ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO

ESCUELA DE POSTGRADO

TESIS

POLÍTICAS INTEGRALES DE CIBERSEGURIDAD EN LA PROTECCIÓN DE LA INFORMACIÓN DIGITAL EN EL EJÉRCITO DEL PERU, 2023

AUTOR

Bach. MIGUEL ÁNGEL MARTÍNEZ ROSALES
0000-0002-3602-0359

Para optar el Grado Académico de

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

ASESOR

Dr. PEDRO ANASTASIO PAUCAR LUNA
0000 0002 8287 4064

LIMA-PERÚ
2024

ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO
ESCUELA DE POSTGRADO

DEPARTAMENTO GESTIÓN DE INVESTIGACIÓN

ACTA DE SUSTENTACIÓN DE TESIS No 018 – 2024/ DGI

En la Escuela Superior de Guerra del Ejército - Escuela de Postgrado, a los veintiocho (28) días del mes de agosto del año dos mil veinticuatro, siendo las ...15:30... horas, se reunió el jurado evaluador conformado por los docentes:

❖	**Doctor**	**GAMALIEL MANUEL GUSTAVO TALAVERA PRADO**	**Presidente**
❖	**Doctor**	**JOSE MANUEL PALACIOS SANCHEZ**	**Secretario**
❖	**Doctora**	**LILIANA RODRÍGUEZ SAAVEDRA**	**Vocal**

Designados según Resolución de Expedito para Sustentación de Tesis **N° 018-2024/SIE/DGI/ESGE-EPG** del 13 de agosto de 2024, para evaluar la sustentación presencial y defensa de la Tesis de Grado titulada **"POLÍTICAS INTEGRALES DE CIBERSEGURIDAD EN LA PROTECCIÓN DE LA INFORMACIÓN DIGITAL EN EL EJÉRCITO DEL PERÚ, 2023"**, presentado por el Bachiller **MIGUEL ANGEL MARTINEZ ROSALES**, 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 EXCELENCIA

En mérito del cual, el jurado ...APROBADO... (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 veintiocho (28) días del mes de agosto del año dos mil veinticuatro.

DR. GAMALIEL MANUEL GUSTAVO TALAVERA PRADO PRESIDENTE	DR. JOSE MANUEL PALACIOS SANCHEZ SECRETARIO	DRA. LILIANA RODRIGUEZ SAAVEDRA VOCAL

Autorización para Publicación y Uso

Yo. Bach. Miguel Ángel MARTÍNEZ ROSALES a través del presente documento autorizo a la Escuela Superior de Guerra del Ejército-Escuela de Postgrado la publicación del texto completo o parcial de la tesis de grado titulada: **Políticas integrales de ciberseguridad en la protección de la información digital en el Ejército del Perú, 2023,** presentada para optar al 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 Superintendencia Nacional de Educación Superior Universitaria (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.

Chorrillos 02 de abril de 2022

Bach. Miguel Ángel MARTÍNEZ ROSALES
DNI 16125380

Declaración Jurada de Autoría

Mediante el presente documento. Yo Bach Miguel Ángel MARTÍNEZ ROSALES identificado con Documento Nacional de Identidad N°16125380 con domicilio real en la Villa Militar Este, Block "J". Departamento No 101, Chorrillos, provincia de Lima, departamento de Lima, egresado de la Maestría en Ciencias Militares de la Escuela Superior de Guerra del Ejército-Escuela de Postgrado (ESGE-EPG) declaro bajo juramento que:

Soy el autor de la investigación titulada **Políticas integrales de ciberseguridad en la protección de la información digital en el Ejército del Perú, 2023**, que presento a los dos días del mes de abril del año 2024, ante esta institución con fines de optar al grado académico de Maestro en Ciencias Militares con mención en Planeamiento Estratégico y Toma de Decisiones.

Dicha investigación se ha desarrollado respetando los principios éticos propios 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 y otros que corresponden al suscrito o 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, duplicados 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 del Ejército-Escuela de Postgrado y me declaro como el único responsable.

Chorrillos 02 de abril de 2022

Bach. Miguel Ángel MARTÍNEZ ROSALES
DNI 16125380

Dedicatoria

Este aporte de la investigación se lo dedico a mi familia, a mi amada esposa Jessica, quien con sus palabras de aliento, consejos y caricias me motivo día a día a seguir, a mis hijos Adrian y Daixa que espero comprendan y me sepan disculpar por el tiempo robado y a mi madre que siempre creyó en mí.

Así también, agradecer a cada uno de mis compañeros de estudio, docentes y ascensores, quienes vertieron valiosos conocimientos los que han servido para culminar esta investigación

Lista de tablas

Capítulo I: Introducción

En la era digital actual, caracterizada por un rápido avance tecnológico y una avizorada demanda hacia el uso de las nuevas tecnologías y nuevas formas de comunicación a través de estas, es que se genera un nuevo problema de seguridad en este nuevo dominio, por lo que la ciberseguridad se hace indispensable y fundamental; por lo tanto, es inmensurable revisar exhaustivamente las políticas de ciberseguridad existentes y/o generar políticas apropiadas al respecto en el Ejército Peruano.

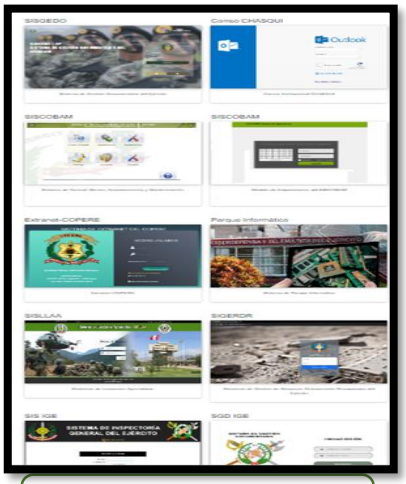
A pesar de los nuevos conocimientos en ciberseguridad a nivel global, el Perú se ve inmerso en un gran desafío en este nuevo dominio, constituyéndose los ciberataques, el espionaje y el sabotaje de forma digital, en un grave peligro para la seguridad de la información y la infraestructura critica digital, constituyendo un gran riesgo para la soberanía nacional.

El Ejército Peruano no es ajeno a estas amenazas. De hecho, se enfrenta a una serie de riesgos cibernéticos cada vez más sofisticados que podrían comprometer la seguridad nacional, la capacidad operativa y particularmente la integridad, confidencialidad y disponibilidad de la información en todos los niveles.

La falta de políticas de ciberseguridad adecuadas dejaría a las Fuerzas Armadas en general y particularmente al Ejército Peruano, expuesta a las diferentes modalidades de ataques informáticos. Es por ello que resulta imperativo desarrollar e implementar políticas integrales de ciberseguridad a fin de proteger y salvaguardar los activos digitales del Ejército y los activos críticos digitales de la nación que sean de responsabilidad del Ejército Peruano.

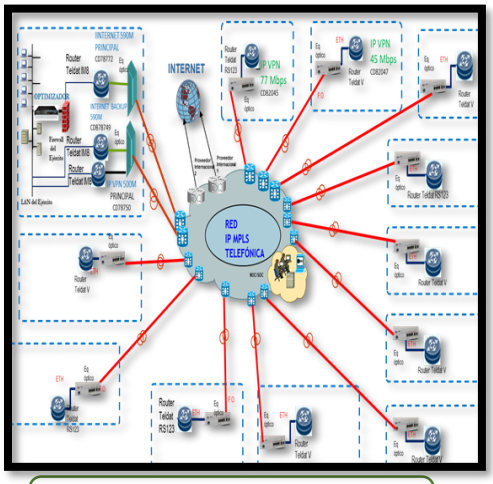
Figura 1.

Infraestructura critica por monitorear



APLICATIVOS INFORMATICOS

SALA DE SERVIDORES



INFRAESTRUCTURA DE RED

Nota: *La figura muestra la infraestructura critica que va a ser monitoreada por personal especialista*

Es de destacar también algunos de los ataques informáticos más notables que han tenido como objetivo a las Fuerzas Armadas del Perú y que a medida que el uso de la guerra cibernética se vuelve más común, es probable que las fuerzas armadas peruanas continúen enfrentando este tipo de ataques en el futuro; algunos acontecimientos sobre ataques cibernéticos ocurridos contra las fuerzas armadas del Perú a continuación se indican;

El 12 de julio de 2009, la Armada peruana sufrió un ataque de denegación de servicio distribuido (DDoS) que dejó sin servicio su portal sitio web y otros servicios que se realizan en línea, por un periodo de tiempo relativamente largo. Según análisis forenses se presume que el ataque fue con autoría de algunos grupos hacktivistas, por su modalidad, procedimiento y mensaje de protesta contra las acciones de los derechos humanos gestionadas en el gobierno peruano, aunque no hay evidencia contundente que lo confirme.

En el año 2011, la Fuerza Aérea del Perú sufrió un grave ataque cibernético cuando un malware de tipo troyano, con características parecidas al Stuxnet, infectó

sus sistemas informáticos. El malware se propagó a través de memorias USB infectadas y se dirigió específicamente a los sistemas de control de los misiles tierra-aire, causando una interrupción generalizada que incluyó la destrucción de datos y la inaccesibilidad a algunos servicios en línea. Se cree que el ataque fue obra del algún grupo cibernético, que presuntamente actuó con el apoyo de un gobierno extranjero.

En el año 2013, el Ejército peruano fue víctima de un sofisticado ataque de phishing por correo electrónico que engañó a un número no revelado de miembros del personal militar para que revelaran su información personal y credenciales de acceso. Los ciberdelincuentes luego utilizaron esta información obtenida de forma fraudulenta para acceder a los sistemas informáticos del ejército, lo que causó interrupciones en las operaciones durante varias horas. Aunque no hay evidencia que sugiera que se haya comprometido información confidencial, este incidente sirvió como un recordatorio alarmante de lo critico que significa de la seguridad digital en el entorno militar. Tras el ataque, los encargados de la ciberseguridad en el Ejército implementaron una serie de medidas para mejorar la postura en cuanto a la seguridad cibernética, incluyendo para tal caso, un aspecto muy importante como son las capacitaciones y la sensibilización sobre phishing para todo el personal, paralelamente se actualizaron los sistemas informáticos con las últimas medidas de seguridad.

En el año 2017, la Marina de Guerra del Perú fue víctima de un ataque cibernético por ransomware WannaCry que cifró una cantidad significativa de sus archivos. Los ciberdelincuentes iniciaron la campaña de extorción, exigiendo dinero a cambio de desencriptar sus archivos, caso contrario dejar encriptado sus archivos y vender información confidencial, pero la Marina con mucha responsabilidad se negó rotundamente a ceder ante esta extorsión. Gracias a la implementación de buenas prácticas, robustas medidas de seguridad como copias de seguridad en diferentes niveles y la oportuna resiliencia del personal técnico, se logró recuperar los archivos sin necesidad de negociar con los ciberdelincuentes. El ataque duró aproximadamente dos días y afectó principalmente a sistemas administrativos, sin causar daños en los sistemas críticos de la Marina.

A medida que el uso de la guerra cibernética se vuelve más común, es probable que las fuerzas armadas peruanas continúen enfrentando este tipo de ataques en el futuro algunos acontecimientos sobre ataques cibernéticos ocurridos contra las fuerzas armadas del Perú; Además de estos ataques específicos, también ha habido una serie de informes generales de intrusiones cibernéticas en las redes del gobierno peruano. En 2016, por ejemplo, el Ministerio de Defensa peruano reveló que también al igual que otros países de la región fue víctima de varios ciberataques. El ministerio también aclaro que los ataques habían causado algunas interrupciones, pero que no se habían comprometido datos confidenciales.

La creciente frecuencia de ciberataques contra las Fuerzas Armadas del Perú es motivo de preocupación. Estos ataques tienen sin duda alguna un gran impacto que puede causar daños colaterales a la infraestructura critica digital de la nación. También pueden dañar la reputación de las fuerzas armadas y hacer que sea más difícil reclutar y retener personal calificado.

El gobierno peruano ha tomado algunas medidas para mejorar la seguridad de sus redes informáticas. Sin embargo, se necesita hacer más para proteger a las fuerzas armadas de los ataques cibernéticos. El gobierno debe invertir en nuevas tecnologías de seguridad y capacitar a su personal sobre cómo identificar y responder a las amenazas cibernéticas. También es primordial trabajar con socios internacionales para socializar data correspondiente a amenazas y vulnerabilidades informáticas, para poder desarrollar de manera conjunta acciones y estrategias que puedan mitigar estos ataques en este nuevo dominio.

En base a lo expuesto, esta investigación la cual hace el enfoque de su objetivo principal el presentar una propuesta de políticas integrales de ciberseguridad que responda a las falencias específicas de seguridad digital en el Ejército del Perú. Esta política debe ser integral y holística, para cumplir con el rol de la protección de activos críticos digitales, gestión de amenazas, gestión de vulnerabilidades, gestión de riesgos, respuesta a incidentes, resiliencia y formación constante del personal.

La implementación, promulgación y adecuación de políticas de ciberseguridad, son básicas y fundamentales para que el Ejército Peruano pueda cumplir una de sus

funciones que es velar por la defensa nacional en el entorno digital por diversas razones:

- Protección de activos críticos: El Ejército Peruano protege información sensible y sistemas críticos que podrían ser el objetivo de ciberataques. Una política de ciberseguridad robusta ayudará a proteger estos activos y garantizar la estabilidad en los trabajos de los activos críticos digitales, lo que permitirá continuar realizando las operaciones de manera oportuna.
- Gestión de riesgos: La ciberseguridad es un riesgo constante que debe ser gestionado de manera efectiva. Una política de ciberseguridad ayudará a la identificación y evaluación, para así realizar la mitigación de los riesgos cibernéticos.
- Respuesta a incidentes**:** Es inevitable que ocurran ciberataques. Una política de ciberseguridad debe establecer una guía y un plan que permita dar respuesta oportuna a incidentes para mitigar cualquier tipo de impacto de cualquier tipo de ataque informático y así restaurar y continuar con las operaciones lo antes posible y de manera oportuna.
- Formación del personal: La ciberseguridad es una responsabilidad de todos los miembros del Ejército Peruano. Una política de ciberseguridad debe incluir programas de formación para concienciar al personal sobre las amenazas cibernéticas y enseñarles cómo protegerse.

En definitiva, la adecuación e implementación de políticas de ciberseguridad robusta, son fundamentales para que el Ejército Peruano pueda defenderse de las amenazas cibernéticas y proteger su información, sus sistemas y su capacidad operativa, en fin, todos sus activos críticos digitales.

En el contexto actual son permanentes y constantes amenazas, extorciones y todo tipo de ataque digital en el ámbito personal y organizacional con el objetivo de robar información, es que se hace preponderante una investigación profunda para fortalecer la ciberseguridad en el Ejército Peruano. Por lo que esta investigación tiene como norte principal mejorar la postura de seguridad cibernética del Ejército, permitiéndole dar

frente de manera efectiva los desafíos que representan los fraudes informáticos, el espionaje, el robo de información y otros ataques cibernéticos.

Se espera que las políticas integrales de ciberseguridad propuestas en esta investigación tengan un impacto positivo en dos ámbitos principales:

1. Ámbito académico:

- Aportar al conocimiento existente en el campo de la ciberseguridad: Los hallazgos de esta investigación contribuirán a la comprensión de las amenazas cibernéticas y las estrategias para combatirlas en el contexto militar.
- Servir como referencia para futuras investigaciones: Las experiencias adquiridas de este estudio podrán ser utilizados como base para futuras investigaciones respecto a la ciberseguridad, tanto en el ámbito civil como en el ámbito militar, con el objetivo de mejorar permanentemente la seguridad informática.

2. Mejora de las operaciones de ciberseguridad en el Ejército Peruano:

- Incrementar la velocidad de reacción ante incidentes y ataques cibernéticos: La implementación de las políticas propuestas en relación a ciberseguridad, permitirá al Ejército responder de manera rápida y efectiva a los ciberataques, mitigando su impacto y mejorando su resiliencia.
- Fortalecer la integridad del sistema de protección: Las políticas integrales de ciberseguridad ayudarán a robustecer el sistema de protección del Ejército, haciéndolo más resistente a las intrusiones y ataques cibernéticos.
- Mejorar la resiliencia del sistema **informático:** La implementación de las medidas propuestas mejorara la capacidad de recuperación ante incidentes y ataques informáticos en nuestra institución de manera rápida y eficiente.

En definitiva, esta investigación tiene como propósito particular la mejora constante en todos los aspectos relacionados a la ciberseguridad en el Ejército Peruano, protegiendo sus activos críticos, su información y su capacidad operativa digital frente a las crecientes amenazas cibernéticas.

Esta investigación se enfoca exclusivamente en el Ejército del Perú y su entorno operativo, sin abordar las políticas de ciberseguridad de otras organizaciones o sectores. Esta delimitación permite un análisis profundo y específico de las necesidades y desafíos del Ejército Peruano en materia de ciberseguridad.

Sin embargo, cabe reconocer que la investigación presenta algunas limitaciones:

- Disponibilidad limitada de datos: La escasez de datos relevantes y actualizados sobre incidentes de seguridad cibernética, vulnerabilidades y amenazas específicas dificulta la evaluación precisa del panorama de amenazas y la toma de decisiones informadas. Además, la naturaleza clasificada de gran parte de esta información limita aún más su accesibilidad.
- Evolución constante de las amenazas: En cuanto a este aspecto en particular se evidencian de manera continua amenazas cibernéticas nuevas e innovadoras. Esto significa que la investigación y las políticas de ciberseguridad deben actualizarse de forma constante y permanente para mantenerse a la vanguardia.
- Restricciones presupuestarias y operativas: La formulación e implementación de todas las medidas propuestas en las políticas de ciberseguridad pueden verse afectada por limitaciones presupuestarias y operativas. Por lo que la investigación debe considerar cuidadosamente la viabilidad práctica de las recomendaciones y proponer soluciones que sean asequibles y factibles de implementar.

A pesar de estas limitaciones, la investigación ofrece un valioso aporte a la mejora constante de la ciberseguridad en el Ejército Peruano**.** El análisis de las necesidades y desafíos específicos del Ejército, junto con las propuestas de políticas y medidas de seguridad, sentarán las bases para fortalecer la postura cibernética del Ejército y proteger sus activos críticos frente a las crecientes amenazas.

El problema general se centra en la falta de políticas integrales y específicas de ciberseguridad adaptada a las necesidades y desafíos propios en el Ejército del Perú genera situaciones de vulnerabilidad en la seguridad de la información digital. Esta carencia se traduce en la ausencia de directrices claras, la falta de coordinación y colaboración entre las diferentes áreas del Ejército, y una protección inadecuada de la

información estratégica, por lo que el problema principal que se plantea es ¿Cómo las políticas integrales de ciberseguridad brindan protección ante los desafíos específicos de la información digital en el Ejército del Perú, 2023? y tres preguntas específicas (1) ¿Cómo la toma de conciencia y capacitación en ciberseguridad brindan protección ante los desafíos específicos de la información digital en el Ejército del Perú ,2023? (2) . ¿Cómo los recursos de ciberseguridad brindan protección ante los desafíos específicos de la información digital de las Fuerzas Armadas del Perú,2023? (3) ¿Cómo la permanencia del personal técnico especialista de ciberseguridad brinda protección ante los desafíos específicos de la información digital de las Fuerzas Armadas del Perú,2023? Habiendo determinado como Objetivo general**; Implementar** políticas integrales de ciberseguridad en **la protección de la información digital** en el Ejército del Perú, 2023. y como objetivos específicos (1) **Explicar** cómo la **toma de conciencia y capacitación en ciberseguridad** brindan protección ante los desafíos específicos de la información digital en el Ejército del Perú ,2023.(2) **Explicar** cómo los **recursos de ciberseguridad brindan** protección ante los desafíos específicos de la información digital de las Fuerzas Armadas del Perú,2023.(3) **Explicar** cómo la **permanencia del personal técnico especialista en ciberseguridad** brinda protección ante los desafíos específicos de la información digital de las Fuerzas Armadas del Perú,2023.

Para el marco teórico presentamos algunos antecedentes que se considera más resaltantes dentro del ámbito nacional como:

Ormachea, J. (2019). En su tesis Doctoral del CAEN. titulada "*Estrategias integradas de ciberseguridad para el fortalecimiento de la seguridad Nacional"* la desarrolla *con* un enfoque cualitativo concluyendo en que la sociedad y el estado, aún se enfocan en la concientización y el desarrollo de las capacidades cibernéticas Militares como indicadores de relevancia". Esta propuesta coincide con otros autores nacionales como Bonilla y Ortiz (2020), quienes en su texto titulado "*Estrategia Nacional de Ciberdefensa y Ciberseguridad"*. (p. 12) señalan que "la ciberdefensa es un componente esencial de la seguridad nacional y debe ser abordada de manera integral, considerando aspectos legales, técnicos, organizativos y de cooperación internacional".

Sánchez, M. (2017). En un artículo para la Revista Peruana de Ciencia Política, (pp. 123-142). titulado *Ciberseguridad en el sector público peruano*, realiza un análisis

del caso en un área específica del Ejército peruano que es el Comando de Personal – COPERE, a lo que se concluye que la gran mayoría de las entidades públicas en el Perú no cuentan con planes de ciberseguridad, y si los cuenta no están actualizados, tampoco cuenta con personal capacitado para enfrentar las amenazas cibernéticas"

Lo señalado por Sánchez coincide con lo señalado por Torres y Rojas (2018), quienes en su artículo denominado "*Amenazas cibernéticas y desafíos de la ciberseguridad en el Perú*" (p. 5) afirman que "la mayoría de las instituciones públicas en el Perú no cuentan con planes de ciberseguridad actualizados ni con personal capacitado para enfrentar las amenazas cibernéticas".

