el personal de Oficiales, Técnicos, Sub Oficiales y Personal Civil que laboran en las instalaciones del Estado Mayor de la 5ª Brig. Mtñ. y en las unidades de las guarniciones de Cusco y Andahuaylas. Al respecto, para realizar el trámite documentario entre las unidades y el Estado Mayor de la 5ª Brig. Mtñ., aproximadamente ciento noventa (190) personas, del personal que integran los Estados Mayores del Cuartel General y de las unidades, vienen empleando un nuevo sistema informático de tramite documentario, sistema informático que, mediante el empleo de firmas digitales, permite gestionar la documentación que ingresa y sale del Estado Mayor a las Unidades y viceversa. Para tal efecto, el señor Comandante General de la 5ª Brig. Mtñ., los señores coroneles jefes de los estados mayores, el señor coronel inspector, los jefes de sección del estado mayor y los comandantes de las Unidades orgánicas de la 5ª Brig. Mtñ., tienen habilitado la firma digital para su empleo.

Este sistema ha permitido la automatización del trámite documentario, gracias a que se puede acceder a este desde cualquier dispositivo con acceso a internet, como los teléfonos inteligentes, laptop, tablet etc. y se puede tener acceso a toda la documentación recibida y remitida, así mismo permite decretar la documentación, dar indicaciones, y con una lectora de DNI electrónico se pueden firmar los documentos manera digital. También, la 5ª Brig. Mtñ. dispone de una mesa de partes virtual, cuya dirección en la red es de conocimiento de todas las instituciones de la guarnición de Cusco y Apurímac. Por este medio, ingresa gran parte de los documentos remitidos por las instituciones. Asimismo, el personal de las secciones del Estado Mayor también emplea los sistemas de mensajería del instituto, lo que facilita las comunicaciones con otras dependencias.

De acuerdo a lo descrito en los anteriores párrafos, en la 5ª Brigada de Montaña se emplean diariamente durante el manejo de la documentación, las tecnologías de información y comunicaciones, en vista que estas tecnologías facilitan a nuestro instituto la organización y administración de las mismas. Sin embargo, se debe tener en consideración que la documentación que pasa por el sistema de tramite documentario, también queda almacenada en la nube, bajo las medidas de seguridad que brindan las empresas dedicadas a este servicio.

En todos los sistemas informáticos que utiliza la 5ª Brigada de Montaña, es necesario la aplicación de medidas y/o sistemas de ciberseguridad, a fin de reducir y/o eliminar los riesgos de sufrir ciberataques, que podrían permitir la obtención de información valiosa que es gestionada por intermedio de los sistemas de tramite documentario virtuales que recientemente han sido incorporados y que, además, podría poner en riesgo la privacidad de sus usuarios. Por lo que es pertinente plantear esta investigación, puesto que permitirá analizar las medidas de ciberseguridad enfocadas a los sistemas informáticos, que se están empleando en la 5ª Brigada de Montaña 2022.

1.2 Justificación

La rápida evolución de la tecnología ha incrementado la disponibilidad de medios tecnológicos, del mismo modo producto del avance de la tecnología, también han evolucionado las formas de delinquir, en la actualidad los ciberataques ocurren con excesiva frecuencia, ahora son más difíciles de detectar y su investigación es muy compleja.

Por otro lado, se debe tener presente que de acuerdo a las investigaciones realizadas, se tiene conocimiento que el eslabon más débil de la ciberseguridad, son los propios usuarios de los sistemas informáticos, esto es debido a que no dedican el tiempo necesario para realizar las configuraciones de seguridad que les son requeridas, o porque no toman consciencia de las amenazas del ciberentorno, y porque no dan cumplimiento a las normas de seguridad de las organizaciones.

Por esta razón la ciberseguridad ha adquirido mayor importancia en los gobiernos e instituciones, porque permite proteger los sistemas, redes y programas de los ataques online y las ciberamenazas.

Se justifica la presente tesis de metodología cualitativa, debido a que analizó la ciberseguridad enfocada a los sistemas informáticos en la 5ª Brigada de Montaña en el año 2022, mediante la identificación de las vulnerabilidades a las que están expuestos los sistemas informáticos de la 5ª Brigada de Montaña, también se detectaron las ciberamenazas y delitos informáticos a los que está expuesto los sistemas informáticos de la 5ª Brigada de Montaña. Se debe tener en consideración que a medida que se generaliza la tendencia al uso de las herramientas informáticas, plataformas digitales y estos recursos sean más modernos, se hace imperativo implementar mejores sistemas de ciberseguridad.

Como resultado del análisis de los resultados, se pudo presentar una propuesta moderna sobre la ciberseguridad enfocada a los sistemas informáticos de la 5ª Brigada de Montaña. Esto implicó, observar el actual funcionamiento de los sistemas informáticos, recursos humanos, y otros elementos tecnológicos de uso comercial que son empleados en la 5ª Brigada de Montaña. Esta investigación es muy relevante en vista que permitió proponer estrategias de ciberseguridad, con el objetivo de limitar las brechas de seguridad, reducir el riesgo de exfiltración de datos y combatir los ataques cibernéticos en general.

1.3 Delimitación de la investigación

1.3.1 Delimitación temática

La información detallada para el presente trabajo estuvo constituida en base a los datos obtenidos del personal experto de las secciones de los Estados Mayores del Cuartel General de la 5ª Brigada de Montaña y de las Unidades orgánicas. Además, se complementó con la bibliografía relacionada al manejo de la documentación electrónica que es utilizada en el Ejército del Perú y con otras publicaciones referentes al tema en mención.

1.3.2 Delimitación teórica

La presente investigación estuvo enfocada a los sistemas informáticos, se sustentó en base a los conceptos afines con la ciberseguridad que se emplean en la actualidad en la 5ª Brigada de Montaña.

1.3.3 Delimitación espacial

El trabajo se desarrolló en el ámbito de responsabilidad de la 5ª Brigada de Montaña, cuyo sector comprende los departamentos de Cusco y Apurímac.

1.3.4 Delimitación temporal

El trabajo se desarrolló desde el mes de febrero del 2022, hasta el mes de julio del 2022, lapso que permitió culminar la investigación.

1.4 Limitaciones de la investigación

Durante el desarrollo de la presente investigación, la revisión doctrinaria realizada, la ejecución de las entrevistas, la ubicación del estudio, entre otros; no mostró ninguna limitación inherente al tema.

1.5 Formulación del problema

Pregunta principal

¿Cómo es la ciberseguridad enfocada a los sistemas informáticos en la 5ª Brigada de Montaña 2022?

Preguntas específicas:

¿Cuáles son las vulnerabilidades, amenazas, delitos informáticos que pueden presentarse en la 5ª Brigada de Montaña 2022?

¿Qué políticas y normas de ciberseguridad ha implementado la 5ª Brigada de Montaña 2022?

¿Qué acciones se deben realizar frente a la ciberseguridad enfocada a los sistemas informáticos en la 5ª Brigada de Montaña 2022?

1.6 Objetivos de la investigación

Objetivo principal:

Analizar la ciberseguridad enfocada a los sistemas informáticos en la 5ª Brigada de Montaña 2022.

Objetivos específicos:

Estudiar las vulnerabilidades, amenazas y delitos informáticos que pueden presentarse en la 5ª Brigada de Montaña 2022.

Identificar las políticas y normas de ciberseguridad que ha implementado la 5ª Brigada de Montaña 2022.

Proponer acciones que se deben realizar en la ciberseguridad enfocada a los sistemas informáticos en la 5ª Brigada de Montaña 2022.

CAPÍTULO II
MARCO TEÓRICO

2.1 Antecedentes de la investigación

2.1.1 Antecedentes Nacionales

Ormachez (2019) su tesis tuvo como objetivo proponer una estrategia integral de ciberseguridad, debido a que es necesaria para fortalecer la seguridad nacional. Concluye que el país se encuentra en un proceso de concientización de los usuarios y de perfeccionamiento de las capacidades cibernéticas militares, que van a servir de indicadores, para el diseño de las políticas de ciberseguridad en el país.

Rivera (2019) su tesis tuvo el objetivo conocer como los riesgos de ciberseguridad influyen en la incidencia de los fraudes a las compañías industriales del distrito de Yanakancha. Se utilizó el método descriptivo. La población estuvo conformada por los trabajadores de las empresas industriales del distrito de Yanacancha. Se concluyó que en el Perú como un objetivo estratégico se debe aumentar la seguridad del ciberespacio, lo que va a influir en el incremento de la seguridad nacional. Debido a que la culminación de una amenaza en el ciberespacio, tendría repercusiones negativas en muchos aspectos de nuestro país.

Reyes (2018) en su investigación reconoce la existencia de dificultades debido a los retrasos en los trámites documentarios de los gobiernos locales, el objetivo fue implementar un sistema de tramites documentarios vía web que permita gestionar los documentos del gobierno local, con el fin mejorar algunos obstáculos administrativos. El enfoque fue cuantitativo, descriptivo, de diseño no experimental. Los resultados hallados fueron que el 95,00% de la primera dimensión indicó que no estaba satisfecho con su gestión documental actual, y en cuanto a la segunda dimensión el 100% indicó que se debe implementar sistema de tramites documentarios vía web, para mejorar la gestión de la documentación.

Inoguchi (2017) su tesis tuvo el objetivo fue conocer la capacidad de gestión de la ciberseguridad para poder prevenir ciberataques en las PYMES del Perú en el año 2016. Para ello se realizó una metodología cuantitativa y descriptiva de diseño no experimental. Los trabajadores de la Empresa de Transporte Zavala

Cargo S.A.C. fueron seleccionados como muestra representativa. Se concluye que la empresa carece de un plan operativo para afrontar ataques de ciberseguridad y que permitan proteger la información de las empresas.

El Ejercito del Perú (2015) en su Reglamento del Sistema de Telemática, instituye la doctrina general del Sistema de Telemática del Ejército y sirve de guía para los Oficiales que se desempeñan en los diferentes órganos de Telemática, en sus diferentes niveles. Para lo cual ha tenido en consideración los últimos avances en el campo de Telemática y otras Tecnologías de Información. También considera la actual normatividad vigente establecida por la Oficina Nacional de Gobierno Electrónico (ONGEI), del Comando Conjunto de las Fuerzas Armadas y el Ministerio de Defensa. Además, considera la misión asignada a la Dirección de Telemática del Ejército y lo establecido en el Plan Estratégico en Tecnologías de la Información, aprobados por el Comando del Ejército. Este reglamento ha constituido un medio de consulta y ha servido de referencia para la presente investigación.

2.1.2 Antecedentes Internacionales

Matinz (2020) su tesis tuvo como objetivo proponer políticas de ciberseguridad para las instituciones de las Fuerzas Armadas, que permitan incrementar la protección de la información digital, a través de la cooperación y coordinación con otras agencias nacionales que tengan experiencia en ciberseguridad. Esta investigación permitió analizar estándares de seguridad internacionales y políticas de seguridad digital, a través de un análisis legal integrado a nivel nacional en conjunto con varias instituciones, lo que permitió facilitar las coordinaciones interinstitucionales durante la gestión de los riesgos en el ciberespacio. Como conclusión, se formularon lineamientos de ciberseguridad para mejorar la protección de los datos que son tramitados de manera digital, en concordancia a la normativa de algunos Ministerios, que tienen experiencia en la gestión de la ciberseguridad.

Román (2018) el propósito del estudio fue proponer una sistematización de documentos que permita el acceso a todas las personas. Se empleó el enfoque de la investigación mixto cualitativo - cuantitativo. los trabajadores de la alcaldía fueron seleccionados como población. Se concluyó que los gobiernos locales deben realizar inversiones en sistemas que permitan la gestión de documentos, con la

finalidad de brindar un adecuado almacenamiento y conservación de la información, lo que va a permitir la mejora de la gestión administrativa.

Aguirre (2017) su investigación tuvo la finalidad de analizar las estrategias de ciberseguridad del país, en concordancia con las estrategias que son aplicadas por otros países y su relación con la seguridad de las infraestructuras estratégicas del país. Para ello se propusieron controles de ciberseguridad para ser implementadas en las infraestructuras críticas del país. Los controles se definieron en base a buenas prácticas de ciberseguridad que son utilizadas y reconocidas internacionalmente. También se tuvo en cuenta medidas de seguridad destinadas a fortalecer la seguridad informática de las organizaciones públicas y privadas. De esta investigación se llegó a la conclusión que, en el país de Ecuador, las medidas de ciberseguridad son implementadas de manera independiente en cada organización.

2.2 Bases teóricas

2.2.1 Ciberseguridad

la Unión Internacional de Telecomunicaciones (2013) define a la ciberseguridad, como los conceptos sobre seguridad, protecciones de seguridad, normas, métodos de gestión de riesgos, ejercicios, prácticas habilidosas y tecnologías que son empleados para proteger los activos de las instituciones y a los usuarios del ciberentorno. Los activos de las instituciones, son los servicios, las aplicaciones, los sistemas de comunicaciones y todas las informaciones gestionadas y almacenadas en el ciberentorno. Hoy en día los desarrollos tecnológicos alcanzados por la humanidad han permitido que se acorten los trayectos y las velocidades de transmisión de datos, por lo que es pertinente darle la debida seguridad a los datos que son transmitidos por intermedio de la web.

Vargas (2017) en su investigación afirma que la ciberseguridad es un importante campo en la investigación estratégica. Según su análisis, la evolución de las nuevas tecnologías, han permitido el surgimiento de nuevas amenazas en la red, a las que están expuestos todos los equipos informáticos que están conectados a la red. El predominio del desarrollo de la tecnología ha contribuido a la aparición del quinto dominio de la guerra moderna, como una categoría de las operaciones de apoyo.

Según Castro (2015) hoy en día la soberanía de las naciones alrededor del mundo se está viendo vulneradas por los medios tecnológicos a través de los ciberataques que pueden paralizar los sistemas financieros, electrónicos, de comunicaciones y de armas, pudiendo causar un impacto negativo en las infraestructuras críticas. Las vulnerabilidades pueden surgir cuando no existe un equipo de ciberdefensa con capacidad de poder hacer frente de modo exitoso a estas amenazas. Se concluye que, debido al incremento de los riesgos tecnológicos, es pertinente establecer un organismo encargado de la ciberdefensa a nivel nacional, la cual debería estar bajo el comando los institutos armados, cuya responsabilidad sea la de dar protección a las infraestructuras críticas digitales de la nación. Algunos sitios oficiales ya han sido víctimas de hackeos. Por lo que en la actualidad los gobiernos están asignando mayores presupuestos para abordar la posibilidad de una guerra cibernética, lo que va a permitir incrementar la seguridad y soberanía de las naciones.

Vargas (2017) señala que la revolución tecnológica y digital en la actualidad, han incrementado la velocidad de la transmisión de datos e informaciones. Sin embargo, se han incrementado los riesgos en las naciones y sociedades debido a las nuevas formas de ciberataques. En la actualidad, el país ha podido apreciar una gran cantidad de delitos informáticos, en algunos casos se divulga información confidencial de los gobiernos. Ante el surgimiento de actores como los piratas informáticos, la tecnología actual ha desafiado la privacidad y la confidencialidad de nuestros datos, en contraste con los esfuerzos del gobierno por crear una plataforma tecnológica segura, eficaz y transparente. Mejorar la capacidad de vigilancia y respuesta de los sistemas informáticos, es todo un reto en el mundo actual.

2.2.2 Políticas de ciberseguridad

Vargas (2017) en su investigación las define como la disponibilidad de planes que permitan neutralizar los riesgos a la seguridad, o que permiten mantener cierto nivel de seguridad. Lo que va a contribuir a mejorar la protección de la privacidad de los usuarios, durante el empleo de la web.

para Viollier et al. (2013) la ciberseguridad ha ganado una mayor relevancia en los gobiernos e instituciones, pasando a ser un tema de interés que involucra a todas las instituciones públicas y privadas. La creciente sofisticación y frecuencia

de los ataques informáticos a gran escala, es un tema de preocupación en las empresas y del gobierno. Pues es una prioridad para garantizar el buen funcionamiento de las empresas dependientes de la red, por lo que se ha vuelto un tema estratégico para los gobiernos.

2.2.3 Importancia de una política de ciberseguridad

Vargas (2017) afirma que estas políticas son imprescindibles, porque permiten a las instituciones incrementar la seguridad en el ciberespacio, lo que va a permitir que las personas puedan realizar sus actividades con normalidad mientras navegan por la web y promueven la mejora de las medidas de seguridad en los sistemas informáticos y las redes del sector público y privado, especialmente las que permiten el funcionamiento de un país. También, permiten fortalecer la confianza en el personal que hace uso de las redes y ayudan a identificar las amenazas, los riesgos y las vulnerabilidades durante el procesamiento de las informaciones.

2.2.4 Amenazas y vulnerabilidades existentes en el ciberespacio

Rosario (2020) afirma que, en términos de Seguridad y Defensa, las amenazas del ciberespacio representan una nueva área de operaciones militares, uniéndose a las tradicionales áreas físicas (terrestre, marítima, aeroespacial). En la actualidad se le considera como un nuevo campo de las actividades militares, debido a los crecientes avances tecnológicos, así como al incremento de los últimos ciberataques y campañas de desinformación, que buscan la inestabilidad política y el robo de datos e informaciones.

La seguridad nacional puede verse perjudicada por varios elementos, en particular los de carácter geopolítico, tecnológico, económico o social. Además, existen elementos que, sin tener la configuración de una amenaza, pueden incrementar las vulnerabilidades y provocar inestabilidad en las organizaciones, que a la vez también pueden propiciar el origen de otros riesgos.

2.2.5 Análisis de amenazas

Los análisis de amenazas permiten determinar las vulnerabilidades y los riesgos a los que se encuentran expuestos los productos, aplicaciones, redes y su entorno. Para poder analizar una amenaza se requiere conseguir información

relacionado a ella y ser capaz de realizar una exhaustiva evaluación, para que de esta manera se pueda determinar la probabilidad de que esta amenaza se pueda materializar. Algunas de las amenazas existentes en el ciberespacio incluyen:

Conflicto armado. Amenazas y Desafíos a la Seguridad Nacional (2017) expresa que el conflicto armado es una de las amenazas con más probabilidad de afectar a la seguridad nacional, más aún en el actual contexto de tensiones geopolíticas y alteración del orden internacional. La creciente capacidad de la proyección militar de los Estados, en la dimensión del ciberespacio, es una de las tendencias asociadas al incremento de dicha amenaza.

Crimen organizado. Según Threats and Challenges to National Security (2017) el crimen organizado es una amenaza que traspasa fronteras y tiene un formidable potencial para poder desestabilizar a un Estado, en vista que contribuye a su debilitamiento. El crimen organizado se está trasladando al ciberespacio, por ser un nuevo escenario que les permiten realizar sus actividades delictivas, manteniendo el anonimato, debido a la dificultad de poder ubicar a los responsables de estos delitos.

Actividades de espionaje. Threats and Challenges to National Security (2017) señala que los avances tecnológicos han permitido que esta amenaza se pueda adaptar rápidamente, pues brinda muchas posibilidades para poder realizar acciones de espionaje.

El ciberespacio hoy en día tiene un muy significativo rol durante las actividades de espionaje. Las naciones u organizaciones al ser atacadas, brindan acceso a individuos que no tienen autorización, a grandes cantidades de informaciones y datos confidenciales. Esta actividad se puede realizar gracias a la disponibilidad de programas sofisticados. Ante estas actividades ilícitas, es necesario mejorar nuestra capacidad técnica e intelectual, que permita brindar una rápida respuesta ante estas amenazas.

