

ESCUELA MILITAR DE CHORRILLOS
“CORONEL FRANCISCO BOLOGNESI”



**Aplicación de la ciberinteligencia en el proceso de inteligencia en la
dirección de inteligencia del ejército del Perú**

**Trabajo de Suficiencia Profesional para optar el Título Profesional de
Licenciado en Ciencias Militares con Mención en Ingeniería**

Autor

Jorge Enrique Leon Pinedo

Lima – Perú

2018

INDICE

RESUMEN	ii
INTRODUCCION	iii
CAPITULO I: INFORMACION GENERAL	Pág.
1.1 Dependencia o Unidad (donde se desarrolla el tema)	01
1.2 Tipo de actividad (Función y puesto)	01
1.3 Lugar y Fecha	04
CAPITULO II: MARCO TEORICO	
2.1 Campos de aplicación	05
2.2 Tipo de aplicación (Operativo, administrativo y/ o técnico)	05
2.3 Definición de términos	05
CAPITULO III: DESARROLLO DEL TEMA	
3.1 Antecedentes	28
3.2 Descripción	29
3.3 Propuesta de innovación	31
CONCLUSIONES	
RECOMENDACIONES	
REFERENCIAS BIBLIOGRAFICAS	
ANEXOS	
01. Informe profesional	
02. Fotos, esquemas, flujograma	

RESUMEN

El presente trabajo se desarrolló en la Dirección de Inteligencia del Ejército (DIE), en el distrito de San Borja en el Departamento de Lima y tuvo como objetivo general; Formular una propuesta innovadora orientada a enriquecer la doctrina referente a la **Aplicación de la Ciberinteligencia en la Dirección de Inteligencia del Ejército**; realizando un estudio de la situación del empleo actual del ciberespacio en dicho estamento, para contribuir a optimizar cada una de las fases del proceso de inteligencia.

La Dirección de Inteligencia del Ejército, es el ente rector de la producción de inteligencia en el Ejército Peruano, por tal motivo, es de nuestro interés conocer si esta Dirección utiliza y aplica los instrumentos que el ciberespacio y la ciberinteligencia proporcionan a fin de mejorar y optimizar los procedimientos empleados en el proceso de producción de inteligencia; por lo tanto cabe preguntarnos, ¿ Es necesario implementar una nueva Subdirección en la Dirección de Inteligencia del Ejército que se encargue de producir inteligencia cibernética que permita potenciar la Producción de Inteligencia en la Dirección de Inteligencia del Ejército.

Los resultados obtenidos del presente trabajo demuestran que el personal de especialistas, desconoce los nuevos conceptos de Ciberespacio y Ciberinteligencia; lo que hace imprescindible crear la Subdirección de Ciberinteligencia en la Dirección de Inteligencia del Ejército, lo cual conlleva realizar una difusión de los nuevos conceptos doctrinarios establecidos en la doctrina aprobada el año 2014; así mismo se debe mejorar la infraestructura de recursos materiales existente en la Dirección de Inteligencia del Ejército, dotándola con tecnología de punta en lo que a medios cibernéticos se refiere.

INTRODUCCIÓN

Habiendo el suscrito realizado en el año 2014, el Curso de Inteligencia Estratégica, en la Dirección Nacional de Inteligencia (DINI), y habiendo adquirido nuevos conocimientos relacionadas a las herramientas vigentes que contribuyen de manera muy eficaz a mejorar la Producción de Inteligencia en los diferentes estamentos y siendo la ciberinteligencia una herramienta que está actualmente en boga, cuya aplicación es indispensable en el desarrollo del Proceso de Inteligencia porque va permitir el empleo masivo de la tecnología de punta y de última generación en beneficio de la labor de inteligencia que se desarrolla en el Ejército del Perú.