Taipe, R. (2020). En su tesis para magister en la Universidad de Piura titulada "*Percepción pública sobre la ciberseguridad en el Perú*" realiza un análisis de los riesgos y desafíos. "Amenazas cibernéticas y desafíos de la ciberseguridad en el Perú" afirmando que "la falta de políticas públicas efectivas en materia de ciberseguridad genera un ambiente de vulnerabilidad en el país, poniendo en riesgo la seguridad nacional y la protección de información sensible".

Los antecedentes dentro del ámbito Internacional tenemos a:

Rubio, J. (2016), de la Universidad Rey Juan Carlos de España, en su tesis Doctoral titulada "Un *Marco para el Análisis de Riesgos en Ciberseguridad*", concluye que se debe crear instituciones especializadas en la seguridad del ciberespacio, la identificación y protección de puntos sensibles o críticos, y el establecimiento de aspectos regulatorios de acuerdo a ley que defina de forma clara y precisa las responsabilidades y funciones respectivas. Esta propuesta surge en un contexto de creciente preocupación por las ciberamenazas a nivel global, y busca fortalecer la capacidad de cualquier estado o nación que involucra la protección de sus ciudadanos y sus infraestructuras críticas digitales.

Cano, J. (2015), de la Universidad Politécnica de Madrid en su libro titulado "*Evaluación por competencias en educación superior*", resalta la prioridad de protección que deben de tener los medios tecnológicos contra las amenazas cibernéticas para garantizar su correcto funcionamiento y disponibilidad. Esta afirmación se realiza en el contexto de una creciente preocupación por todos los

aspectos relacionados a la seguridad digital y todo tipo de dato o información en el ámbito académico. Cano advierte que las instituciones educativas son particularmente vulnerables a los ataques cibernéticos.

Arias y Celis (2015), Universidad Libre-Colombia en su trabajo de grado titulado *"Modelo experimental de ciberseguridad y ciberdefensa para Colombia*", sostienen que, para la defensa cibernética de Colombia, es fundamental otorgar igual importancia a todos los aspectos relacionados a ciberseguridad y ciberdefensa a fin de proteger el ciberespacio nacional, mediante la implementación de acciones contundentes para contrarrestar las actividades de los piratas informáticos. Esta recomendación se realiza en el contexto de un panorama global cada vez más complejo en materia de ciberseguridad, donde las amenazas cibernéticas son hoy en día una preocupación prioritaria para cualquier Estado. Arias y Celis advierten que Colombia ni ningún otro país es hoy en día inmune a este tipo de amenazas, y que es necesario tomar medidas urgentes para proteger su infraestructura crítica y la información de sus ciudadanos.

La ciberseguridad se define como la capacidad técnica para salvaguardar el correcto funcionamiento todos los dispositivos electrónicos conectados o no al internet, protegiéndolos contra amenazas y vulnerabilidades en el ámbito digital. Esta perspectiva técnica se encuentra consagrada en el Decreto Urgencia 07-2020 (2020), en su artículo 3, inciso h), sobre Seguridad Digital, emitido por el Gobierno peruano. En este decreto, se observa a la ciberseguridad como un componente fundamental de la seguridad nacional y que es necesario adoptar medidas para proteger la infraestructura crítica digital del país contra ataques cibernéticos.

Existen entidades internacionales como es la Unión Internacional de Telecomunicaciones (UIT), quien dentro de sus potestades aprobó una definición de ciberseguridad. Esta abarca diferentes aspectos como conceptos de seguridad informática, salvaguardas de seguridad digital, directrices relacionadas a aspectos de ciberseguridad, métodos de gestión de amenazas, vulnerabilidades y riesgos, acciones a adoptar, formación a realizarse, prácticas idóneas que seguir, seguros y uso de

tecnologías apropiadas. Estos conceptos son de todos los elementos a utilizarse para proteger los activos digitales de la organización, activos digitales críticos y a los mismos usuarios por tratarse de vectores de ataque muy codiciados.

La gestión de amenazas, vulnerabilidades y riesgos en el dominio cibernético*, deben estar referenciados por políticas integrales de ciberseguridad, estas políticas* y directrices constituyen documentos que establecen normas y procedimientos que en una organización debe regir para proteger sus datos, información y sistemas informáticos. Estos lineamientos y directrices son diseñadas con el propósito de garantizar la confidencialidad, integridad y disponibilidad de la información en todos los niveles de la empresa. Adicionalmente, buscan proteger la información confidencial de usuarios, clientes y todos los actores involucrados, a fin de preparar a la organización en todo su contexto para enfrentar posibles ciberataques. La implementación de estas políticas es indispensable para cualquier organización y con mayor énfasis en una institución como el ejercito que vela por garantizar la soberanía nacional.

En la era digital y el nuevo dominio llamado ciberespacio, la protección de la información digital se ha convertido en un aspecto crucial para la seguridad digital de personas, empresas y organizaciones. Esta protección digital en el nuevo dominio se define como un conjunto de prácticas, estrategias y procesos implementados para salvaguardar la confidencialidad, disponibilidad e integridad de los datos, información y sistemas informáticos. La confidencialidad se refiere a la protección de los datos e información de accesos no autorizados, la disponibilidad se refiere al acceso oportuno y confiable a la información cuando se requiera, y la integridad se refiere a la exactitud y completitud de la información. La implementación de medidas de protección de la información digital es esencial para mitigar los riesgos asociados a las vulnerabilidades y amenazas cibernéticas, como el malware, el phishing y los ataques de denegación de servicio.

- **Bases teóricas de las categorías apriorísticas**

1. **La concientización y capacitación en un sistema de gestión de calidad**

Actualmente el activo más importante de toda organización es la persona, por lo que existen políticas de inversión en su desarrollo continuo para mejorar sus habilidades. Este proceso, conocido como desarrollo de personal, implica comprometer a los empleados con los objetivos organizacionales, capacitándolos y motivándolos para que puedan asumir mayores responsabilidades dentro de la organización. Según Chiavenato I. (2002), el adiestramiento es esencial para desarrollar las cualidades de los recursos humanos y aumentar su productividad, contribuyendo así a los objetivos de la empresa. El objetivo principal es mejorar la productividad de los trabajadores, influyendo en sus comportamientos en sus puestos de trabajo.

En síntesis, todas las organizaciones deben planificar la implementación de programas de capacitación y desarrollo que mejoren las competencias y habilidades de sus colaboradores, con el único propósito de producir bienes y servicios de manera eficiente y responsable. Es ahí donde radica la importancia de renovar constantemente el talento humano para adaptarse a los cambios en el entorno económico. Según Alles M. (2000), el adiestramiento es un proceso de aprendizaje que proporciona las habilidades y conocimientos necesarios para alcanzar los objetivos de la empresa, alineados con su visión, y objetivos comerciales.

Concientización

La concientización se refiere a un proceso de reconstrucción en el que se transfiere información desde un nivel inferior e inconsciente hacia un nivel superior y consciente, permitiendo así una conceptualización. En uno de sus escritos sobre psicología genética, Piaget (1980) presenta un concepto novedoso: el inconsciente cognoscitivo. Para desarrollar esta idea, el autor se basa en el conocido inconsciente freudiano, con el que, según confiesa Piaget (en Bringuier, 2004), está de acuerdo en ciertos aspectos. Establece una primera distinción entre el inconsciente afectivo y el inconsciente cognoscitivo. Según Piaget (1999), la acción tiene dos dimensiones: una afectiva y otra cognoscitiva. La afectividad actúa como el motor de la conducta, representando el aspecto energético de la acción, mientras que el componente

cognoscitivo se ocupa de encontrar los medios para que la acción logre su propósito, constituyendo así el elemento estructural del comportamiento. Aunque estos dos aspectos son diferentes, no pueden ser considerados de manera aislada, ya que mantienen una relación de interdependencia (Piaget, 1980; 1999). Piaget, J. (1988). Psicología evolutiva de Jean Piaget.

Capacitación

La capacitación se compone de un conjunto de actividades diseñadas y fundamentadas en los requerimientos de la empresa, con el objetivo de promover una mejora en los conocimientos, habilidades y actitudes de sus respectivos colaboradores, permitiéndoles realizar sus tareas de manera más eficiente. Según Silicio (2004, p. 20), “la capacitación es una actividad planificada y basada en las necesidades reales de una empresa u organización, enfocada en modificar los conocimientos, habilidades y actitudes del colaborador”. Por otro lado, Chiavenato (2008) sostiene que “la capacitación es un proceso educativo a corto plazo, que se aplica de forma sistemática y organizada, mediante el cual las personas adquieren conocimientos y desarrollan habilidades y competencias en función de objetivos específicos” (p. 386)

2. Recursos de ciberseguridad

Las herramientas o recursos fundamentales en el ámbito de la ciberseguridad, permiten a las organizaciones gestionar y analizar de forma centralizada los registros y eventos de seguridad en su infraestructura. Su función principal es detectar amenazas, responder a incidentes y cumplir con los requisitos de seguridad. Estos sistemas recopilan registros de diversas fuentes, como sistemas operativos y dispositivos de red, correlacionan eventos para identificar patrones anómalos, generan alertas ante actividades sospechosas y almacenan información para investigaciones posteriores y cumplimiento de normativas. Se debe encontrar conexiones entre eventos que no parecen tener relación entre sí para detectar patrones y comportamientos inusuales. con capacidad de almacenamiento y búsqueda de registros y eventos recopilados a lo largo del tiempo, lo que facilita investigaciones futuras y el cumplimiento de las

disposiciones, directivas y normatividad. Además, ofrecen herramientas de búsqueda avanzadas para facilitar la investigación de incidentes de seguridad en el entorno digital.

Recursos humanos

Es una necesidad básica para cualquier tipo de organización. El principal motivo de la competencia es el factor común que la impulsa, pues es necesario mostrarlo, medirlo y compararlo (González, 2005). En las organizaciones, qué tan bien compiten se puede ver por la calidad de los servicios o productos que brindan a sus clientes. González cree que ser competitivo significa más que sólo ser productivo y ganar dinero. Se trata de entender que el mercado reconoce y premia las decisiones y acciones tomadas por las organizaciones, lo que se refleja en el logro de sus objetivos (Montoya & Boyero, 2015).

Recursos digitales

Los recursos digitales son cualquier tipo de contenido que puedes ver y guardar en tu computadora o teléfono, y también puedes encontrarlos en línea. Estos recursos se presentan en diferentes formas, como vídeos, podcasts, documentos, presentaciones, libros, sistemas interactivos, animaciones, simulaciones, juegos, sitios web y redes sociales. Estos recursos son muy útiles para el aprendizaje, especialmente para los estudiantes que tienen problemas para concentrarse o comprender cosas en clase o en los libros. Proporcionan diferentes formas de aprender, como imágenes, sonidos y actividades interactivas, lo que hace que sea más fácil de entender para todos. Son excelentes para todos porque nos ayudan a comprender mejor las cosas, facilitan la búsqueda de información y se ven realmente interesantes.

3. Permanencia del personal técnico especialista

Cuando los empleados dejan una empresa, se llama rotación de personal. Puede resultar costoso y afectar el funcionamiento de la empresa porque tienen que seguir contratando gente nueva. La rotación se produce cuando las personas dejan un trabajo y entran nuevas personas para ocupar su lugar. La rotación laboral es cuando los trabajadores van y vienen en una empresa, dependiendo de cuántas personas nuevas se incorporan y cuántas se van. Macario de paz (2018) explica que cuando las personas dejan una empresa, en realidad puede ser algo bueno. Demuestra que a la empresa le va bien y puede adaptarse a los cambios. Sin embargo, la rotación se mide por el

número de empleados que dejan la empresa durante un período de tiempo específico, en comparación con el número total de personas de la organización, excluyendo aquellos que se van sin otra opción.

Oficiales especialistas

Son Oficiales militares expertos en ciberseguridad y/o en seguridad informática, tecnologías de la información, gestión de los sistemas de información o ingeniería del software son algunos de los másteres que se pueden estudiar para especializarse en un área de la ciberseguridad. Normalmente se exige tener una formación previa en programación informática para tener unas bases (Díaz 2020).

Personal Auxiliar especialista

Son profesionales militares con el rango de Técnico/Suboficial que poseen conocimientos en diversos sistemas operativos, redes y lenguajes de programación, enfocados en el ámbito de las comunicaciones y la seguridad informática. Su labor incluye entre muchos aspectos, analizar las vulnerabilidades, amenazas y gestionar los riesgos para mitigar los probables impactos, con el único propósito de salvaguardar la información y desarrollar estrategias de prevención, así como diseñar proyectos relacionados con la seguridad informática y de las comunicaciones. También se encargan de realizar diferentes pruebas y auditorias, actualizar los sistemas de seguridad, parametrar y designar permisos de acceso para los diferentes niveles de usuarios, supervisar los accesos a la información y ejecutar programas de defensa y en coordinación con ciberdefensa ejecutar programas de respuesta ante posibles intrusiones o violaciones. Por lo tanto, la presencia de un especialista en ciberseguridad es esencial para garantizar la protección de su información. (Cybersecurity Strategy Advisory, 2020)

Personal civil especialista

Los profesionales civiles especialistas desempeñan funciones similares a las de los técnicos y suboficiales, aunque bajo un régimen laboral diferente. Estos expertos dominan diversos sistemas operativos, redes y lenguajes de programación, centrándose en aspectos muy técnicos y especializados. Su labor incluye analizar las medidas de seguridad existentes para salvaguardar la información, identificar amenazas de seguridad, desarrollar técnicas de prevención y participar en proyectos innovadores

relacionados con la seguridad digital institucional. También se encargan de realizar pruebas de vulnerabilidad, actualizar los sistemas de seguridad, otorgar acceso a los usuarios autorizados, monitorear el acceso a la información y ejecutar programas de defensa ante posibles violaciones o intrusiones. Por lo tanto, la presencia de un especialista en ciberseguridad es esencial para garantizar la confidencialidad de una empresa y la protección de su información. (Cybersecurity Strategy Advisory, 2020)

Las categorías apriorísticas y sus respectivas subcategorías con las que el investigador inicio son:

Tabla 1

Categorías y subcategorías apriorísticas Políticas integrales de seguridad

CATEGORIAS	**SUBCATEGORIAS**
C1: Concientización y capacitación	SC1: Concientización
	SC2:Capacitación
C2: Recursos de ciberseguridad	SC1: Recursos Humanos
	SC2:Recursos digitales
C3: Permanencia del personal técnico especialista	SC3:Oficiales especialistas
	SC2:Personal Auxiliar especialista
	SC3:Personal Civil especialista

Hipótesis

La hipótesis o supuesto de este estudio cualitativo sugiere que implementar políticas de ciberseguridad en el Ejército fomenta un entorno cibernético adecuado con protección y con la capacidad de hacer frente a posibles amenazas.

Capítulo II. Materiales y métodos

Para la presente investigación, se trabajó bajo un enfoque cualitativo con un diseño teórico-empírico. Esta elección de trabajo se fundamentó en la necesidad de comprender en profundidad las percepciones y experiencias de los participantes en relación con la ciberseguridad en el Ejército Peruano. Un enfoque cualitativo permite explorar temas complejos y matizados de forma muy adecuada, como es en este caso particular la ciberseguridad, desde la perspectiva de todos los actores involucrados.

Este tipo de investigación es teórico-empírico, lo que nos permitió combinar la teoría existente con la recolección y el análisis de los datos empíricos. Fue particularmente útil para explorar un tema relativamente nuevo en esta región y en las respectivas fuerzas armadas de cada país. A medida que se avanzaba en la investigación, se ajustaban los objetivos y se profundizaba en la comprensión del fenómeno en el Ejercito del Perú.

La hermenéutica se utilizó como método de investigación para interpretar el significado de las entrevistas, las observaciones y los documentos recopilados. Este método permitió comprender las perspectivas y experiencias de los participantes en relación con la ciberseguridad en el Ejército Peruano.

La presente investigación tiene como objetivo principal analizar la ciberseguridad y la protección de la información digital en el Ejército del Perú. Tal como lo indica Vargas (2011), "la identificación del objeto de estudio es fundamental para delimitar el ámbito de investigación" (p. 56). En este caso, el objeto de estudio se centra en las prácticas, estrategias y desafíos relacionados con la ciberseguridad en el contexto del Ejército Peruano.

Esta investigación se desarrolló bajo el enfoque de la metodología de tipo cualitativa, utilizando un enfoque descriptivo. Este enfoque permite explorar en profundidad las percepciones, experiencias y conocimientos de los participantes, en este caso, oficiales ingenieros de sistemas con amplia experiencia en ciberseguridad en el Ejército del Perú.

La población objetivo de la investigación está conformada por todos los oficiales ingenieros de sistemas del Ejército del Perú que se desempeñan en áreas relacionadas

con la ciberseguridad**.** Se considera que esta población posee un conocimiento y experiencia valiosos sobre el tema de estudio.

La muestra seleccionada para la investigación es de tipo no probabilística por conveniencia, compuesta por cuatro oficiales ingenieros de sistemas**.** La elección de esta muestra se basa en la experiencia y conocimiento de los participantes en el tema de investigación, lo que permite obtener información rica y relevante que garantizaron una saturación de datos adecuada.

Las técnicas de recolección de datos utilizadas en la investigación han sido:

Entrevistas semiestructuradas: Se entrevistaron con formatos de entrevistas semiestructuradas a cuatro oficiales ingenieros de sistemas de la muestra seleccionada. Las entrevistas fueron guiadas por un cuestionario flexible que permitió a los participantes profundizar en sus experiencias y conocimientos sobre la ciberseguridad en el Ejército del Perú entre el 14 de agosto al 30 noviembre del 2023.

Observación participante: El investigador realizó observación participante en dos actividades relacionadas con la ciberseguridad en el Ejército del Perú. Esta observación permitió al investigador obtener información contextual sobre las prácticas y desafíos relacionados con la ciberseguridad en el ámbito militar. Habiendo sido realizada entre el mes de mayo al 30 de octubre del 2023, haciendo notar que el investigador trabajo en esa oportunidad en la Dirección de telemática del Ejercito

Análisis documental: Se analizaron documentos oficiales del Ejército del Perú relacionados con la ciberseguridad, tales como políticas, procedimientos y planes estratégicos. El análisis documental permitió complementar la información obtenida a través de las entrevistas y la observación participante, para el análisis documental, este análisis se realizó durante todo el periodo que duro la investigación es decir entre el año 2023 y febrero del año 2024.

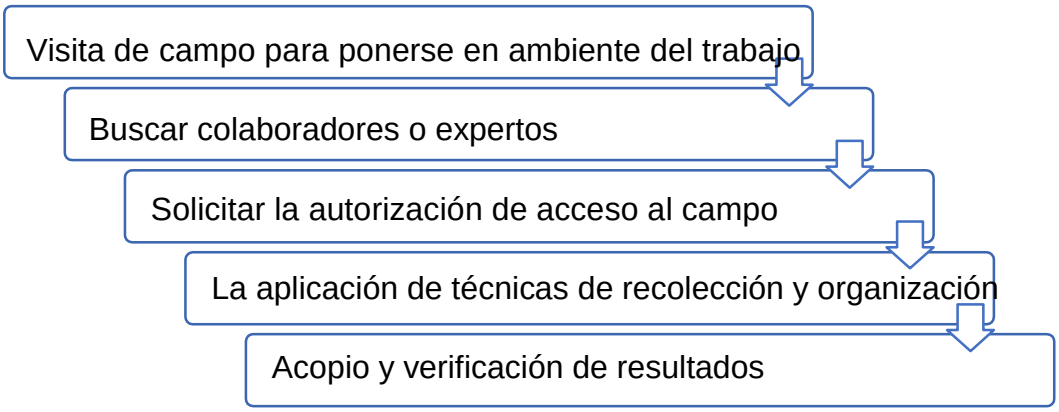
El análisis de los datos se realizó siguiendo un enfoque cualitativo inductivo. Los datos obtenidos a través de las entrevistas, la observación participante y el análisis documental fueron categorizados y analizados siguiendo un proceso iterativo de codificación y análisis temático. Este proceso permitió identificar patrones, tendencias y significados emergentes en los datos, lo que contribuyó a la construcción de conocimiento sobre la ciberseguridad en el Ejército del Perú.

La triangulación de datos, el juicio de expertos y la experiencia del investigador se utilizaron para garantizar la confiabilidad y validez de la investigación**.** La triangulación de datos consistió en comparar los resultados obtenidos a través de las diferentes técnicas de recolección de datos. El juicio de expertos involucró la consulta con expertos en ciberseguridad.

Para la primera fase de acceso al campo de la investigación se empleó el siguiente procedimiento:

Figura 2

Primera fase de acceso al campo



Nota: *La figura muestra la fase de acceso al campo con sus correspondientes procedimientos*

Capitulo III: Resultados

4.1 Recolección de datos

En la recopilación exhaustiva de información diversa sobre el tema de estudio, se emplearon tres métodos de investigación cualitativa**,** los cuales garantizaron una saturación de datos adecuada para su posterior organización.