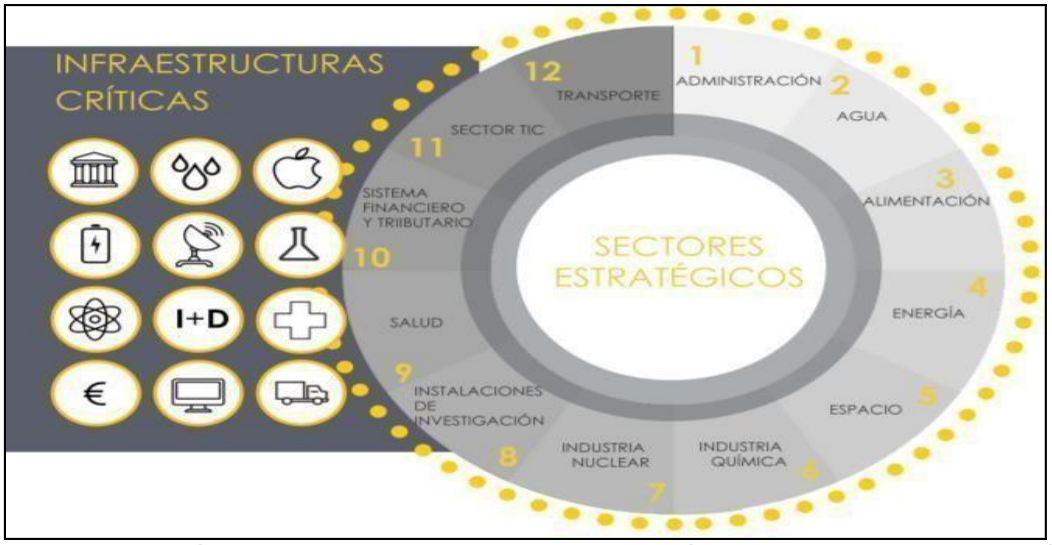
Daño a Infraestructuras críticas. Amenazas y Desafíos a la Seguridad Nacional (2017) se refiere con respecto a las infraestructuras críticas, que son las que tienen un fin estratégico, cuyo funcionamiento es esencial y no son reemplazables con facilidad.

La infraestructura crítica cibernética, es aquella soportada por las tecnologías de las informaciones y comunicaciones, cuya labor permite la prestación de servicios en red, que son esenciales para los usuarios y el Estado.

La infraestructura critica incluye a los sistemas y equipos físicos de comunicaciones, a las redes e instalaciones que permiten la operación de los servicios críticos (Figura 1).

Figura 1

Infraestructuras críticas



Nota. *En el gráfico se aprecia las infraestructuras críticas en los sectores estratégicos. Tomado de Amenazas y desafíos a la seguridad nacional 2017.*

2.2.6 Análisis de vulnerabilidades

El Departamento de Seguridad Nacional (2017) afirma que se debe considerar las crecientes ciberamenazas de la actualidad, para comprender las vulnerabilidades que existen en el ciberespacio.

Los Estados buscan la expansión por sus beneficios geopolíticos, para ello pueden efectuar operaciones ofensivas y subversivas, que son ejecutadas por grupos terroristas que aprovechan el anonimato que les ofrece el ciberespacio, para lograr sus metas, con un menor riesgo, gracias a las dificultades para poder localizar a los criminales por la web.

El análisis de vulnerabilidades permite la identificación y priorización de las debilidades en las aplicaciones y sistemas, con la finalidad de poder realizar una

exhaustiva valoración de las amenazas previsibles, para poder reaccionar rápida y apropiadamente. Los análisis de vulnerabilidades permiten a las organizaciones tener sus entornos más seguros y reducir el riesgo de sufrir ciberataques.

En la actualidad, las actividades ilegales, las acciones de desinformación, la propaganda y el uso del ciberespacio como medio para realizar actividades delictivas organizadas, perturban la seguridad de las naciones e incrementan la inseguridad de las personas y organizaciones (Figura 2).

Figura 2

Vulnerabilidades del ciberespacio.

***Nota**. En el gráfico se muestra las vulnerabilidades del ciberespacio. Tomado de Amenazas y desafíos para la seguridad nacional 2017.*

Las vulnerabilidades pueden ser entendidas como debilidades dentro de los sistemas de seguridad de un entorno, porque crean las condiciones para que una amenaza se pueda materializar. Regularmente, dentro del contexto del ciberespacio las vulnerabilidades pueden ocurrir por mala configuración o por defectos en el software. Para un mejor entendimiento a continuación se describe como se conforma el ciberespacio (Figura 3).

Figura 3

Elementos del ciberespacio

***Nota**. En el gráfico se visualiza como está conformado el ciberespacio. Tomado de Machin 2016.*

2.2.7 Delitos informáticos cometidos en el ciberespacio

Acurio (2016) afirma que la constante evolución tecnológica de la sociedad, también ha permitido la evolución de las formas delictivas, dando lugar a nuevas formas de delincuencia. Las personas capaces de cometer delitos informáticos, no presentan las características de los delincuentes comunes, estos individuos poseen destrezas para la operación de los sistemas informáticos. Generalmente laboran en lugares donde se suele tener a disposición información clasificada.

Según Acurio (2016) es la ejecución de actos realizados utilizando elementos informáticos y/o telemáticos, los cuales vulneran los derechos del titular del ordenador. Esta actividad delictiva emplea una computadora como objeto de la acción criminal.

De acuerdo a Acurio (2016) las principales características de los delitos informáticos son:

- Pocas personas pueden cometerlos.
- Conducta delictiva en la que el sujeto ocupa un determinado estatus socioeconómico, por lo que no puede justificarse su actitud por pobreza, falta de recursos o inestabilidad emocional.
- Muy difíciles de verificar por su carácter técnico.
- Necesita urgente regulación legal por su propensión a proliferar.
- Delitos que son difíciles de probar.

- Acciones rápidas y fáciles. Estos delitos pueden llevarse a cabo en segundos usando solo una computadora y sin estar físicamente presente en la escena del crimen.
- La ciberdelincuencia tiende a aumentar y evolucionar, complicando aún más su identificación y persecución.

Realizar una investigación relacionada a los delitos que ocurren en el ciberespacio, es una labor muy compleja, debido a los autores pueden estar en cualquier lugar del mundo. Estos criminales pueden robar propiedad intelectual e información importante de los organismos estatales o privados y como en la mayoría de los casos las empresas que resultan afectadas no se dan por enteradas de la sustracción.

2.2.8 Sistemas informáticos

Salas (2016) define a los sistemas informáticos como el conjunto de partes interrelacionadas hardware, software que, acompañados del personal técnico en informática, permiten la gestión de las informaciones en el entorno de la web.

Por otro lado, según Lujan (2016) indica que un sistema web es un conjunto de herramientas de ofimática que se notifican empleando protocolos de transferencias de información de hipertextos HTTP, que son los protocolos de transferencia de información que son usados entre las computadoras.

2.3 Categorías y subcategorías

El sistema metodológico empleado fue el resultado de un estudio cualitativo, en el cual se emplean íntegramente las categorías apriorísticas (ver Tabla 1). El estudio permitió evaluar los antecedentes del sistema informático de la 5ª Brigada de Montaña, asi como el comportamiento durante la elaboración de los hechos del problema de investigación.

Asimismo, posteriormente se realizó la triangulación de la información recopilada y se procedió a categorizarlas, las mismas que causaron incidencia en el mismo problema. Como consecuencia de esta actividad, se pretendió contribuir con una propuesta que permitió mejorar la ciberseguridad de los sistemas informáticos de la 5ª Brigada de Montaña.

Tabla 1

Categorías y subcategorías apriorísticas.

OBSERVABLE	OBJETIVOS ESPECÍFICOS	CATEGORÍAS APRIORÍSTICAS	SUB-CATEGORÍAS APRIORÍSTICAS	DEFINICIÓN CONCEPTUAL
Situación de los sistemas informáticos en la 5ª Brigada de Montaña 2022	Estudiar las vulnerabilidades, amenazas y delitos informáticos que pueden presentarse en la 5ª Brigada de Montaña 2022.	Ciberseguridad	• Vulnerabilidades • Ciberamenazas	El Departamento de Seguridad Nacional (2017) afirma que se debe considerar las ciberamenazas, para comprender las vulnerabilidades que existen en el ciberespacio. Las vulnerabilidades pueden provocar inestabilidad en las organizaciones, que a la vez también pueden propiciar el origen de otros riesgos. Las ciberamenazas se refieren al grado de convicción de los Estados y/o empresas, de que las infraestructuras estratégicas, que se encuentran presentes en el ciberespacio, pueden sufrir ciberataques por parte de organizaciones criminales.
	Identificar las políticas y normas de ciberseguridad que ha implementado la 5ª Brigada de Montaña 2022.		• Políticas de ciberseguridad	Vargas (2017) expresa que una política de ciberseguridad es primordial para dar a los usuarios la seguridad que les posibilite realizar sus actividades en la web de modo seguro.

	Proponer acciones que se deben realizar en la ciberseguridad enfocada a los sistemas informáticos en la 5ª Brigada de Montaña 2022.	Sistemas informáticos	• Funcionamiento de la plataforma • Conexiones a la nube	Salas (2016) precisa que los sistemas informáticos son equipos de informática que emplean la conectividad con la web, para acceder a la información a nivel global, para lo cual debe emplear un computador. Para ello la plataforma se encuentran en permanente modernización y actualización. La conexión a la nube permite conectarse a los servicios y aplicaciones disponibles en la nube.

2.4 Definición de términos

Ciberseguridad

la Unión Internacional de Telecomunicaciones (2013) define a la ciberseguridad, como los conceptos sobre seguridad, protecciones de seguridad, normas, métodos de gestión de riesgos, ejercicios, prácticas habilidosas y tecnologías que son empleados para proteger los activos de las instituciones y a los usuarios del ciberentorno. Los activos de las instituciones, son los servicios, las aplicaciones, los sistemas de comunicaciones y todas las informaciones gestionadas y almacenada en el ciberentorno.

Ciberespacio

EcuRed (2012) manifiesta que la palabra Ciberespacio tiene su origen en la palabra griega "CIBERNAO" (pilotear una nave).

El ciberespacio se refiere al universo no físico, y sin límites, donde los usuarios pueden conectarse gracias a una conexión a la red, con inteligencia colectiva, que permite a los usuarios la interacción a nivel global.

Para Stel (2014) el ciberespacio es el nuevo mundo no físico por donde circula el noventa por ciento de las comunicaciones de todo el mundo, haciendo uso de la inteligencia artificial. El ciberespacio permite la interconexión de los sistemas de información.

Ciberamenaza

Teniendo en consideración lo manifestado por Stel (2014) las ciberamenazas se refieren al grado de convicción de los Estados y/o empresas, de que sus infraestructuras estratégicas, que se encuentran presentes en el ciberespacio, pueden sufrir ciberataques por parte de organizaciones criminales.

Ciberdefensa

Conpes (2011) se refiere a la ciberdefensa como la capacidad de respuesta de las organizaciones para poder reducir las vulnerabilidades y los riesgos a las que se encuentran expuestos sus sistemas informáticos.

Ciberguerra

Teniendo en consideración lo manifestado por Cubeiro (2016) define la ciberguerra como el conjunto de operaciones que son empleadas para negar las comunicaciones del adversario. Además, se refiere a las acciones que permiten proteger nuestros sistemas de información y comunicaciones.

Ciberataque

Según Cubeiro (2016) los ciberataques engloban todas las acciones que se realizan por intermedio de las redes informáticas, a fin de negar, impedir o eliminar las informaciones del adversario. Un ciberataque emplea el ciberespacio para causar daños a las infraestructuras críticas de los adversarios.

Hacker

Para Castro (2015), la palabra hacker deriva del vocablo inglés “hack” (cortar, golpear). Este término es empleado para definir a una persona que ha desarrollado conocimientos en el área de informática y pueden desempeñarse extraordinariamente en el tema informático. Emplean sus conocimientos para realizar actividades ilícitas desde un ordenador.

CAPÍTULO III
MÉTODO

3.1 Enfoque de investigación

Como señalaron Blasco y Pérez (2007) el enfoque adoptado fue cualitativo: “La investigación cualitativa extrae e interpreta los fenómenos de acuerdo a sus características. se estudian cómo ocurre" (pág. 25). Por lo tanto, el enfoque cualitativo realiza una investigación basada en lo que realmente sucedió respecto a la ciberseguridad enfocada a los sistemas informáticos en la 5ª Brigada de Montaña.

3.2 Tipo de investigación

La investigación fue un estudio del caso. Referente a los estudios de casos: Yin (2003) manifiesta que este método es una valiosa herramienta de investigación, en vista que permite medir e investigar cómo se comportan las personas involucradas en los fenómenos estudiados.

Dado que el propósito de esta investigación fue comprender una situación fáctica, se consideró utilizar la herramienta de estudio del caso. Debido a que se pretende comprender los hechos desde el punto de vista de los actores comprometidos en la investigación, en este caso el personal que emplea los sistemas informáticos en la 5ª Brigada de Montaña.

Este estudio del caso buscó comprender las vulnerabilidades ante ciberataques a las que estaba expuesta el sistema informático de la 5ª Brigada de Montaña. Debido a que en la actualidad los dispositivos que emplean la conexión a internet, pueden ser rastreados y monitoreados automáticamente por las redes. Por lo tanto, es pertinente examinar las medidas, las salvaguardas, las mejores prácticas, las políticas, las metodologías de gestión de riesgos y las tecnologías que se pueden implementar para mejorar la protección de los activos de la 5ª Brigada de Montaña y los datos de los usuarios en los entornos cibernéticos.

3.3 Método de investigación

El método de investigación empleado fue el interpretativo – hermenéutico. Gadamer (2003) afirma que este método nos permite comprender el significado desde la perspectiva del sujeto y poder realizar estudios del contexto en el que actúan. Este método de trabajo intenta aclarar la relación entre estructuras semánticas y sociales. Permite al investigador comprender el objeto de estudio y las categorías relacionadas con él, para que posteriormente sean analizadas e interpretadas.

3.4 Escenario de estudio

El escenario de estudio donde se desarrolló fue la 5ª Brigada de Montaña cuya sede se encuentra acantonada en la ciudad de Cusco, pero su influencia abarca los departamentos de Cuzco y Apurímac.

3.5 Objeto de estudio

El objeto de estudio fue realizar una innovación en los procedimientos de ciberseguridad, en los sistemas informáticos que actualmente se emplea en la 5ª Brigada de Montaña, los que deben estar acordes con las actuales amenazas, a fin que se incremente la seguridad de las informaciones que se gestionan por intermedio del sistema de tramite documentario de la 5ª Brigada de Montaña.

3.6 Muestra de estudio

La muestras de estudio lo conformaron seis (06) participantes expertos de la 5ª Brigada de Montaña y un (01) ingeniero de sistemas de una empresa particular que tiene conocimiento sobre ciberseguridad. los cuales constituyen una fuente importante de análisis y permitieron presentar una propuesta innovadora sobre los procedimientos para proteger los sistemas informáticos de la 5ª Brigada de Montaña.

3.7 Fuentes de información

Están dadas por entrevistas que se aplicaron a los seis (06) expertos de la 5ª Brigada Montaña y a un (01) ingeniero de sistemas que tiene conocimiento sobre ciberseguridad. Estas fuentes de información constituyen una importante herramienta para el análisis y permitió obtener una propuesta innovadora de los procedimientos de protección para los sistemas informáticos.

3.8 Técnica e instrumentos de acopio de información

Se empleó para el acopio de la información la técnica de la entrevista y la revisión documental. La técnica de la entrevista permitió saber la opinión de cada individuo que fue entrevistado, los mismos que fueron personal calificado en el uso de las redes informáticas. La técnica de revisión documental permitió conocer los aportes doctrinarios y conclusiones de los autores. La revisión de las referencias bibliográficas e investigaciones fueron revisadas con anticipación, permitiendo delinear el objeto de estudio, que permitió disponer de una base teórica de respaldo, que facilitó hacer relaciones entre las investigaciones. La unión de las dos técnicas de investigación, permitió conocer la opinión de los expertos que fueron

entrevistados, sobre los hábitos de empleo de los sistemas informáticos; y la opinión de los autores sobre la ciberseguridad.

3.9 Rigor científico

El rigor científico de la investigación se sostiene en las entrevistas y en la revisión documental, los hallazgos que se han obtenido se muestran en la trascripción de estas, debido a que la muestra elegida son personas que experimentaron el fenómeno estudiado y en base a ello se procedido a realizar el análisis correspondiente para posteriormente poder realizar la interpretación de los datos, mediante el uso y desarrollo de la triangulación, como un mecanismo de contrastación y cruce de información, cuyo encadenamiento permite elaborar una propuesta innovadora. Como sostiene Diaz (2011) la triangulación es parte del rigor científico que permite asegurar la calidad metodológica de una investigación tipo cualitativa.

3.10 Técnica de procesamiento y análisis de datos

Para Yin (2003) un correcto diseño de investigación de tipo cualitativo tuvo 5 partes: Las preguntas de investigación, las proposiciones, si es que tuvieran, la unidad de análisis, los datos unidos en forma lógica con las proposiciones y los criterios presentados para poder interpretar los hallazgos.

Las informaciones fueron analizadas en fases con el siguiente orden:

a. Fase pre-activa. En esta fase se realizó la elaboración de las preguntas, para lo cual se tuvo en consideración el análisis de las categorías y subcategorías analíticas.

b. Fase interactiva. Esta fase incluyó la realización del trabajo de campo, para lo cual se realizaron reuniones con el personal experto de la 5ª Brigada de Montaña, los cuales fueron entrevistados y se les aplicó las evidencias documentales. Aquí también fue muy relevante el proceso de triangulación, la información obtenida fue contrastada con otras fuentes.

c. Fase post-activa. En esta fase se arribó a las conclusiones y recomendaciones de la investigación, para posteriormente proceder a la elaboración del informe final del estudio, donde se hizo una descripción del análisis de carácter crítico sobre el estudio de caso.

CAPÍTULO IV
ANALISIS Y SÍNTESIS

4.1 Recolección de datos

La recopilación de datos fue realizada mediante la aplicación de entrevistas a seis (06) expertos de la 5ª Brigada Montaña, y a un (01) ingeniero de sistemas que tiene conocimiento sobre ciberseguridad. (Ver Anexo 4) Las entrevistas fueron realizadas al personal que se menciona a continuación:

- Un oficial superior del servicio de Ciencia y Tecnología del Ejercito, que se encuentra encargado de la sección telemática.
- Dos ingenieros de sistemas que colaboran con la 5ª Brigada de Montaña en el soporte técnico de los sistemas informáticos, quienes se encuentran calificados en la manipulación de redes y sistemas de informáticos, y tienen conocimientos sobre las normas y disposiciones vigentes referidos a ciberseguridad.
- Tres personal de oficiales del arma de comunicaiones, que se han desempeñado como comandantes de las compañía de comunicaciones de la 5ª Brigada de Montaña, y que tienen conocimiento de telemática y de las medidas de ciberseguridad que deben ser empleadas en los medios tecnológicos que usan el internet.
- Del mismo modo se realizó una (01) entrevista a un ingeniero de sistemas de una empresa privada, el mismo que tiene conocimientos de las medidas de ciberseguridad que se deben adoptar en entornos virtuales. Para lo cual se le ilustró sobre el empleo del sistema de informatico de la 5ª Brig. Mtñ. Para luego de un análisis del mismo, procedió a darnos la intreviste.

Estas fuentes de información permitieron conocer la opinión individual del personal calificado en el uso de las redes informáticas, referente a la situación que se está investigando.

4.2 Organización de datos

Siguiendo a Álvarez-Gayou (2005) la secuencia de la organización de datos cualitativos se realizó de la siguiente manera:

- Primero se obtuvo la información mediante el registro sistemático de las entrevistas abiertas.
- Seguidamente la captura de la información mediante el uso de grabadoras o grabación de las reuniones virtuales mediante el empleo de la Plataforma Zoom.

- Transcripción de la información tal cual ha sido expresada por los participantes, codificando a los participantes siempre manteniendo la anonimia de la opinión vertida.
- Ordenamiento de los datos teniendo en consideración las categorías y las subcategorías establecidas en la investigación.
- Codificación de la información agrupándola de acuerdo a ideas, conceptos y temas parecidos, que se enmarcan en las categorías y las subcategorías.
- Interpretación, para ello se aplicó la técnica de la triangulación que permite contrastar las bases teorías que respaldan la presente investigación, con los hallazgos que fueron obtenidos de manera empírica, que corresponden a las opiniones de los participantes. A partir de ese momento nace un constructo que son los enunciados descriptivos que permitieron llegar a las conclusiones de la investigación.
- Para desarrollar esta actividad lógica de organización, por ser un proceso hermenéutico, cada vez que se revisa la información recopilada, se van enriqueciendo con los hallazgos. Se tuvo en consideración los criterios de coherencia y conciencia de la complejidad, transparencia, autenticidad/credibilidad, perspectiva holística y reflexividad.