El suscrito pone a consideración del DIDOC de la EMCH CORONEL FRANCISCO BOLOGNESI, el presente Trabajo de Suficiencia Profesional cuyo título es: “Aplicación de la Ciberinteligencia en el Proceso de Inteligencia en la Dirección de Inteligencia del Ejército del Perú”

El Trabajo de Suficiencia Profesional, realizado en la Dirección de Inteligencia del Ejército, establece conceptos relacionados a la Ciberinteligencia con el Proceso de Inteligencia que deben ser aplicados y desarrollados por la Dirección de Inteligencia del Ejército del Perú y todos sus elementos subordinados a fin de optimizar eficazmente el producto final que se entregará al Comandante General del Ejército para la toma de decisiones.

La estructura del trabajo comprende 03 capítulos. El texto se ha organizado didácticamente y considera el siguiente orden metodológico:

Capítulo I, Información General; en este capítulo desarrollamos una descripción general de la dependencia donde se realizó la experiencia profesional.

Capítulo II, Marco Teórico; en el presente capítulo se describe el campo de aplicación y contiene la definición de términos más importantes.

Capítulo III, Desarrollo del tema; en este capítulo desarrollamos la descripción la situación encontrada y presentamos nuestra propuesta para la solución a la problemática encontrada.

Conclusiones; culminamos con las conclusiones del trabajo realizado, donde presentamos los pasos a seguir para solucionar la problemática encontrada.

CAPITULO I: INFORMACION GENERAL

1.1 Dependencia o Unidad

Dirección de Inteligencia del Ejército – DIE

Ente rector del sistema de inteligencia del Ejército y encargada de producir inteligencia militar y realizar actividades de contrainteligencia.

Realizar el Planeamiento Estratégico de Inteligencia y asesorar al Comandante General del Ejército en aspectos de Inteligencia, Contrainteligencia y administración del Sistema de Inteligencia del Ejército.

1.2 Tipo de actividad

La Dirección de Inteligencia del Ejército está organizada en 05 Sub – direcciones; la Subdirección de Frente Externo, Subdirección de Frente Interno, Subdirección de Contrainteligencia, Subdirección de Personal y Subdirección de Inteligencia Técnica.

Estas Subdirecciones reciben informaciones de los órganos de inteligencia subordinados de todas las guarniciones del Ejército del Perú; insumo que luego de sufrir un procesamiento y análisis se convierte en inteligencia, insumo útil para el proceso de la toma de decisiones por el comando del Ejército y para el Sistema de Inteligencia Nacional.

a. Subdirección de Contrainteligencia

(1) Funciones

- a** Planear, conducir, coordinar, recomendar y supervisar los procedimientos y medidas de contrainteligencia y seguridad a nivel Ejército, a fin de detectar, neutralizar y/o destruir las acciones del enemigo externo e interno que atenten contra la seguridad militar y/o nacional.
- b** Coordinar con el CCFFAA, Ministerio de Interior, para asegurar la participación de todos sus miembros en los diferentes Comités Regionales de Contrainteligencia de las DE, GU y UU independientes que tengan responsabilidad en un ASN.

- c** Asesorar, controlar y verificar la ejecución y cumplimiento de las disposiciones generales y específicas emanadas por el Sr. General Director de Inteligencia del Ejército.
- d** Secundar al Director en el ejercicio de sus funciones, administrativas y disciplinarias.

b. Subdirección de Frente Externo

(1) Funciones

- a** Formular la Apreciación de Inteligencia Estratégica, así como su difusión a los elementos de la DINI y SIDE en los plazos establecidos.
Orientar el Esfuerzo de Búsqueda, Procesamiento de las Informaciones, determinando las necesidades de información que requiere la DIE y asegurar la oportuna producción y difusión de inteligencia del frente externo que requiere el comando para la toma de decisiones.
- b** Formular los temas y las exposiciones para las conferencias bilaterales de inteligencia en las que participa la DIE.
- c** Asesorar, controlar y verificar la ejecución y cumplimiento de las disposiciones generales y específicas emanadas por el Sr. General Director de Inteligencia del Ejército.

c. Subdirección de Frente Interno

(1) Funciones

- a** Formular la Apreciación de Inteligencia Estratégica, así como su difusión a los elementos del SINA y SIDE en los plazos establecidos.
- b** Orientar el Esfuerzo de Búsqueda, Procesamiento de las Informaciones, determinando las necesidades de información que requiere la DIE y asegurar la oportuna producción y difusión

de inteligencia del frente interno que requiere el comando para la toma de decisiones.