1. Observación participante: El investigador aprovechó su experiencia como miembro de la institución para observar de primera mano el funcionamiento y la evolución de las Unidades Militares especializadas en tecnologías de la información y comunicaciones. Esta experiencia permitió obtener una comprensión profunda de las prácticas y desafíos relacionados con la ciberseguridad en el ámbito militar.
2. Entrevistas semiestructuradas: Se realizaron entrevistas semiestructuradas a cuatro Ingenieros expertos con conocimiento y experiencia en el tema de estudio, estas entrevistas permitieron obtener diferentes perspectivas sobre la ciberseguridad en el Ejército Peruano, incluyendo las experiencias, percepciones y opiniones de los participantes.
3. Análisis documental: Se analizaron diversos documentos oficiales del Ejército Peruano relacionados con la ciberseguridad, tales como políticas, procedimientos, planes estratégicos, informes y estudios. El análisis documental complementó la información obtenida a través de la observación participante y las entrevistas, proporcionando una visión más amplia del contexto institucional y las estrategias de ciberseguridad implementadas.

Estas técnicas resultaron muy efectivas para recopilar la información necesaria, la cual ahora requiere ser organizada de manera adecuada.

La triangulación de métodos y la saturación de datos garantizaron la confiabilidad y validez de la investigación**.** La triangulación de métodos consistió en combinar diferentes técnicas de recolección de datos para obtener una comprensión más

completa del fenómeno de estudio. La saturación de datos se alcanzó cuando se recopiló suficiente información para responder a las preguntas de investigación y no se identificaron nuevos datos relevantes.

La información recopilada a través de estos métodos ha sido organizada y sistematizada para su posterior análisis e interpretación. El análisis de los datos permitirá identificar patrones, tendencias y significados emergentes en la información, lo que contribuirá a la construcción de conocimiento sobre la ciberseguridad en el Ejército Peruano.

4.2 Organización de los datos

Después de recopilar los datos, se llevó a cabo la estructuración de la información. Para lograrlo, se inició por establecer un orden debido al volumen considerable de datos capturados, con el objetivo de luego poder categorizarlos y facilitar así un análisis más fácil.

Tabla 2

Matriz de Políticas integrales de ciberseguridad

Titulo : Políticas integrales de ciberseguridad en la protección de la información digital en el Ejército del peru, 2023			
Temas	**Categorías**	**Subcategorías**	**Código**
Políticas Integrales de Ciberseguridad	C1: Concientización y capacitación	SC1: Concientización	TCT
		SC2: Capacitación	TCC
	C2: Recursos de ciberseguridad	SC1: Recursos Humanos	RRH
		SC2: Recursos digitales	RRD
Protección de la Información	C3: Permanencia del personal técnico especialista	SC3: Oficiales especialistas	POE
		SC2: Personal de tecnicos y soboficiales	PEA
		SC3: Personal Civil	PPE

4.2.1. Categoría 1: Concientización y capacitación

Tabla 3

Organización de datos a partir de las entrevistas de la Categoría C1: Concientización y capacitación

Categoría	Testimonios	
C1: Toma de conciencia y capacitación	*P1.¿Que politicas sobre ciberseguridad cree Ud. que se deba adoptar para el personal que maneja la informacion digital tome conciencia en la protección de la información digital del Ejercito del Perú?*	
	RE1	Buscamos concientizar a la sociedad civil sobre la importancia de la seguridad en línea, identificar posibles puntos débiles o amenazas y tomar medidas adecuadas para protegerse. El plan incluirá una estrategia de difusión que involucre la organización de conferencias para diferentes niveles educativos y la divulgación entre ciudadanos y entidades públicas y privadas. Además, se llevarán a cabo foros para facilitar el intercambio de ideas y experiencias entre diferentes organizaciones, la sociedad civil y el ámbito académico, con el objetivo de compartir las mejores prácticas en ciberseguridad y ciberdefensa. Las políticas sobre ciberseguridad que se deben adoptar, deben estar enfocadas en los siguientes aspectos: - Política de contraseñas fuertes. - Actualizaciones y parches. - Controles de acceso. - Respuesta a incidentes
	RE2	- Políticas para el correcto uso de los sistemas informáticos - Políticas de disaster recovery (resilencia) - Políticas de actualización de software
	RE3	Las políticas de ciberseguridad deben centrarse en los siguientes aspectos: - Es importante tener una política de contraseñas sólida - Actualizaciones y mejoras Controles de acceso para gestionar y abordar incidentes o emergencias

Categoría	Testimonios	
	RE4	Las políticas sobre ciberseguridad que se deben adoptar, deben estar enfocadas en los siguientes aspectos: - Política de seguridad de la red - Política de respaldo de datos - Política de acceso y privilegios
	P2. ¿En qué aspectos sobre la ciberseguridad de la información digital considera Ud. que se deba capacitar al personal que maneja la informacion digital en las dependencias del Ejercito del Perú	
	RE1	En los siguientes aspectos: - Higiene cibernética. - Correcto uso de los sistemas de información
	RE2	En las siguientes áreas: - Educación sobre riesgos cibernéticos. - Conocimiento de ciberataques. - Manejo de la información digital.
	RE3	En los siguientes aspectos: - Concientización sobre amenazas cibernéticas. - Reconocimiento de los ataques cibernéticos. - Gestión de la información digital.
	RE4	Acerca de: - Gestionar las comunicaciones digitales - Comprender las amenazas cibernéticas - Comprender los ataques cibernéticos
	P3. ¿Qué aspectos de mejora considera Ud. que se deba implementar para la concientización y capacitación sobre la Ciberseguridad en todo el personal del Ejercito del Perú?	
	RE1	Evaluar el efecto de la capacitación para asegurarse de que sea efectiva. Desde los líderes hasta el personal técnico, la capacitación en ciberseguridad debe ser un esfuerzo integral que involucre a todos los niveles de la organización..

Categoría	Testimonios	
	RE2	Para asegurarse de que la capacitación sea efectiva, es fundamental evaluar su impacto. Desde los líderes hasta el personal técnico, la capacitación en ciberseguridad debe ser un esfuerzo integral que involucre a todos los niveles de la organización
	RE3	Es importante medir el impacto de la capacitación para garantizar que sea eficaz. La capacitación en ciberseguridad debe ser un esfuerzo holístico que involucre a todos los niveles de la organización, desde los líderes hasta el personal técnico.
	RE4	Para garantizar que su formación sea eficaz, es importante medir su eficacia. La capacitación en ciberseguridad debe ser un esfuerzo integral que involucre a todos los niveles de la organización, desde el liderazgo hasta el personal técnico..

Nota*: La tabla corresponde a la codificación abierta de la primera categoría*

4.2.2. Categoría 2: Recursos de ciberseguridad

Tabla 4

Organización de datos a partir de las entrevistas de la Categoría C2: Recursos de ciberseguridad

Categoria	Testimonios	
C2: Recursos de ciberseguridad	*P4. ¿Qué estrategias en los recursos humanos sobre ciberseguridad deben aplicar en las dependencias del Ejercito?*	
	RE1	Contar con un manual de normas para todos los empleados de la empresa es fundamental para garantizar la protección de los datos y actividades de la organización. Este documento incluye una serie de acciones, procedimientos y procesos que deben seguirse para asegurar la seguridad de la información. Dentro de estas políticas se encuentran medidas para prevenir posibles crisis, así como planes de contingencia en caso de que ocurran filtraciones o vulnerabilidades. La guía de buenas prácticas se enfoca en la prevención de riesgos, pero también en la contención de posibles incidentes de seguridad. Este documento está en constante evolución, adaptándose a los cambios y avances tecnológicos del ámbito cibernético. Se revisa periódicamente para asegurar su efectividad y se incorporan criterios de habilidades y conocimientos en ciberseguridad al momento de contratar nuevo personal. Además, se valora la experiencia previa en ciberseguridad como un activo relevante, y se ofrecen programas de formación en esta materia como parte del desarrollo profesional continuo de los empleados o servidores .
	RE2	Al contratar nuevos empleados, considere los estándares de habilidades y conocimientos en ciberseguridad. Considere la experiencia previa en ciberseguridad como una ventaja clave. Ofrezca programas de capacitación en ciberseguridad como parte integral de su desarrollo profesional.

Categoria	Testimonios	
	RE3	Es crucial medir la eficacia de la formación midiendo su impacto Es importante brindar capacitación en ciberseguridad a todos los empleados, desde los ejecutivos de alto nivel hasta el personal técnico, para crear una estrategia de seguridad integral y efectiva.
	RE4	Proporcione un programa de capacitación en ciberseguridad como una parte importante del desarrollo profesional. Incluya criterios de conocimientos y habilidades de ciberseguridad al contratar nuevos empleados. Considere la experiencia previa en ciberseguridad como una ventaja.
	P5. ¿ Qué estrategias en los recursos digitales sobre ciberseguridad deben aplicare en las dependencias del Ejercito?	
	RE1	Para detectar actividades inusuales o amenazas potenciales, implemente sistemas de monitoreo continuo. Realizar auditorías de seguridad regulares para evaluar la efectividad de las medidas de seguridad implementadas y resolver posibles vulnerabilidades
	RE2	Aplique cifrado a datos confidenciales para proteger la información en tránsito y en reposo. Configure un sistema de monitoreo continuo para detectar actividades anómalas y amenazas potenciales en tiempo real. Realizar auditorías de seguridad periódicas para evaluar la eficacia de las medidas de seguridad implementadas y abordar posibles vulnerabilidades.
	RE3	Se debe utilizar cifrado para proteger datos confidenciales cuando se envíen o almacenen, configurar los sistemas que vigilen constantemente cualquier acción anormal o peligro potencial en tiempo real Realizar auditorías de seguridad de rutina para evaluar la eficiencia de las medidas de seguridad implementadas e identificar posibles debilidades
	RE4	Aplicación de cifrado a datos confidenciales para proteger la información en tránsito y en reposo. Establecer sistemas de seguimiento continuo para detectar actividades inusuales o amenazas potenciales en tiempo real.

Categoria	Testimonios	
	P6. Qué aspectos de mejora considera Ud. que se deba implementar en recursos humanos y recursos digitales para la Ciberseguridad en las dependencias del Ejercito del Perú?	
	RE1	Reconocer y recompensar al personal por su compromiso con la ciberseguridad Crear un programa de capacitación en ciberseguridad que sea obligatorio para todo el personal que maneje información digital. Impartir la capacitación en ciberseguridad por instructores calificados y experimentados.
	RE2	Crear un programa de formación obligatorio en ciberseguridad para todos los empleados que trabajan con información digital. Ofrecemos capacitación en ciberseguridad impartida por instructores calificados y experimentados. Reconocer y recompensar el compromiso de los empleados con la ciberseguridad
	RE3	Desarrollar un programa de formación que todos los empleados que trabajan con datos digitales deben completar, proporcionar formación en ciberseguridad impartida por instructores cualificados y con experiencia. Reconozca y aprecie a los empleados por su dedicación a salvaguardar los activos digitales de la organización
	RE4	Crear un programa de formación obligatorio en ciberseguridad para todos los empleados que trabajan con información digital.

Nota*:* *La tabla corresponde a la codificación abierta de la segunda categoría*

4.2.3. Categoría 3: Permanencia del personal técnico especialista

Tabla 5

Organización de datos a partir de las entrevistas de la Categoría C3: Permanencia del personal técnico especialista

Categoría	Testimonios	
C3: Permanencia del personal técnico especialista	*P7. ¿Qué opinión le merece sobre la permanencia del personal de Oficiales especialistas en ciberseguridad en las dependencias del Ejercito?*	
	RE1	Es fundamental para la continuidad de los objetivos estratégicos del ejército, para la protección de la información digital del Ejército. Estos Oficiales tienen la formación y las habilidades necesarias para comprender y mitigar los riesgos de ciberseguridad
	RE2	Crear un programa de formación obligatorio en ciberseguridad para todos los empleados que trabajan con información digital. Ofrecemos capacitación en ciberseguridad impartida por instructores calificados y experimentados. Reconocer y recompensar el compromiso de los empleados con la ciberseguridad.
	RE3	Creo que es crucial para la información digital del Ejército contar con un equipo de Oficiales Especialistas en Ciberseguridad que estarán en el Ejército por mucho tiempo. "Los oficiales tienen la formación y las habilidades necesarias para comprender y mitigar los riesgos de ciberseguridad".
	RE4	Creo que la durabilidad de la fuerza laboral de expertos en ciberseguridad en las unidades del Ejército del Perú es fundamental para la protección de la información digital del Ejército. Este personal tiene la formación y las habilidades necesarias para comprender y mitigar los riesgos de ciberseguridad.
	P8. ¿Qué opinión le merece sobre la permanencia del personal de tecnicos y Suboficiales especialistas en ciberseguridad en las dependencias del Ejercito?	
	RE1	Se sugiere que es un enfoque útil y complementario para reforzar la perspectiva de seguridad digital.

Categoría	Testimonios	
		Estos especialistas están capacitados para comprender y reducir los peligros de ciberseguridad.
	RE2	Los puestos en el Ejército son bastante rotativos, muchas veces se capacita al personal y cuando ya manejan una solución, son cambiados a otro puesto de trabajo
	RE3	Creo que es muy importante contar con técnicos y suboficiales expertos en ciberseguridad en las unidades del Ejército del Perú, porque pueden ayudar a mantener la información y los sistemas digitales a salvo de ciberataques, ya que tienen las habilidades y las herramientas para hacerlo.
	RE4	Estoy convencido de que la sostenibilidad del personal de técnicos y suboficiales especializados en ciberseguridad en las unidades del Ejército del Perú es de vital importancia para garantizar la protección de la información sensible y la infraestructura digital frente a las ciberamenazas.
	P9. ¿Qué opinión le merece sobre la permanencia del personal civil especialista en ciberseguridad en las dependencias del Ejercito?	
	RE1	Se sugiere que es un enfoque útil y complementario para reforzar la perspectiva de seguridad digital. Estos especialistas están capacitados para comprender y reducir los peligros de ciberseguridad.
	RE2	La retención de personal civil en el Ejército especializado en seguridad cibernética será una estrategia adicional importante para fortalecer la base de seguridad digital. Estos profesionales cuentan con la formación y las habilidades necesarias para reconocer y mitigar los riesgos de ciberseguridad.
	RE3	Tener expertos civiles en ciberseguridad en las unidades del Ejército puede ser un enfoque beneficioso y adicional para mejorar la seguridad digital del Ejército, los expertos tienen el conocimiento y las habilidades para comprender y abordar las amenazas a la ciberseguridad.
	RE4	La entrada y estancia de personal civil especializado en ciberseguridad en las dependencias del Ejército puede fortalecer y complementar la seguridad digital.

Categoría	Testimonios	
		Estos especialistas tienen las habilidades necesarias para entender y templar los perjuicios de ciberseguridad
	P10.¿Qué estrategia vinculada a la ciberseguridad considera Ud que se debe aplicar respecto a la permanencia del personal especialista ?	
	RE1	Modificación de los anexos que encamina la ruta profesional del personal que trabaja en la institución, Implementar programas de incentivos, como bonificaciones, reconocimientos y oportunidades de ascenso, para retener a profesionales altamente calificados en ciberseguridad. Fomentar una cultura de aprendizaje continuo, donde el personal esté motivado para mantenerse actualizado sobre las últimas amenazas y tecnologías en ciberseguridad.
	RE2	Implementar programas de incentivos, como bonificaciones, reconocimientos y oportunidades de ascenso, para retener a profesionales altamente calificados en ciberseguridad. Fomentar una cultura de aprendizaje continuo, donde el personal esté motivado para mantenerse actualizado sobre las últimas amenazas y tecnologías en ciberseguridad
	RE3	Para mantener profesionales de ciberseguridad altamente capacitados y preparados, es muy importante ofrecer programas de incentivos como bonificaciones, reconocimiento y oportunidades para el ascenso. Fomentar un entorno de aprendizaje donde los empleados estén motivados para mantenerse informados sobre las últimas amenazas y tecnologías de ciberseguridad
	RE4	Implementar programas de incentivos como bonificaciones, reconocimiento y oportunidades de promoción para retener profesionales de ciberseguridad de alta calidad. Fomente una cultura de aprendizaje continuo donde los empleados estén motivados para mantenerse actualizados con las últimas amenazas y tecnologías de ciberseguridad.

Nota*:* *La tabla corresponde a la codificación abierta de la tercera categoría*

4.3 Definición de las categorías

Estos instrumentos de clasificación permiten estructurar el pensamiento de manera que se pueda comprender mejor el objeto de estudio (Aguaded Ramírez et al., 2020). Una vez identificadas las categorías y analizados los manuales de doctrina consultados se procede a definir las categorías – subcategorías y los patrones.

Tabla 6

Definición de categorías a partir de la entrevista (Codificación axial)

Tema	Categoría	Sub-Categorías	Frecuencia	Síntesis del análisis documental
Políticas Integrales De Ciberseguridad	C1: Toma de conciencia y capacitación	SC1: Toma de conciencia	4	Es fundamental concienciar al personal sobre la importancia de estar alerta, además de organizar encuentros para facilitar el intercambio de ideas y experiencias entre diversas entidades y sectores, con el fin de compartir las mejores estrategias en ciberseguridad y ciberdefensa. Las políticas sobre ciberseguridad que se deben adoptar, deben estar enfocadas en política de contraseñas fuertes., actualizaciones y parches., controles de acceso. y respuesta a incidentes
		SC2: Capacitación	4	La capacitación del personal en todos los niveles se debe orientar en la Concientización sobre amenazas cibernéticas el Reconocimiento de los ataques cibernéticos y la Gestión de la información digital, luego evaluar el efecto de la capacitación para asegurarse de que sea efectiva, la capacitación va desde los líderes hasta el personal técnico, la capacitación en ciberseguridad debe ser un esfuerzo integral que involucre a todos los niveles de la organización. Para asegurarse de que la capacitación sea efectiva, es fundamental evaluar su impacto. Desde los líderes hasta el personal técnico, la capacitación en ciberseguridad debe ser un esfuerzo integral que involucre a todos los niveles de la organización

Tema	Categoría	Sub-Categorías	Frecuencia	Síntesis del análisis documental
	C2: Recursos de ciberseguridad	SC3: Recursos Humanos	4	La gestión de recursos humanos en la administración del riesgo cibernético es una preocupación importante para los líderes de seguridad, ya que los empleados móviles/remotos han sido una de las principales vulnerabilidades de las organizaciones a nivel mundial. Estos colaboradores acceden a redes y aplicaciones a través de la nube desde dispositivos múltiples, compartiendo una red doméstica insegura, lo que aumenta significativamente el riesgo. Es necesario ir más allá de la capacitación para concienciar a los usuarios sobre diferentes tipos de fraudes y compromisos de seguridad.
		SC4: Recursos Digitales	4	En el ámbito de la tecnología digital, es fundamental cifrar los datos importantes para resguardar la información tanto en su envío como en su guardado. Asimismo, es necesario contar con sistemas de vigilancia constante para detectar posibles actividades sospechosas o amenazas inminentes en tiempo real. Por último, es crucial llevar a cabo revisiones de seguridad de forma periódica para evaluar la eficiencia de las medidas de protección implementadas y corregir posibles fallas o vulnerabilidades
Protección de la Información	C3: Permanencia del personal	SC5: Oficiales	4	Es crucial para la información digital del Ejército contar con un equipo de Oficiales Especialistas en Ciberseguridad que estarán en el Ejército por mucho tiempo. "Los oficiales tienen la formación y las habilidades necesarias para comprender y mitigar los riesgos de ciberseguridad".

Tema	Categoría	Sub-Categorías	Frecuencia	Síntesis del análisis documental
	técnico especialista	SC6: Personal de Tcos y SSOO	4	Es muy importante contar con técnicos y suboficiales expertos en ciberseguridad en las unidades del Ejército del Perú, porque pueden ayudar a mantener la información y los sistemas digitales a salvo de ciberataques, ya que tienen las habilidades y las herramientas para hacerlo, la sostenibilidad del personal de técnicos y suboficiales especializados en ciberseguridad en las unidades del Ejército del Perú es de vital importancia para garantizar la protección de la información sensible y la infraestructura digital frente a las ciberamenazas.
		SC7: Personal Civil especialista	4	La retención de personal civil en el Ejército especializado en seguridad cibernética será una estrategia adicional importante para fortalecer la base de seguridad digital. Los profesionales civiles cuentan con la formación y las habilidades necesarias para reconocer y mitigar los riesgos de ciberseguridad, tener expertos civiles en ciberseguridad en las unidades del Ejército puede ser un enfoque beneficioso y adicional para mejorar la seguridad digital del Ejército, los expertos tienen el conocimiento y las habilidades para comprender y abordar las amenazas a la ciberseguridad, por último la entrada y estancia de personal civil especializado en ciberseguridad en las dependencias del Ejército puede fortalecer y complementar la seguridad digital, estos especialistas tienen las habilidades necesarias para entender y templar los perjuicios de ciberseguridad

Tabla 7

Definición de categorías a partir de la observación (Codificación axial)

Tema	Categoría	Sub-Categorías	Frecuencia	Síntesis de la observación
Políticas Integrales De Ciberseguridad	C1: Toma de conciencia y capacitación	SC1: Toma de conciencia	2	Se evidencio en la observación que el personal del ejército no toma conciencia en la seguridad cibernética, porque a nivel ejército no existe una cultura adecuada de ciberseguridad ya que no son conscientes de la realidad del peligro cibernético que existe actualmente.
		SC2: Capacitación	2	Se pudo verificar que el Ejército no dicta cursos recurrentes en ciberseguridad de forma transversal a todo el personal militar y civil del Ejército, únicamente dicta cursos de capacitación a nivel especialización solo para Oficiales del arma de Comunicaciones.
	C2: Recursos de ciberseguridad	SC3: Recursos Humanos	2	Se evidenció que El personal que labora en las dependencias del ejército no se encuentra suficientemente preparado, porque únicamente se dicta cursos de capacitación a nivel básico en la Escuela De Comunicaciones y los pocos oficiales que llevan estos cursos son mal empleados en otras funciones que no son acordes con su especialización.
		SC4: Recursos digitales	2	El ejército no dispone de recursos digitales en suficiente cantidad y con tecnología actual y acorde para asegurar la ciberseguridad porque las tecnologías de ciberseguridad del Ejército Peruano no se encuentran orquestadas entre sí, cada una cumple una función individual y no se tiene claro que fase de un posible ciberataque se mitiga y cuáles son las fases que no se están mitigando.