Se revisó la información recopilada realizando una reflexión de autocrítica y de la repercusión de las opiniones para las decisiones concluyentes de la investigación. Las entrevistas se transcribieron tal cual fueron expresadas por los participantes, valorando cada una de sus opiniones, manteniendo así la transparencia de la información obtenida. Los individuos interrogados son expertos en el tema, por lo que se tiene credibilidad de sus opiniones. Con la perspectiva holística, el investigador procura en cada momento organizar los datos por ideas y conclusiones. Todo se sistematiza de manera ordenada, analizando las perspectivas y abordaje de la problemática que se analiza. Finalmente se mantiene la coherencia y conciencia del análisis, cruzando la información empírica con la revisión documental.

4.3 Definición de categorías

Los datos recopilados pasaron por un proceso de codificación con la finalidad de ser comprendidos de mejor forma, se hizo un resumen de estos; además, se analizaron cuantitativamente.

Las unidades recopiladas fueron codificadas en secciones y estas se compararon entre sí mismas con la intención de crear grupos por cada tema para encontrar futuros vínculos. En la categorización de primer plano, las unidades fueron identificadas y seccionadas para posteriormente asignarles un código a fin con su sección. Se empleó la comparación constante” como proceso para formular categorías nuevas, asignándoles a

estos diferentes códigos. Luego de ello, se evaluó si la categorización y la asignación de códigos iban a satisfacer las necesidades que se requieren para poder realizar la interpretación de los datos.

Fueron seleccionados por segmentos que tenían las mismas características y significados, asignándoles un código. Con respecto a los diferentes segmentos, fueron colocados en otras secciones, asignándoles códigos diferentes. Estos se tomaron como unidades luego de obtener un significado y cuando su esencia apareció en los datos recolectados, se convirtieron en categorias.

Tabla 2
Unidades del estudio

Nombre del estudio	Participantes	Método de recolección de los datos	Ejemplos de unidades (Línea)
La ciberseguridad enfocada a los sistemas informáticos en la 5ª Brigada de Montaña, 2022	Expertos en informática de la 5ª Brigada Montaña.	Entrevistas Revisión documental.	"Equipos de informática se encuentran conectados a la red de datos de la 5ª Brigada de Montaña". "Los equipos conectados al internet son vulnerables a un ataque informático". "Uso de firewall y otros programas informáticos de seguridad, limitaría a que agentes externos maliciosos roben información y vulneren nuestros sistemas informáticos". "Determinar políticas de ciberseguridad, analizar, valorar riesgos y sus alternativas para reducirlos, definir controles de seguridad".

Los segmentos o unidades se analizaron empleando las palabras de los participantes.

4.3.1 Descripción de Categorías

Se generaron tres probables categorías para el análisis, teniendo como referencia la información de la Tabla 2. A continuación, se muestran las categorías de estudio (Tabla 3).

Tabla 3

Categorías del estudio

Nombre del estudio	Participantes	Método de recolección de los datos	Categorías
La ciberseguridad enfocada a los sistemas informáticos en la 5ª Brigada de Montaña, 2022	Expertos en informática de la 5ª Brigada Montaña.	Entrevistas Análisis documental.	Conexión segura de los equipos informáticos. Política de seguridad y protección de datos frente a las vulnerabilidades y ciberamenazas. Utilización de programas informáticos para protección de datos.

Se analizaron las unidades o segmentos de la Tabla 2; siendo las categorías obtenidas:

- Conexión segura de los equipos informáticos.
- Política de seguridad y protección de datos frente a las vulnerabilidades y ciberamenazas.
- Utilización de programas informáticos para protección de datos.

Las mismas que coinciden con las categorías y subcategorías apriorísticas que se habían delimitado al inicio de esta investigación.

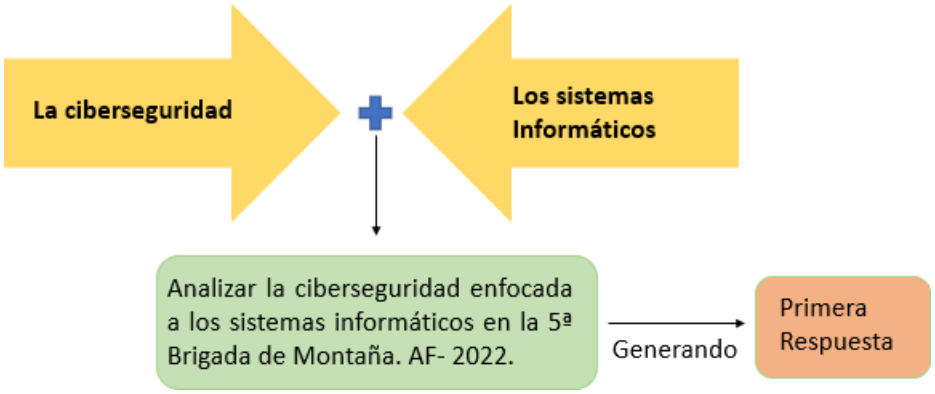
4.4 Soporte de categorías

Tabla 4
Soporte de las categorías del estudio

Tema	Categorías nuevas a raíz de la investigación	Patrones	Descripción
La ciberseguridad enfocada a los sistemas informáticos en la 5ª Brigada de Montaña, 2022	Conexión segura de los equipos informáticos.	Equipos de informática conectados a la internet.	Implementación de equipamiento seguro conectado al internet.
		Equipos utilizados son las computadoras, celulares y tablets.	Establecer los equipos de conexión a la información con contraseñas seguras.
	Política de seguridad y protección de datos frente a las vulnerabilidades y ciberamenazas.	Existencia de softwares maliciosos y hackers.	Protección de la información ante los ataques cibernéticos.
		Cada vez es más frecuente los ataques cibernéticos.	Actualización de contraseñas seguras.
		Acceso desde dispositivos externos.	Evitar el acceso desde dispositivos externos.
		Necesidad de un sistema de alertas.	Instalación de sistemas de alarmas.
		Necesidad de acciones frente a las amenazas cibernéticas.	Establecer normas y políticas de ciberseguridad.
	Utilización de programas informáticos para protección de datos.	Necesidad de personal especialista en sistemas informáticos y ciberseguridad.	Formación de personal especialista en sistemas informáticos y ciberseguridad.
		Se necesita sistemas de detección de anomalías.	Implementación de sistemas de detección de anomalías.
		Falta de sistemas de seguridad y de equipamiento.	Adquisición de equipamiento con sistemas de seguridad actualizados.
		Falta de adiestramiento a los usuarios sobre ciberseguridad.	Capacitación al personal en la ciberseguridad.
		Ausencia de mantenimiento frecuente del sistema informático.	Establecimiento del mantenimiento frecuente del sistema informático.

4.5 Red semántica

Figura 4
Red semántica



***Nota**. El gráfico representa la interacción entre las categorías de estudio.*

4.6 Triangulación

Tabla 5
Triangulación de la información recopilada

CATEGORIA	HALLAZGO EMPIRICO (RESULTADO DE LAS ENTREVISTAS)	REVISIÓN DOCUMENTAL	SINTESIS INTEGRATIVA
Categoría 1 Conexión segura de los equipos informáticos	De la presente investigación, se corrobora que todos los equipos informáticos conectados a los sistemas de la 5ª Brig. Mtñ. están conectados a una red LAN física, como es el caso de la Comandancia y Estados Mayores de las unidades, a través de un punto de internet; tal es el caso de las Computadoras, Laptops, Servidores, Switch's, Routers y Access Point.	UIT (2020) define a la ciberseguridad, como los conceptos sobre seguridad, protecciones de seguridad, normas, métodos de gestión de riesgos, ejercicios, prácticas habilidosas y tecnologías que son empleados para proteger los activos de las instituciones y a los usuarios del ciberentorno. Los activos de las instituciones, son los servicios, las aplicaciones, los sistemas de comunicaciones y todas	De acuerdo con el presente hallazgo, se muestra concordancia en la forma de gestionar los recursos tecnológicos para generar la ciberseguridad dentro de los sistemas de la 5ª Brigada de Montaña, donde coinciden en la asignación de componentes de comunicaciones mediante internet y la relación con los

		las informaciones gestionadas y almacenada en el ciberentorno	usuarios. Asimismo, se menciona que los datos recopilados por los sistemas informáticos funcionan como su recurso más valioso.
Categoría 2 Políticas de seguridad y protección de datos frente a las vulnerabilidades y ciberamenazas.	En la identificación, las políticas que pueden implementarse son el uso de firewall, VPN´s, acceso monitoreado y autorizado solo por el administrador a los usuarios que necesite la 5ta Brig. Mtñ. Ademas, la mayoría piensa una de las medidas más importantes que contribuyen a las medidas de seguridad en cualquier red informática es la concientización y capacitación del personal en todos los niveles, incidiendo bastante en el nivel usuario. Con respecto a las contraseñas, estas son creadas por el administrador del SETEL, con el fin de incrementar la seguridad. Según normas y disposiciones el mantenimiento a los equipos vinculados a la informática es en forma periódica.	Viollier et al. (2013) La ciberseguridad ha ganado una mayor relevancia en los gobiernos e instituciones, pasando a ser un tema de interés que involucra a todas las instituciones públicas y privadas. La creciente sofisticación y frecuencia de los ataques informáticos a gran escala, es un tema de preocupación en las empresas y gobiernos, pues es una prioridad garantizar el buen funcionamiento de las empresas dependientes de la red, por lo que se ha vuelto un tema estratégico para los gobiernos.	Como refieren los entrevistados, las políticas y normas son muy importantes para reducir los ataques y vulneraciones en los sistemas de información. Asimismo, los hallazgos muestran que, al ser un factor importante dentro de cualquier modelo de negocios de una empresa actual, es pertinente actualizar las políticas de ciberseguridad que permitan a la 5ta Brig. Mtñ. Reducir las vulnerabilidades de su sistema informarico. Asimismo, es importante remarcar que, el interés público es un rol necesario para generar conciencia acerca de esta problemática.

Categoría 3 Utilización de programas informáticos para la protección de datos.	Asimismo, la mayoría manifiesta que ningún sistema es 100% seguro; por lo que siempre estamos alertas ante cualquier ataque cibernético. Asimismo, las posibles amenazas son hackers, crackers, ransomware, virus, gusanos y troyanos. Por otro lado, siempre existe la probabilidad de que un sistema sea vulnerado; entonces, lo importante aquí es el tiempo de resiliencia que se tiene, para poder sobreponerse y recuperar el control de nuestro sistema. En sí, la seguridad es un componente clave en todo sistema, no puede existir un sistema en producción sin el componente de seguridad, porque estarían exponiendo los datos de la empresa al alcance de todos.	El Departamento de Seguridad Nacional (2017) menciona que, para comprender las vulnerabilidades, es necesario considerar lo relativo a las ciberamenazas. Existen varios campos de defensa para proteger los sistemas informáticos, estos cubren segmentos particulares y son los siguientes: Firewalls, antivirus, Antispyware y Confidencialidad. Considerar estas líneas de defensa permite incrementar la ciberseguridad.	Nadie está exento completamente de ataques informáticos, ambos se refieren a las ciber amenazas como una problemática que burla la seguridad de los sistemas informáticos, haciendo que personas o entidades puedan acceder a los datos de la empresa. También, se comparten descripciones de los ataques como ransomware y los hackeos a los sistemas e infraestructuras que son vulneradas, tomando el control de los sistemas de forma temporal.
Categoría 4 Proponer acciones para proteger los sistemas informáticos.	No obstante, los participantes coincidieron en que es posible implementar y mejorar el sistema, para lo cual deben solicitar el presupuesto necesario para que se haga efectivo. De igual forma, para realizarse la	La seguridad de las informaciones tiene la finalidad de protegerlas, por la relevancia especial que tienen dentro de un contexto determinado, garantizar su seguridad es de mucha importancia para las organizaciones e instituciones públicas y	De forma concisa, en el caso de proponer medidas para gestionar la ciberseguridad enfocada en los sistemas informáticos, se relacionan a la idea de proteger la

	configuración de la seguridad se debe tener en cuenta la disposición de un Firewall bien configurado y actualizado, actualizar los sistemas operativos de los dispositivos electrónicos que serán empleados para abrir los sistemas informáticos, y disponer de contraseñas robustas por parte de los usuarios.	privadas. Por lo que es pertinente desarrollar proyectos de seguridad informática, que contengan medidas técnicas, organizativas y legales que garanticen la disponibilidad, integridad y accesibilidad a las informaciones.	información y sistemas del atacante, ello puede darse mediante un Firewall bien configurado, y concientizando a los usuarios para que actualicen sus configuraciones y emplear contraseñas más robustas.

CAPÍTULO V
DIALOGO TEÓRICO – EMPÍRICO

5.1 En relación al objetivo general

De acuerdo al objetivo general: Analizar la ciberseguridad enfocada a los sistemas informáticos en la 5ª Brigada de Montaña 2022, la Unión Internacional de Telecomunicaciones (2020) define a la ciberseguridad, como los conceptos sobre seguridad, protecciones de seguridad, normas, métodos de gestión de riesgos, ejercicios, prácticas habilidosas y tecnologías que son empleados para proteger los activos de las instituciones y a los usuarios del ciberentorno.

Al respecto, se muestra concordancia en la forma de gestionar los recursos tecnológicos para generar ciberseguridad en los sistemas informáticos de la 5ª Brigada de Montaña. Teniendo en consideración las referencias bibliográficas que fueron consultadas, referentes a las medidas de ciberseguridad que debe adoptar el personal encargado del funcionamiento del sistema de tramites documentario de la 5ª Brigada de Montaña y las medidas de seguridad que deben adoptar los usuarios de dicho sistema.

5.2 En relación con el objetivo específico 1

De acuerdo con el objetivo específico 1: Estudiar las vulnerabilidades, amenazas y delitos informáticos que pueden presentarse en la 5ª Brigada de Montaña 2022. Se tiene la opinión del Departamento de Seguridad Nacional (2017) que afirma que se debe considerar las crecientes ciberamenazas de la actualidad, para comprender las vulnerabilidades que existen en el ciberespacio. En la actualidad los Estados buscan la expansión territorial por sus beneficios geopolíticos, para ello pueden efectuar operaciones ofensivas y subversivas, que son ejecutadas por grupos terroristas que aprovechan el anonimato que les ofrece el ciberespacio, para lograr sus metas con un menor riesgo, por la dificultad de poder localizar a los criminales que emplean la web para sus actividades delictivas.

Con respecto a lo mencionado por Rosario (2020) quien afirma que referente a la seguridad y defensa, en la actualidad las ciberamenazas representan una nueva área de operaciones militares, uniéndose a las tradicionales áreas físicas (terrestre, marítima, aeroespacial). Esta consideración como campo de la actividad militar se debe a la creciente importancia de los avances tecnológicos, así como al incremento de los últimos ciberataques y campañas de desinformación, dirigidas fundamentalmente a causar inestabilidad política y el robo de datos e información.

En la actualidad, el sistema informático de la 5ª Brigada de Montaña no está exento a las las ciberamenazas, en vista que estas son un riesgo que burla la seguridad de los sistemas informáticos, y permiten que personas no autorizadas o entidades puedan acceder a los datos de nuestra institución. Además, a pesar de las medidas de ciberseguridad que fueron adoptadas, existe la posibilidad que poder ser víctimas de ataques ransomware y hackeos a nuestros sistemas o infraestructuras críticas, lo que ocasionaría que el personal no autorizado pueda tomar el control de los sistemas informáticos en forma temporal y tenga acceso a la información que es tramitada por dicho sistema.

5.3 En relación al objetivo específico 2

De acuerdo con el objetivo específico 2: Identificar las políticas y normas de ciberseguridad que ha implementado la 5ª Brigada de Montaña 2022. Sobre ello, Viollier, et al. (2013) comenta que, La ciberseguridad ha ganado una mayor relevancia en los gobiernos e instituciones, pasando a ser un tema de interés que involucra a todas las instituciones públicas y privadas. La creciente sofisticación y frecuencia de los ataques informáticos a gran escala, es un tema de preocupación en las empresas y gobiernos. Pues es una prioridad para garantizar el buen funcionamiento de las empresas dependientes de la red, por lo que se ha vuelto un tema estratégico para los gobiernos.

En adición, Vargas (2017) sostiene en su investigación las importancia de disponer de planes que permitan neutralizar los riesgos de seguridad y que permiten mantener cierto nivel de seguridad. Lo que va a contribuir a mejorar la defensa de la privacidad de los usuarios durante el empleo de la web.

Tras recopilar información referente al cumplimiento de las normas y políticas sobre ciberseguridad, se pudo apreciar que los usuarios del sistema de tramite documentario de la 5ª Brig. Mtñ, dan cumplimiento a las normas de ciberseguridad que ha implementado la 5ª Brigada de Montaña, lo que ha permitido que todos los usuarios incrementen la seguridad de los datos e informaciones que gestionan, generan y procesan por las redes, por medio de las computadoras, dispositivos móviles y servidores. Se puede apreciar de acuerdo a los hallazgos, que gracias a ello se ha incrementado los estándares de ciberseguridad y ha permitido minimizar los riesgos de un ataque digital.

5.4 En relación con el objetivo específico

De acuerdo con el objetivo específico 3: Proponer acciones que se deben realizar relacionado a la ciberseguridad enfocada a los sistemas informáticos en la 5ª Brigada de Montaña 2022. Según Vargas (2017) afirma que las políticas de ciberseguridad son imprescindibles, porque permiten a las instituciones incrementar la seguridad en el ciberespacio, lo que va a permitir que las personas puedan realizar sus actividades con normalidad mientras navegan por la web y promueven la mejora de las medidas de seguridad en los sistemas informáticos y las redes del sector público y privado.

Como refieren los entrevistados en el caso de proponer medidas para gestionar la ciberseguridad enfocada en los sistemas informáticos, estas medidas permitirán mejorar la protección de las informaciones que se gestionan por intermedio del sistema de tramite documentario de la 5ª Brigada de Montaña.

Igualmente, de acuerdo con Castro (2015) hoy en día la soberanía de las naciones alrededor del mundo se está viendo vulneradas por los medios tecnológicos a través de los ciberataques que pueden paralizar los sistemas financieros, electrónicos, de comunicaciones y de armas, pudiendo causar un impacto negativo en las infraestructuras críticas. Las vulnerabilidades pueden surgir cuando no existe un equipo de ciberdefensa con capacidad de poder hacer frente de modo exitoso a estas amenazas. Por lo que es fundamental contar con un Comando de Ciberdefensa que permita incrementar la seguridad de la infraestructura critica digital de la 5ª Brigada de Montaña, en vista que de no contar con personal calificado, se corre el riesgo de la aparición de vulnerabilidades tecnológicas.

En este momento, ya se dio el caso que varias páginas oficiales de la institución en estudio fueron hackeadas, lo que puso al descubierto información clasificada. En ese contexto, resulta pertinente la asignación de un mayor presupuesto, para poder invertir en mejorar las medidas de ciberseguridad que permitan reducir el riesgo de posibles ciberataques.

Luego del análisis de las encuestas teniendo en consideración los objetivos trazados para el presente trabajo de investigación, a fin de incrementar la ciberseguridad de los sistemas informáticos de la 5ª Brigada de Montaña, se propone lo siguiente:

a. Con respecto a las políticas y normas relacionadas al manejo de los sistemas informáticos, se debe tener en consideración el empleo de las siguientes normas:
   - ISO 27000: Gestión de la Seguridad de las Informaciones.