- c** Formular los temas y las exposiciones para las conferencias bilaterales de inteligencia en las que participa la DIE.
- d** Asesorar, controlar y verificar la ejecución y cumplimiento de las disposiciones generales y específicas emanadas por el sr. General Director de Inteligencia del Ejército.

d. Subdirección de Inteligencia Técnica

(1) Funciones

- a** Asesorar al Director de Inteligencia del Ejército y Órganos del SIDE en aspectos de tecnología de información (administración y automatización de datos) y telecomunicaciones (teleproceso, conectividad, correo electrónico e internet), orientadas al acopio, procesamiento y explotación de la información en actividades de Inteligencia y Contrainteligencia.
- b** Promover, ejecutar proyectos informáticos a nivel DIE y SIDE.
- c** Dirigir, controlar y asegurar la producción de Inteligencia y Contrainteligencia en el Frente Interno y Frente Externo a través del sistema kryhasoft.
- d** Asegurar el soporte técnico en hardware y software de la DIE y del Sistema de Inteligencia del Ejército (SIDE)

e. Subdirección de Personal

(1) Funciones

- a** Asesorar al Señor General de Brigada Director de Inteligencia del Ejército en los aspectos de la administración del personal de inteligencia a nivel SIDE, que sirve en el activo.

- b** Dirigir, controlar y supervisar la correcta aplicación de los procedimientos administrativos, desarrollando y mejorando la administración de la carrera del personal de Técnicos y Sub Oficiales de Inteligencia del Ejército.
- c** Participar en las sesiones del consejo de investigación para el personal de Técnicos y Sub Oficiales de Inteligencia del Ejército.
- d** Mantener informado al comando de la DIE de los aspectos que afecten la moral y disciplina del personal de Técnicos y Sub Oficiales de Inteligencia a nivel SIDE.

1.3 Lugar y Fecha

El presente trabajo se realizó en la ciudad de Lima, de marzo a setiembre del año 2014

CAPITULO II: MARCO TEORICO

2.1 Campos de aplicación

El empleo de la Ciberinteligencia dentro del Proceso de Inteligencia en la Dirección de Inteligencia del Ejército, permitirá su conocimiento y aplicación en todo el Sistema de Inteligencia del Ejército, desde pequeñas unidades hasta las Divisiones de Ejército, en los niveles Táctico y Estratégico lo que permitirá a los Comandantes realizar un adecuado Proceso de Toma de Decisiones.

2.2 Tipo de aplicación

La aplicación de la ciberinteligencia se dará en el campo Técnico; permitiendo adoptar las medidas de contrainteligencia para evitar la vulnerabilidad de nuestra seguridad de instalaciones y la seguridad de personal; además, permitirá conocer los avances de la ciencia y tecnología relacionados al armamento, material y equipo con que cuenta nuestra institución a fin de evitar su obsolescencia.

2.3 Definición de términos

1. LA CIBERINTELIGENCIA¹

a. Definición

Conocimiento de las amenazas del ciberespacio, sus actores, capacidades, vulnerabilidades, formas de acción y sus correspondientes escenarios de riesgos, proporcionado para la toma de decisiones y la protección de Activos Críticos Nacionales.

¹DINI. FUNDAMENTOS DOCTRINARIOS. 14 FEBRERO 2014.