Tema	Categoría	Sub-Categorías	Frecuencia	Síntesis de la observación
Protección de la Información	C3: Permanencia del personal técnico especialista	SC5: Oficiales	2	El personal de oficiales especialista en ciberseguridad no permanece en el puesto el tiempo suficiente puesto que el principal objetivo del oficial es alcanzar el grado inmediato superior a través de un ascenso y esto se logra gracias a las calificaciones anuales ya que esto varía de acuerdo a la unidad donde presta servicio el oficial (unidades con mayor coeficiente de calificación).
		SC6: Personal Auxiliar especialista	2	El personal de técnicos y suboficiales especialistas en ciberseguridad al igual que los oficiales no permanece en el puesto el tiempo suficiente puesto que el principal objetivo de los TCOS y SSOO es alcanzar el grado inmediato superior a través de un ascenso y esto se logra gracias a las calificaciones anuales ya que esto varía de acuerdo a la unidad donde presta servicio el oficial (unidades con mayor coeficiente de calificación).
		SC7: Personal Civil especialista	2	Se pudo apreciar que no se cuenta con personal civil especialista en ciberseguridad y además pero no se otorga cursos de especialidad, sin embargo, si se tiene oficiales de la especialidad de ciencia y tecnología que son de procedencia Universitaria con el grado académico de Ingenieros de sistemas y que dado al grado militar que ostentan de igual forma que los oficiales de carrera y los Tcos y Suboficiales tienen aspiraciones de ascenso a los grados superiores

-

Tabla 8

Definición de categorías a partir del análisis documental (Codificación axial)

Tema	Categoría	Sub-Categorías	Frecuencia	Síntesis de las entrevistas
Políticas Integrales de Ciberseguridad	C1: Toma de conciencia y capacitación	SC1: Toma de conciencia	2	Los ciberataques suelen ocurrir con mayor frecuencia debido a la falta de conciencia de las personas, lo cual los delincuentes aprovechan para obtener información financiera y privada, así como para extorsionar a sus víctimas. Por lo tanto, es crucial que las organizaciones se enfoquen en la formación y monitoreo de la conciencia de las personas para evitar este tipo de situaciones. Zambrano (2019)
				El Obj 1 de la Política Nacional de Ciberseguridad, PCM: El fortalecimiento de las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el de la ciberseguridad, creando un entorno y las condiciones necesarias que permitan brindar protección en el ciberespacio. Donde se señala que es fundamental fortalecer las capacidades del Estado en materia de ciberseguridad para garantizar la protección de la información y la seguridad de la población. Esto requiere una acción coordinada y colaborativa entre diferentes sectores, además de una concienciación general sobre la importancia de la ciberseguridad. La cooperación internacional también desempeña un papel crucial en este proceso, así como el apoyo a investigaciones relacionadas con ataques informáticos.
		SC2:	2	Obj 2 de la Política Nacional de Ciberseguridad (PCM): señala que se debe brindar capacitación especializada en

Tema	Categoría	Sub-Categorías	Frecuencia	Síntesis de las entrevistas
		Capacitación		seguridad de la información y ampliar las líneas de investigación en materia de ciberseguridad dentro de la administración pública. Este objetivo busca desarrollar y fortalecer las habilidades en seguridad cibernética, con el fin de enfrentar las amenazas que afectan los objetivos establecidos. En principio, se brindará formación a los funcionarios responsables de la gestión de incidentes cibernéticos, con la intención de luego ampliar esta formación a todas las entidades gubernamentales. El Pe-CERT, con el respaldo del CICTE de la OEA, creará un Plan de Formación para el resto de los empleados del Estado, además de programas de concienciación para la población en general. Además, el MININTER buscará incluir asignaturas de seguridad de la información, ciberseguridad y ciberdefensa en la formación de oficiales y suboficiales en las escuelas correspondientes UNAM, (2022) Boletín No. 1, 7 P.11……Además de trabajar en mejorar la seguridad cibernética, es fundamental enfocarse en la educación digital, la cual abarca habilidades, conocimientos y actitudes necesarias para desenvolverse eficazmente en el mundo digital. Esto incluye la capacidad de utilizar herramientas digitales, entender el funcionamiento del hardware, aplicaciones, programas y motores de búsqueda, así como la habilidad de buscar y procesar información de manera efectiva en entornos electrónicos.
	C2:	SC3:	2	Después de revisar la información de la empresa y su rendimiento en un entorno de alta rotación de personal, se

Tema	Categoría	Sub-Categorías	Frecuencia	Síntesis de las entrevistas
	Recursos de ciberseguridad	Recursos Humanos		intenta analizar la influencia significativa que esto tiene en la gestión de recursos humanos y en el rendimiento global de la empresa. En una industria de ciberseguridad, donde el talento es escaso y las habilidades técnicas son esenciales, la rotación de empleados puede tener un impacto profundo en la continuidad y calidad de los servicios ofrecidos. Además, se debe considerar el elevado costo y tiempo que conlleva el proceso de reclutamiento, selección, contratación y formación de nuevos trabajadores. (Pérez y Salazar. 2023)
		SC4: Recursos digitales	1	El aumento en el número de dispositivos y el uso generalizado de la virtualización están abriendo nuevas posibilidades para amenazas, riesgos y ataques digitales. La actividad maliciosa está en aumento debido a las vulnerabilidades en aumento y a la facilidad de entrada en la industria del ransomware, así como a la baja probabilidad de ser extraditado, enjuiciado o sancionado. La tendencia del "ransomware como servicio" permite que incluso personas no técnicas lleven a cabo ataques, una tendencia que podría amplificarse con la llegada del malware impulsado por inteligencia artificial (AI, por sus siglas en inglés) (Foro Económico Mundial, 2022). (Universidad Nacional autónoma de México, vigilancia tecnológica en Ciberseguridad Boletín No. 1, 7 de junio de 2022. P.21
Protección de la Información	C3: Permanencia del personal	SC5: Oficiales especialistas	1	Pero tal vez el peor problema surgido de este cambio traumático fue la falta de formación adecuada de los líderes militares para planificar operaciones en línea, intentando compensar esta deficiencia con personal versado en

Tema	Categoría	Sub-Categorías	Frecuencia	Síntesis de las entrevistas
	técnico especialista			ciberseguridad en el ámbito civil o empresarial. Mientras que en el ámbito civil la seguridad se centra en proteger la información dentro de la empresa, en el ámbito militar se planifican operaciones estratégicas de recopilación de información, defensa y ataques cibernéticos. Esta falta de planificación ha llevado a una transición abrupta de la seguridad informática a operaciones cibernéticas sin una preparación adecuada, lo que ha generado la mayoría de los problemas actuales. Aunque se utilice la ciberdefensa como tema político, no se abordan las lagunas existentes, posiblemente porque se considera que el uso del ciberespacio para operaciones militares es algo de ficción. El ciberespacio, un aspecto a tener en cuenta en el planeamiento militar CM (r) R. Mato Ex J.E.M. Cdo.de Ciberdefensa ESGCFFAA-2016.
		SC6: Personal Auxiliar especialista	1	Es necesario establecer un programa integral de formación y concienciación, adaptado a los riesgos específicos de cada categoría de empleados, en lugar de ofrecer módulos genéricos sin una visión estratégica. Es esencial también prestar atención a los usuarios ocasionales de los sistemas corporativos de TI, quienes pueden no estar familiarizados con las políticas y prácticas de seguridad de la organización. (La ciberseguridad en las organizaciones del sistema de las Naciones Unidas. (2021) El personal como primera línea defensiva p.8.)
		SC7:	1	El Ejército de Estados Unidos ha aprobado un programa para reclutar especialistas en ciberseguridad con experiencia

Tema	Categoría	Sub-Categorías	Frecuencia	Síntesis de las entrevistas
		Personal Civil especialista		directa en el servicio, con el fin de fortalecer un área que los líderes militares consideran esencial para la seguridad nacional. Esta iniciativa, apoyada por el Pentágono y el Congreso, es un proyecto piloto destinado a incorporar cinco nuevos oficiales anualmente durante un período de cinco años. En España, se han puesto en marcha varias iniciativas para abordar los desafíos presupuestarios y de formación en las FFAA. Recientemente, el Mando Conjunto de Ciberdefensa implementó una medida destinada a formar un grupo de expertos para situaciones concretas, sin proporcionar compensación económica. Resolver esta problemática no es sencillo. A pesar de los intentos por reubicar y capacitar al personal interno de otras áreas en estos puestos, no existen procesos formales para reclutar personal civil que pueda cubrir las necesidades de estos organismos públicos. Los procedimientos actuales de reclutamiento no parecen ser atractivos para estos perfiles especializados. Además, los controles de seguridad exigidos podrían dificultar la selección de candidatos altamente especializados. CyberSecurityPulse: (2017) El Ejército de EEUU “lanzamiento de un programa para captar civiles en ciberseguridad”.

Nota: *La tabla corresponde a la codificación axial a partir del análisis documental*

Tabla 9

Referencias utilizadas en el análisis documental

Subcategoría	Documentación	Disponibilidad
SC1: Toma de conciencia	Zambrano, Dayhan (2019) La ausencia de conciencia como una vulnerabilidad latente para la seguridad de la información – Cali, Colombia	Archivo Digital
	Política Nacional de Ciberseguridad PCM, Perú Obj 1- p.8	Archivo Digital
SC2: Capacitación	Política Nacional de Ciberseguridad PCM, Perú . Obj 1 p.11	Archivo Digital
	Universidad Nacional Autónoma de México "vigilancia tecnológica en ciberseguridad Boletín No. 1, 7 de junio de 2022. P.31"	Archivo Digital
SC3: Recursos Humanos	Perez y Salazar (2023) Universidad peruana de ciencias aplicadas .Impacto de la rotación laboral en la gestión de recursos humanos y el desempeño organizacional de una empresa de Ciberseguridad en Lima	Archivo Digital
SC4: Recursos digitales	Universidad Nacional Autónoma de México (2022) vigilancia tecnológica en ciberseguridad p.21	Archivo Digital
SC5: Oficiales especialistas	El ciberespacio, "un factor a considerar en la planificación militar, CM (r) R. Mato Ex J.E.M. Cdo. de Ciberdefensa ESGCFFAA-2016"	Archivo Digital
SC6: Personal de TCOS y SSOO especialista	La ciberseguridad en las organizaciones del sistema de las Naciones Unidas (2021) señala "que el personal constituye la primera línea de defensa, p. 8."	Archivo Digital
SC7: Personal Civil especialista	CyberSecurityPulse (2017) reporta que "el Ejército de Estados Unidos ha iniciado un programa para reclutar civiles en el área de ciberseguridad."	Archivo Digital

4.4 Soporte de las categorías

En esta sección del análisis, se busca consolidar las categorías en temas más amplios y centrales, basados en sus características (codificación axial) que emergen del primer plan de agrupación de categorías de codificación abierta. “Para identificar temas, es necesario encontrar patrones recurrentes en todas las categorías. Cada tema detectado recibirá un código, similar al proceso utilizado con las categorías. Estos temas constituirán la base de las conclusiones del análisis” (Hernández, 2018, p. 490).

Tabla 10

Matriz de soporte de las categorías

Tema	Categoría	Sub-Categorías	Patrones /Ítems	Síntesis
Políticas Completas	C1: Toma de conciencia y capacitación	SC1: Toma de conciencia	- Seguridad - Responsabilidad. - Cultura de seg. - Disciplina	El personal del ejército que labora en las diferentes dependencias de la institución debe tomar conciencia en de la seguridad cibernética, identificar posibles vulnerabilidades o amenazas y tomar acciones oportunas .
		SC2: Capacitación	- Capacitación - Especialidad - Autodidacta	La capacitación del personal en todos los niveles se enfoca en la concienciación sobre amenazas cibernéticas, el reconocimiento de ataques cibernéticos y la gestión de la información digital.
	C2: Recursos de ciberseguridad	SC3: Recursos Humanos	- Personal - Capacitaciones - Funciones	La administración del riesgo cibernético en la gestión de recursos humanos es una preocupación clave para los líderes en seguridad.
		SC4: Recursos digitales	- Ciberataque - Filtro Web - Antivirus - Plataforma	Se refiere a todo lo relacionado con el sistema de computadoras, especialmente en el ámbito digital, donde la información está codificada en formatos digitales y se utiliza software para su procesamiento.
Protección de la Información	C3: Permanencia del personal técnico especialista	SC5: Permanencia Oficiales	- Ascenso - Línea de carrera - Calificación	En el campo de la ciberseguridad, la falta de talento se ha convertido en un problema urgente para las organizaciones.
		SC6: Permanencia Personal TCOS Y SSOO	- Ascenso - Línea de carrera - Calificación -	En el campo de la ciberseguridad, la falta de personal cualificado se ha convertido en un desafío importante. Estos expertos son fundamentales para proteger las redes y la información, gestionar la seguridad informática de una organización. redes y la información,
		SC7:Personal Civil especialista	- Permanencia - Convocatoria - Oficiales CT	Un Especialista en Ciberseguridad es un profesional que se dedica a proteger los sistemas informáticos, redes y datos de ataques, daños o accesos no autorizados.

4.4.1 Soporte de categorías:

Categoría 1: Toma de conciencia y capacitación

En esta categoría se analizará la toma de conciencia y la capacitación, dicha categoría tiene dos subcategorías que son la toma de conciencia y la capacitación

Sub-Categoría 1: Toma de conciencia

Los expertos entrevistados opinan lo siguiente:

El objetivo es generar conciencia entre el personal y llevar a cabo actividades de divulgación dirigidas a ciudadanos y entidades tanto públicas como privadas. También se organizarán foros para el intercambio de experiencias y mejores prácticas en ciberseguridad y ciberdefensa entre entidades del sector público y privado, la sociedad civil y la academia. Las políticas de ciberseguridad que se deben implementar deberían enfocarse en aspectos como la política de contraseñas fuertes, actualizaciones y parches, controles de acceso y respuesta a incidentes (RE1). Otro entrevistado opina que las políticas para el uso adecuado de los sistemas informáticos deben incluir políticas de recuperación ante desastres (resiliencia) y políticas de actualización de software (RE2). Otro entrevistado sugiere que las políticas de ciberseguridad deben centrarse en tener una política de contraseñas sólidas, actualizaciones y mejoras en los controles de acceso para gestionar y abordar incidentes o emergencias (RE2). Finalmente, se debe adoptar políticas de ciberseguridad enfocadas en la seguridad de la red, respaldo de datos, y control de acceso y privilegios.

De la observación realizada

En la observación realizada se evidencio que el personal del ejército no toma conciencia en la seguridad cibernética, porque a nivel ejército no existe una cultura adecuada de ciberseguridad ya que no son conscientes de la realidad del peligro cibernético que existe actualmente.

De la ruta documentaria los autores afirman:

Por un lado, Zambrano (2019) afirma que los ciberataques son cada vez más comunes debido a la falta de conciencia entre las personas, lo que los delincuentes explotan para obtener información financiera y privada, así como para extorsionar a sus víctimas. Por ello, es esencial que las organizaciones se concentren en la formación y el monitoreo de la conciencia de las personas para prevenir estas situaciones.

Asimismo, El Objetivo 1 de la Política Nacional de Ciberseguridad, PCM, establece que es esencial reforzar las capacidades del Estado en ciberseguridad para asegurar la protección de la información y la seguridad de la población. Esto requiere una acción coordinada y colaborativa entre diversos sectores, así como una concienciación general sobre la importancia de la ciberseguridad. La cooperación internacional también es fundamental en este proceso, junto con el apoyo a investigaciones sobre ataques informáticos.

Sub-Categoría 2: Capacitación.

Los expertos entrevistados opinan lo siguiente:

La capacitación del personal encargado de manejar la información digital en las dependencias del Ejército del Perú debe enfocarse en varios aspectos: la higiene cibernética y el uso adecuado de los sistemas de información **(E1).** Según otro entrevistado, también es necesario incluir educación sobre riesgos cibernéticos, identificación de ciberataques y manejo de la información digital **(E2).** Además, el **(RE3)** sugiere que la capacitación debe abarcar la concienciación sobre amenazas cibernéticas, el reconocimiento de ataques cibernéticos y la gestión de la información digital. Finalmente, el **(RE3)** también menciona que la formación debe incluir la gestión de las comunicaciones digitales, el entendimiento de las amenazas cibernéticas y la comprensión de los ataques cibernéticos.

De la observación realizada

La observación reveló que el Ejército no ofrece cursos regulares de ciberseguridad de manera general a todo su personal militar y civil. En cambio, solo proporciona formación especializada en ciberseguridad para los Oficiales del arma de Comunicaciones.

De la ruta documentaria los autores afirman:

El Objetivo 2 de la Política Nacional de Ciberdefensa establece que, inicialmente, se proporcionará capacitación a los funcionarios encargados de la gestión de incidentes cibernéticos, con el objetivo de expandir esta formación a todas las entidades gubernamentales en una etapa posterior. El Pe-CERT, con el apoyo del CICTE de la OEA, elaborará un Plan de Formación para el personal estatal restante y desarrollará programas de concienciación para el público en general. Además, el MININTER se enfocará en integrar asignaturas sobre seguridad de la información, ciberseguridad y ciberdefensa en la formación de oficiales y suboficiales en las instituciones educativas correspondientes.

Según el Boletín No. 1 de la UNAM (2022), además de avanzar en la mejora de la seguridad cibernética, es crucial centrarse en la educación digital. Esta abarca las habilidades, conocimientos y actitudes necesarios para operar eficazmente en el entorno digital. Esto incluye la capacidad para utilizar herramientas digitales, comprender el funcionamiento del hardware, aplicaciones, programas y motores de búsqueda, así como la habilidad para buscar y procesar información de manera efectiva en entornos electrónicos.

- ***Categoría 2: Recursos de ciberseguridad***

La seguridad informática abarca diversas perspectivas y estrategias para proteger los sistemas, redes y datos contra posibles amenazas en línea. Esto incluye la defensa contra intrusiones de hackers, la detección de malware, la prevención del robo de identidad y cualquier otro intento que pueda comprometer la seguridad de

la información digital. Esta área se desarrolla mejor al enfocarse en estos aspectos clave. se ha fraccionado en dos subcategorías que son los recursos humanos y los recursos digitales; los resultados muestran lo siguiente:

Sub-Categoría 3: Recursos Humanos.

Los expertos entrevistados opinan lo siguiente:

Según los expertos entrevistados, se recomienda tener una guía de buenas prácticas que todos los empleados deben seguir en la empresa. Esta guía incluye diferentes formas de acción, procedimientos y procesos para asegurar los datos y actividades de la institución. Además, estas políticas también contemplan planes de acción en caso de crisis. Aunque el enfoque principal es la prevención de la inseguridad, si se produce una filtración o vulnerabilidad, se implementan medidas para contenerla. Dado que está vinculada a la tecnología informática, esta estrategia se actualiza regularmente en función de los cambios y avances en el ámbito cibernético. Por lo tanto, la política de seguridad se revisa periódicamente para adaptarse a las nuevas necesidades y desafíos. Además, se debe considerar la inclusión de criterios de habilidades y conocimientos en ciberseguridad al contratar nuevo personal. Considerar la experiencia previa en ciberseguridad como un activo importante. Proporcionar programas de capacitación en ciberseguridad como parte integral del desarrollo profesional continuo***. (RE1)***

El segundo entrevistado señala que, al contratar nuevos empleados, considere los estándares de habilidades y conocimientos en ciberseguridad. Considere la experiencia previa en ciberseguridad como una ventaja clave. Ofrezca diplomados de capacitación en ciberseguridad como parte integral de su desarrollo profesional***(RE2).***

El tercer entrevistado dice que es crucial medir la eficacia de la formación midiendo su impacto. Es importante brindar capacitación en ciberseguridad a todos los empleados, desde los ejecutivos de alto nivel hasta el personal técnico, para crear una estrategia de seguridad integral y efectiva. ***(RE3).***

Por último, el cuarto entrevistado opina que se debe realizar un programa de capacitación en ciberseguridad como una parte importante del desarrollo

profesional. Incluya criterios de conocimientos y habilidades de ciberseguridad al contratar nuevos empleados. Considere además la experiencia previa en ciberseguridad como una ventaja. ***(RE4).***

De la observación realizada

En la observación realizada se ha evidenciado que el personal que labora en las dependencias del Ejército no se encuentra suficientemente preparado, porque únicamente se dicta cursos de capacitación a nivel básico en la Escuela De Comunicaciones y los pocos oficiales que llevan estos cursos son mal empleados en otras funciones que no son acordes con su especialización.

En la ruta documentaria los autores afirman:

Pérez, Christian y Salazar, Melissa (2023) argumentan que, tras revisar la información de la institución y su desempeño en un entorno con alta rotación de personal, se busca analizar el impacto significativo que esto tiene en la gestión de RRHHH y en el rendimiento general de la empresa. En el sector de ciberseguridad, donde el talento es limitado y las habilidades técnicas son cruciales, la rotación de empleados puede afectar profundamente la continuidad y la calidad de los servicios prestados. Además, es necesario tener en cuenta el alto costo y el tiempo involucrado en el proceso de captación, selección, contratación y capacitación de nuevos empleados.