- ISO 27001: Requisitos del sistema de gestión de seguridad de la información.
- ISO 27002: Es una guía de buenas prácticas y recomendables en cuanto a seguridad de las informaciones.
- ISO 27005: Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

b. Implementación de los siguientes sistemas de seguridad:
   - Servidores de Datos, que permitan separar la base de datos de las aplicaciones e independizar el servidor de datos en una zona DMZ .
   - Empleo de un Firewall que emplee seguridad por capas (seguridad del perímetro (red), seguridad del dispositivo, seguridad de las aplicaciones y seguridad de los datos. Cada capa dispone de un conjunto de protocolos, equipos y técnicas de seguridad y deben ser capaces de identificar y controlar las aplicaciones, autenticación de los usuarios, protección contra exploits, filtrado de contenido (incluido el filtrado de URL) y control de acceso basado en la ubicación, protección contra malware.
   - Se debe considerar el empleo de un sistema criptográfico asimétrico, desarrollado por el Ejército (con un método propio), en las redes que comprenden la comunicación con el escalón superior y con las Unidades subordinadas, las mismas que impidan el acceso a nuestras informaciones a personas no autorizadas.
   - Implementación de doble factor de autenticación para ingresar al sistema, que da una seguridad adicional a los usuarios que la emplean.
   - Implementación de una red privada virtual (VPN). Para poder acceder a la red de la 5ª Brig. Mtñ. que permite a los administradores abordar los problemas de seguridad, garantizando que solo los usuarios autorizados tengan acceso a los recursos corporativos. Ademas, asegura la confidencaialidad e integridad de la información, evita que sea modificada y/o alterada, lo que incrementa la ciberseguridad de los sistemas.

c. También se debe tener en consideración las siguientes medidas:
   - Coordinar con la DIE - DITELE sobre la implementación de medidas de seguridad que son necesarias de acuerdo a nuestras necesidades, a fin de obtener su opinión técnica. En vista que para el tráfico de esta información se debe usar varias capas de seguridad como el cifrado.
   - Contar con un adecuado Plan de Contingencia que haya identificado los procesos críticos, que evalue los recursos utilizados en las operaciones y haya especificado

los escenarios donde pueden ocurrir problemas, a fin de determinar medidas preventivas y planes de acción.

- Programar charlas de ciberseguridad a fin de concientizar y capacitar al personal que emplea los sistemas informaticos, incidiendo bastante en el nivel usuario.
- Implementar funciones de supervisión, generación de informes y alertas de eventos de seguridad a los sistemas informáticos.
- Contar con un plan de verificación del cumplimiento de las normas de seguridad, para los usuarios de los sistemas informáticos.
- Exigir y verificar el uso de claves robustas y el cambio de las mismas en un tiempo prudencial (06 meses).
- Implementar funciones de supervisión, generación de informes y alertas de eventos de seguridad, a los sistemas informáticos.
- Migrar del proveedor de servicios de nuve actual al AWS, Google Cloud o AZURE, que tienen mayor respaldo y seguridad.

d. Con respecto a la plataforma Linux que es la que se emplea actualmente en el Sistema de Tramite documentario de la 5ª Brigada de Montaña, nos permite un grado de seguridad adicional. Asimismo, los servidores en el data center del Ejercito funcionan bajo la misma plataforma Linux, lo que nos permite integrarnos fácilmente a la red del Ejercito.

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Primera: De acuerdo al objetivo general: Analizar la ciberseguridad enfocada a los sistemas informáticos en la 5ª Brigada de Montaña 2022, esta investigación ha encontrado que los recursos tecnológicos que posee la 5ª Brigada de Montaña ofrecen un alto nivel de ciberseguridad, el cual posee componentes de comunicación mediante conexión a internet, así como también posee sistemas informáticos capaces de gestionar los datos que recopilen, equipos como Laptops, Servidores, Impresoras, Switch's, Routers y Access Point.

Segunda: De acuerdo al objetivo específico 1: Estudiar las vulnerabilidades, amenazas y delitos informáticos que pueden presentarse en la 5ª Brigada de Montaña 2022, la investigación ha encontrado que en efecto, los sistemas informáticos de la 5ª Brigada de Montaña no están exentos de vulnerabilidades, debido a que con el paso del tiempo la tecnología va avanzando y con ello aparecen nuevas amenazas que buscan vulnerabilidades en los sistemas informáticos, para que entidades o personas sean capaces de filtrar o alterar los datos de la misma, mediante una gran gama de herramientas (virus, gusanos, troyanos, entre otros).

Tercera: De acuerdo al objetivo específico 2: Identificar las políticas y normas de ciberseguridad que ha implementado la 5ª Brigada de Montaña 2022, de acuerdo a lo recabado, se valida que la mejor forma de protegerse de las amenazas virtuales, es implementando un correcto sistema de políticas y normas capaces de reducir la vulnerabilidad, a su vez que permita brindar opciones de qué hacer en caso de que la información de la 5ª Brigada de Montaña sea vulnerada, así como brindar equipos vinculados a la informática que realicen sostenimiento a los sistemas de información de manera periódica.

Cuarta: De acuerdo al objetivo específico 3: Proponer acciones que se deben realizar en la ciberseguridad enfocada a los sistemas informáticos en la 5ª Brigada de Montaña 2022, demuestra que el equipo informático en la 5ª Brigada de Montaña ofrece una configuración de la seguridad donde se debe tener en cuenta la disposición de un Firewall bien configurado, se deben actualizar los sistemas operativos de los dispositivos electrónicos y capacitar a los usuarios para permitir el cambio de contraseñas a nuevas que posea un mayor nivel de seguridad.

Recomendaciones

Primera: Se recomienda a la 5ª Brigada de Montaña implementar una propuesta de recursos tecnológicos que estén a la par de los últimos avances de la tecnología, que contribuyan a mejorar el funcionamiento de sus sistemas informáticos, como son los servidores de datos, firewall de seguridad, cifradores de datos, entre otros.

Segunda: La 5ª Brig. Mtñ. debe implementar tecnologías de nivel avanzado que permitan evitar ser vulnerables frente a las diversas amenazas que actualmente existen en el ciberespacio, evitando que se filtren los datos que se manejan. A través de la implementación de una VPN, y habilitación de la doble autenticación para ingresar al sistema.

Tercera: La 5ª Brigada de Montaña debe tener un sistema de políticas y normas relacionados al manejo de los sistemas informáticos, que incida en la protección de datos frente a los posibles daños cibernéticos. Utilizando las normas ISO 27000: Gestión de la Seguridad de las Informaciones, ISO 27001, ISO 27002, ISO 27003, ISO 27004, ISO 27005, ISO 27006, ISO 27007.

Cuarta: La 5ª Brigada de Montaña debe tener sistemas operativos de alto nivel que permitan la protección y seguridad de la información que manejan, como la implementación del Unix y Linux. Asi mismo, se recomienda que implemente sus sistemas con un proveedor de nube wordclass, que permita minimizar los riesgos de ciberataques. Migrar a los servicios de Azure, AWS. Google cloud.

Referencias bibliográficas

Acurio, S. (2016). *Delitos Informáticos. Universidad de Guadalajara*. http://148.202.167.116:8080/xmlui/bitstream/handle/123456789/599/Delitos%20Inform%c3%a1ticos.%20generalidades.pdf?sequence=1&isAllowed=y

Aguirre, A. (2017). *Ciberseguridad en Infraestructuras Críticas de Información*. Universidad de Buenos Aires 2017.

Álvarez-Gayou, J.L. (2005). *Cómo hacer investigación cualitativa. Fundamentos y metodología*. México: Paidós.

Arias, M. (2017). *Aprender programación web con PHP y MySQL*. 2da Edición, IT, Campus Academy.https://books.google.com.pe/books?id=mP00DgAAQBAJ&printsec=frotcover&hl= es#v=onepage&q&f=false.

Blasco, J. y Pérez, J. (2007). *Metodologías de investigación en educación física y deporte: Ampliando horizontes*. Alicante, España. Editorial Club Universitario. Imprenta Gamma.

Reyeso, M y Guzmán F. (2019). *Sistema web para la mejora de gestión administrativa de los laboratorios de cómputo en la Universidad Nacional de Trujillo*. Tesis pregrado.

Castro, E. (2015). *Estudio prospectivo de la ciberdefensa en las Fuerzas Armadas del Ecuador.* http://repositorio.espe.edu.ec/handle/21000/11583.

Clark, J. (2016). *Google Cuts Its Giant Electricity Bill With DeepMind- Powered AI.* Technology, Bloomberg, 19 July 2016 https://www.bloomberg.com/news/articles/2016-07-19/google-cuts-its- giant-electricity-bill-with-deepmind-powered-ai.

Conpes 3701. (2011). *Lineamientos de política para ciberseguridad y ciberdefensa*. https://www.mintic.gov.co/portal/604/articles- 3510_documento.pdf.

Cortez, R. (2018). *Implementación de sistema web de trámite documentario y gestión*

documental para Petroperú. Tesis pre grado. Universidad San Ignacio de Loyola.

Cubeiro, E. (2016). *Conceptos Fundamentales de Inteligencia*. Valencia: Tirant loBlanch Schmitt, M. (2013). http://www.collaboratory.de/images/4/4b/TallinnManual-on-the- International-Law-Applicable-to-Cyber-Warfare-Draft-.p.

Deléchamp, F. y Laugié, H. (2016). *Java y Eclipse Desarrolle una aplicación con Java y Eclipse.* Ediciones ENI.

Departamento de Seguridad Nacional (2017). *Estrategia de Seguridad Nacional 2017.*https://www.dsn.gob.es/es/estrategiaspublicaciones/estrategias/estrategia-seguridad-nacional-2017.

Diaz, C. (2011). *Tácticas para asegurar la calidad metodológica*. Pontificia Universidad Católica del Perú. http://blog.pucp.edu.pe/item/34744/tacticas-para-asegurar-la-calidad-metodologica-en-lainvestigacion-cualitativa.

EcuRed. (2012). *EcuRed*. https://www.ecured.cu/Ciberespacio.

Ejercito del Perú (2015). *Reglamento RE 42 – 1, Sistema de Telemática*. Ejercito del Perú.

Heurtel, O. (2014). *PHP y MySQL*. Barcelona: Ediciones ENI. 4ta edición.

Inoguchi, A. (2017). *Gestión de la Ciberseguridad y Prevención de los Ataques Cibernéticos en las Pymes del Perú, 2016*. Universidad San Ignacio de Loyola. https://repositorio.usil.edu.pe/items/9449a061-bfd2-4ecc-8cf1-770fba7cee45.

Luján, J. (2016). *HTML, CSS Y JAVASCRIPT, crea tu web y apps con el estándar de desarrollo.* RC Libros. Colombia.

Martínez, P. (2020) *Propuesta de una Política de Ciberseguridad. Universidad de las Fuerzas Armadas.* http://repositorio.espe.edu.ec/xmlui/bitstream/handle/21000/23372/T- ESPE-044157.pdf?sequence=1&isAllowed=y.

McCarthy, D. (2007). *What is artificial intelligence?,* Computer Science Departmen,

Stanford University, 2007, http://www- formal.stanford.edu/jmc/whatisai.pdf.

MDNWeb. (2020). developer.mozilla.org. https://developer.mozilla.org/es/docs/Learn/JavaScript/First_steps/Qu%C 3 %A9_es_JavaScript.

Moore, E. (1965). *Electronics*. Volume 38, Number 8, April 19.

Montejo, Y Perez, H. (2012). *Gestión documental, de información y del conocimiento.* Nociones e interrelaciones. Bibliotecas anales de investigación. La Habana.

Muñoz, A.; Zunzarren, H.; Herrera, M. (2016). *Guía de la Consultoría en Inteligencia Competitiva en España.* https://issuu.com/antoniomunozcanavate/docs/guiaconsultorasinteligenci a2016.

Ormachez, F. (2019). *Estrategias integradas de ciberseguridad para el fortalecimiento de la seguridad nacional.* Universidad del CAEN. 2019. https://recide.caen.edu.pe/index.php/Recide/article/view/29.

Rivera, O. (2019). *Riesgos de ciberseguridad y sus consecuencias en la prevención de fraudes en las empresas industriales del Distrito de Yanacancha – Pasco*. Universidad Daniel Alcides Carrión 2019. http://repositorio.undac.edu.pe/handle/undac/1372.

Reyes, A. y Brayam J. (2018) *Implementación de Aplicativo web para mejorar la gestión documentaria en el área de administración de la Municipalidad Distrital de Nuevo Chimbote*. Universidad César Vallejo. https://repositorio.ucv.edu.pe/handle/20 500.12692/31242

Rodríguez, D. (1990) *Análisis de la Ley de Fraude Informático*. Revista de Derecho de UNAM.

Román, N. (2018). *Tesis Diseño de sistema de gestión documentaria en la alcaldía de Cartagena de Indias*. Universidad de La Salle, Colombia.

Rosario, T. (2020). *Amenazas desde el ciberespacio*. Las claves del mundo en tus manos. https://atalayar.com/blog/amenazas-desde-el-ciberespacio.

Rosenberg, D., y Stephens, M. (2011). *Agile Development with ICONIX Process: People, Process, and Pragmatism.* New York: Apress: ISBN 978- 1590594643.

Salas, R. (2016). *Diseño y análisis de sistema web educativo considerando los estilos de aprendizaje.* Editorial, Área de Innovación -Desarrollo, S.L. España. 2016.

Satpathy, T. (2017). *Una guía para el cuerpo de conocimientos de Scrum*. 3ra edición VMEdu: SCRUM Study. ISBN: 978-0-9899252-0-4.

Stel, E. (2014). *Seguridad y Defensa del Ciberespacio*. Buenos Aires: Dunken.

Unión Internacional de Telecomunicaciones (2013). *Estudio de la Conectividad Internacional de Internet*. Unión Internacional de Telecomunicaciones (UIT) https://www.itu.int/pub/D-PREF-EF.IIC.CAR/es.

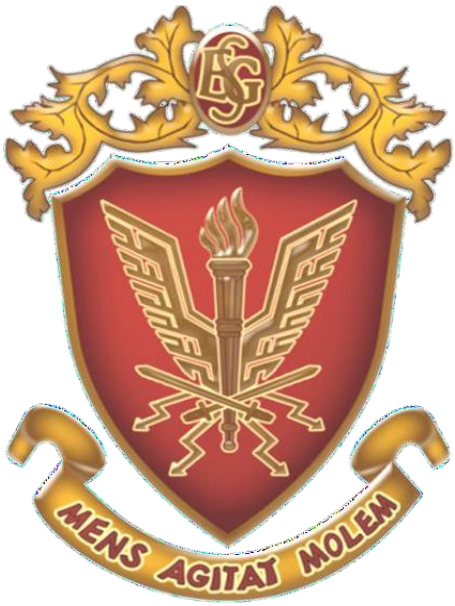
Vargas, R. (2017). *Ciberdefensa y ciberseguridad, más allá del mundo virtual*: modelo ecuatoriano de gobernanza en ciberdefensa.

Viollier, P. y Martínez, M. (2013). *Los delitos informáticos bajo la lupa de la evidencia empírica.* https://www.derechosdigitales.org/6645/los-delitos- informaticos-bajo-la-lupa-de la-evidencia-empirica-que-tan-necesaria-es- una-ley.

Wild Code School (2021). *Contrarrestar los ciberataques: tecnología y ejércitos en simbiosis*.https://www.wildcodeschool.com/es-ES/blog/ciberataque-tecnologia-ejercitos-ciberespacio-ciberseguridad.

Yin, R. (2003). *Case study research: design and methods*. Thousand Oaks: Sage Publications.

ANEXO 1



MATRIZ DE CONSISTENCIA

Anexo 1: Matriz de consistencia de la tesis titulada:

LA CIBERSEGURIDAD ENFOCADA A LOS SISTEMAS INFORMÁTICOS EN LA 5ª BRIGADA DE MONTAÑA, 2022

Descripción de la realidad problemática	**Preguntas de Investigación**	**Objetivos**	**Teorías**	**Categorías**	**Subcategorías**	**Metodología**	**Plan de Análisis de Datos**
En la actualidad en la 5ª Brig. Mtñ. para facilitar el cumplimiento de su misión, su personal está haciendo uso diariamente de tecnologías con acceso a internet, las mismas que permiten admiten conectar distintos equipos entre sí, que proporcionan información en tiempo real, que pueden generar riesgos con la información que se maneja de manera interna.	**Pregunta principal** ¿Cómo es la ciberseguridad enfocada a los sistemas informáticos en la 5ª Brigada de Montaña 2022? **Preguntas específicas:** ¿Cuáles son las vulnerabilidades, amenazas, delitos informáticos que pueden presentarse 5ª Brigada de Montaña 2022? ¿Qué políticas y normas de ciberseguridad ha implementado la 5ª Brigada de Montaña	**Objetivo principal** Analizar la ciberseguridad enfocada a los sistemas informáticos en la 5ª Brig. Mtñ. **Objetivos específicos:** Estudiar las vulnerabilidades, amenazas y delitos informáticos que pueden presentarse 5ª Brig. Mtñ. 2022. Identificar las políticas y normas de ciberseguridad que ha implementado la 5ª Brigada de Montaña	**Ciberseguridad** La Unión Internacional de Telecomunicaciones (2020) dice que son las acciones, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Sistemas informáticos Salas (2016) define a los sistemas informáticos como herramientas de	Ciberseguridad Sistemas informáticos	• Políticas de ciberseguridad. • Vulnerabilidades • Ciberamenazas • Funcionamiento de la plataforma • Conexiones en la nube	Paradigma: Cualitativo debido a que se analizará el problema que afronta la 5ª Brigada de Montaña y se buscará la solución de forma participativa. Tipo: Entrevista semiestructurada Enfoque: Cualitativo	**Técnicas:** Entrevista, revisión documental **Instrumento:** Guía de entrevista **Técnica de análisis de datos** Triangulación

2022? ¿Qué acciones se deben realizar frente a la ciberseguridad enfocada a los sistemas informáticos en la 5ª Brigada de Montaña 2022?	2022. Proponer acciones que se deben realizar en la ciberseguridad enfocada a los sistemas informáticos en la 5ª Brigada de Montaña 2022.	informática que están interconectados a nivel global mediante la web, lo cual conlleva la rapidez de acceder a toda información al instante usando un computador con solo tener instalado un navegador sin tener distinción de un sistema operativo conocido, la plataforma y la información está en constante actualización para el beneficio de todos los usuarios		Diseño de la investigación: Estudio de caso Explicativo Informantes: Participantes de la 5ª Brigada de Montaña Muestreo: Casos tipo

ANEXO 2

INSTRUMENTO DE RECOLECCIÓN DE DATOS

Instrumento de acopio de información

Guía de entrevista a los integrantes de la 5ª Brigada de Montaña.

Introducción:

buenos días/tardes/noches, mi nombre es José Luis BURGOS VIEYRA, como parte de mi tesis titulada “LA CIBERSEGURIDAD ENFOCADA A LOS SISTEMAS INFORMÁTICOS EN LA 5ª BRIGADA DE MONTAÑA, 2022 estoy realizando una investigación cuyo objetivo es analizar la ciberseguridad enfocada a los sistemas informáticos en la 5ª Brigada de Montaña 2022.

Al mismo tiempo, hago de tu conocimiento que la información brindada en esta entrevista es de carácter confidencial y solo será utilizada para los propósitos de esta investigación. el tiempo de duración aproximado de la entrevista se estima en 30 minutos. agradezco anticipadamente tu participación y colaboración totalmente voluntaria; si deseas puedes culminarla en cualquier momento. a continuación, iniciaremos con las preguntas.

¿Aceptas ser entrevistado? sí no
¿Aceptas ser grabado? sí no

GUION BÁSICO PARA LA ENTREVISTA APLICADA A PARTICIPANTES DE LA 5ª BRIGADA DE MONTAÑA

Los participantes se presentan: nombre, edad, sexo, ocupación.

1) ¿Qué equipos informáticos que se utilizan en la 5ª Brigada de Montaña están conectados a una red informática?
2) ¿Cómo cree que estos equipos pueden ser vulnerables a un ataque informático, que ponga en riesgo la ciberseguridad?
3) ¿A qué amenazas a la seguridad informática se enfrentan en la 5ª Brigada de Montaña? Sustente su respuesta.
4) ¿Qué probabilidad hay que el sistema informático sufra un ataque cibernético o sea monitoreado de forma remota por otros (externos)? Por ejemplo, robo de datos, conocimiento público de información reservada o de inteligencia. Explique
5) ¿La información de los sistemas de tramites documentarios que se tramitan en la 5ª Brigada de Montaña se comparte en la nube? ¿Porque? Explique.
6) ¿Cuáles son los riesgos que suponen el uso de los sistemas informáticos, cuando se acceden desde dispositivos externos?
7) ¿Cuáles son los dispositivos más comunes que son empleados en la 5ª Brigada de Montaña para acceder a los sistemas de información? Explique.