Como proceso está definida como el conjunto de actividades de generación y difusión de conocimientos oportuno y veraz.

b. Dimensiones

La ciberinteligencia tiene tres dimensiones básicas de desarrollo:

- (1) Como fuente específica de nuevas amenazas y sus correspondientes escenarios de riesgos.
- (2) Como medio para desarrollar nuevas formas de acción para la explotación de las amenazas tradicionales y sus escenarios de riesgos.
- (3) Como medio para detectar, identificar y explotar oportunidades para la actividad de inteligencia y contrainteligencia.

c. El ciberespacio.

Nuevo dominio, creado por el hombre y que está en una evolución permanente, de ámbito mundial, compuesto por el ambiente de información, redes interdependientes de infraestructuras de información, incluye internet, redes de telecomunicaciones, sistemas de cómputo, procesadores y controladores.

La infraestructura cibernética del Estado peruano está referida a todos aquellos activos críticos que la conforman, pudiendo estos estar administrados u operados por entidades del estado o privados, y que de materializarse un riesgo, cuyo origen puede estar en el ciberespacio o en cualquiera de los dominios tradicionales (tierra, mar, aire y espacio), generarían un impacto negativo que podría afectar, de acuerdo con su magnitud, diferentes sectores del Estado o al país en su conjunto.

El ciberespacio opera en el espectro electromagnético y sus nodos físicos están en los dominios tradicionales, por lo cual están relacionados y sus riesgos pueden ser transversales a los otros dominios.

d. Componentes del Ciberespacio.

Los componentes del ciberespacio si bien están principalmente relacionados a internet, tienen otros diversos elementos que conforman su ecosistema, tales como, las redes de comunicaciones convergentes (Sistemas de telefonía IP, teleconferencia), las infraestructuras de servicios públicos y privados (Redes de telefonía celular, Portales de gobierno, Servicios Municipales, Servicios de salud, etc.), redes LAN / WAN de empresas privadas (Redes Bancarias, Entidades de Salud, Servicios de Transporte, Fábricas, Puertos, entre otros) y sectores de gobierno (Fuerzas Armadas, Policía Nacional, Cuerpo de Bomberos, Empresas de Agua y Saneamiento); asimismo, están todos aquellos activos tecnológicos (Redes inalámbricas - Wi Fi, Tarjetas de cajeros automáticos, computadoras, telefonía fija, grifos de combustible, televisión, radio) que usa la población para sus diversas actividades sociales y económicas, conformando en su conjunto el Quinto Dominio del ciberespacio del país.

e. La ciberinfraestructura y los Activos Críticos Nacionales

La tecnología del ciberespacio es fundamental para el adecuado funcionamiento de todos los sectores productivos y de servicios de cada país. Estos servicios y procesos básicos están compuestos por múltiples activos críticos que se interrelacionan cada día más por el ciberespacio, por lo cual sus vulnerabilidades pueden ser explotadas por diversas amenazas de cualquier dominio y sus riesgos específicos pueden desencadenar impactos en cadena para el país.

En este contexto, la infraestructura cibernética o ciberinfraestructura es el conjunto de activos físicos y lógicos (por ejemplo, TIC, redes SCADA, nodos satelitales, sistemas de comando y control militares) que se convierten en el eje principal que relaciona la infraestructura física, información y recursos naturales, con los procesos, actividades

y operaciones del país, generando de esta manera nuevos escenarios de riesgo para la seguridad nacional.

f. La Ciberseguridad

Situación de confianza obtenida por la efectiva gestión de los riesgos, identificados por la ciberinteligencia y la implementación de las medidas de cibercontrainteligencia, para la protección de los ACN.

La ciberseguridad comprende el conjunto de acciones destinadas a identificar las amenazas cibernéticas que pueden afectar a los ACN, analizando previamente sus vulnerabilidades y gestionando medidas de mitigación del impacto de los riesgos evaluados.

La ciberseguridad debe considerar las amenazas de origen humano, físico y cibernético en su conjunto, considerando que cada vez están más interrelacionadas. Entre las amenazas de origen cibernético, al punto de vista policial, debemos considerar principalmente las siguientes:

- (1) Ciberespionaje.
- (2) Ciberterrorismo.
- (3) Ciberoperaciones de lavado de activos.
- (4) Ciberoperaciones de identidad de personas.
- (5) Ciberoperaciones del narcotráfico.
- (6) Ciberoperaciones de tráfico de armas.