Sub-Categoría 4: Recursos digitales.

Los expertos entrevistados opinan lo siguiente:

- Los expertos entrevistados opinan que para detectar actividades inusuales o amenazas potenciales se deben implementar sistemas de monitoreo continuoy realizar medidas de control en forma continua. ***(RE1).***
- Aplicar cifrado a datos confidenciales para proteger la información en tránsito y en reposo. Configurar un sistema de monitoreo continuo para detectar actividades anómalas y amenazas potenciales en tiempo real. *(**RE2**))*
- Se debe emplear cifrado para salvaguardar la información confidencial durante su envío o almacenamiento, configurar los sistemas para que supervisen

continuamente cualquier actividad inusual o amenaza potencial en tiempo real, y llevar a cabo auditorías de seguridad periódicas para evaluar la efectividad de las medidas de protección implementadas y detectar posibles vulnerabilidades.

- Implementación de cifrado para asegurar la protección de datos confidenciales tanto en tránsito como en reposo. Configuración de sistemas para el monitoreo constante con el fin de identificar actividades inusuales o amenazas potenciales en tiempo real. ***(RE4)***

De la observación realizada

En la observación realizada se evidencio que el Ejército no dispone de recursos digitales en suficiente cantidad y con tecnología actual y acorde para asegurar la ciberseguridad porque las tecnologías de ciberseguridad del Ejército Peruano no se encuentran orquestadas entre sí, cada una cumple una función individual y no se tiene claro que fase de un posible ciberataque se mitiga y cuáles son las fases que no se están mitigando.

En la ruta documentaria los autores afirman:

Según la UNAM (2022), el incremento en el número de dispositivos y el uso extendido de la virtualización están creando nuevas oportunidades para amenazas, riesgos y ataques digitales. La actividad maliciosa está en aumento debido a las crecientes vulnerabilidades y la facilidad de acceso a la industria del ransomware, así como a la baja probabilidad de ser extraditado, enjuiciado o sancionado. La tendencia del “ransomware como servicio” permite que incluso personas sin conocimientos técnicos realicen ataques, una tendencia que podría intensificarse con la llegada del malware impulsado por inteligencia artificial (Foro Económico Mundial, 2022).

- ***Categoría 3: Permanencia del personal técnico especialista***

Esta categoria aborda la permanencia del personal especialista en ciberseguridad que cumple funciones en las diferentes dependencias del Ejercito en los tres niveles, (1) el status de Oficial,(2) los Tcos y Suboficiales y (3) del personal civil, todo ello con la finalidad de conocer cómo es que la rotación o movilidad de puestos que es por necesidad de servicio afecta a la ciberseguridad conociéndose que la capacitación y grado de experiencia recién se obtiene a partir del segundo año ininterrumpido.

Sub-Categoría 5: Oficiales especialistas

Los expertos entrevistados sobre la permanencia del personal de oficiales especialistas opinan lo siguiente*:*

Es fundamental para la continuidad de los objetivos estratégicos del ejército la permanencia en el puesto, para la seguridad de la información digital del Ejército. Estos Oficiales tienen la formación y las habilidades necesarias para comprender y mitigar los riesgos de ciberseguridad*.* **(*RE1*)**

Crear un diplomado de formación obligatorio en ciberseguridad para todo el personal que trabajan con información digital. Ofrecer capacitación en ciberseguridad impartida por instructores calificados y experimentados. Reconocer y recompensar el compromiso de los empleados con la ciberseguridad*. (**RE2)***

Es crucial para la información digital del Ejército contar con un equipo de Oficiales Especialistas en Ciberseguridad que estarán en el Ejército por mucho tiempo. "Los oficiales tienen la formación y las habilidades necesarias para comprender y reducir los riesgos de ciberseguridad*. (**RE3**)*

La permanencia de los expertos en ciberseguridad en las unidades del Ejército del Perú es esencial para proteger la información digital del Ejército. Estos profesionales poseen la formación y las habilidades necesarias para identificar y mitigar los riesgos de ciberseguridad. **(*E4*).**

De la observación realizada:

En la observación se evidencio que el personal de oficiales especialista en ciberseguridad no permanece en el puesto el tiempo suficiente puesto que el principal objetivo del oficial es alcanzar el grado inmediato superior a través de un ascenso y esto se logra gracias a las calificaciones anuales ya que esto varía de acuerdo a la unidad donde presta servicio el oficial (unidades con mayor coeficiente de calificación).

En la ruta documentaria los autores afirman:

En su recopilación documental, Mato, R. (2016) argumenta que uno de los mayores problemas derivados del cambio tecnológico abrupto es la falta de formación adecuada de los líderes militares para planificar operaciones en línea. Para compensar esta deficiencia, se ha recurrido a personal especializado en ciberseguridad del ámbito civil o empresarial. Mientras que en el sector civil la seguridad se enfoca en proteger la información interna de la empresa, en el ámbito militar se planifican operaciones estratégicas de recopilación de información, defensa y ataques cibernéticos. Esta falta de planificación ha provocado una transición brusca de la seguridad informática a las operaciones cibernéticas sin la preparación adecuada, generando la mayoría de los problemas actuales. Aunque la ciberdefensa se utiliza como tema político, no se abordan las brechas existentes, posiblemente porque se percibe el uso del ciberespacio para operaciones militares como algo ficticio.

Sub-Categoría 6: Personal de técnicos y suboficiales especialistas

Los expertos entrevistados opinan lo siguiente:

Los expertos entrevistados sobre la permanencia del personal técnico y suboficiales especialistas opinan lo siguiente:

Se sugiere que es un enfoque útil y complementario para reforzar la perspectiva de seguridad digital. Estos especialistas están capacitados para comprender y reducir los peligros de ciberseguridad*. **(RE1**)*

Los puestos en el Ejército son bastante rotativos, muchas veces se capacita al personal y cuando ya manejan una solución, son cambiados a otro puesto de trabajo (***RE2****)*

Es muy importante contar con técnicos y suboficiales expertos en ciberseguridad en las unidades del Ejército del Perú, porque pueden ayudar a mantener la información y los sistemas digitales a salvo de ciberataques, ya que tienen las habilidades y las herramientas para hacerlo. ***(RE3)***

Estoy seguro de que mantener un equipo de “TÉCNICOS y SUBOFICIALES” especializados en ciberseguridad en las unidades del Ejército del Perú es crucial para proteger la información sensible y la infraestructura digital contra las ciberamenazas. ***(RE4)***

De la observación realizada

En la Observación realizada se evidenció que el personal de “TÉCNICOS y SUBOFICIALES” especialistas en ciberseguridad al igual que los oficiales no permanece en el puesto el tiempo suficiente puesto que el principal objetivo de los TCOS y SSOO es alcanzar el grado inmediato superior a través de un ascenso y esto se logra gracias a las calificaciones anuales ya que esto varía de acuerdo a la unidad donde presta servicio el oficial (unidades con mayor coeficiente de calificación).

En la ruta documentaria los autores afirman:

> En el acopio de información documentaria la ONU expresa que es necesario establecer un programa integral de formación y concienciación, adaptado a los riesgos específicos de cada categoría de empleados, en lugar de ofrecer módulos genéricos sin una visión estratégica. Es esencial también prestar atención a los usuarios ocasionales de los sistemas corporativos de TI, aquellos que pueden no estar al tanto de las políticas y prácticas de seguridad de la organización.

Sub-Categoría 7: Personal Civil especialista

Los expertos entrevistados opinan lo siguiente:

Se sugiere que a permanencia del personal especializado en ciber seguridad es un enfoque útil y complementario para reforzar la perspectiva de seguridad digital, estos especialistas están capacitados para comprender y reducir los peligros de ciberseguridad. (***RE1***)

La retención de personal civil en el Ejército especializado en seguridad cibernética será una estrategia adicional importante para fortalecer la base de seguridad digital, este profesional tiene la formación y las habilidades necesarias para reconocer y mitigar los riesgos de ciberseguridad. **(*RE2*)**

Tener expertos civiles en ciberseguridad en las unidades del Ejército puede ser un enfoque beneficioso y adicional para mejorar la seguridad digital del Ejército, Los especialistas poseen el conocimiento y las capacidades necesarias para entender y enfrentar las amenazas en el ámbito de la ciberseguridad. **(*RE3*)**

La entrada y estancia de personal civil especializado en ciberseguridad en las dependencias del Ejército puede fortalecer y complementar la seguridad digital. Estos especialistas tienen las habilidades necesarias para entender y templar los perjuicios de ciberseguridad **(*RE4*)**

De la observación realizada

Se evidencio que no se cuenta con personal civil especialista en ciberseguridad y además no se otorga cursos de especialidad, sin embargo, se cuenta con oficiales de la especialidad de ciencia y tecnología de procedencia Universitaria Ingenieros de sistemas que aportan significativamente a la ciberseguridad sin embargo dado que el rango otorgado por la institución es Oficial en ciencia y tecnología al igual que los oficiales de carrera tienen aspiraciones de ascenso a los grados superiores.

De la ruta documentaria los autores afirman:

En 2017, el Ejército de Estados Unidos aprobó un programa para reclutar especialistas en ciberseguridad con experiencia directa en el servicio militar. Este

esfuerzo, considerado vital por los líderes militares para la seguridad nacional, es una iniciativa piloto respaldada por el Pentágono y el Congreso. El objetivo del programa es reclutar cinco nuevos oficiales cada año durante un periodo de cinco años.

En España, también se han implementado diversas acciones para hacer frente a las dificultades presupuestarias y de formación en las FFAA. Recientemente, el "Mando Conjunto de Ciberdefensa (MCCE)", publicó una medida que tenía como objetivo contar con un grupo de expertos solo para situaciones específicas, pero sin ofrecer compensación económica.

Resolver esta problemática no es sencillo. A pesar de los intentos por reubicar y capacitar al personal interno de otras áreas en estos puestos, no existen procesos formales para reclutar personal civil que pueda cubrir las necesidades de estos organismos públicos. Los procedimientos actuales de reclutamiento no parecen ser atractivos para estos perfiles especializados. Además, los controles de seguridad exigidos podrían dificultar la selección de candidatos altamente especializados.

4.5 Red semántica

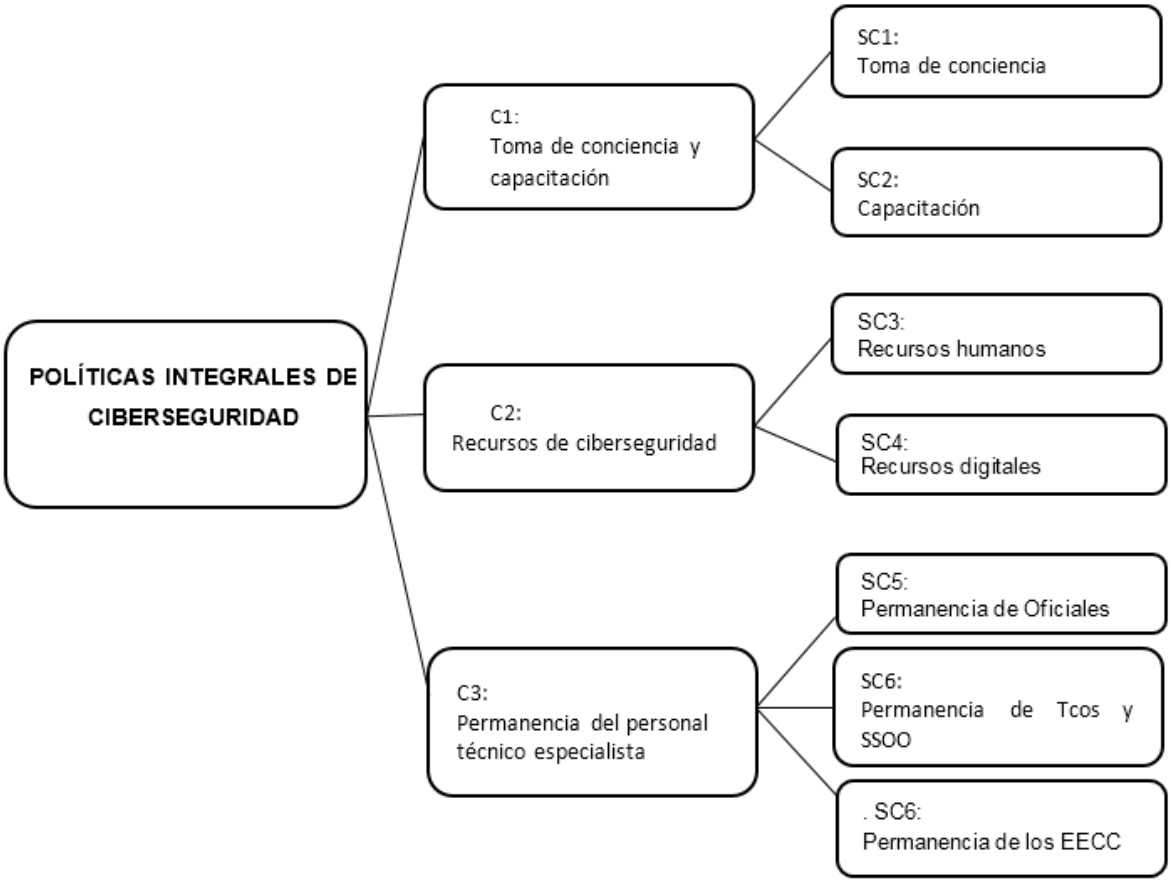
Las redes semánticas se elaboraron meticulosamente, alineándose con las categorías de cada instrumento de investigación. Este método permitió visualizar las complejas relaciones entre los conceptos clave en cada contexto. Además, se creó una red semántica integradora que combinó las principales categorías de todos los instrumentos, proporcionando una visión global y coherente de los temas analizados en los datos recopilados. Esta estrategia facilitó la identificación de patrones, conexiones y temas recurrentes, así como una comprensión más completa y estructurada del contenido, enriqueciendo el análisis categorial. Para llegar a la red semántica final, se desarrollaron diferentes redes específicas.

- Red semántica del Objetivo general
- Red semántica de la primera Categoría con sus respectivas subcategorías que soportan al objetivo general

- Red semántica de la segunda Categoría con sus respectivas subcategorías que soportan al objetivo general
- Red semántica de la tercera Categoría con sus respectivas subcategorías que soportan al objetivo general

Figura 3

Red semántica integral

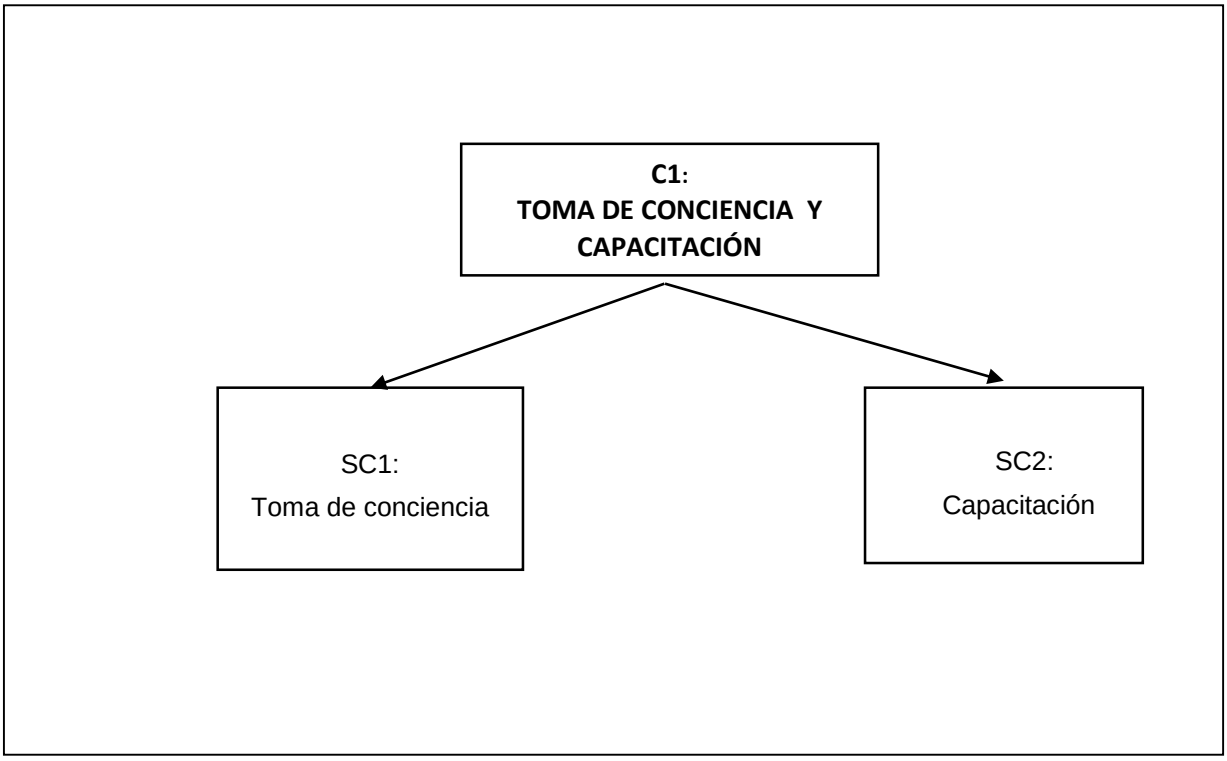


Nota: *La red semántica integral o general muestra la subdivisión en tres subcategorías que son C1, Toma de conciencia y capacitación., C2, Recursos de ciberseguridad y C3, Permanencia del personal técnico especialista.*

Categoría 1: C1_ Toma de conciencia y capacitación

Figura 4

Toma de conciencia y capacitación



Nota: La figura representa la construcción de la red semántica para la categoría de Toma de conciencia y capacitación, junto con sus subcategorías SC1: Toma de conciencia y SC2: Capacitación.

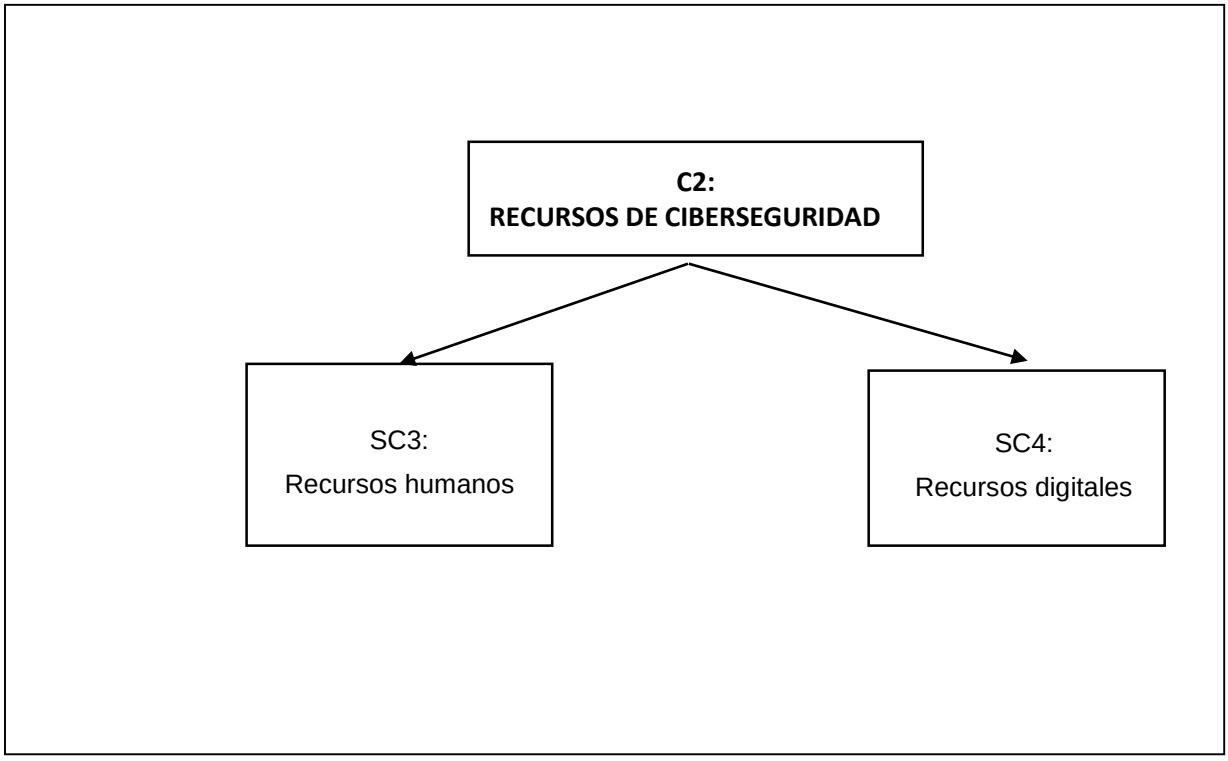
⟷ Se relaciona con

→ Tiene dependencia de

Categoría 2: C1_ Recursos de ciberseguridad

Figura 5

Recursos de ciberseguridad



Nota: La figura representa la construcción de la red semántica para la categoría de recursos de ciberseguridad, incluyendo sus subcategorías: SC3, que corresponde a Recursos Humanos, y SC4, que se refiere a Recursos Digitales.