8) ¿Como puede afectar la falta de seguridad a la información que se gestiona por los sistemas de tramites documentarios que son empleados por la 5ª Brigada de Montaña?
9) ¿Qué políticas o medidas de ciberseguridad se disponen y cuales pueden implementarse, para evitar ser monitoreados por externos? Es decir que se pueden implementar para evitar los ataques cibernéticos, ¿Las medidas que existen son viables?
10) ¿Se implementan funciones de supervisión, generación de informes y alertas de eventos de seguridad a los sistemas informáticos?
11) ¿Existen elementos para la detección de anomalías y la detección de intrusos?
12) ¿Qué propone en caso no exista, o cómo se debe mejorar?
13) ¿Cómo son las contraseñas de los usuarios en los servicios de autenticación?
14) ¿Son robustas?
15) ¿Qué normas tiene que cumplir el personal, para protegerse de un ataque cibernético o ser monitoreados por externos? Es decir, qué medidas de seguridad debe aplicar cada participante)
16) ¿Qué frecuencia de mantenimiento tienen los equipos vinculados a la informática? por ejemplo cambio de contraseña, actualización del sistema, etc.
17) ¿Qué plan de emergencia tiene la 5ª Brigada de Montaña en caso sufran de un ataque cibernético? Explicar y proponer algunas medidas.
18) ¿Qué posibilidades existen de implementar un sistema de detección de alertas, imprevistos o de presencia de productos nocivos que pueden presentarse en el ámbito de la 5ª Brigada de Montaña?
19) ¿Cómo debe realizarse la configuración de seguridad de los sistemas informáticos, antes de hacer uso de ellos?
20) ¿Qué acciones propone para aplicar la ciberseguridad en los sistemas informáticos?

Guía de entrevista para el personal de otras instituciones.

Introducción:

buenos días/tardes/noches, mi nombre es José Luis BURGOS VIEYRA, como parte de mi tesis titulada “LA CIBERSEGURIDAD ENFOCADA A LOS SISTEMAS INFORMÁTICOS EN LA 5ª BRIGADA DE MONTAÑA, 2022 estoy realizando una investigación cuyo objetivo es analizar la ciberseguridad enfocada a los sistemas informáticos en la 5ª Brigada de Montaña 2022.

Al mismo tiempo, hago de tu conocimiento que la información brindada en esta entrevista es de carácter confidencial y solo será utilizada para los propósitos de esta investigación. el tiempo de duración aproximado de la entrevista se estima en 30 minutos. agradezco anticipadamente tu participación y colaboración totalmente voluntaria; si deseas puedes culminarla en cualquier momento. a continuación, iniciaremos con las preguntas.

¿Aceptas ser entrevistado? sí no
¿Aceptas ser grabado? sí no

GUION BÁSICO PARA LA ENTREVISTA

1) ¿Conoce el funcionamiento del sistema de tramite documentario que se utiliza en la 5ª Brigada de Montaña?
2) ¿Cuáles son los riesgos que suponen el uso de los sistemas informáticos, cuando se acceden desde dispositivos externos?
3) ¿Cuál es su opinión de los servicios en la nube que emplea la 5ª Brigada de Montaña?
4) ¿Qué políticas o medidas de ciberseguridad pueden implementarse, para los usuarios a fin de evitar los ataques cibernéticos?
5) ¿Qué acciones o tecnologías de seguridad propone para incrementar la ciberseguridad de los sistemas informáticos de la 5ª Brig. Mtñ?

FICHA DE REVISIÓN DOCUMENTAL

Se seleccionó los documentos considerados de mayor relevancia para la elaboración del estudio de la base de datos de repositorios académicos, Google Académico y fuentes primarias, tales como: libros, tesis de investigación y revistas electrónicas especializadas.

De esta forma, los documentos claves que cumplieron a cabalidad con los criterios establecidos en las fases del estudio, y que dieron sustento al estudio conceptual, son los que se describen a continuación:

Tipo de documento	País	Referencias	Tema
Informe	Colombia	Conpes 3701. (2011). Lineamientos de política para ciberseguridad y ciberdefensa. https://www.mintic.gov.co/portal/604/articles- 3510_documento.pdf.	Ciberseguridad y ciberdefensa
Libro	España	Cubeiro, E. (2016). Conceptos Fundamentalesde Inteligencia. Valencia: Tirant lo Blanch Schmitt, M. (2013). chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://intranet.mpr.bage.es/intranet-tmpl/prog/local_repository/documents/201555.pdf.	Inteligencia
Informe	Ecuador	Martínez, P. (2020) Propuesta de una Política de Ciberseguridad. Universidad de las Fuerzas Armadas. http://repositorio.espe.edu.ec/xmlui/bitstream/handle/21000/23372/T- ESPE-044157.pdf?sequence=1&isAllowed=y.	Ciberseguridad
Reglamento	Perú	RE 42 – 1, Sistema de Telemática.	Telemática

ANEXO 3

VALIDACIÓN DE INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Juicio de experto: Validez del instrumento de evaluación

ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO

ESCUELA DE POSTGRADO

Apellido y Nombre del Informante	Cargo o Institución donde labora	Nombre del instrumento	Autor del Instrumento
Mendoza Vela Ana Luisa	Gerente	Entrevista	José Burgos
Título de la Investigación:			

I. ASPECTOS DE EVALUACIÓN:

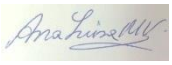
CRITERIOS	INDICADORES	DEFICIENTE				REGULAR				BUENO				MUY BUENO				EXCELENTE			
		00-20%				21-40%				41-60%				61-80%				81-100%			
		0	6	11	16	21	28	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje apropiado																				98
2. OBJETIVO	Está expresado en Capacidades observables																				98
3. ACTUALIDAD	Adecuado a la identificación del conocimiento de las variables de investigación																				98
4. ORGANIZACIÓN	Existe una organización lógica en el instrumento																				98
5. SUFICIENCIA	Comprende los aspectos en cantidad Y calidad con respecto a las variables de investigación																				98
6. INTENCIONALIDAD	Adecuado para valorar aspectos de las variables de investigación																				98
7. CONSISTENCIA	Basado en aspectos teóricos de conocimiento																				98
8. COHERENCIA	Existe coherencia entre los índices e indicadores y las dimensiones																				98
9. METODOLOGÍA	La estrategia responde al propósito de la investigación																				98
10. PERTINENCIA	El inventario es aplicable																				98

II. OPINIÓN DE APLICACIÓN:

Conforme……

……,,,,,……

III. PROMEDIO DE VALORACIÓN: 98

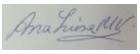
LUGAR Y FECHA	DNI	FIRMA DEL EXPERTO INFORMANTE	N" DE TELÉFONO
10 de mayo del 2022	16753409		969652378

Validación de guía de entrevista por experto
ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO
ESCUELA DE POSTGRADO

TÍTULO DE LA INVESTIGACIÓN:

LA CIBERSEGURIDAD ENFOCADA A LOS SISTEMAS INFORMÁTICOS EN LA 5ª BRIGADA DE MONTAÑA, 2022

I. DATOS DEL EXPERTO:

a. Apellidos y nombres : MENDOZA VELA ANA LUISA
b. Grado académico-profesión : INGENIERA METODOLOGA
c. D.N.I. 16753409
d. N° de teléfono : 969652378
e. Lugar y fecha : LIMA,10 DE MAYO DEL 2022
f. Firma : 

II. **DATOS DEL INSTRUMENTO DE EVALUACIÓN** (entrevista)

a. Autor(es) del instrumento : José Luis BURGOS VIEYRA
b. Institución a la que pertenece : EJERCITO DEL PERÚ
c. Método de investigación : CUALITATIVO
d. Tipo de entrevista :

III. ASPECTOS DE EVALUACIÓN

N°	Criterios	Indicadores	Valoración De: O a 1
01	Diseño	Convocatoria: Lugar – tiempo. Contenidos: Propuesta de temas- preguntas – respuestas.	1
02	Organización	Selección: informantes – representación de temas – tipo de respuesta – número de entrevistas.	1
03	Estructuración	Guía de entrevista : Dirección a seguir - Objetivos - N° de preguntas según tipo de entrevista. Contexto de los datos: Conocer experiencias del entrevistado. Tema propios : Aspectos que interesen	1
04	Secuencial	Con relación a variables – dimensiones e indicadores.	1

		Sigue un orden lógico y pre-requisitorial.	
05	Conectividad	Conjuga el tipo de pregunta con el objetivo de investigación y se armoniza con las experiencias que esperan ser revaloradas en el cuestionario.	1
06	Intencionalidad	Adecuado para valorar aspectos desconocidos y/o modificados de las variables de investigación.	1
07	Actualidad	Existe coherencia entre resultados alcanzados con la realidad por conocer en el marco de doctrina, leyes, teorías vigentes.	1
08	Contrastación de otros resultados	Han sido formuladas las preguntas, conociéndose los resultados alcanzados por otro instrumento para comparar la hipótesis de investigación.	1
09	Orientación a solución de problemas	Se concatenan las preguntas para alcanzar criterios, juicios, conceptos que ayuden a solucionar el problema de investigación planteado.	1
10	Análisis e interpretación	Se ha adecuado algún instrumento o herramienta para verter los resultados de la entrevista y analizarlos /interpretarlos.	1

IV. RESULTADO DE VALORACIÓN:1	**V. OPINIÓN DE APLICACIÓN**
<u>Aspectos para la valoración</u> - Valida por 05 expertos de la ESGE-EPG - Debe aplicarse la prueba de la “V” de Aiken - Resultado mínimo aprobatorio: 0.85 u 85% - La validación solo se hará hasta dos decimales que terminen en cero o en cinco. Ejemplo: 0.60; 0.75	Conforme para su aplicación

Juicio de experto: Validez del instrumento de evaluación

ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO

ESCUELA DE POSTGRADO

Apellido y Nombre del Informante	Cargo o Institución donde labora	Nombre del	Autor del
García Vela Teresa Maximina	Abogada Gestión Pública	Entrevista	José Burgos
Título de la Investigación:			

I. ASPECTOS DE EVALUACIÓN:

CRITERIOS	INDICADORES	DEFICIENTE				REGULAR				BUENO				MUY BUENO				EXCELENTE			
		00-20%				21-40%				41-60%				61-80%				81-100%			
		0	6	11	16	21	28	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje apropiado																				98
2. OBJETIVO	Está expresado en Capacidades observables																				98
3. ACTUALIDAD	Adecuado a la identificación del conocimiento de las variables de investigación																				98
4. ORGANIZACIÓN	Existe una organización lógica en el instrumento																				98
5. SUFICIENCIA	Comprende los aspectos en cantidad Y calidad con respecto a las variables de investigación																				98
6. INTENCIONALIDAD	Adecuado para valorar aspectos de las variables de investigación																				98
7. CONSISTENCIA	Basado en aspectos teóricos de conocimiento																				98
8. COHERENCIA	Existe coherencia entre los índices e indicadores y las dimensiones																				98
9. METODOLOGÍA	La estrategia responde al propósito de la investigación																				98
10. PERTINENCIA	El inventario es aplicable																				98

II. OPINIÓN DE APLICACIÓN:

Conforme……

……

III. PROMEDIO DE VALORACIÓN: 98

LUGAR Y FECHA	DNI	FIRMA DEL EXPERTO INFORMANTE	N" DE TELÉFONO
10 de mayo del 2022	41964058		969652378

Validación de guía de entrevista por experto

ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO

ESCUELA DE POSTGRADO

TÍTULO DE LA INVESTIGACIÓN:

LA CIBERSEGURIDAD ENFOCADA A LOS SISTEMAS INFORMÁTICOS EN LA 5ª BRIGADA DE MONTAÑA, 2022

VI. DATOS DEL EXPERTO:

a. Apellidos y nombres : GARCIA VELA TERESA MAXIMINA
b. Grado académico-profesión : ABOGADA – GESTIÓN PÚBLICA
c. D.N.I. 41964058
d. N° de teléfono 969652378
e. Lugar y fecha :LIMA,10 DE MAYO DEL 2022
f. Firma :

VII. **DATOS DEL INSTRUMENTO DE EVALUACIÓN** (entrevista)

a. Autor(es) del instrumento : José Luis BURGOS VIEYRA
b. Institución a la que pertenece : EJERCITO DEL PERÚ
c. Método de investigación : CUALITATIVO
d. Tipo de entrevista :

VIII. ASPECTOS DE EVALUACIÓN

N°	Criterios	Indicadores	Valoración De: O a 1
01	Diseño	Convocatoria: Lugar – tiempo. Contenidos: Propuesta de temas- preguntas – respuestas.	1
02	Organización	Selección: informantes – representación de temas – tipo de respuesta – número de entrevistas.	1
03	Estructuración	Guía de entrevista : Dirección a seguir - Objetivos - N° de preguntas según tipo de entrevista Contexto de los datos: Conocer experiencias del entrevistado Tema propios : Aspectos que interesen	1

04	Secuencial	Con relación a variables – dimensiones e indicadores. Sigue un orden lógico y pre-requisitorial.	1
05	Conectividad	Conjuga el tipo de pregunta con el objetivo de investigación y se armoniza con las experiencias que esperan ser revaloradas en el cuestionario.	1
06	Intencionalidad	Adecuado para valorar aspectos desconocidos y/o modificados de las variables de investigación.	1
07	Actualidad	Existe coherencia entre resultados alcanzados con la realidad por conocer en el marco de doctrina, leyes, teorías vigentes.	1
08	Contrastación de otros resultados	Han sido formuladas las preguntas, conociéndose los resultados alcanzados por otro instrumento para comparar la hipótesis de investigación.	1
09	Orientación a solución de problemas	Se concatenan las preguntas para alcanzar criterios, juicios, conceptos que ayuden a solucionar el problema de investigación planteado.	1
10	Análisis e interpretación	Se ha adecuado algún instrumento o herramienta para verter los resultados de la entrevista y analizarlos /interpretarlos.	1

IX. RESULTADO DE VALORACIÓN:1	**X. OPINIÓN DE APLICACIÓN**
<u>Aspectos para la valoración</u> - Valida por 05 expertos de la ESGE-EPG - Debe aplicarse la prueba de la “V” de Aiken - Resultado mínimo aprobatorio: 0.85 u 85% - La validación solo se hará hasta dos decimales que terminen en cero o en cinco. Ejemplo: 0.60; 0.75	Conforme para su aplicación

Juicio de experto: Validez del instrumento de evaluación

ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO

ESCUELA DE POSTGRADO

Apellido y Nombre del Informante	Cargo o Institución donde labora	Nombre del instrumento	Autor del Instrumento
VALERO ENRIQUEZ CESAR	Inspector - 5ª Brig. Mtñ.	Entrevista	José Burgos
Título de la Investigación:			

I. ASPECTOS DE EVALUACIÓN:

CRITERIOS	INDICADORES	DEFICIENTE				REGULAR				BUENO				MUY BUENO				EXCELENTE			
		00-20%				21-40%				41-60%				61-80%				81-100%			
		0	6	11	16	21	28	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje apropiado																				98
2. OBJETIVO	Está expresado en Capacidades observables																				98
3. ACTUALIDAD	Adecuado a la identificación del conocimiento de las variables de investigación																				98
4. ORGANIZACIÓN	Existe una organización lógica en el instrumento																				98
5. SUFICIENCIA	Comprende los aspectos en cantidad Y calidad con respecto a las variables de investigación																				98
6. INTENCIONALIDAD	Adecuado para valorar aspectos de las variables de investigación																				98
7. CONSISTENCIA	Basado en aspectos teóricos de conocimiento																				98
8. COHERENCIA	Existe coherencia entre los índices e indicadores y las dimensiones																				98
9. METODOLOGÍA	La estrategia responde al propósito de la investigación																				98
10. PERTINENCIA	El inventario es aplicable																				98

II. OPINIÓN DE APLICACIÓN:

Conforme……

……,,,,,……

III. PROMEDIO DE VALORACIÓN: 98

LUGAR Y FECHA	DNI	FIRMA DEL EXPERTO INFORMANTE	N" DE TELÉFONO
18 de mayo del 2022	09941717		945095370

Validación de guía de entrevista por experto

ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO
ESCUELA DE POSTGRADO

TÍTULO DE LA INVESTIGACIÓN:

LA CIBERSEGURIDAD ENFOCADA A LOS SISTEMAS INFORMÁTICOS EN LA 5ª BRIGADA DE MONTAÑA, 2022

XI. DATOS DEL EXPERTO:

g. Apellidos y nombres : VALERO ENRIQUEZ CESAR
h. Grado académico-profesión : MAGISTER – MILITAR.
i. D.N.I. 09941717
j. N° de teléfono : 945095370
k. Lugar y fecha : LIMA,18 DE MAYO DEL 2022
l. Firma :

XII. **DATOS DEL INSTRUMENTO DE EVALUACIÓN** (entrevista)

e. Autor(es) del instrumento : José Luis BURGOS VIEYRA
f. Institución a la que pertenece : EJERCITO DEL PERÚ
g. Método de investigación : CUALITATIVO
h. Tipo de entrevista :

XIII. ASPECTOS DE EVALUACIÓN

N°	Criterios	Indicadores	Valoración De: O a 1
01	Diseño	Convocatoria: Lugar – tiempo. Contenidos: Propuesta de temas- preguntas – respuestas.	1
02	Organización	Selección: informantes – representación de temas – tipo de respuesta – número de entrevistas.	1
03	Estructuración	Guía de entrevista : Dirección a seguir - Objetivos - N° de preguntas según tipo de entrevista. Contexto de los datos: Conocer experiencias del entrevistado. Tema propios : Aspectos que interesen	1
04	Secuencial	Con relación a variables – dimensiones e	1

		indicadores. Sigue un orden lógico y pre-requisitorial.	
05	Conectividad	Conjuga el tipo de pregunta con el objetivo de investigación y se armoniza con las experiencias que esperan ser revaloradas en el cuestionario.	1
06	Intencionalidad	Adecuado para valorar aspectos desconocidos y/o modificados de las variables de investigación.	1
07	Actualidad	Existe coherencia entre resultados alcanzados con la realidad por conocer en el marco de doctrina, leyes, teorías vigentes.	1
08	Contrastación de otros resultados	Han sido formuladas las preguntas, conociéndose los resultados alcanzados por otro instrumento para comparar la hipótesis de investigación.	1
09	Orientación a solución de problemas	Se concatenan las preguntas para alcanzar criterios, juicios, conceptos que ayuden a solucionar el problema de investigación planteado.	1
10	Análisis e interpretación	Se ha adecuado algún instrumento o herramienta para verter los resultados de la entrevista y analizarlos /interpretarlos.	1

XIV. RESULTADO DE VALORACIÓN:1	**XV. OPINIÓN DE APLICACIÓN**
<u>Aspectos para la valoración</u> - Valida por 05 expertos de la ESGE-EPG - Debe aplicarse la prueba de la “V” de Aiken - Resultado mínimo aprobatorio: 0.85 u 85% - La validación solo se hará hasta dos decimales que terminen en cero o en cinco. Ejemplo: 0.60; 0.75	Conforme para su aplicación

ANEXO 4

AUTORIZACIÓN PARA LA RECOLECCIÓN DE DATOS

Cusco, 10 de marzo del 2022.

Oficio N°025/Secretraria/5ª Brig. Mtñ.

Señor Tte Crl. Ing. Jose Luis BURGOS VIEYRA

Asunto : Autorización para realizar investigación.

Ref : Oficio Nº 015/JLBV

Tengo el agrado de dirigirme a Ud. en relación al documento de la referencia para manifestarle que este comando le autoriza a realizar el levantamiento de datos e informaciones para su investigación titulada "LA CIBERSEGURIDAD ENFOCADA A LOS SISTEMAS INFORMÁTICOS EN LA 5ª BRIGADA DE MONTAÑA 2022"

Sin otro en particular aprovecho la oportunidad para expresarle mis consideraciones y deferente estima.

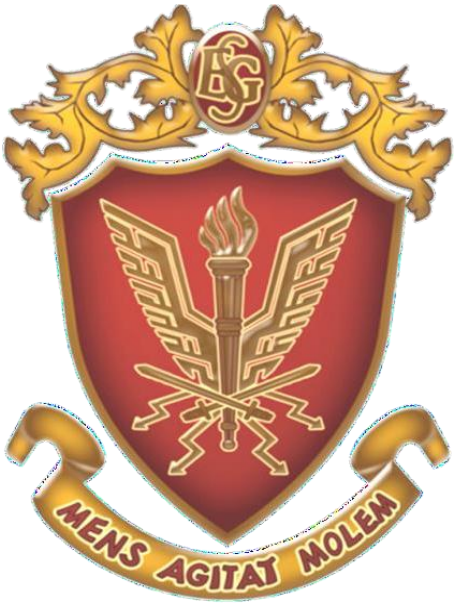
Dios guarde a Ud.