Estas amenazas pueden ser aprovechadas por múltiples actores, no fácilmente identificables, y generarse diversos tipos de ataques, entre los cuales tenemos los siguientes:

- (1) Vandalismo cibernético (por ejemplo, denegación de servicio, hacking, entre otros).
- (2) Guerra psicológica en el ciberespacio.

- (3) Ataques contra los equipos electrónicos.
- (4) Ataques contra infraestructuras críticas (redes SCADA): Energía, agua, comunicaciones, entre otros.

g. Proceso de Ciberinteligencia.

Al igual que el Proceso de Inteligencia (PI), la Ciberinteligencia es el conjunto de actividades de generación y difusión de conocimiento oportuno y veraz, basado en necesidades y requerimientos a fin de obtener el conocimiento de los escenarios de riesgos y capacidades, vulnerabilidades y formas de acción de los actores en el ciberespacio, para la toma de decisiones y la protección de Activos Críticos Nacionales (ACN). Comprende la orientación del esfuerzo de búsqueda en la nube, la búsqueda y análisis de información en el ciberespacio, principalmente de fuente cerrada, cuyo producto final es la inteligencia que es diseminada para su utilización.

Entre las fases del Procesamiento de Información y la Orientación del Esfuerzo de Búsqueda se puede dar una reorientación, siempre que la información obtenida lleve a replantear la hipótesis inicial sobre un escenario de riesgo y consecuentemente se generen nuevas necesidades de información.

2. EL PROCESO DE INTELIGENCIA²

a. Definición

Conjunto de actividades de generación y difusión de conocimiento oportuno y veraz, basado en necesidades y requerimientos a fin de obtener el conocimiento de los escenarios de riesgos y capacidades, vulnerabilidades y formas de acción de los actores, para la toma de decisiones y la protección de Activos Críticos Nacionales (ACN).

Comprende la orientación del esfuerzo de búsqueda, la búsqueda y análisis de información, principalmente de fuente cerrada, cuyo

²DINI. FUNDAMENTOS DOCTRINARIOS. 14 FEBRERO 2014.

producto final es la inteligencia que es diseminada para su utilización. El PI es conocido también como Ciclo de Producción de Inteligencia.

b. Descripción del Proceso de Inteligencia

Previo a la ejecución del PI, es indispensable para los componentes del SINA tener en consideración los objetivos y escenarios de riesgos establecidos en el PPI a fin de contar con las necesidades de inteligencia determinadas por el usuario, así como con los recursos para el cumplimiento de dichos requerimientos.

Los titulares de los componentes, durante el desarrollo del PI, mantienen la dirección, coordinación y control de todas las actividades que lo comprenden.

Para el logro del objetivo descrito, el PI comprende las siguientes fases:

1. Orientación del Esfuerzo de Búsqueda
2. Búsqueda de Información
3. Procesamiento de Información
4. Difusión y Utilización de Inteligencia

Entre las fases del Procesamiento de Información y la Orientación del Esfuerzo de Búsqueda se puede dar una reorientación, siempre que la información obtenida lleve a replantear la hipótesis inicial sobre un escenario de riesgo y consecuentemente se generen nuevas necesidades de información.

Después de la difusión del producto de inteligencia se debe efectuar una evaluación de su utilización y pertinencia por el usuario, así como del proceso seguido para su elaboración, cuyos resultados sirven para la retroalimentación.

c. Las Fases del Proceso de Inteligencia

(1) Fase 1.- Orientación del Esfuerzo de Búsqueda (OEB)

(a) Definición

Es el conjunto de acciones que realiza de manera permanente un órgano de inteligencia, con la finalidad de orientar las capacidades de búsqueda hacia la satisfacción de las necesidades de inteligencia expresadas por los usuarios.