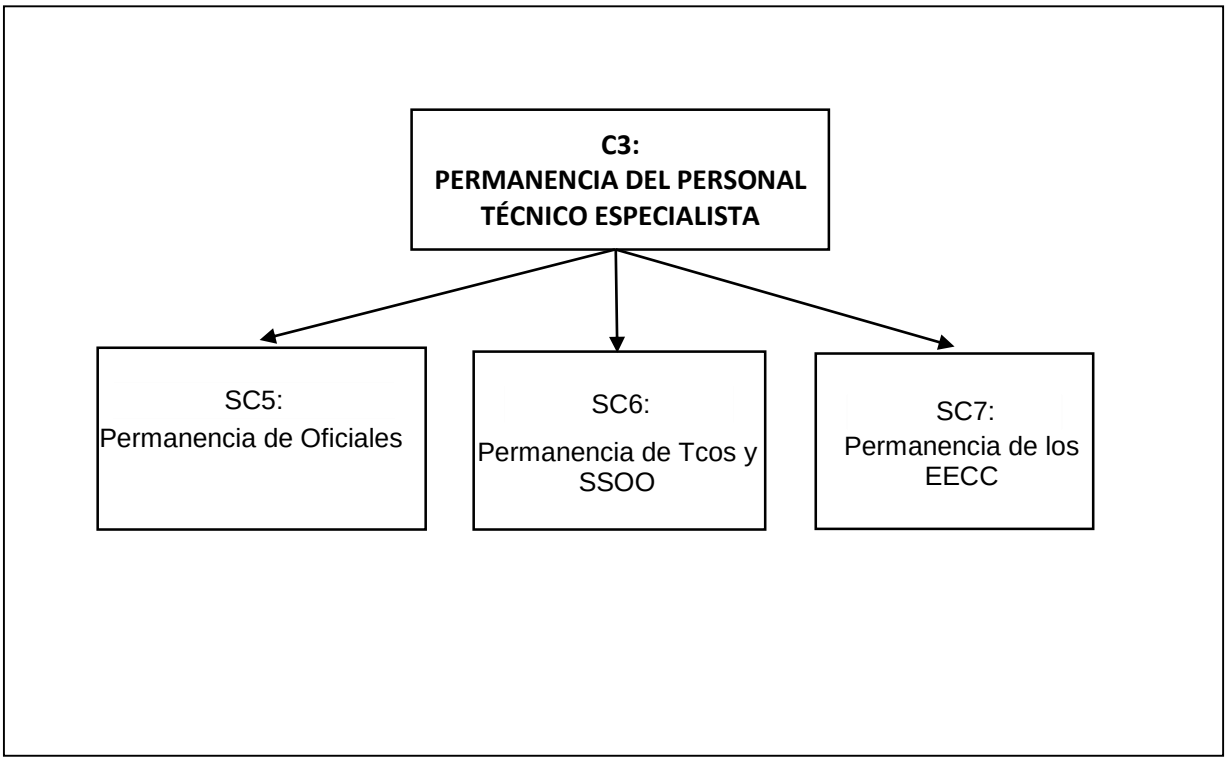
Se relaciona con

Tiene dependencia de

Categoria 3: C3_ Permanencia del personal técnico especialista

Figura 6

Permanencia del personal técnico especialista



Nota: La figura ilustra la creación de la red semántica relacionada con la tercera categoría, que es la Permanencia del personal técnico especialista, junto con sus subcategorías correspondientes: Permanencia de Oficiales.

Se relaciona con

Tiene dependencia de

4.6 Triangulación

Entiéndase por triangulación

La triangulación consiste en cruzar información obtenida de diversas fuentes y métodos de recolección para lograr una mejor comprensión interpretativa de los datos recopilados (Vargas, 2011). En esta investigación, la triangulación se ha llevado a cabo combinando la información obtenida a través de entrevistas y la indagación documental con cada una de las categorías obtenidas, incrementando así la certeza interpretativa de los datos presentados en la síntesis integrativa de cada una de ellas.

Tabla 11

Triangulación integral por categorías y subcategorías

Sub-Categorías	Entrevistas	Observación	Análisis Documental
SC1: Toma de conciencia	Se debe sensibilizar al personal sobre la toma de conciencia, realizar foros intercambiar posiciones y experiencias entre todas las entidades. Las políticas sobre ciberseguridad que se deben adoptar, deben estar enfocadas en política de contraseñas fuertes., actualizaciones y parches., controles de acceso. y respuesta a incidentes	Se evidencio que el personal del ejército no toma conciencia en la seguridad cibernética, porque a nivel ejército no existe una cultura adecuada de ciberseguridad ya que no son conscientes de la realidad del peligro cibernético que existe actualmente.	Los ciberataques suelen ocurrir con mayor frecuencia debido a la falta de conciencia de las personas, lo cual los delincuentes aprovechan para obtener información financiera y privada, así como para extorsionar a sus víctimas. Se requiere de una concienciación general sobre la importancia de la

Sub-Categorías	Entrevistas	Observación	Análisis Documental
			ciberseguridad. así como el apoyo a investigaciones relacionadas con ataques informáticos

Conclusión Parcial 1:

Es necesario concienciar al personal sobre la importancia de la ciberseguridad y organizar foros que faciliten el intercambio de opiniones y experiencias entre entidades públicas y privadas, la sociedad civil y el ámbito académico, con el fin de compartir las mejores prácticas en ciberseguridad y ciberdefensa. Las políticas de ciberseguridad que se deben adoptar deben centrarse en el uso de contraseñas robustas, actualizaciones y parches, controles de acceso y respuesta a incidentes. Se deben implementar sistemas de monitoreo continuo, realizar auditorías y aplicar cifrado a los datos confidenciales para detectar actividades sospechosas y posibles amenazas. Además, es fundamental configurar un sistema de monitoreo en tiempo real para identificar anomalías y riesgos potenciales.

Se ha observado que el personal militar no está suficientemente concienciado sobre la seguridad cibernética, ya que carecen de una cultura de ciberseguridad adecuada y subestiman la amenaza que representan los ciberataques; en la actualidad los ciberdelincuentes se aprovechan de este desconocimiento para perpetrar

Sub-Categorías	Entrevistas	Observación	Análisis Documental
ataques y obtener información sensible, incluyendo datos financieros y personales, e incluso extorsionar a sus víctimas. Por lo tanto, es crucial fomentar una mayor conciencia sobre la relevancia de la ciberseguridad y apoyar la investigación en la prevención de estos ataques. Además, se debe evaluar la efectividad de la capacitación para asegurar que sea eficiente desde los líderes hasta el personal técnico. La formación en ciberseguridad debe ser un esfuerzo integral que abarque todos los niveles de la organización. Es fundamental medir el impacto de la capacitación para garantizar su eficacia, asegurando que este esfuerzo sea efectivo.			
SC2: Capacitación	La formación del personal en todos los niveles debe enfocarse en la sensibilización sobre las amenazas cibernéticas, el Reconocimiento de los ataques cibernéticos y la Gestión de la información digital, luego evaluar el efecto de la capacitación para asegurarse de que sea efectiva, la capacitación va desde los líderes hasta el personal técnico, la capacitación en ciberseguridad. Para asegurarse	Se pudo evidenciar que el Ejército no dicta cursos recurrentes en ciberseguridad de forma transversal a todo el personal Militar y Civil del Ejército, únicamente dicta cursos de capacitación a nivel especialización solo para Oficiales del arma de Comunicaciones.	“Se debe brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en materia de ciberseguridad dentro de la administración pública.” Es fundamental enfocarse en la educación digital, la cual abarca habilidades,

Sub-Categorías	Entrevistas	Observación	Análisis Documental
	de que la capacitación sea efectiva, s esencial evaluar el impacto de la capacitación en ciberseguridad desde los líderes hasta el personal técnico. Esta formación debe ser un esfuerzo integral que abarque todos los niveles de la institución.		conocimientos y actitudes necesarias para desarrollar eficazmente en el entorno digital.

Conclusión Parcial 2:

Es fundamental que la capacitación del personal en todos los niveles se oriente hacia la concienciación sobre las amenazas cibernéticas, la identificación de ataques y la gestión de la información digital. Además, es crucial evaluar la efectividad de esta formación para asegurar su adecuación. La instrucción debe incluir tanto a los altos cargos como al personal técnico, y ser completa en el ámbito de la ciberseguridad. Se ha notado que el Ejército no ofrece cursos regulares de ciberseguridad para todo su personal, limitándose a cursos especializados para Oficiales de Comunicaciones. Por lo tanto, es necesario proporcionar formación especializada en seguridad de la información y ampliar la investigación en ciberseguridad en el sector público. También es esencial enfocarse en la educación digital, que abarca las habilidades, conocimientos y actitudes necesarias para desenvolverse eficazmente en el entorno digital.

Sub-Categorías	Entrevistas	Observación	Análisis Documental
SC3: Recursos Humanos	Es fundamental contar con un manual de normas y conductas que todos los trabajadores de la compañía deben acatar. Asimismo, esta táctica involucra diversas formas de proceder, protocolos y técnicas para salvaguardar la información y operaciones de la organización. Se debe realizar un programa de capacitación en ciberseguridad como una parte importante del desarrollo profesional.	El personal Militar que labora en las dependencias del EP no se encuentra suficientemente preparado, porque únicamente se dicta cursos de capacitación a nivel básico en la Escuela De Comunicaciones y los pocos oficiales que llevan estos cursos son mal empleados en otras funciones que no son acordes con su especialización.	Tras revisar la información de la empresa y su desempeño en un entorno de alta rotación de personal, se busca analizar la considerable influencia que esto ejerce sobre la gestión de recursos humanos y el rendimiento general de la organización. Además, es importante tener en cuenta el elevado costo y el tiempo que implica el proceso de reclutamiento, selección, contratación y formación de nuevos empleados.

Sub-Categorías	Entrevistas	Observación	Análisis Documental
Conclusión Parcial 3: Es esencial establecer un conjunto de normas y prácticas que todos los empleados deben seguir en la institución para proteger los datos y las operaciones de la organización. Además, es importante implementar un programa de formación en ciberseguridad como parte del desarrollo profesional continuo. El personal en las dependencias del ejército no cuenta con la preparación adecuada, ya que solo recibe formación básica en la Escuela de Comunicaciones, y los pocos oficiales capacitados a menudo se asignan a tareas no relacionadas con su especialización. Tras analizar la información de la empresa y su rendimiento en un entorno de alta rotación de personal, es crucial evaluar el impacto de esto en la gestión de recursos humanos y en el desempeño general de la organización. También se debe considerar el alto costo y tiempo requerido para el reclutamiento, selección, contratación y formación de nuevos empleados.			
SC4: Recursos digitales	Para detectar actividades inusuales o amenazas potenciales se deben implementar sistemas de monitoreo continuo llevar a cabo auditorías de seguridad periódicas para evaluar la eficacia de las medidas de protección	Se evidencio que el Ejército no dispone de recursos digitales en suficiente cantidad y con tecnología actual y acorde para asegurar la ciberseguridad porque las tecnologías de ciberseguridad del Ejército Peruano no se encuentran orquestadas entre sí,	El incremento en el número de dispositivos y la expansión de la virtualización están generando nuevas oportunidades para amenazas, riesgos y ataques digitales. La

Sub-Categorías	Entrevistas	Observación	Análisis Documental
	implementadas y resolver posibles vulnerabilidades por ultimo Realizar auditorías de seguridad periódicas de seguridad cibernética.	cada una cumple una función individual y no se tiene claro que fase de un posible ciberataque.	actividad maliciosa está en aumento debido a las vulnerabilidades en aumento y a la facilidad de entrada en la industria del ransomware. -

Conclusión Parcial 4:

Para identificar actividades sospechosas o posibles amenazas, es fundamental implementar sistemas de monitoreo continuo y llevar a cabo auditorías de seguridad de forma regular para evaluar la eficacia de las medidas de seguridad aplicadas y abordar posibles puntos vulnerables. Asimismo, es imprescindible realizar auditorías periódicas de ciberseguridad para mantener la protección de la información. Se ha observado que el Ejército carece de recursos digitales suficientes y adecuados en términos de tecnología para garantizar la ciberseguridad. Las tecnologías de ciberseguridad utilizadas por el Ejército Peruano no están integradas entre sí, funcionan de manera individual y no se tiene claridad sobre en qué etapa de un posible ciberataque intervienen. El crecimiento en el número de dispositivos y el uso generalizado de la virtualización están generando nuevas oportunidades para amenazas, riesgos y ataques cibernéticos. La actividad maliciosa está en aumento debido a las vulnerabilidades crecientes y a la accesibilidad en la industria del ransomware.

Sub-Categorías	Entrevistas	Observación	Análisis Documental
SC5: Permanencia Oficiales	Es fundamental para la continuidad de los objetivos estratégicos del ejército la permanencia en el puesto de los oficiales especializados en la protección de la información digital Estos Oficiales tienen la formación y las habilidades necesarias para comprender y mitigar los riesgos de ciberseguridad. Se debe crear diplomados de formación obligatorio en ciberseguridad para todo el personal que trabajan con información digital. La durabilidad de la fuerza laboral de expertos en ciberseguridad en las unidades del Ejército es importante para la protección de	Se observó que el personal de oficiales especialista en ciberseguridad no permanece en el puesto el tiempo suficiente puesto que el principal objetivo del oficial es alcanzar el grado inmediato superior a través de un ascenso y esto se logra gracias a las calificaciones anuales ya que esto varía de acuerdo a la unidad donde presta servicio el oficial (unidades con mayor coeficiente de calificación).	El peor problema surgido de este cambio tecnológico traumático fue La falta de una formación adecuada de los líderes militares para planificar operaciones en línea, intentando compensar esta deficiencia con personal versado en ciberseguridad en el ámbito empresarial. Mientras que en el ámbito civil la seguridad se centra en proteger la información dentro de la empresa, en el ámbito militar se planifican operaciones estratégicas

Sub-Categorías	Entrevistas	Observación	Análisis Documental
	la información alojada digitalmente .		de recopilación de información, defensa y ataques cibernéticos.

Conclusión Parcial 5:

Es fundamental para la continuidad de los objetivos estratégicos del ejército la permanencia en el puesto de los oficiales especializados en la protección de la información digital Estos Oficiales tienen la formación y las habilidades necesarias para comprender y mitigar los riesgos de ciberseguridad. La durabilidad de la fuerza laboral de expertos en ciberseguridad en las unidades del Ejército es fundamental para la protección de la información digital. Se observó que el personal de oficiales especialista en ciberseguridad no permanece en el puesto el tiempo suficiente puesto que el principal objetivo del oficial es alcanzar el grado inmediato superior a través de un ascenso y esto se logra gracias a las calificaciones anuales ya que esto varía de acuerdo a la unidad donde presta servicio el oficial (unidades con mayor coeficiente de calificación).El peor problema surgido el cambio tecnológico traumático fue La falta de una formación adecuada de los mandos militares para planificar operaciones en línea, intentando compensar esta deficiencia con personal versado en ciberseguridad en el ámbito empresarial. Mientras que en el ámbito empresarial la seguridad se centra en proteger la información dentro de la empresa, en la parte castrense se planifican operaciones estratégicas de recopilación de información, defensa y ataques cibernéticos. Se debe Implementar programas de incentivos, Es fundamental para la continuidad de los objetivos estratégicos del ejército la permanencia en el puesto de los oficiales especializados en la protección de la información digital Estos Oficiales tienen la formación y las habilidades necesarias para comprender y mitigar los riesgos de ciberseguridad.

Sub-Categorías	Entrevistas	Observación	Análisis Documental
Se debe crear un diplomado de formación obligatorio en ciberseguridad para todo el personal que trabajan con información digital. La durabilidad de la fuerza laboral de expertos en ciberseguridad en las unidades del Ejército es importante para la confiabilidad, disponibilidad e integridad de la información digital. Se observó que el personal de oficiales especialista en ciberseguridad no permanece en el puesto el tiempo suficiente puesto que el principal objetivo del oficial es alcanzar el grado inmediato superior a través de un ascenso y esto se logra gracias a las calificaciones anuales ya que esto varía de acuerdo a la unidad donde presta servicio el oficial (unidades con mayor coeficiente de calificación). El peor problema surgido de este cambio tecnológico traumático fue La falta de una formación adecuada de los líderes militares para planificar operaciones en línea, intentando compensar esta deficiencia con personal versado en ciberseguridad en el ámbito civil o empresarial. Mientras que en el ámbito civil la seguridad se centra en proteger la información dentro de la empresa, en el ámbito militar se planifican operaciones estratégicas de recopilación de información, defensa y ataques cibernéticos. resulta destacable también la entrega de incentivos como bonificaciones, reconocimientos y oportunidades de ascenso, para retener a profesionales altamente calificados en ciberseguridad. Fomentar una cultura de aprendizaje continuo, donde el personal esté motivado para mantenerse actualizado sobre las últimas amenazas y tecnologías en ciberseguridad.			

Sub-Categorías	Entrevistas	Observación	Análisis Documental
SC6: Permanencia Personal TCOS Y SSOO	Estos especialistas están capacitados para comprender y reducir los peligros de ciberseguridad. Los puestos en el Ejército son bastante rotativos, muchas veces se capacita al personal y cuando ya manejan una solución, son cambiados a otro puesto de trabajo Es muy importante contar con técnicos y suboficiales expertos en ciberseguridad en las unidades del Ejército del Perú, porque pueden ayudar a mantener la información y los sistemas digitales a salvo de ciberataques, ya que tienen las habilidades y las herramientas para hacerlo.	En la Observación realizada se evidenció que el personal de TÉCNICOS y SUBOFICIALES especialistas en seguridad Informática al igual que los oficiales no permanece en el puesto el tiempo suficiente puesto que el principal objetivo de los TCOS y SSOO es alcanzar el grado inmediato superior a través de un ascenso y esto se logra gracias a las calificaciones anuales ya que esto varía de acuerdo a la unidad donde presta servicio en unidades con mayor coeficiente de calificación.	La ONU expresa que es necesario establecer un programa integral de formación y concienciación, adaptado a los riesgos específicos de cada categoría de empleados, en lugar de ofrecer módulos genéricos sin una visión estratégica. Es esencial también prestar atención a los usuarios ocasionales de los sistemas corporativos de TI, quienes pueden no estar familiarizados con las normas y prácticas de ciberseguridad de la organización.

Sub-Categorías	Entrevistas	Observación	Análisis Documental
Conclusión Parcial 6: Es fundamental contar con personal especializado en ciberseguridad en el EP, ya que tienen la capacidad de proteger la información y los sistemas digitales de posibles ciberataques. Sin embargo, se observó que tanto los técnicos como los suboficiales expertos en este tema, al igual que los oficiales, suelen ser rotados con frecuencia en los puestos de trabajo debido a su aspiración de ascender de grado. Además, la ONU recomienda establecer un programa de concienciación y formación adaptado a los diversos niveles de empleados, prestando especial atención a aquellos usuarios que no conocen las políticas de seguridad de la organización.			
SC7: Personal Civil especialista	La retención de personal civil en el Ejército especializado en seguridad cibernética será una estrategia adicional importante para fortalecer la base de seguridad digital, estos profesionales tienen la formación y destrezas para reconocer y mitigar los riesgos de ciberseguridad. Tener expertos civiles en ciberseguridad en las unidades	Se evidencio que no se cuenta con personal civil especialista en ciberseguridad y además no se otorga cursos de especialidad, pero si se tiene oficiales del servicio de ciencia y tecnología de procedencia Universitaria Ingenieros de sistemas que aportan significativamente a la ciberseguridad sin embargo dado que el rango otorgado por la institución es Oficial en ciencia y	A pesar de los intentos por reubicar y capacitar al personal interno de otras áreas en estos puestos, no existen procesos formales para reclutar personal civil que pueda cubrir las necesidades de estos organismos públicos. Los procedimientos actuales de reclutamiento no

Sub-Categorías	Entrevistas	Observación	Análisis Documental
	del Ejército puede ser un enfoque beneficioso y adicional para mejorar la seguridad digital del Ejército, Los expertos poseen las habilidades y el conocimiento necesario para entender y enfrentar las amenazas a la ciberseguridad.	tecnología al igual que los oficiales de carrera tienen aspiraciones de ascenso a los grados superiores .	parecen ser atractivos para estos perfiles especializados. Además, los controles de seguridad exigidos podrían dificultar la selección de candidatos altamente especializados.

Conclusión Parcial 7:

La incorporación de personal civil especializado en ciberseguridad en el Ejército es esencial para reforzar la seguridad digital. Estos expertos poseen la formación y las habilidades necesarias para identificar y reducir los riesgos cibernéticos. Integrar profesionales civiles en ciberseguridad dentro de las unidades del Ejército puede ser una estrategia eficaz para mejorar la protección digital. A pesar de las limitaciones actuales, se valora la contribución de los oficiales de ciencia y tecnología en este ámbito. Sin embargo, la carencia de personal especializado y de procesos de reclutamiento adecuados dificulta la satisfacción de las necesidades de ciberseguridad en estos organismos públicos, y los controles de seguridad necesarios también representan un reto para la selección de candidatos altamente cualificados

Capítulo V: Discusión de resultados y Conclusiones

A lo largo de la investigación, se realizaron lecturas y fichas bibliográficas para reunir fragmentos de textos teóricos relevantes, además del trabajo de campo. En esta etapa, se dispone de una estructura empírica de los hallazgos, organizados en categorías lógicas, características, nodos y relaciones, junto con numerosas fichas con fragmentos de texto teórico relacionados con la información obtenida. Ahora es el momento de conectar la teoría con la evidencia empírica, estableciendo vínculos entre los hallazgos empíricos y la literatura teórica revisada. En este sentido, se procedió a verificar la teoría de las Políticas integrales de ciberseguridad en la protección de la información digital en el Ejército del Perú, con los hallazgos empíricos obtenidos a través de la observación y las entrevistas, encontrando tanto conformidades como discrepancias., por lo siguiente:

En la primera categoría C1: Concienciación y formación del personal, enfocándose en la concienciación.