5ta BRIGADA DE MONTAÑA COMANDANCIA GENERAL

O - 28034057 - O+
FERNANDO MARTIN TABAYCO BOGGIO
GRAL BRIG
Cmdte. Gral. de la 5ª Brig Montaña

Distribución:
Interesado 01
Archivo..... 01/02

ANEXO 5



COMPROMISO ÉTICO

Declaración de Compromiso Ético

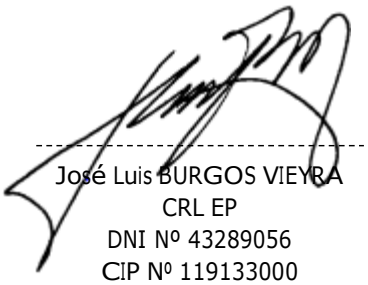
El presente trabajo de investigación titulado: **La Ciberseguridad Enfocada a los Sistemas Informáticos en la 5ª Brigada de Montaña, 2022**

Se ha realizado en estricto apego a la metodología de la investigación y a las normas éticas para investigación de la Escuela Superior de Guerra del Ejercito promulgadas por el Departamento de Gestión de la Investigación de la Escuela Superior de Guerra del Ejército-Escuela de Postgrado.

En vista de lo anterior:

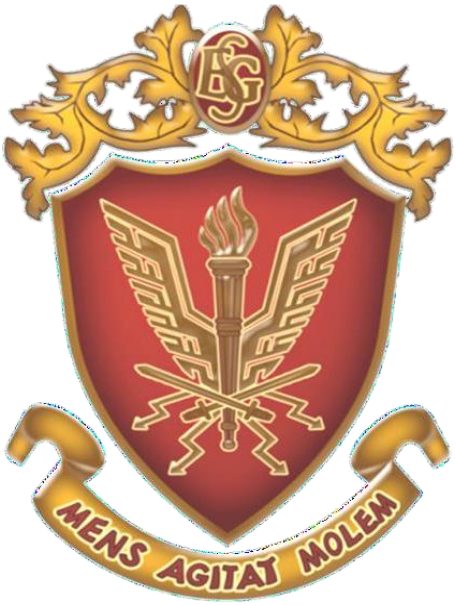
Yo Bach. José Luis BURGOS VIEYRA, egresado de la de la VI MCM de la Escuela Superior de Guerra-Escuela de Postgrado (ESGE-EPG), declaro bajo juramento que he desarrollado esta investigación siguiendo las instrucciones brindadas por el Departamento de Gestión de la Investigación, desde la elaboración del marco referencial y recolección de la información, hasta el análisis de datos y elaboración del informe final.

En tal sentido la información contenida en el presente documento es producto de mi trabajo personal, apegándome a la legislación sobre propiedad intelectual, sin haber incurrido en falsificación de la información o cualquier tipo de fraude, por lo cual me someto al marco legal y normativo vigente relacionado a dicha responsabilidad, así como a las normas disciplinarias establecidas en la ESGE-EPG.



José Luis BURGOS VIEYRA
CRL EP
DNI Nº 43289056
CIP Nº 119133000

ANEXO 6



HOJA DE DATOS PERSONALES

HOJA DE DATOS PERSONALES

GRADO: **CORONEL**

NOMBRES: **JOSÉ LUIS**

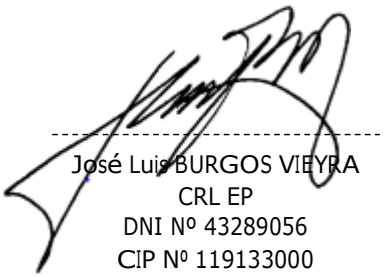
APELLIDOS: **BURGOS VIEYRA**

EMAIL: **JLBURGOSV@HOTMAIL.COM**

DIRECCIÓN: **AV. EJERCITO N° 214, URBANIZACIÓN QUINTA JARDÍN – SANTIAGO – CUSCO.**

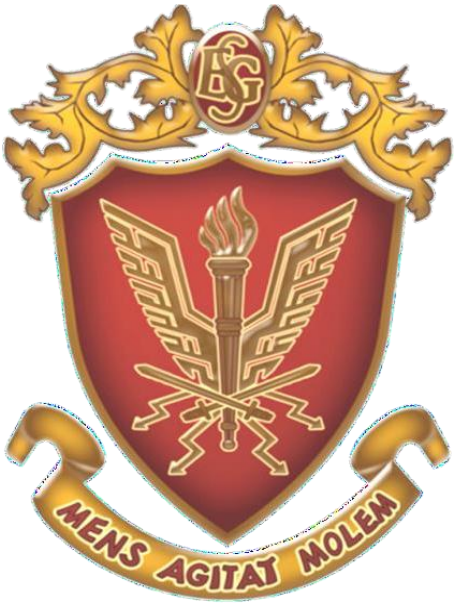
CELULAR: **993059416**

FIRMA



José Luis BURGOS VIEYRA
CRL EP
DNI Nº 43289056
CIP Nº 119133000

ANEXO 7



APORTES DE LA INVESTIGACIÓN

Aportes a la Investigación

De acuerdo con el objetivo específico 3: Proponer acciones que se deben realizar en la ciberseguridad enfocada a los sistemas informáticos en la 5ª Brigada de Montaña 2022. Según Cubeiro (2016) menciona que el conflicto bélico que utiliza el ciberespacio como escenario principal, en lugar de los campos de batalla convencionales. Lo realizan por medio de un conjunto de acciones que permiten alterar las informaciones y los sistemas del enemigo, a la vez que protegen la información y los sistemas del atacante.

Como refieren los entrevistados en el caso de proponer medidas para gestionar la ciberseguridad enfocada en los sistemas informáticos, estas medidas se relacionan con la idea de proteger las informaciones y los sistemas de la organización, Para ello contribuye el empleo de un Firewall de seguridad perimétrica y un sistema criptográfico asimétrico bien configurados.

Igualmente, de acuerdo con Castro (2015) hoy en día la soberanía de los Estados a nivel mundial ha sido quebrantada a través de los medios tecnológicos, afectando la infraestructura crítica que en algunos casos ha logrado niveles alarmantes de daños a través de ataques cibernéticos que podrían paralizar sus principales sistemas; que pueden ser vulnerables sino se dispone de un sistema de ciberdefensa que pueda enfrentar este tipo de amenazas. Es necesario contar con un Comando de Ciberdefensa que permita proteger la infraestructura critica digital de la 5ª Brigada de Montaña, en vista que existe vulnerabilidad tecnológica; varias páginas oficiales ya han sido hackeadas. Hay que tener en consideración que en la actualidad los gobiernos asignan presupuestos para enfrentar una eventual ciberguerra y que permitirían salvaguardar la seguridad y la soberanía ante posibles ciberataques.

Luego del análisis de las encuestas en el contexto de los objetivos trazados para la presente investigación, con la finalidad de mejorar las medidas de ciberseguridad de los sistemas informáticos de la 5ª Brigada de Montaña, se propone lo siguiente:

a. Con respecto a las políticas y normas relacionadas al manejo de los sistemas informáticos, se debe tener en consideración el empleo de las siguientes normas:
   - ISO 27000: Gestión de la Seguridad de las Informaciones.
   - ISO 27001: Requisitos del sistema de gestión de seguridad de la información.
   - ISO 27002: Es una guía de buenas prácticas y recomendables en cuanto a seguridad de las informaciones.

- ISO 27005: Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

b. Implementación de los siguientes sistemas de seguridad:
   - Servidores de Datos, que permitan separar la base de datos de las aplicaciones e independizar el servidor de datos en una zona DMZ .
   - Empleo de un Firewall que emplee seguridad por capas (seguridad del perímetro (red), seguridad del dispositivo, seguridad de las aplicaciones y seguridad de los datos. Cada capa dispone de un conjunto de protocolos, equipos y técnicas de seguridad y deben ser capaces de identificar y controlar las aplicaciones, autenticación de los usuarios, protección contra exploits, filtrado de contenido (incluido el filtrado de URL) y control de acceso basado en la ubicación, protección contra malware.
   - Se debe considerar el empleo de un sistema criptográfico asimétrico, desarrollado por el Ejército (con un método propio), en las redes que comprenden la comunicación con el escalón superior y con las Unidades subordinadas, las mismas que impidan el acceso a nuestras informaciones a personas no autorizadas.
   - Implementación de doble factor de autenticación para ingresar al sistema, que da una seguridad adicional a los usuarios que la emplean.
   - Implementación de una red privada virtual (VPN). Para poder acceder a la red de la 5ª Brig. Mtñ. que permite a los administradores abordar los problemas de seguridad, garantizando que solo los usuarios autorizados tengan acceso a los recursos corporativos. Ademas, asegura la confidencaialidad e integridad de la información, evita que sea modificada y/o alterada, lo que incrementa la ciberseguridad de los sistemas.

c. También se debe tener en consideración las siguientes medidas:
   - Coordinar con la DIE - DITELE sobre la implementación de medidas de seguridad que son necesarias de acuerdo a nuestras necesidades, a fin de obtener su opinión técnica. En vista que para el tráfico de esta información se debe usar varias capas de seguridad como el cifrado.
   - Contar con un adecuado Plan de Contingencia que haya identificado los procesos críticos, que evalue los recursos utilizados en las operaciones y haya especificado los escenarios donde pueden ocurrir problemas, a fin de determinar medidas preventivas y planes de acción.

- Programar charlas de ciberseguridad a fin de concientizar y capacitar al personal que emplea los sistemas informaticos, incidiendo bastante en el nivel usuario.
- Implementar funciones de supervisión, generación de informes y alertas de eventos de seguridad a los sistemas informáticos.
- Contar con un plan de verificación del cumplimiento de las normas de seguridad, para los usuarios de los sistemas informáticos.
- Exigir y verificar el uso de claves robustas y el cambio de las mismas en un tiempo prudencial (06 meses).
- Implementar funciones de supervisión, generación de informes y alertas de eventos de seguridad, a los sistemas informáticos.
- Migrar del proveedor de servicios de nuve actual al AWS, Google Cloud o AZURE, que tienen mayor respaldo y seguridad.

d. Con respecto a la plataforma Linux que es la que se emplea actualmente en el Sistema de Tramite documentario de la 5ª Brigada de Montaña, nos permite un grado de seguridad adicional. Asimismo, los servidores en el data center del Ejercito funcionan bajo la misma plataforma Linux, lo que nos permite integrarnos fácilmente a la red del Ejercito.

ANEXO 8

CD CONTENIENDO TESIS EN PDF

ESCUELA SUPERIOR DE GUERRA
DEL EJÉRCITO

ESCUELA DE POSTGRADO

TESIS

LA CIBERSEGURIDAD ENFOCADA A LOS SISTEMAS INFORMÁTICOS EN LA 5ª BRIGADA DE MONTAÑA, 2022

AUTOR:
Bach. José Luis BURGOS VIEYRA

2023

ANEXO 9

REPORTE DE SIMILITUD DE TURNITIN


BURGOS VIEYRA CIBERSEGURIDAD ENFOCADA A LOS SISTEMAS INFORMATICOS 5A BRIG. MTÑ. ABRIL 2023 CRL ...
Submission Details
Help
turnitin
ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO
ESCUELA DE POSTGRADO
TESIS
LA CIBERSEGURIDAD ENFOCADA A LOS SISTEMAS INFORMÁTICOS EN LA 5ª BRIGADA DE MONTAÑA, 2022
AUTOR
Bach. José Luis BURGOS VIEYRA
0000-0002-5830-5793
Para optar el Grado Académico de
MAESTRO EN CIENCIAS MILITARES
Con mención en Planeamiento Estratégico y Toma de Decisiones
ASESOR TEMÁTICO
Mg. Adrián CAMACHO SORIANO
0000-0003-1961-9666
ASESOR METODOLOGICO
Dr. Hugo Ricardo PRADO LOPEZ
0000-0003-4010-3517
2022
Sources Overview
24%
OVERALL SIMILARITY
1 repositorio.esge.ed... INTERNET 12%
2 repositorio.espe.edu.ec INTERNET 3%
3 esge.edu.pe INTERNET <1%
4 Universidad Europe... SUBMITTED WORKS <1%
5 Escuela Politecnica ... SUBMITTED WORKS <1%
6 Juan Ignacio Alcaid... CROSSREF <1%
7 www.arxivers.com INTERNET <1%
8 ESIC Business & Ma... SUBMITTED WORKS <1%
hdl.handle.net
0 Flags
24% Overall Similarity
-- AI
Share
Page 1 of 115
Buscar
13:18
9/05/2023

ANEXO 10

TRANSCRIPCIÓN DE LAS ENTREVISTAS

Transcripción de entrevistas

1. ¿Qué equipos informáticos que se utilizan en la 5ª Brigada de Montaña están conectados a una red informática?

   Participante 1: Dijo que todos los equipos de informática están conectados a la red de datos de la 5ª Brig. Mtñ, entre los que podemos mencionar: Computadoras, Laptops, Servidores, Impresoras, proyectores, Switch's, Routers, Access Point, Firewall de seguridad, entre otros.

   Participante 2: Dijo que todos los equipos de informática que están conectados a los sistemas de la de la 5ª Brig. Mtñ, algunos a una red LAN física como es el caso de la Comandancia y los demás a través de un punto de internet; tal es el caso de Computadoras, Laptops, Servidores, Impresoras, Switch's, Routers, Access Point y otros que se conecten en la red de la 5ª Brig. Mtñ.

   Participante 3: Dijo que todos los equipos de informática, se encuentran conectados a la red de datos de la 5ª Brig. Mtñ, porque es necesario para poder acceder al sistema de tramite documentario de la 5ª Brigada de Montaña.

   Participante 4: Dijo que la gran mayoría de los equipos de informática, se encuentran conectados a la red de datos de la 5ª Brig. Mtñ, con la finalidad de poder acceder al sistema de tramite documentario de la 5ª Brigada de Montaña y poder gestionar la documentación.

   Participante 5: Dijo que son empleados todos los dispositivos informáticos, que permitan el acceso a los sistemas informáticos de la 5ª Brig. Mtñ. laptop, celulares, Tablet, entre otros.

   Participante 6: Dijo que los equipos informáticos que están conectados en la 5ª Brigada de Montaña son las computadoras personales, Laptops, Servidores, Impresoras, Switch's, Routers, Access Point entre otros mediante una red Local Área Networks (LAN) o red de área local que son sistemas informáticos independientes conectados entre sí, de tal forma que posibilitan un intercambio de datos, para lo que es necesario tanto la conexión física como la conexión lógica de los sistemas. La red se configura con el objetivo de transmitir datos de un sistema a otro o de disponer recursos en común, como servidores, bases de datos o impresoras.

2. ¿Cómo cree que estos equipos pueden ser vulnerables a un ataque informático, que ponga en riesgo la ciberseguridad?

   Participante 1: Mencionó que disponemos de un firewall de seguridad que restringe los accesos y/o intromisiones de elementos no deseados a la red interna de la Gran Unidad; del mismo modo restringe a los usuarios a acceder a ciertas páginas de dudosa reputación. Desde el punto de vista informático; se vienen adoptando todas las medidas de seguridad a fin de evitar intromisiones y perdidas de información; sin embargo, somos conscientes de que ningún sistema es 100% seguro; por lo que siempre estamos alertas ante cualquier ataque cibernético.

   Participante 2: Mencionó que para que sean vulnerados por un ataque informático, primero han tenido que ser vulnerado con acciones de ciberinteligencia o acciones pasivas de cibernética (hackeos) que le permitan saber los puntos vulnerables de nuestros equipos o de la red en su conjunto. Sin embargo, al estar conectados al internet podrían ser vulnerados a través de virus, o algún software malicioso que le permita burlar las medidas de seguridad de la red y de manera física podría ser más fácil vulnerar la seguridad de la red a través del uso de USB u otro dispositivo preparado para instalación de programas que dañen los programas y aplicaciones que usemos en nuestra red o también podrían ser usados para el robo de información.

   Participante 3: Mencionó que, en la actualidad, se vienen adoptando todas las medidas de seguridad, desde el punto de vista informático, con la finalidad de evitar ataques. Sin embargo, con los avances tecnológicos de la actualidad, ningún sistema es 100% seguro; por lo que siempre habrá la posibilidad de ser vulnerables, más aún si no se dan cumplimiento estricto a las políticas de seguridad, si no se realiza una supervisión adecuada de los sistemas informáticos, si no se disponen de adecuados elementos de detección de anomalías, si no se dispone de contraseñas robustas, entre otros.

   Participante 4: Mencionó que los equipos siempre son susceptibles de ser vulnerados en su seguridad, puede ser que el intruso quiera solo entrar en los sistemas (a lo que se llama vulneración de seguridad) y otra que quiera llevarse datos de estos sistemas (vulneración de datos).

   Participante 5: Mencionó que, al estar conectados al internet, siempre existirá la posibilidad de ser vulnerables a un ataque informático. Los equipos informáticos pueden ser vulnerados a través de virus, y/o softwares maliciosos que puedan dañar los programas y aplicaciones que son empleados por nuestro personal.

Participante 6: Mencionó que desde el solo hecho que estamos conectados a internet y en este caso la 5ª Brigada de Montaña ya es vulnerable a distintos ataques informáticos que pondrá en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por más que disponga de firewall de seguridad (programa informático que restringe los accesos y/o intromisiones de elementos no deseados a la red interna); por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos «agujeros» pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos.

3. ¿A qué amenazas a la seguridad informática se enfrentan en la 5ª Brigada de Montaña? Sustente su respuesta.

   Participante 1: Acotó que todas las amenazas que existen en el Internet: Hackers, crackers, virus, gusanos, troyanos, etc. Quiero acotar que el sistema de tramite documentario empleado en la 5ª Brig. Mtñ. emplea la plataforma Linux, y nos permite un grado de seguridad adicional. Asimismo, los servidores en el data center del Ejercito del Perú funcionan bajo la misma plataforma, lo que nos permite integrarnos fácilmente a la red del Ejercito

   Participante 2: Acotó que, a hackers, crackers, virus, gusanos, troyanos, robo de información a través de medios físicos, a desastres naturales o artificiales que afecten nuestros equipos físicos, etc. Es preciso mencionar que todo va a depender del nivel de conocimiento y los medios disponibles del atacante informático.

   Participante 3: Acotó que a todas las amenazas que existen en el Internet, las más comunes son: softwares maliciosos que son capaces de invadir los sistemas operativos y causar todo tipo de daños. También son vulnerables a la suplantación de identidad, a los ataques de inyección SQL, que emplean códigos maliciosos para acceder a los servidores y extraen información como usuarios, contraseñas, datos importantes, entre otros.

   Participante 4: Acotó que a todas las amenazas que existen en el Internet, como son: softwares maliciosos ataques de inyección SQL, robo de identidad etc.

   Participante 5: Acotó que, a softwares maliciosos, a la suplantación de identidad, a los ataques de inyección SQL, que emplean códigos maliciosos para acceder a los servidores y extraen información como usuarios.

   Participante 6: Acotó que las principales amenazas a la seguridad informática que enfrenta la 5ª Brigada de Montaña en cada día, son las siguientes:

Los usuarios: aunque no muchos lo crean, es la principal amenaza, ya sea porque estos no adoptan buenas prácticas de ciberseguridad y se convierten en blancos fáciles o porque son ellos quienes roban información de forma intencional.

Programas maliciosos: son los que se conocen como malware y consisten en software maliciosos que se encargan de destruir archivos, espiar o robar información. Dentro de ellos están los virus, gusano, troyanos y otros.

Fallos de programación: aunque se deban a errores en el desarrollo, representa un gran peligro porque fácilmente podrían infiltrarse softwares maliciosos y robar información, por esta razón se deben mantener actualizados los sistemas operativos en todos los equipos.

Intrusos: se trata de personas no autorizadas que se introducen en los programas y archivos para espiar, robar o destruir información.

Siniestros: en este caso se produce pérdida de información o recursos materiales a consecuencia de la negligencia por falta de oficio de los usuarios o mal intención de estos. Dentro de los siniestros más frecuentes están los incendios e inundaciones.

Catástrofes naturales: a diferencia de los siniestros, estas se dan por causas naturales.

Fallos electrónicos: estos pueden afectar los sistemas debido a fallas en la energía eléctrica o por desperfectos propios de los equipos.

4. ¿Qué probabilidad hay que el sistema informático sufra un ataque cibernético o sea monitoreado de forma remota por otros (externos)? Por ejemplo, robo de datos, conocimiento público de información reservada o de inteligencia. Explique.
   Participante 1: Dijo que siempre existe la probabilidad de que un sistema sea vulnerado; tenemos los casos de que empresas como Google, Microsoft, IBM y otros que sus sistemas han sido hackeados, y son empresas que invierten millones de millones en software y en seguridad; y nuestro sistema no está libre de algún ataque; entonces, lo importante aquí es el tiempo de resiliencia que se tiene, para poder sobreponerse y recuperar el control de nuestro sistema.

   Participante 2: Dijo que la probabilidad seria media, pero esto va a depender del interés del atacante y de la información que tengamos en nuestra red, hasta podría decirse que ahora mismo podríamos ser víctimas de acciones pasivas de ciberinteligencia, acciones pasivas de ciberataques como la explotación (hackeos y otros). En cuanto al tráfico de información reservada o de inteligencia no debe usarse esta red informática porque atenta contra la seguridad de la información clasificada solo deben usarse

medios autorizados por la institución (DIE y CITELE), en vista que para el tráfico de esta información se debe usar varias capas de seguridad como el cifrado, encriptado, firewall, llaves físicas de seguridad informática, entre otras herramientas que permiten mayores niveles de seguridad para la información. Asimismo, soy de la opinión que para el tráfico de toda información militar debe pasar por estándares militares de seguridad puesto, que así sea documentación común, esta puede ser aprovechada por la inteligencia de algún País o agente externo a nuestra institución.

Participante 3: Dijo que la probabilidad que un sistema sea atacado o monitoreado es muy alta, por ello deben estar siempre alertas ante un posible ataque interno o externo y deben contar con procedimientos para afrontar rápidamente la caída del sistema por un ataque. Se sugiere planificar y ejecutar simulacros para validar la correcta ejecución de los procedimientos.

Participante 4: Dijo que cada día que pasa aumenta la probabilidad de sufrir un ataque cibernético, ya que en estos tiempos cualquier ciudadano tiene acceso a internet y con mayor uso de sistemas y dispositivos conectados a la red, el personal no calificado para el uso de estos sistemas y se deja mayor vulnerabilidad en el uso de software, la mala configuración de los sistemas, malos hábitos de seguridad, el uso de dispositivos móviles.

Participante 5: Dijo que es muy probable, por lo que se requiere de una supervisión permanente, y se debe contar con procedimientos establecidos para afrontar rápidamente la cualquier ataque.

Participante 6: Dijo que el solo hecho que estemos conectados a un punto de internet ya sea por cable o wifi siempre existirá la probabilidad de que suframos ataques cibernéticos ya sea para robos de datos, hackeos o nuestra información reservada sea expuesta para conocimiento público ajeno a nuestra institución o esta puede ser aprovechada por la inteligencia de algún País vecino al nuestro.

5. ¿La información de los sistemas de tramites documentarios que se tramitan en la 5ª Brigada de Montaña se comparte en la nube? ¿Por qué? Explique.

   Participante 1: Mencionó que sí, es un sistema entorno web, y para su funcionamiento es necesario alquilar los servicios de dominio y hosting a fin de que sean publicados en el internet y los usuarios puedan acceder desde el lugar donde se encuentren; desde sus oficinas en el centro de trabajo, desde sus casas, o desde cualquier parte de mundo.

Participante 2: Dijo que se comparte con los usuarios que el administrador de red informática lo permite; sin embargo, al usar servidores externos para el soporte de este sistema, pues somos dependientes del proveedor; si bien es cierto que al pagar el servicio de dominio nos ofrecen cierto grado de confidencialidad y seguridad, pero seguimos siendo dependientes de empresas o proveedores externos y que en muchas veces no sabemos ni en qué país están ubicados físicamente estos servidores.

Participante 3: Dijo que sí es compartida en la nube, para eso emplea los servicios de dominio y un hosting, a fin de que puedan ser publicados en el internet y que los usuarios puedan acceder desde cualquier lugar y dispositivo con acceso a internet.

Participante 4: Dijo que sí es compartida en la nube, con el propósito que los usuarios puedan tener acceso desde cualquier dispositivo con acceso a internet.

Participante 5: Mencionó que tengo conocimiento que es así, la 5ª Brig. Mtñ. emplea los servicios de dominio y hosting, con la finalidad de poder publicar la información en internet, y que los usuarios puedan acceder a ella desde cualquier dispositivo.

Participante 6: Dijo que desde el año 2021 pasado, nuestros tramites documentarios se comparten por la nube, esto nos facilita conocer y dar trámite en tiempo y espacio la rapidez en la información las 24 horas del día mediante un soporte de sistema de servicio de dominio que si bien es cierto se paga para cierto grado de confidencialidad y seguridad, todavía seguimos siendo vulnerables con nuestra información de confidencialidad porque todas nuestras informaciones se van a estos servidores de estas empresas y proveedores externos.

6. ¿Cuáles son los riesgos que suponen el uso de los sistemas informáticos, cuando se acceden desde dispositivos externos?

Participante 1: Dijo que siempre existe el riesgo de intromisión, robo de información; y se debe por una mala operación de los usuarios, porque usan sus claves en lugares públicos, o porque dan sus contraseñas a otras personas. El personal de informática hace los esfuerzos para proteger nuestros sistemas de información; sin embargo, existe un riesgo que no se puede controlar: que es el Usuario, y eso lo saben muy bien los piratas informáticos, es por ello que a través de la ingeniería social intentar obtener cuentas de usuario válidas para poder acceder a las bases de datos y a las informaciones.

Participante 2: Mencionó que a cualquier riesgo informático y esto va a depender de la intención y conocimiento del usuario del dispositivo externo, puesto que se está abriendo una puerta de entrada a nuestra red informática en otras palabras, estamos

dando un punto vulnerable en nuestra red que fácilmente puede ser aprovechado por cualquier persona o agente externo.

Participante 3: Dijo que cuando se accede a un sistema desde dispositivos externos (no controlados por la seguridad de la institución), se corre el riesgo de captura de datos de acceso a la aplicación, los cuales pueden ser compartidos con personal no autorizado para que ingresen y hagan uso del sistema.

Participante 4: Dijo que se corre el riesgo de captura de datos de acceso a la aplicación, los cuales pueden ser compartidos con personal no autorizado para que ingresen y hagan uso del sistema. También puede ocurrir una suplantación de identidad.

Participante 5: Dijo que, al acceder desde dispositivos externos, se abre una puerta de entrada a la red informática de la 5ª Brig. Mtñ. lo que lo hace vulnerable a muchos riesgos externos.

Participante 6: Mencionó que siempre habrá riesgos a los sistemas informáticos en todo momento desde los usuarios y los intrusos que son personas no autorizadas que se introducen en los programas y archivos para espiar, robar o destruir información.

7. ¿Cuáles son los dispositivos más comunes que son empleados en la 5ª Brigada de Montaña para acceder a los sistemas de información? Explique.
   Participante 1: Dijo que laptop y desktop, aunque los sistemas por tener tecnología responsive, pueden ser utilizados desde un celular o una Tablet.

   Participante 2: Dijo que las computadoras, celulares, Tablet, ya que a través de la conexión a internet permiten acceder a los sistemas de la 5ª Brigada de Montaña como el sistema QUIPHU, mesa de partes y otros. En el caso de la mesa de partes virtual deberíamos tener cuidado, ya que podría ser una puerta o punto de conexión a nuestra red vulnerable que podría ser usado por cualquier persona y de cualquier punto del planeta para intentar vulnerar la red informática.

   Participante 3: Dijo que el sistema de tramite documentario, permite su empleo desde cualquier dispositivo con acceso a internet, y los más empleados son las laptops, desktop, tablet y los teléfonos celulares.

   Participante 4: Dijo que los más empleados son las laptops, tablet y los teléfonos celulares.

   Participante 5: Dijo que los más empleados son las laptops, desktop, tablet y celulares.

Participante 6: Dijo que los dispositivos más comunes y usados para el intercambio de información son las Laptops, Computadoras, celulares propios de cada usuario, Tablet, ya que a través de esta conexión a internet permiten acceder a la plataforma QUIPU de la 5ª Brigada de Montaña.

8. ¿Como puede afectar la falta de seguridad a la información que se gestiona por los sistemas de tramites documentarios que son empleados por la 5ª Brigada de Montaña?
Participante 1: Acotó que puede ocurrir robo de información, o que información clasificada aparezca por otro lado; o en manos de elementos externos a la institución; sin embargo, se ha adoptado todas las medidas de seguridad disponibles para evitar la pérdida de información como almacenar la documentación cifrada; sin contar que hacemos copias de seguridad (backup) a fin de evitar pérdidas de información.

Participante 2: Acotó que, Podríamos ser víctimas de robo de información, hackeos, acciones de ciberinteligencia por parte de países que tengan interés en obtener información de nuestra Brigada, como por ejemplo Chile, Bolivia, etc. También podríamos ser víctimas de la pérdida total de nuestra información, si es que no contamos con las medidas de seguridad informática ya sea virtual o física. Asimismo, podría estar afectando la seguridad de la información, si el sistema no ha recibido la autorización de uso correspondiente y los niveles de seguridad que establece la DUFSITELE (Directiva Única de Funcionamiento del Sistema de Telemática del Ejército) y otras normas y directivas que establece el órgano de línea encargado en nuestro Ejército (CITELE: Ciberdefensa y telemática del Ejército).

Participante 3: Acotó que la seguridad es un componente clave en todo sistema, no puede existir un sistema en producción sin el componente de seguridad, porque estarían exponiendo los datos de la empresa al alcance de todos (es como construir nuestra casa y no considerar una puerta principal). Al estar expuestos los datos del sistema, serán indexados por los motores de búsqueda y estaría disponible para cualquier usuario de internet, afectando la imagen, credibilidad y confidencialidad de la institución.

Participante 4: Acotó que la falta de seguridad a la información, lleva inevitablemente al acceso no autorizado de datos de la Brigada, estos podrían ser fallos intencionales, fallos del propio sistema y fallos causados por error humano.

Participante 5: Acotó que la falta de seguridad en el sistema informático, puede ocasionar el robo de la información, suplantación, hackeos, acciones de ciber inteligencia, y pérdida parcial o total de la información.

Participante 6: Acotó que el más común seria al robo de información, hackeos y otras acciones que permitan vulnerar nuestra seguridad de información.

9. ¿Qué políticas o medidas de ciberseguridad se disponen y cuales pueden implementarse, para evitar ser monitoreados por externos? Es decir que se pueden implementar para evitar los ataques cibernéticos, ¿Las medidas que existen son viables?

   Participante 1: Dijo que, no existen sistemas 100% seguros; sin embargo, debemos considerar:

   - Disponer de un firewall de seguridad.
   - Un sistema operativo actualizado.
   - El firewall de cada computadora activado.
   - Tener el antivirus actualizado.
   - No ingresar a páginas de dudosa procedencia.
   - No realizar conexiones punto a punto.
   - No recibir correos electrónicos o hacer click en enlaces que no solicitamos.
   - Dar charlas de seguridad de las informaciones al personal a fin de evitar que sean víctimas de la ingeniería social.

   Participante 2: Dijo que, Uso de firewall, VPN´s, códigos fuente propios de las aplicaciones que usemos, acceso monitoreado y autorizado solo por el administrador a los usuarios de la 5ta Brig. Mtñ, también debería hacerse auditorias informáticas periódicas, a fin de detectar cualquier punto vulnerable en nuestros equipos o sistemas informáticos. Además, soy de la opinión que una de las medidas más importantes que contribuyen a mejorar las medidas de seguridad en cualquier red informática es la concientización y capacitación del personal en todos los niveles, incidiendo bastante en el nivel usuario.

   Participante 3: Dijo que ninguna política evita ser monitoreado o atacado. Los mecanismos para minimizar el riesgo de ataque son:

   - Firewall con protección DDoS.
   - Sistemas operativos actualizados.
   - Hacer uso de herramientas de desarrollo licenciadas.
   - Sistema implementado en ambiente de producción en una DMZ.
   - Los sistemas deben ser construidos haciendo uso de los estándares de desarrollo seguro según OWASP.
   - Uso de herramientas para validar que las Aplicaciones Web sean seguras.

- Participante 4: Mencionó que:
- Debemos seguir capacitando al personal usuario para que no caigamos en error humano.
- Realizar copias de seguridad.
- Control de acceso a los datos más estrictos.
- Utilizar contraseñas seguras.
- Involucrar a toda la Brigada en la seguridad.
- Monitorear constantemente la información que brindamos.

Participante 5: Acotó que empleo adecuado de firewall, VPN´s, códigos fuente propios de las aplicaciones que usemos, auditorias informáticas periódicas a fin de detectar cualquier punto vulnerable en nuestros equipos o sistemas informáticos. Además, uno de los aspectos más importantes es crear conciencia de seguridad en el personal.

Participante 6: Dijo que hasta el momento no hay programas informáticos 100% seguros, pero el uso de firewall y otros programas informáticos de seguridad limitaría a que agentes externos maliciosos roben información y vulneren nuestros equipos o sistemas informáticos.

10. ¿Se implementan funciones de supervisión, generación de informes y alertas de eventos de seguridad a los sistemas informáticos?
    Participante 1: Acotó que nuestro sistema de tramite documentario no genera informes de seguridad, sin embargo, se ha implementado un registro de todas las operaciones que realizan los usuarios al cual se le denomina “archivos LOG.”

    Participante 2: Dijo que “no tengo conocimiento”, en vista que eso lo monitorea directamente el administrador de la red (SETEL).

    Participante 3: Dijo que, el sistema en la actualidad, si es supervisado por el personal especialista. Sin embargo, no está programado para generar informes ni alertas sobre eventos de seguridad.

    Participante 4: Acotó que el sistema es monitoreado permanentemente por el personal de la sección telemática de la 5ª Brig. Mtñ., no tengo la seguridad de que generen informes ni alertas de seguridad.

    Participante 5: Dijo que el sistema en la actualidad, es supervisado por el personal especialista. Sin embargo, no genera informes ni alertas sobre eventos de seguridad.

    Participante 6: Dijo que tengo conocimiento que el personal que supervisa y realiza el control desde el punto de vista seguridad, es el administrador de la red (SETEL).

11. ¿Existen elementos para la detección de anomalías y la detección de intrusos?

    Participante 1: Dijo que, nuestros sistemas de información y sobre todo nuestra base de datos dispone de sistemas de detección de anomalías a través de archivos “LOG”, que son archivos de configuración y registro de los accesos a las bases de datos; los cuales nos indican el momento exacto (días, horas, minutos y segundos), en que un usuario ingresó y las operaciones que realizó; esto a fin de evitar que los usuarios dentro de la red y/o elementos externos puedan alterar las informaciones. Si alguien lo hizo podemos identificar quien, cuando, donde, y que lo realizó.

    Participante 2: Mencionó que, si existen, pero no sé si la 5ta Brig. Mtñ lo dispone, en vista que eso lo monitorea directamente el administrador de la red (SETEL). También es preciso mencionar que este equipamiento es altamente costoso y debe ser complementado por personal especializado para su operación.

    Participante 3: Dijo que la base de datos dispone de sistemas de detección de anomalías a través de archivos “LOG”, que indican el momento en que un usuario ingresa. Pero no tengo la seguridad de que tenga la capacidad de detectar intrusos.

    Participante 4: Dijo que se disponen de elementos para la detección de anomalías y la detección de intrusos, pero no tengo la certeza de saber cuan efectivos son en realidad.

    Participante 5: Mencionó que el sistema tiene la posibilidad de detección de anomalías, pero no tengo la seguridad de que tenga la capacidad de detectar intrusos, en vista que son muy difíciles de detectar.

    Participante 6: Dijo que, si existen y son monitoreados directamente por el administrador de la red (SECCION TELEMATICA).

12. ¿Qué propone en caso no exista, o cómo se debe mejorar?

    Participante 1: Dijo que se propone continuar trabajando en la seguridad de las informaciones, implementar nuevos sistemas de seguridad, actualizar nuestros sistemas y actualizar al personal técnico, ya que la ciencia y la tecnología avanzan a pasos agigantados y cada vez aparecen nuevos riesgos de seguridad. Muchos piensan que los sistemas funcionan solos, pues desconocen que detrás de un sistema debe haber un equipo que brinde soporte técnico para que todo pueda funcionar con normalidad; (mientras no suceda nada significa que el equipo está trabajando, pues los problemas empiezan cuando este equipo deja de trabajar).

Participante 2: Mencionó que, de no existir se debería invertir en la infraestructura necesaria para el equipamiento que permita tener esa capacidad, ya que existen riesgos potenciales y latentes y más si se trata de una brigada que geográficamente está ubicada en el sur y que su sector de responsabilidad es fronterizo, en consecuencia es necesario que la compañía de comunicaciones como unidad ejecutante de las acciones en ciberseguridad y ciberdefensa de acuerdo a la nueva doctrina del SITELE (Sistema de Telemática del Ejercito), se alinea tanto en su organización, asignación de personal y sea debidamente equipada. En conclusión, se debería adquirir el equipamiento necesario, la tecnología de última generación y la capacitación especializada del personal involucrado en la administración de nuestros sistemas informáticos.

Participante 3: Dijo que, seguir capacitando al personal técnico, en ciberseguridad, para que vuelquen sus conocimientos y permitan mejorar los procedimientos de seguridad de nuestros sistemas informáticos. Incidir en incrementar la conciencia de seguridad del personal que hace uso de estos sistemas, pues no sirve de nada invertir en seguridad, si es que los usuarios de estos sistemas no le dan la importancia que corresponde

Participante 4: Mencionó que se deben tener en cuenta las siguientes consideraciones:

- Planificar: Fijar una política de seguridad, identificar, analizar y evaluar riesgos, evaluar alternativas de riesgo, definir controles de seguridad.
- Hacer: Establecer un plan de tratamiento de datos. definir un sistema de medidas para evaluar los controles. implantar procedimientos para detectar y resolver los incidentes de seguridad.
- Verificar: Revisar regularmente la efectividad del sistema. actualizar los planes de seguridad, revisar constantemente las evaluaciones de riesgo. realizar periódicamente auditorías internas a los usuarios del sistema.

Participante 5: Mencionó que capacitación del personal técnico, concientización de los usuarios de los sistemas de tramites documentario en lo que respecta a medidas de seguridad. Invertir en sistemas de seguridad digital.

Participante 6: Dijo que en caso de no existir lo principal seria seguir capacitando y especializando al personal militar y civil que por su cargo y función en la 5ª Brigada de Montaña manipulan esta plataforma de tal forma de crear en todo momento conciencia de seguridad.

13. ¿Cómo son las contraseñas de los usuarios en los servicios de autenticación?

    Participante 1: Dijo que, una contraseña mientras más caracteres especiales tenga es más robusta; al crear una contraseña se debe tener en cuenta lo siguiente:

    - Evitar usar nombres de personas, familiares o mascotas
    - Evitar usar números de DNI, fechas de nacimiento o similares
    - Evitar cosas sin sentido (te puedes olvidar)
    - Se debe usar contraseñas largas (mientras más larga es mejor)

    En nuestro sistema de tramite documentario, yo como administrador del sistema tengo la potestad de crear usuarios con sus contraseñas y darle los privilegios que le corresponden; naturalmente creo una contraseña con información del usuario con una Seguridad Media, para ello empleo caracteres especiales. Sin embargo, es responsabilidad del usuario cambiar la contraseña para que solo esa persona disponga de su contraseña y ni el administrador pueda ingresar a ver su información.

    Participante 2: Dijo que, a través de uso de letras, números y símbolos.

    Participante 3: Acotó que, si bien es cierto que los responsables del sistema de tramite documentario, asignan usuarios y contraseñas, con mediana seguridad, al personal que hace uso de este sistema. En mi caso en particular, no he cambiado la contraseña por una más robusta. En vista que no fue un requisito para poder acceder al sistema y por descuido de mi parte.

    Participante 4: Acotó que, en mi caso en particular, no he cambiado la contraseña por una más robusta. En vista que no se me enseño el procedimiento para poder realizarlo.