Respecto a la concienciación del personal militar, Zambrano *(2019)* señala que los ciberataques suelen ocurrir con mayor frecuencia debido a la falta de conciencia de las personas, lo cual los delincuentes aprovechan para obtener información financiera y privada, así como para extorsionar a sus víctimas. Sin embargo, se evidencio que el personal del ejército no toma conciencia en la seguridad cibernética, porque a nivel ejército no existe una cultura adecuada de ciberseguridad ya que no son conscientes de la realidad del peligro cibernético que existe en la actualidad.

El investigador concuerda plenamente con la teoría de Zambrano en que la toma de conciencia es fundamental para prevenir, detectar y anular algún ataque cibernético, pero nos tocamos con que en el ejército no existe una toma de conciencia lo que deviene en que en la institución se ignora el peligro cibernético es decir no existe una cultura de seguridad ciberseguridad.

Respecto a la capacitación Pérez, Christian y Salazar, Melissa (2023); afirma que, es importante tener en cuenta el alto costo y el tiempo que implica el proceso de contratación, reclutamiento, selección y capacitación de nuevos empleados. Sin embargo, el Ejército no dicta cursos recurrentes en ciberseguridad de forma transversal a todo el

personal militar y civil, únicamente dicta cursos de capacitación a nivel especialización solo para Oficiales del arma de Comunicaciones.

Esta situación conlleva a afirmar que la capacitación es esencial para que el personal de todos los niveles conozca los riesgos que se presentan en la ciberseguridad, por lo que el Ejército no puede seguir ignorando esta teoría, debiendo más bien Aumentar la concienciación y la formación del personal, algo que actualmente no se está llevando a cabo.

En relación a la segunda categoría C2: Recursos de ciberseguridad

Pérez, C. y Salazar, M. (2023) destacan que en una industria de ciberseguridad, donde el talento es escaso y las habilidades técnicas son cruciales, la rotación de empleados puede afectar significativamente la continuidad y calidad de los servicios. Además, el proceso de reclutamiento, selección, contratación y formación de nuevos trabajadores implica un alto costo y tiempo. Sin embargo, el personal del ejército no está suficientemente preparado, ya que solo se imparten cursos básicos en la Escuela de Comunicaciones, y los pocos oficiales que los toman son asignados a funciones que no corresponden a su especialización.

El investigador opina que el recurso humano es el elemento más crucial en la cadena de la ciberseguridad. Para ello, es fundamental iniciar con la selección y formación del personal de manera sistemática, a pesar de que el costo de la capacitación sea significativo. Esta inversión es necesaria para desarrollar, con el tiempo, una auténtica conciencia de seguridad cibernética, la cual solo se consigue a través de la capacitación continua.

En los recursos digitales la UNAM (2022) México reconoce que el incremento en la cantidad de dispositivos y el uso extendido de la virtualización están creando nuevas oportunidades para amenazas, riesgos y ataques digitales. La actividad maliciosa está en aumento debido a las crecientes vulnerabilidades y la facilidad de acceso a la industria del ransomware, así como a la baja probabilidad de extradición, enjuiciamiento o sanción. La tendencia del “ransomware como servicio” permite que incluso personas sin conocimientos

técnicos realicen ataques, una tendencia que podría intensificarse con la llegada del malware impulsado por inteligencia artificial (AI, por sus siglas en inglés) (Foro Económico Mundial, 2022). Sin embargo, el ejército no cuenta con suficientes recursos digitales ni con tecnología actualizada para garantizar la ciberseguridad, ya que las tecnologías de ciberseguridad en la institución no están coordinadas entre sí, cada una cumple una función individual y no se tiene claridad sobre las fases de un posible ciberataque.

Al respecto el investigador considera que se debería actualizar los recursos digitales adquiriendo nuevos equipos que sean capaces de neutralizar cualquier intento de atentar contra nuestra información, que desde todo punto de vista es reservada y en mayor medida de clasificación secreta

En relación a la tercera categoría C3: La permanencia del personal de oficiales considerado como técnico especialista.

La permanencia de los oficiales especializados en la ciberseguridad, mencionando a Mato, R (2016) quien sostiene en que la falta de planificación ha llevado a una transición abrupta de la seguridad informática a operaciones cibernéticas sin una preparación adecuada, lo que ha generado la mayoría de los problemas actuales. Aunque se utilice la ciberdefensa como tema político, no se abordan las lagunas existentes, es probable que se piense que el empleo del ciberespacio para fines militares es más propio de la ficción, mientras que en el ámbito civil la seguridad se enfoca en salvaguardar la información interna de las empresas, en el ámbito militar se planifican operaciones estratégicas de recopilación de información, defensa y ataques cibernéticos. Sin embargo, el personal de oficiales especialista en ciberseguridad no permanece en el puesto el tiempo suficiente puesto que el principal objetivo del oficial es alcanzar el grado inmediato superior a través de un ascenso y esto se logra gracias a las calificaciones anuales ya que esto varía de acuerdo a la unidad donde presta servicio el oficial (unidades con mayor coeficiente de calificación.

Esta es otra de las falencias en el manejo de la ciberseguridad en el ejército por lo que el investigador advierte a fin de que se establezca un plan de carrera para el personal

de oficiales, que a fin de cuentas es el encargado de realizar el planeamiento y control de todas las medidas en la ciberseguridad

La permanencia de los Tcos y SSOO especializados en la ciberseguridad, es otro asunto en el campo de personal que no ha sido tratado, al respecto la ONU (2017) expresa que es necesario establecer un programa integral de formación y concienciación, adaptado a los riesgos específicos de cada categoría de empleados, en lugar de ofrecer módulos genéricos sin una visión estratégica. También es crucial considerar a los usuarios ocasionales de los sistemas corporativos de TI, quienes podrían no estar familiarizados con las normas y procedimientos de seguridad de la organización. Sin embargo, tanto los TÉCNICOS y SUBOFICIALES especializados en ciberseguridad como los OFICIALES no permanecen en sus puestos el tiempo necesario, ya que su principal objetivo es ascender al grado inmediato superior. Este ascenso depende de las calificaciones anuales, las cuales varían según la unidad en la que presten servicio, siendo más altas en aquellas con un mayor coeficiente de calificación.

Al respecto el investigador hace notar esta otra parte que afecta en manejo de la ciberseguridad en el ejército por lo que el investigador advierte al igual que los Oficiales a fin de que se establezca un plan de carrera para el personal de Tcos y SSOO ,por otro lado destacar también que dicho personal se ha especializado en forma autodidacta

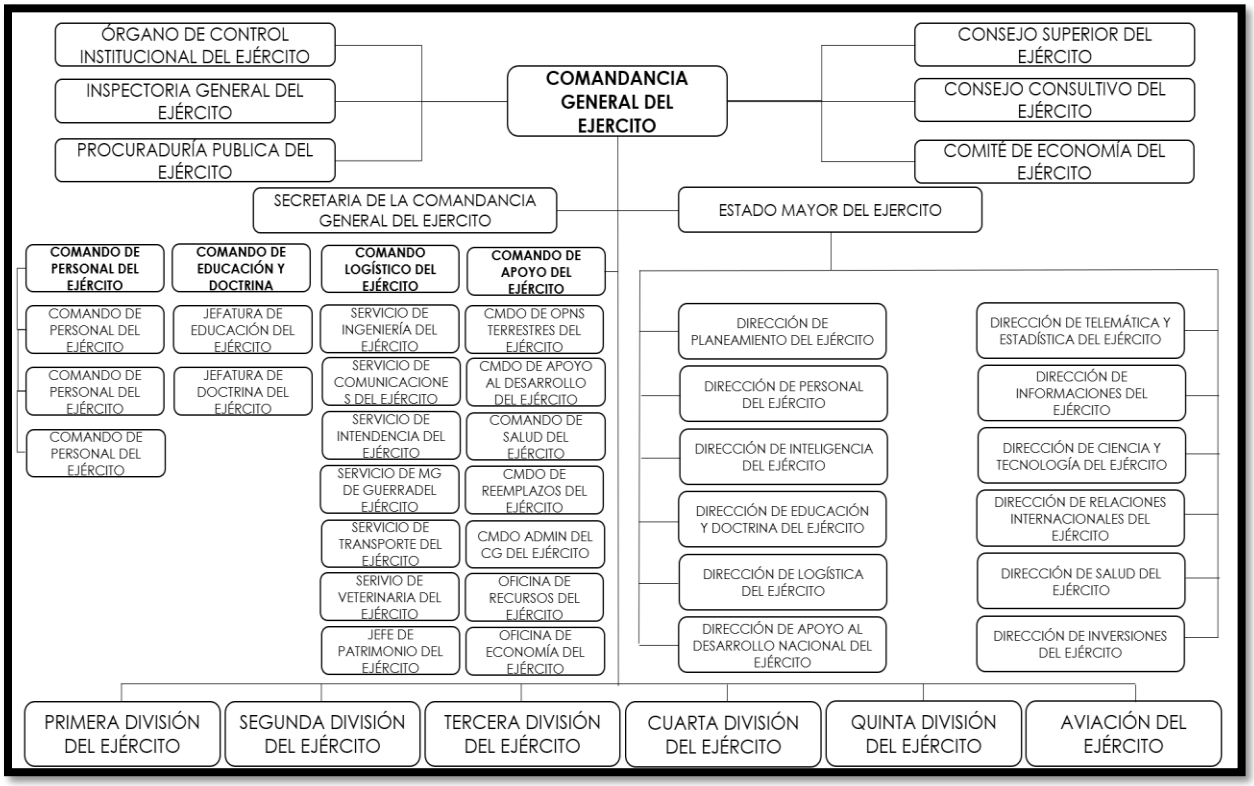
Respecto al personal civil tenemos que el ejército de los Estados Unidos tiene una posición interesante revela que, a pesar de los intentos por reubicar y capacitar al personal interno de otras áreas en estos puestos, no existen procesos formales para reclutar personal civil que pueda cubrir las necesidades, Los procedimientos actuales de reclutamiento no parecen ser atractivos para estos perfiles especializados. Además, los controles de seguridad exigidos podrían dificultar la selección de candidatos altamente especializados. El EP, en ese contexto, no cuenta con personal civil especializado en ciberseguridad y tampoco ofrece cursos de especialización en el área. No obstante, dispone de oficiales con formación universitaria en ingeniería de sistemas, quienes pertenecen a la especialidad de ciencia y tecnología y contribuyen significativamente a la ciberseguridad. Sin embargo, dado que estos oficiales son designados como Oficiales

en Ciencia y Tecnología, al igual que los oficiales de carrera, también aspiran a ascender a rangos superiores.

Al respecto el investigador considera que se debe tomar en cuenta esta situación, ya que la presencia de personal civil altamente calificado, sería de gran ayuda para la Institución en mejorar y mantener en grado óptimo la ciberseguridad anteriormente señalada.

Figura 7

Organización del Ejército Peruano.



Nota: Se observa la estructura organizativa *del Ejército Peruano según su creación.*

5.1 Conclusiones y Recomendaciones

La investigación realizada ha seguido un rigor metodológico científico que ha permitido responder cada una de las preguntas formuladas en este estudio, llegando a las siguientes conclusiones

En relación con el objetivo N° 1, que busca explicar cómo la concienciación y la capacitación en ciberseguridad proporcionan protección frente a los desafíos específicos de la información digital en el Ejército del Perú en 2023, se concluyó que no existe una cultura de ciberseguridad adecuada en la institución, ya que no son conscientes de la realidad del peligro cibernético que existe actualmente, esto se debe a que la institución no adopto implementar un marco de trabajo – FRAMEWORK (modelo de madurez de ciberseguridad de la Universidad de Oxford-CMM, NIST-EEUU, etc.) en ciberseguridad para el diagnóstico y para luego formular lineamientos de seguridad cibernética que deban cumplir los diferentes niveles jerárquicos de la institución. Por otro lado, el Ejército no dicta cursos recurrentes en ciberseguridad de forma transversal a todo el personal militar y civil, únicamente dicta cursos de capacitación a nivel especialización solo para oficiales del arma de comunicaciones, las diferentes capacitaciones son por gestiones propias del personal y en condiciones autodidactas.

Respecto al objetivo N° 2 de explicar cómo los recursos de ciberseguridad brindan protección ante los desafíos específicos de los datos electrónicos de las FFFAA del Perú, 2023. se concluyó en lo que respecta a personal, al personal no se le capacita adecuadamente tal es así que solo se dicta en forma informativa cursos de capacitación a nivel básico en la Escuela De Comunicaciones y los pocos oficiales que llevan estos cursos son mal empleados en otras funciones que no son acordes con su especialización; aún nos falta preparación, entrenamiento y concientización de los peligros que involucra el ciberespacio. La situación se agrava porque las tecnologías de ciberseguridad del Ejército Peruano no se encuentran orquestadas entre sí, cada una cumple una función individual y no se tiene claro que fase de un posible ciberataque se mitiga y cuáles son las fases que no se están mitigando. En la actualidad se tienen el Filtro Web, el Antispam, la VPN, el Antivirus y el Firewall externo que son de tecnologías

de tipo pasivo, pero no se cuenta con tecnologías de detección, por lo cual posiblemente no son capaces de bloquear amenazas emergentes (ZERO DAY). Es preciso indicar que los Tcos y SSOO especialistas en ciberseguridad se formaron de manera autodidacta, en vista que en las escuelas no brindan este tipo de capacitaciones.

Asimismo, el Ejército no cuenta con una arquitectura sólida para la elección e integración de tecnologías de ciberseguridad, puesto que es de vital importancia para el Ejército que todas las plataformas que se adquieran e implementen no se hagan de manera aislada, sino que formen parte de un roadmap (Una guía que actúa como plan estratégico para desarrollar un proyecto) y estrategia alienada a una arquitectura definida. En la industria existen diferentes marcos de referencia para definir una arquitectura de ciberseguridad, tales como: NIST-CSF y Zero Trust.

Respecto al objetivo N° 3 de, explicar cómo la permanencia del personal técnico especializado en ciberseguridad ofrece protección frente a los desafíos específicos de la protección de la información digital de las FFAA del Perú en 2023. En este contexto, se concluye que los oficiales especializados en ciberseguridad no permanecen en sus puestos el tiempo necesario, ya que el principal objetivo del oficial es alcanzar el grado inmediato superior a través de un ascenso y esto se logra gracias a las calificaciones anuales ya que esto varía de acuerdo a la unidad donde presta servicio el oficial (unidades con mayor coeficiente de calificación), es así, como la dependencia encargada de la ciberseguridad no brinda ningún incremento de puntaje el personal busca no quedarse mucho tiempo o simplemente no venir. Con respecto a los Tcos y SSOO sucede parecido a los Oficiales al tener justificadamente como principal alcanzar el grado inmediato superior a través de un ascenso y esto se logra gracias a las calificaciones anuales ya que esto varía de acuerdo a la unidad donde presta servicio el oficial (unidades con mayor coeficiente de calificación). Por ultimo No se cuenta con personal civil especialista en ciberseguridad y además pero no se otorga cursos de especialidad.

En conclusión, la investigación revela que en el Ejército la cultura de ciberseguridad no está lo suficientemente desarrollada, principalmente por la falta de conciencia sobre los riesgos cibernéticos actuales. Esto se debe a la ausencia de un marco de trabajo en ciberseguridad que permita diagnosticar y establecer directrices de

seguridad para los diferentes niveles de la institución. No se ofrecen cursos recurrentes de ciberseguridad para todo el personal, solo para oficiales de comunicaciones, lo que limita la preparación y concienciación de los peligros en el ciberespacio. Además, las tecnologías de ciberseguridad no están integradas y no se cuenta con tecnologías de detección para bloquear amenazas emergentes. El personal especializado se forma de manera autodidacta, ya que no se brindan capacitaciones en las escuelas militares. Los oficiales y los Tcos y SSOO por línea de carrera buscan puestos y lugares que les otorgue puntaje para lograr su ascenso a grados superiores ascensos en lugar de centrarse en la especialidad, lo que afecta la permanencia en el puesto. En general, no se tiene personal civil especializado y no se ofrecen cursos de especialidad en ciberseguridad.

5.2 Recomendaciones

Conforme a las conclusiones pronunciadas párrafo anterior se recomienda lo siguiente:

Que el COEDE debe establecer que las escuelas de armas y servicios ofrezcan cursos de capacitación y especialización en ciberseguridad para Oficiales, Técnicos y Suboficiales, adaptando y reformulando sus planes de estudio.

Que el COLOGE debe llevar a cabo un estudio de necesidades y gestionar la adquisición de equipos actualizados que ofrezcan protección en ciberseguridad para el Ejército.

Que la DIPLANE en coordinación con el COPERE, debe reestructurar el plan de carrera de OFICIALES, TÉCNICOS y SUBOFICIALES para asegurar que permanezcan el tiempo necesario en puestos que garanticen la seguridad cibernética. Además, se debe llevar a cabo la convocatoria correspondiente para contar con personal civil especializado.

Referencias

Aguilar, J. (2020). *La brecha de ciberseguridad en América Latina Frente al Contexto Global de Ciberamenazas*. *Revista de Estudios en Seguridad Internaciónal, 6(2*), 19-30. Apreciación de la Situación. (2019). Centro de Ciberdefensa-Ceciber.

Arias, N y Celis, J. (2015). *Modelo experimental de ciberseguridad y ciberdefensa para Colombia.* Tesis para optar el grado de ingeniero en sistemas. Universidad Libre. Bogotá, Colombia.

Cano, J. (2015*). Arquitecturas Distribuidas de Gobierno Electrónico con Ciberseguridad Critica,*[Tesis de Doctorado, Escuela técnica Superior de Ingenieros Industriales] UNED.https://creativecommons.org/licenses/by-nc-nd/4.0/

Castillo, F. (2021). Operaciones de Ciberdefensa [Conferencia]. *Unidad de Aprendizaje N°1.Generalidades, Lima*, Perú.

Ejército del Perú. (2019). MD 3-0 *Concepción de las Operaciones*.

Ejército del Perú. (2019). *MF 3-1*. *Operaciones y Acciones Terrestres Unificadas*

(OTU). Ejército del Perú. (2020). *TOF Ciberdefensa*.

Ejército del Perú. (2021). *Proyecto de Manual de Operaciones Cibernéticas*

Gómez Bule, J. (2014). Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario. Edición Libro-e. Madrid, España. Editorial Secretaria General Técnica del Ministerio de Defensa de España-Catalogo general de publicaciones oficiales

Hernández, R., Mendoza, Ch. (2018). *Metodología de la Investigación, Las Rutas Cualitativas, Cuantitativas y Mixtas*. Mc Graw Hill. http://renati.sunedu.gob.pe/handle/sunedu/1336266

Junta Interamericana de Defensa (2020). *Guía de Ciberdefensa*. Orientación para el Diseño, Planeamiento, Implementación y Desarrollo de una Ciberdefensa Militar.

Ley de Creación del Ejército. (2012). *Decreto Legislativo N° 1137*. Diario Oficial el Peruano. Leyes N° Reglamentadas. (2005). *La Importancia de las Leyes No Reglamentadas*.

Ministerio del Interior y Seguridad Pública. (2021). *Detalla del Ransoware Conti que afectó al Sistema de Salud en Irlanda*.

Ormachea, F. (2019). *La brecha de ciberseguridad en América Latina Frente al Contexto Global Estrategias de ciberseguridad para el fortalecimiento de la seguridad nacional,* [Tesis de Doctorado, Centro de Altos Estudios Nacionales] Renati.

Pons, V. (2018). *Ciberterrorismo: Amenaza a la seguridad. Respuesta operativa y legislativa, nacional e internacional*.

Real Academia Española. (2020). *Diccionario*.

Resolución Ministerial. (2017). *Resolución N°927*. Aprobación de la Directiva General N° 05- 017-MINDEF-SG-VPD/DIGEPE/DIPPED.

Rubio, J. (2016*). U*n *Marco para el Análisis de Riesgos en Ciberseguridad,* [Tesis de Doctorado, Universidad Rey Juan Carlos] Fundación Dialnet. https://documat.unirioja.es/servlet/tesis?codigo=112490&orden=0&info=link

Sánchez, J. (2017*). Adopción de Estrategias de Ciberseguridad en la Protección de Información en la Oficina Económica del Ejército,* [Tesis de Magister, Instituto Científico y Tecnológico del Ejército] Renati.

Sánchez, Y. (2013, mayo 7). *El Pentágono Acusa a las Fuerzas Armadas Chinas de Ciberespionaje. El País.*

Taipe, D. (2020*). Auditoria de Seguridad Informática y su Relación en la Ciberseguridad en el Sector Publico Año 2018,* [Tesis de Magister, Universidad Nacional de Piura] Renati. http://repositorio.unp.edu.pe/handle/20.500.12676/2361

Trujillo, C., Naranjo, M., Lomas, K., Merlo, M. (2019). *Investigación Cualitativa*. UTN. Vargas, X. (2011). *¿Cómo Hacer Una Investigación Cualitativa?* ETXETA, SC.

Villalba, A., Corchado, J. (2017). Análisis de las Ciberdefensas. *Couter Terrorism Centre (ECTC),1(*3), 99-136.