    Participante 5: Dijo que por defecto fueron asignados usuarios y contraseñas, que guardan relación con sus datos personales, tengo conocimiento que la mayoría no ha cambiado sus contraseñas, en vista que no fue exigido por la sección responsable del control del sistema, además en la instrucción sobre el uso del sistema, tampoco se enseñó el procedimiento para poder realizarlo. Por lo que las contraseñas no son de mediana seguridad.

    Participante 6: Acotó que las contraseñas son creadas por el administrador del SETEL, a través del uso de letras, números y símbolos.

14. ¿Son robustas?

    Participante 1: Dijo que las contraseñas iniciales son de Seguridad Media y son relativamente robustas, ya el usuario debe cambiar su contraseña empleando Letras

mayúsculas y minúsculas, números y caracteres especiales como *, $, &, #, etc., para que sus contraseñas sean lo más robustas posibles.

Participante 2: Mencionó que no, debido a que en muchos casos se usan información de los mismos usuarios, como DNI, CIP u otros.

Participante 3: Acotó que en la actualidad la contraseña que estoy empleando, es de mediana seguridad, no fue cambiada por una más robusta.

Participante 4: Mencionó que la contraseña que estoy empleando, es de mediana seguridad.

Participante 5: Dijo que no lo son, porque no han sido actualizadas, están siendo empleadas las que fueron asignadas por el administrador del sistema.

Participante 6: Dijo que son ligeramente robustas, no me he tomado la molestia de cambiarla por una mejor.

15. ¿Qué normas tiene que cumplir el personal, para protegerse de un ataque cibernético o ser monitoreados por externos? Es decir, qué medidas de seguridad debe aplicar cada participante)
    Participante 1: Mencionó que, la seguridad física está orientada a proteger los equipos de cómputo (servidores, terminales, computadoras, etc.), Periféricos de E/S (impresoras, proyectores, scanner, etc.), medios de almacenamiento (discos duros, CD, DVD, disquetes, memoria USB.

    La seguridad lógica está orientada a proteger el software, la información almacenada. Para lo cual se debe adoptar acciones de contingencia para prever los siguientes riesgos:

    - Ataque de elementos expertos como Hackers y Crackers.
    - Ataques de espías y piratas informáticos.
    - Controles de accesos, identificación y autenticación.
    - Virus, troyanos y gusanos.
    - Infidencia informática.
    - Proveedores de correo electrónico (Hotmail, Gmail, Yahoo, etc.), abiertos a la explotación directa de las instituciones
    - Negación de servicios.
    - Personal desafecto, etc.

Participante 2: Acotó que, cumplir todas las normas y disposiciones en cuanto a ciberseguridad dadas por la 5ta Brigada de Montaña y por el CITELE. Además, con la concientización de todos los usuarios, teniendo en cuenta que todo sistema informático es vulnerable y más si está conectado a internet.

Participante 3: Mencionó que dar cumplimiento a las políticas para minimizar riesgos en los sistemas de seguridad de información en la 5ª Brigada Montaña. Sin embargo, este documento no es de conocimiento de todo el personal que hace uso de los sistemas informáticos, y no se ha verificado que todo el personal que hace uso de estos sistemas, haya cumplido cada una de las políticas de seguridad.

Participante 4: Compartió lo siguiente:

- Contar con un Plan de respuesta a incidentes de seguridad en nuestros sistemas.
- Detener o invalidar la conexión con IP inválidos.
- Revisar la configuración de los firewalls.
- Contar con un sistema de detección y prevención de intrusiones no autorizadas.
- Limitar el tráfico de información desde un único host.
- Limitar el número de conexiones concurrentes al servidor.

Participante 5: Dijo que se deben dar cumplimiento a las políticas de seguridad del instituto y de la 5ª Brig. Mtñ. sin embargo, estas disposiciones no son de conocimiento de todos los usuarios y no se incide en el cumplimiento de las mismas.

Participante 6: Dijo que, se deben cumplir en todo momento con las normas y disposiciones de las directivas del escalón superior en cuanto a seguridad cibernética y ciberseguridad teniendo en cuenta que todo sistema y plataforma informático es vulnerable y más si está conectado a internet.

16. ¿Qué frecuencia de mantenimiento tienen los equipos vinculados a la informática? por ejemplo cambio de contraseña, actualización del sistema, etc.

Participante 1: Acotó que, a los equipos de seguridad informática permanentemente se le hace mantenimiento a fin de evitar que se dañen o malogren, disponen de un sistema eléctrico con Estabilizadores, UPS con bancos de baterías para tener un funcionamiento permanente; de igual manera las contraseñas son cambiadas cada cierto tiempo y solo yo conozco las contraseñas de los servidores, dominio, hosting; respecto a las actualizaciones de los sistemas, estos siempre están actualizados.

Participante 2: Dijo que, se realiza periódicamente y de acuerdo al criterio de los administradores de los sistemas informáticos.

Participante 3: Dijo que el mantenimiento es permanente, con respecto al cambio de contraseñas, desde que se inició el uso de este sistema, hace más de un año, no se ha exigido el cambio de la contraseña, Es responsabilidad de cada usuario, pero en nuestro entorno, sería recomendable que se exija al personal a realizar el cambio de contraseña, lo que puede ser verificado por la sección telemática. Con respecto a la actualización de sistemas, si se realiza con regularidad.

Participante 4: Acotó que el mantenimiento es permanente, no se ha exigido el cambio de las contraseñas, la actualización de sistemas si se realiza con regularidad.

Participante 5: Dijo que el mantenimiento y la actualización del sistema es permanente, sin embargo, no se exige el cambio de las contraseñas, lo que puede afectar la seguridad del sistema.

Participante 6: Dijo que según normas y disposiciones el mantenimiento a los equipos vinculados a la informática es en forma periódica.

17. ¿Qué plan de emergencia tiene la 5ª Brigada de Montaña en caso sufran de un ataque cibernético? Explicar y proponer algunas medidas.
    Participante 1: Dijo que la directiva anteriormente mencionada contempla planes de emergencia y respuesta inmediata ante algún ataque cibernético; y la forma las fácil y simple que he encontrado es la de aislar la red. Esto va a tener consecuencias ya que me va a acarrear la denegación de los servicios y ningún usuario va a poder acceder a los sistemas; pero considero que es un costo demasiado bajo que tenemos que asumir (poniendo a la balanza la denegación del servicio y el robo de información; prefiero denegar el servicio por un tiempo hacer actualizaciones eliminar los riesgos)

    Participante 2: Acotó que, “no tengo conocimiento” si existe, algún plan de emergencia y si es que tenemos la capacidad de respuesta ante un ataque cibernético, ya que depende del equipamiento necesario y de personal altamente especializado.

    Participante 3: Dijo que, en los documentos referidos a las políticas para minimizar riesgos en los sistemas de seguridad de información en la 5ª Brigada Montaña, no especifica ningún plan de emergencia en caso se sufra un ataque cibernético. Tampoco se me hizo conocer si existe algún plan. Por lo que no tengo conocimiento de cuál sería el procedimiento.

    Participante 4: Dijo que no se ha comunicado sobre la existencia de algún plan de emergencia en caso se sufra un ataque cibernético, tampoco de los procedimientos a realizar en caso de que ocurra un ataque cibernético.

Participante 5: Acotó que, “no tengo conocimiento” de la existencia de algún plan de emergencia en caso se sufra un ataque cibernético

Participante 6: Acotó que, en el mes de enero del presente año, la sección de Telemática ha emitido la DIRECTIVA Nº 002 - 2022/5ª BRIG MTÑ/SETEL/13.00 (POLÍTICAS PARA MINIMIZAR RIESGOS EN LOS SISTEMAS DE SEGURIDAD DE INFORMACIÓN EN LA 5ª BRIG MTÑ). En este documento básicamente se habla sobre la seguridad física y la seguridad lógica que debemos darles a las informaciones.

18. ¿Qué posibilidades existen de implementar un sistema de detección de alertas, imprevistos o de presencia de productos nocivos que pueden presentarse en el ámbito de la 5ª Brigada de Montaña?

Participante 1: Dijo que siempre hay la posibilidad de mejorar nuestros sistemas; la ciencia y la tecnología avanza a pasos agigantados, para bien y para mal, entonces nosotros debemos estar a la vanguardia de los nuevos productos, nuevos sistemas de seguridad y sobre todo de los nuevos peligros existentes a fin de poder implementar sistemas para contrarrestar las principales amenazas. Se pueden implementar sistemas de detección de intrusos, sistemas de firewall de seguridad sistemas de video-vigilancia, etc. pero ello no nos garantiza estar 100% seguros.

Participante 2: Dijo que, posibilidades hay muchas, pero depende de cuánto invirtamos y cuanto personal especializado dispongamos, así como el entendimiento y decisión del comando de la brigada y del escalón superior del Ejército.

Participante 3: Acotó que es necesario seguir supervisando, implementando y actualizando sistemas de detección de alertas. Siempre se puede mejorar estos sistemas. Y debemos estar a la par de los avances tecnológicos, que siempre traen consigo nuevas amenazas. Estas actividades deben tener una alta prioridad, para un correcto funcionamiento de los sistemas informáticos.

Participante 4: Acotó que, si es posible, para eso se deben destinar los fondos que permitan mejorar el sistema. Este tipo de sistemas necesitan un mantenimiento permanente, por lo que es necesario invertir en él, a fin de in mejorarlo.

Participante 5: Dijo que es posible implementar y mejorar el sistema, para lo cual deben solicitar el presupuesto necesario para que se haga efectivo. Para lo cual se debe tener en consideración que los avances tecnológicos, siempre traerán consigo nuevas amenazas.

Participante 6: Dijo que en prospectiva siempre habrá posibilidades, sobre todo en este mundo que cada vez es cambiante con respecto en la tecnología que avanza rápidamente, y nosotros que somos parte de ella debemos estar especializados y capacitados en seguridad cibernética y ciberseguridad, esto también dependerá de la decisión de nuestros comandos.

19. ¿Cómo debe realizarse la configuración de seguridad de los sistemas informáticos, antes de hacer uso de ellos?

Participante 1: Mencionó que, hay varios aspectos que podemos tomar en cuenta:

- Primero debemos de disponer de un firewall de seguridad bien configurado y actualizado.
- Tratar de evitar utilizar dispositivos inalámbricos, porque cada wifi es una puerta abierta que podría ser incontrolable para el firewall de seguridad.
- Actualizar los sistemas operativos de las computadoras.
- Tener nuestro antivirus actualizado.
- Capacitar al personal.
- Restringir el Acceso solo para personal autorizado.

Participante 2: Mencionó que, usando dispositivos físicos que permitan niveles de seguridad, como firewall, servidores, contraseñas seguras, evitando conectarse de dispositivos externos o desconocidos, redes no seguras, puntos de internet no confiables, etc.

Participante 3: Mencionó que se debe tener en cuenta lo siguiente:

- Disponer de un firewall bien configurado y actualizado.
- Actualizar los sistemas operativos de los dispositivos electrónicos que serán empleados para abrir los sistemas informáticos.
- Disponer de un antivirus actualizado.
- Disponer contraseñas robustas, por parte de los usuarios de los sistemas informáticos.

Participante 4: Mencionó que se debe tener en cuenta lo siguiente:

- Disponer de un antivirus originales y actualizados.
- Actualizar los sistemas de seguridad de los dispositivos electrónicos que serán empleados para abrir los sistemas informáticos.
- Disponer contraseñas robustas, por parte de los usuarios de los sistemas informáticos.
- Contar con Certificados de servidor seguro.
- Poder pedir ayuda al proveedor de servicios de internet.

Participante 5: Mencionó que se debe tener en consideración lo siguiente:

- Usar antivirus adecuados que permitan protegerse de virus, spyware y demás amenazas. Un sólo equipo desprotegido puede afectar a la seguridad de todo el sistema informático.
- Usar un buen firewall para proteger el acceso a la red privada y poder cifrar la información que se envíe por la red.
- Usar contraseñas fuertes en los Wifi.
- Mantén los ordenadores actualizados.
- Usar contraseñas seguras.
- No instalar programas procedentes de fuentes desconocidas desde internet.
- Configurar el bloqueo del ordenador. Para evitar dar acceso a tu ordenador, a sus datos y a la red de la empresa a todo el que haya pasado por su delante.
- No conectar con frecuencia discos externos.
- Configurar copias de seguridad automáticas de los datos importantes.
- Usar la nube con criterio, asegúrate de emplear una empresa de confianza.

Participante 6: Mencionó que la configuración de seguridad se realiza usando programas informáticos de soporte de seguridad como son el Firewall actualizado, y otros que permitan la seguridad cibernética en la red de la 5ª Brigada de Montaña.

20. ¿Qué acciones propone para aplicar la ciberseguridad en los sistemas informáticos?

Participante 1: Dijo que se proponen sistemas de seguridad criptográfica; debemos de almacenar todos nuestros archivos, documentos, bases de datos, todo debe estar cifrado y con un método propio. Nuestro sistema de tramite documentario almacena todos los archivos cifrados; pero sería bueno que la base de datos también esté cifrada; claro que la base de datos solo almacena datos generales, títulos, fechas, mas no contenido de los documentos, sin embargo, esto puede ser tentador para un hacker ya que le puede dar información de donde buscar y que buscar.

Participante 2: Dijo que, usando equipos de seguridad informática a nivel físico y de software, cumpliendo todas las normas y disposiciones en cuanto a ciberseguridad y ciberdefensa, realizando las actualizaciones oportunas, contando y manteniendo actualizado a nuestro personal especialista. Por último; creo que debemos partir teniendo en nuestra organización tanto a nivel brigada (SETEL), Compañía Comunicaciones y todas las unidades que la integran, incluyan un grupo de ciberseguridad y ciberdefensa, así como guerra electrónica, ya que si bien es cierto aun no contamos con el equipamiento necesario, sin embargo en una situación real necesariamente tendrían que dotarnos de ese equipamiento, además para el caso de ciberdefensa o ciberseguridad las primeras acciones para protegernos empiezan por normar y concientizar a todo nuestro personal, en consecuencia si ni siquiera lo tomamos en cuenta, nunca lograremos tener esa capacidad y pueden estar

sucediendo cosas en el ciberespacio que ni cuenta nos damos.

Participante 3: Dijo que, todo sistema tiene dos componentes claves:

a. Componente de Software
    1) Software Base. Tener actualizado el software base con los parches de seguridad sugeridos por el fabricante.
    2) Servidor de Aplicaciones: Actualizado a la última versión y con soporte del fabricante.
    3) Sistema desarrollado:
        - No hacer uso de componentes gratuitos o de empresas no reconocidas.
        - Seguir los estándares de desarrollo seguro sugerido por el OWASP.
        - Hacer uso de Herramientas para validar el uso de estándares de seguridad en la aplicación.
        - Los datos del sistema deben estar encriptados, minimizando el riesgo de acceso a la información ante un posible hackeo.
b. Componente de Infraestructura
    1) Alojar el sistema en un Servidores Cloud:
        - Microsoft Azure, AWS o Google Cloud.

Participante 4: Dijo que las acciones que propone son:

- Nunca dar información confidencial por internet.
- Crear contraseñas difíciles de adivinar.
- Utilizar y actualizar constantemente los antivirus y firewalls.
- Crear conciencia de ciberseguridad, a base de instrucción permanente.
- no conectar USB o discos externos.
- Uso de la nube con mucho criterio.
- Control del empleo de los equipos solo por personal autorizado.
- No perder de vista a los dispositivos móviles, para evitar que sean manipulados y/o robados.
- Actuar siempre con paciencia y sentido común, el eslabón débil de la cadena de seguridad son los usuarios.
- Implementación de los siguientes sistemas de seguridad:
    - ✓ Servidores de Datos, que permitan separar la base de datos de las aplicaciones e independizar el servidor de datos en una zona DMZ
    - ✓ Firewall de seguridad, que controlen los accesos a la plataforma virtual, así como los accesos a las bases de datos, a las aplicaciones y eviten la intromisión de personas no autorizadas (hacker, crackers, spam, virus, etc.)
    - ✓ Cifradores de datos, que permitan encriptar todos los datos y que la información esté disponible solo para el personal autorizado.

Participante 5: Dijo Con la finalidad de evitar ser vulnerables frente a las diversas amenazas que actualmente existen para las instituciones, se debe considerar el empleo de Firewall de seguridad en hardware que empleen seguridad por capas: capa de red, capa de transporte de datos, capa de aplicaciones, que deben ser capaces de identificar y controlar las aplicaciones, autenticación de los usuarios, protección contra malware, protección contra exploits, filtrado de contenido (incluido el filtrado de URL) y control de acceso basado en la ubicación.

Participante 6: Dijo que, propondría equipos, plataformas y sistemas de seguridad informática, ciberseguridad y cibernética, cumpliendo a detalle todas las normas y disposiciones de las directivas emanadas del escalón superior.

Se debe tener en consideración el empleo de las siguientes normas:

- Las normas ISO 27000: Gestión de la Seguridad de las Informaciones
- ISO 27001: Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Es la norma con arreglo a la cual se certifican por auditores externos. Su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI.
- ISO 27002: Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.
- ISO 27005: Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.
- ISO 27006: Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.
- ISO 27000: Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de la Seguridad de la Información (SGSI). Generalidades y vocabulario.
- ISO 27003: Sistema de Gestión de la Seguridad de la Información (SGSI). Guía de implantación.
- ISO 27004: Tecnología de la información. Técnicas de Seguridad. Gestión de la Seguridad de la Información. Métricas.
- ISO 27007: Tecnología de la información. Técnicas de Seguridad. Guía de auditoría de un SGSI.
- UNE-EN ISO 27799:2010 Informática sanitaria. Gestión de la seguridad de la información en sanidad utilizando la Norma ISO/IEC 27002 (ISO 27799:2008).

Transcripción de la entrevista para el personal de otras instituciones.

1) ¿Conoce el funcionamiento del sistema de trámite documentario que se utiliza en la 5ª Brigada de Montaña?

   SI tengo conocimiento del funcionamiento del sistema de trámite documentario que es empleado por los usuarios de la 5ª Brigada de Montaña. El mismo que permite gracias a los servicios de la nube, que se pueda acceder a la información desde cualquier medio tecnológico que disponga de una conexión a internet, Soy de la opinión que el sistema es una buena herramienta para agilizar la documentación que se maneja en las dependencias

2) ¿Cuáles son los riesgos que suponen el uso de los sistemas informáticos, cuando se acceden desde dispositivos externos?

   Como todos los sistemas que se funcionan en línea, ninguno está libre de un ciberataque. Es cuestión de tiempo, lo importante es tener la capacidad de poder resistir los ataques y recuperarse de forma rápida y efectiva, para asegurar la integridad y funcionamiento de todos sus sistemas.

3) ¿Cuál es su opinión de los servicios en la nube que emplea la 5ª Brigada de Montaña?

   Las empresas proveedoras de servicios en las nubes, disponen de tecnologías y protocolos que permiten proteger los entornos informáticos en la nube, se debe tener en cuenta que es importante elegir un proveedor que garantice la seguridad de sus informaciones, además deben concentrarse en la configuración adecuada del servicio y en asegurar los hardware y las redes de los usuarios.

4) ¿Qué políticas o medidas de ciberseguridad pueden implementarse, para los usuarios a fin de evitar los ataques cibernéticos?

   Con frecuencia se debe dar chaslas sobre normas de ciberseguridad, que incluyan buenas prácticas en el uso de los sistemas informáticos. Es muy importante verificar su cumplimiento, por lo que se debe elaborar un plan de verificación del desempeño de los usuarios, respecto al cumplimiento de las normas de seguridad.

5) ¿Qué acciones o tecnologías de seguridad propone para incrementar la ciberseguridad de los sistemas informáticos de la 5ª Brig. Mtñ?

   Se recomienda implementar lo siguiente:

- A fin de incrementar la seguridad de los servicios de la nube, deben evalauar migrar del proveedor de servicios de nuve actual al AWS, Google Cloud o AZURE, que tienen mayor respaldo y seguridad.
- Contar con un plan de verificación del cumplimiento de las normas de seguridad, para los usuarios de los sistemas informáticos.
- Implementación de doble factor de autenticación para ingresar al sistema, que da una seguridad adicional a los usuarios que la emplean.
- Implementación de una red privada virtual (VPN), para poder acceder a la red de la 5ª Brig. Mtñ. que permite a los administradores abordar los principales problemas de seguridad.