Wernerfelt, B. (1984). A resource-based view of the firm. *Strategic management journal*, *5*(2171-180)

ANEXO 1

MATRIZ DE CONSISTENCIA

MATRIZ DE CONSISTENCIA

Título: Políticas integrales de ciberseguridad en la protección de la información digital en el Ejército del Perú, 2023

Preguntas	Objetivos	Teorías	Categorías	Sub categorías	Metodología	Análisis de datos
Pe1. ¿Cómo la toma de conciencia y capacitación en ciberseguridad brindan protección ante los desafíos específicos de la información digital en el Ejército del Perú ,2023? **Pe2**. ¿Cómo los recursos de ciberseguridad brindan protección ante los desafíos específicos de la información digital de las Fuerzas Armadas del Perú,2023? **Pe3**. ¿Cómo la permanencia del personal técnico especialista de ciberseguridad brinda protección ante los desafíos específicos de la información digital de las Fuerzas Armadas del Perú,2023	**Oe1**. Explicar cómo la toma de conciencia y capacitación en ciberseguridad brindan protección ante los desafíos específicos de la información digital en el Ejército del Perú ,2023. **Oe2.** Explicar cómo los recursos de ciberseguridad brindan protección ante los desafíos específicos de la información digital de las Fuerzas Armadas del Perú,2023. **Oe3.** Explicar cómo la permanencia del personal técnico especialista en ciberseguridad brinda protección ante los desafíos específicos de la información digital de las Fuerzas Armadas del Perú,2023.	Teoría la modernización Ley Marco para el Desarrollo e Integración Fronteriza Decreto Supremo que establece las acciones de desarrollo sostenible e integración para la atención prioritaria de las áreas críticas de frontera.	C1: Toma de conciencia y capacitación C2: Recursos de ciberseguridad C3: Permanencia del personal técnico especialista	SC1: Toma de conciencia SC2: Capacitación SC1: Recursos Humanos SC2: Recursos digitales SC3: Oficiales especialistas SC2: Personal Auxiliar especialista SC3: Personal Civil especialista	**Paradigma**: Hermenéutico Interpretativo **Enfoque**: Cualitativo **Tipo**: Teórico – empírico **Método**: Hermenéutico Fenomenológico **Muestra**: 04 expertos, ingenieros de sistema	**Técnicas:** - Observación - Entrevista - Análisis documental **Instrumentos:** - Guía de observación - Guía de entrevista - Ficha de registro documental **Técnica de análisis de datos:** - Empírica /artesanal

ANEXO 2

INSTRUMENTOS DE RECOLECCIÓN DE DATOS

GUÍA DE ENTREVISTA (SEMIESTRUCTURADA)

Sr. ……. buenos días, se esta desarrollando un trabajo de investigación de tesis para obtener el grado académico de Maestro en Ciencias Militares con mención en Planeamiento Estratégico y Toma de Decisiones en la Escuela Superior de Guerra del Ejército-Escuela de Postgrado, habiendo elegido el tema las Políticas integrales de ciberseguridad en la protección de la información digital en el Ejército del Perú, 2023**,**expresamos de antemano nuestroa agradecimiento por el tiempo y la atención prestada para poder realizar esta entrevista, cuya información y comentarios proporcionados serán muy valiosos para profundizar la presente investigación.

Entrevistado	
Grado Académico	
DNI	
Lugar – fecha	
Experiencia alcanzada:	

Título de la investigación:
"Políticas integrales de ciberseguridad en la protección de la información digital en el Ejército del Perú, 2023",

GUÍA DE ENTREVISTA

- Para el Objetivo 1 :Toma de conciencia y capacitación

P1.¿Que politicas sobre ciberseguridad cree Ud. que se deba adoptar para el personal que maneja la informacion digital *tome conciencia* en la protección de la información digital del Ejercito del Perú?	
Rpta	
P2. ¿En qué aspectos sobre la ciberseguridad de la información digital considera Ud. que se deba *capacitar* al personal que maneja la informacion digital en las dependencias del Ejercito del Perú?	
Rpta	
P3. ¿Qué aspectos de mejora considera Ud. que se deba implementar para la toma de conciencia y capacitación sobre la Ciberseguridad en *todo el personal* del Ejercito del Perú?	
Rpta	

- Para el objetivo 02: Recursos de ciberseguridad

P4. ¿Qué estrategias en los recursos humanos sobre ciberseguridad deben aplicare en las dependencias del Ejercito?	
Rpta	
P5. ¿ Qué estrategias en los recursos digitales sobre ciberseguridad deben aplicare en las dependencias del Ejercito?	
Rpta	

P6. Qué aspectos de *mejora* considera Ud. que se deba implementar en recursos humanos y recursos digitales para la Ciberseguridad en las dependencias del Ejercito del Perú?	
Rpta	
• Para el objetivo 03 :Permanencia del personal especialista	
P7. ¿Qué opinión le merece sobre la permanencia del personal de Oficiales especialistas en ciberseguridad en las dependencias del Ejercito?	
Rpta	
P8. ¿Qué opinión le merece sobre la permanencia del personal de tecnicos y Suboficiales especialistas en ciberseguridad en las dependencias del Ejercito?	
Rpta	
P9. ¿Qué opinión le merece sobre la permanencia del personal civil especialista en ciberseguridad en las dependencias del Ejercito?	
Rpta P.10	¿Qué estrategia vinculada a la ciberseguridad considera Ud que se debe aplicar respecto a la permanencia del personal especialista ?

_____

Firma del entrevistado

FICHA DE ANÁLISIS 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**:**

Documento	País	Referencia	Temas
Tesis	Argentina	Albarracín, A. (2019). Inteligencia Nacional y estrategia de ciberseguridad nacional (Tesis de Maestría). Universidad Nacional de la Plata,	Formación sobre ciberseguridad Competencias de ciberseguridad y ciberdefensa
ArtÍculo	Perú	Álvarez, A. (2018). Ciberseguridad y ciberdefensa, ¿Estamos preparados?. Revista	Adiestramiento Formación sobre ciberseguridad Aplicación de
Tesis	Argentina	Baretto, J. (2017). La Defensa Nacional y la estrategia militar de seguridad cibernética (Tesis de Maestría). Escuela Superior de Guerra Conjunta, La	Formación sobre ciberseguridad Competencias de ciberseguridad y
ArtÍculo	España	Del Río, J. (2011). La ciberseguridad en el ámbito militar. En Ministerio de la Defensa (2011). Ciberseguridad, Retos y Amenazas a la seguridad nacional en el ciberespacio,	Adiestramiento Formación sobre ciberseguridad Aplicación de ciberseguridad Competencias de
ArtÍculo	Venezuela	Revilla, N., Acosta, I. y Marval, E. (2009). Necesidades de entrenamiento del personal basado en el enfoque de competencias: Estudio de un caso.	Formación sobre ciberseguridad Aplicación de ciberseguridad Competencias de ciberseguridad y ciberdefensa

		Revista Venezolana de Gerencia, 14(46), 195-214.	
Tesis	Perú	Vilcarromero, L. y Vilchez, E. (2018). Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones de seguridad (SOC) de una empresa de telecomunicaciones (Tesis de Maestría).	Adiestramiento Formación sobre ciberseguridad Aplicación de ciberseguridad Competencias de ciberseguridad y ciberdefensa

GUÍA DE OBSERVACIÓN

ASPECTOS POR EVALUAR		SÍNTESIS
• Para el Objetivo 01		
01	Observar la capacitación sobre ciberseguridad ante los desafíos específicos de la información digital del personal que maneja la información digital en el CITELE .	
• Para el Objetivo 02		
02	Indagar sobre los recursos humanos y los recursos digitales en el CITELE.	
• Para el Objetivo 03		
03	Verificar el estado y permanencia del personal especialista en ciberseguridad en el CITELE.	

ANEXO 3

VALIDACIÓN DE INSTRUMENTOS

HOJA DE VALIDACIÓN DE INSTRUMENTO 1

TÍTULO DE LA INVESTIGACIÓN: "Políticas integrales de ciberseguridad en la protección de la información digital en el Ejército del Perú, 2023"

I. DATOS DEL EXPERTO:

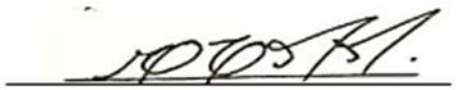
a. Apellidos y nombres : Dr. Talavera Prado Gamaliel
b. Grado académico-profesión : Doctor en Educación– Tte. Crl EP (R)
c. D.N.I. : 09771027
d. N° de teléfono : 996132050
e. Lugar y fecha : 24 Setiembre 2023

II. **DATOS DEL INSTRUMENTO DE EVALUACIÓN**

a. Autor del instrumento :
b. Método de investigación : cualitativo
c. Tipo de entrevista : Semiestructurada

III. ASPECTOS DE EVALUACIÓN

N°	Criterios	Indicadores	Si	No	Observaciones
1	CONSISTENCIA	Las preguntas de la entrevista son congruentes a los objetivos de la investigación	**X**		Si tienen congruencia con los objetivos
2	CLARIDAD	Está formulada con una sintaxis y semántica que permita la comprensión adecuada	**X**		Son comprensibles y de buena sintaxis
3	ORGANIZACION	Existe una organización lógica en el instrumento	**X**		Su construcción es lógica y está organizada
4	SUFICIENCIA	Contiene preguntas necesarias para recabar información suficiente	**X**		Con las preguntas realizadas son suficientes al logro de sus objetivos
5	RELEVANCIA	Las preguntas se orientan a la obtención de información trascendente y substancial.	**X**		Si están orientadas para obtener una validación coherente y substancial
Sugerencias y/o Recomendaciones		**Instrumento aplicable** La evaluación del instrumento en forma virtual impide una comunicación fluida con el tesista			



Dr. GAMALIEL TALAVERA PRADO
Docente Asesor de tesis
CO: 0000-0002-5167-1897

HOJA DE VALIDACIÓN DE INSTRUMENTO 2

TÍTULO DE LA INVESTIGACIÓN: "Políticas integrales de ciberseguridad en la protección de la información digital en el Ejército del Perú, 2023"

IV. DATOS DEL EXPERTO:

f. Apellidos y nombres : CHUQUIVILCA ECHEVARRIA JUAN
g. Grado académico-profesión : Magister
h. D.N.I. : 08149384
i. N° de teléfono : 985211454
j. Lugar y fecha :

V. **DATOS DEL INSTRUMENTO DE EVALUACIÓN**

d. Autor del instrumento :
e. Método de investigación : Cualitativo
f. Tipo de entrevista : Semiestructurada

VI. ASPECTOS DE EVALUACIÓN

N°	Criterios	Indicadores	Si	No	Observaciones
1	CONSISTENCIA	Las preguntas de la entrevista son congruentes a los objetivos de la investigación	**X**		tiene congruencia con los objetivos de investigación
2	CLARIDAD	Está formulada con una sintaxis y semántica que permita la comprensión adecuada	**X**		Son de buena sintaxis, comprensibles y claras
3	ORGANIZACION	Existe una organización lógica en el instrumento	**X**		La construcción es lógica y está organizada
4	SUFICIENCIA	Contiene preguntas necesarias para recabar información suficiente	**X**		Las preguntas realizadas son suficientes al logro de la información a sus objetivos
5	RELEVANCIA	Las preguntas se orientan a la obtención de información trascendente y substancial.	**X**		Están orientadas para obtener una validación coherente.
Sugerencias y/o Recomendaciones		**Instrumento aplicable** La evaluación del instrumento ha sido de manera virtual, que conlleva a impedir una comunicación fluida y estable con el tesista.			

Mg. Juan Chuquivilca Echevarria
DNI: 08149384

HOJA DE VALIDACIÓN DE INSTRUMENTO 3

TÍTULO DE LA INVESTIGACIÓN: "Políticas integrales de ciberseguridad en la protección de la información digital en el Ejército del Perú, 2023"

VII. DATOS DEL EXPERTO:

k. Apellidos y nombres : ZUÑIGA IGUEROA JESUS ROLANDO
l. Grado académico-profesión : Magister
m. D.N.I. : 40549919
n. N° de teléfono : 971641133
o. Lugar y fecha : 19 abril 2024

VIII. **DATOS DEL INSTRUMENTO DE EVALUACIÓN**

g. Autor del instrumento : Wilson Mendoza Hinost
h. Método de investigación : Cuantitativo-Aplicada
i. Tipo de entrevista : Semiestructurada

IX. ASPECTOS DE EVALUACIÓN

N°	Criterios	Indicadores	Si	No	Observaciones
1	CONSISTENCIA	Las preguntas de la entrevista son congruentes a los objetivos de la investigación	**X**		Las preguntas si tienen congruencia con los objetivos
2	CLARIDAD	Está formulada con una sintaxis y semántica que permita la comprensión adecuada	**X**		La formolización Son comprensibles y de muy bien sintaxis
3	ORGANIZACION	Existe una organización lógica en el instrumento	**X**		Si existe construcción es lógica y está bien organizada
4	SUFICIENCIA	Contiene preguntas necesarias para recabar información suficiente	**X**		Con las preguntas realizadas son suficientes al logro de los objetivos
5	RELEVANCIA	Las preguntas se orientan a la obtención de información trascendente y substancial.	**X**		Si están orientadas para obtener una validación coherente y substancial
Sugerencias y/o Recomendaciones		**Instrumento aplicable** La evaluación del instrumento fue de manera virtual, lo que conlleva a impedir una comunicación fluida con el tesista.			

Mg. Jesus R. Zuñiga Figueroa
DNI: 40549919

ANEXO 4

COMPROMISO ÉTICO

DECLARACIÓN DE COMPROMISO ÉTICO

El presente trabajo de investigación titulado: **"Políticas integrales de ciberseguridad en la protección de la información digital en el Ejército del Perú, 2023"**, se ha realizado en estricto apego a la metodología de la investigación y a las normas éticas para investigación en Ciencias Militares 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 Miguel Ángel Martínez Rosales, egresado de la Maestría en Ciencias Militares de la Escuela Superior de Guerra del Ejército-Escuela de Postgrado (ESGE-EPG), declaro bajo juramento que he desarrollado esta investigación siguiendo las instrucciones brindadas por el Departamento de Gestión de 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, con apego 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.

.

ANEXO 5

CONSENTIMIENTO INFORMADO

Consentimiento Informado

Yo Ing RUMICHE BURGA David Ubaldo, declaro que he sido informado e invitado a participar en una investigación denominada “Políticas integrales de ciberseguridad en la protección de la información digital en el Ejército del Perú, 2023”, éste es un proyecto de investigación científica que cuenta con el respaldo de la Escuela Superior de Guerra del ejercito Escuela de postgrado.

Entiendo que este estudio busca conocer sobre las Políticas integrales de ciberseguridad en la protección de la información digital en el Ejército del Perú**,** y sé que mi participación se llevará a cabo en el Cuartel general del Ejército (Pentagonito)), y consistirá en responder una entrevista que demorará alrededor de 90 minutos. Me han explicado que la información registrada será confidencial, y que los nombres de los participantes serán asociados a un número de serie, esto significa que las respuestas no podrán ser conocidas por otras personas ni tampoco ser identificadas en la fase de publicación de resultados.

Estoy en conocimiento que los datos no me serán entregados y que no habrá retribución por la participación en este estudio, sé que esta información podrá beneficiar de manera indirecta como un beneficio para la sociedad dada la investigación que se está llevando a cabo.

Asimismo, sé que puedo negar la participación o retirarme en cualquier etapa de la investigación, sin expresión de causa ni consecuencias negativas para mí.

Por lo expuesto: Acepto voluntariamente participar en este estudio y he recibido una copia del presente documento.

Chorrillos 23 de setiembre de 2023

David Ubaldo RUMICHE BURGA

DNI: 40050118

Consentimiento Informado

Yo Ing QUIN RENDON, Jimmy Ronald, declaro que he sido informado e invitado a participar en una investigación denominada “Políticas integrales de ciberseguridad en la protección de la información digital en el Ejército del Perú, 2023”, éste es un proyecto de investigación científica que cuenta con el respaldo de la Escuela Superior de Guerra del ejercito Escuela de postgrado.

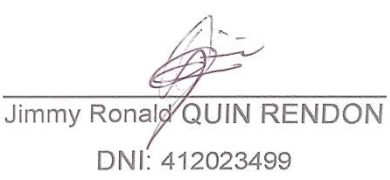
Entiendo que este estudio busca conocer sobre las Políticas integrales de ciberseguridad en la protección de la información digital en el Ejército del Perú**,** y sé que mi participación se llevará a cabo en el Cuartel general del Ejército(Pentagonito)), y consistirá en responder una entrevista que demorará alrededor de 90 minutos. Me han explicado que la información registrada será confidencial, y que los nombres de los participantes serán asociados a un número de serie, esto significa que las respuestas no podrán ser conocidas por otras personas ni tampoco ser identificadas en la fase de publicación de resultados.

Estoy en conocimiento que los datos no me serán entregados y que no habrá retribución por la participación en este estudio, sé que esta información podrá beneficiar de manera indirecta como un beneficio para la sociedad dada la investigación que se está llevando a cabo.

Asimismo, sé que puedo negar la participación o retirarme en cualquier etapa de la investigación, sin expresión de causa ni consecuencias negativas para mí.

Por lo expuesto: Acepto voluntariamente participar en este estudio y he recibido una copia del presente documento.

Chorrillos, 19 de abril de 2024



Jimmy Ronald QUIN RENDON
DNI: 412023499

Consentimiento Informado

Yo Ing CANCHARI ORTIZ, Frank Wilder declaro que he sido informado e invitado a participar en una investigación denominada “Políticas integrales de ciberseguridad en la protección de la información digital en el Ejército del Perú, 2023”, éste es un proyecto de investigación científica que cuenta con el respaldo de la Escuela Superior de Guerra del ejercito Escuela de postgrado.

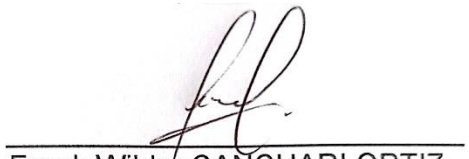
Entiendo que este estudio busca conocer sobre las Políticas integrales de ciberseguridad en la protección de la información digital en el Ejército del Perú**,** y sé que mi participación se llevará a cabo en el Cuartel general del Ejército(Pentagonito)), y consistirá en responder una entrevista que demorará alrededor de 90 minutos. Me han explicado que la información registrada será confidencial, y que los nombres de los participantes serán asociados a un número de serie, esto significa que las respuestas no podrán ser conocidas por otras personas ni tampoco ser identificadas en la fase de publicación de resultados.

Estoy en conocimiento que los datos no me serán entregados y que no habrá retribución por la participación en este estudio, sé que esta información podrá beneficiar de manera indirecta como un beneficio para la sociedad dada la investigación que se está llevando a cabo.

Asimismo, sé que puedo negar la participación o retirarme en cualquier etapa de la investigación, sin expresión de causa ni consecuencias negativas para mí.

Por lo expuesto: Acepto voluntariamente participar en este estudio y he recibido una copia del presente documento.

Chorrillos, 19 de abril de 2024



Frank Wilder CANCHARI ORTIZ

DNI: 46203691

Consentimiento Informado

Yo Ing SOTELO RIVERA, Rafael Antonio, declaro que he sido informado e invitado a participar en una investigación denominada “Políticas integrales de ciberseguridad en la protección de la información digital en el Ejército del Perú, 2023”, éste es un proyecto de investigación científica que cuenta con el respaldo de la Escuela Superior de Guerra del ejercito Escuela de postgrado.

Entiendo que este estudio busca conocer sobre las Políticas integrales de ciberseguridad en la protección de la información digital en el Ejército del Perú, y sé que mi participación se llevará a cabo en el Cuartel general del Ejército(Pentagonito)), y consistirá en responder una entrevista que demorará alrededor de 90 minutos. Me han explicado que la información registrada será confidencial, y que los nombres de los participantes serán asociados a un número de serie, esto significa que las respuestas no podrán ser conocidas por otras personas ni tampoco ser identificadas en la fase de publicación de resultados.

Estoy en conocimiento que los datos no me serán entregados y que no habrá retribución por la participación en este estudio, sé que esta información podrá beneficiar de manera indirecta como un beneficio para la sociedad dada la investigación que se está llevando a cabo.

Asimismo, sé que puedo negar la participación o retirarme en cualquier etapa de la investigación, sin expresión de causa ni consecuencias negativas para mí.
Por lo expuesto: Acepto voluntariamente participar en este estudio y he recibido una copia del presente documento.

Chorrillos, 19 de abril de 2024

Rafael Antonio SOTELO RIVERA
DNI: 43287193

ANEXO 6

CD CON LA TESIS EN PDF

ESCUELA SUPERIOR DE GUERRA DEL EJÉRCITO

ESCUELA DE POSTGRADO

TESIS

POLÍTICAS INTEGRALES DE CIBERSEGURIDAD EN LA PROTECCIÓN DE LA INFORMACIÓN DIGITAL EN EL EJÉRCITO DEL PERU, 2023

AUTOR

Bach. MIGUEL ANGEL MARTINEZ ROSALES

2024

ANEXO 6

REPORTE DE SIMILITUD DE TURNITIN

turnitin

Identificación de reporte de similitud: oid:12350:375160927

NOMBRE DEL TRABAJO

Pyto final MARTINEZ ROSALES 2024 (1).docx

AUTOR

MARTINEZ ROSALES

RECUENTO DE PALABRAS

23346 Words

RECUENTO DE CARACTERES

135794 Characters

RECUENTO DE PÁGINAS

115 Pages

TAMAÑO DEL ARCHIVO

2.8MB

FECHA DE ENTREGA

Aug 22, 2024 10:06 AM GMT-5

FECHA DEL INFORME

Aug 22, 2024 10:07 AM GMT-5

● 16% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- **12% Base de datos de Internet**
- **1% Base de datos de publicaciones**
- **Base de datos de Crossref**
- **Base de datos de contenido publicado de Crossref**
- **9% Base de datos de trabajos entregados**

● Excluir del Reporte de Similitud

- **Material bibliográfico**
- **Material citado**