Estas acciones se materializan con la confección de la Hoja de Trabajo de Búsqueda de Información (HTBI), que sirve para el planeamiento y supervisión de las actividades de orientación y búsqueda, mediante la determinación de las indicaciones, los Elementos Esenciales de Información (EEI) y Otras Necesidades de Información (ONI), formulación de las bases para los Pedidos de Información (PDI), determinación de los órganos, y la supervisión y control.

La HTBI permite al analista coordinar e integrar los esfuerzos de los órganos de búsqueda y mantenerse informado.

(b) Etapas de la OEB

1 Comunicación de necesidades de inteligencia

En esta etapa los analistas de los órganos de inteligencia reciben las necesidades de inteligencia de la instancia superior.

2 Determinación de las indicaciones

Una indicación es cualquier indicio, evidencia o característica del actor y entorno, que sustenta una presunción sobre hechos, fenómenos, situaciones, conductas, posibilidades, vulnerabilidades y formas de acción, planteadas como EEI u ONI.

3 Determinación de la prioridad de necesidades de inteligencia

Las necesidades de inteligencia recibidas son

analizadas para establecer las variables de información, las que luego son clasificadas por orden de prioridad en Elementos Esenciales de Información (EEI) y Otras Necesidades de Información (ONI).

Ello evitará la dispersión del esfuerzo; permitirá utilizar a los órganos de búsqueda en forma más eficiente y eficaz, además de tener la información solicitada con oportunidad y de conformidad con su importancia.

Tanto los EEI como las ONI constituyen el total de las informaciones requeridas y sirven para la formulación de la Hoja de Trabajo de Búsqueda de Información (HTBI) y del Plan de Búsqueda (PDB).

a Elementos Esenciales de Información (EEI)

Son las variables o vacíos de información prioritarios, formuladas en forma de pregunta, que de no ser respondidas impiden el logro de objetivos previamente establecidos.

b Otras Necesidades de Información (ONI)

Son las variables o vacíos de información de segunda prioridad a los EEI, formuladas en forma de pregunta, que de no ser respondidas afectan pero no impiden el logro de objetivos.

4 Determinación de las bases para los pedidos

Son las informaciones específicas que se solicitarán para responder a los EEI y las ONI planteados.

5 Determinación de los órganos

Es la selección de los órganos de búsqueda más

adecuados para cada situación e información requerida, a los cuales se les va a ordenar ejecutar la búsqueda de información.

Al hacer esta selección se deben observar los siguientes factores:

a Acceso

Implica tener en consideración el nivel de ingreso y sin restricciones, que tiene el órgano de búsqueda respecto a la fuente de información.

b Posibilidad

Los órganos de búsqueda deben ser físicamente capaces de poder obtener la información deseada.

c Adaptabilidad

Las misiones de búsqueda asignadas a los órganos correspondientes deben ser compatibles con las misiones que estos cumplen normalmente. Sólo se deben emplear los órganos que sean los más adecuados para obtener la información deseada, considerando aspectos de personal, economía y material.

d Multiplicidad

Para obtener cada información requerida es necesario emplear más de un órgano de búsqueda, con el objetivo de que la evaluación de información sea comparada con la información recibida de otras fuentes y órganos.

e Balance

Es la racionalización, en forma equitativa, del trabajo de búsqueda entre los órganos disponibles.

f Ubicación

Consiste en tener en cuenta la proximidad del órgano con relación a la fuente de información.

6 Formulación de los Pedidos de Información (PDI)

El Pedido de Información (PDI) es un documento dirigido a cualquier órgano de inteligencia, para que proporcione una información específica.

7 Coordinación y supervisión permanente

Es el seguimiento y monitoreo de la labor de los órganos de búsqueda, incluyendo el análisis de los resultados parciales o finales, a fin de realizar los reajustes y las modificaciones necesarios en el proceso de búsqueda de información.

(2) Fase 2.- Búsqueda de Información

(a) Definición

Es el proceso de ejecución de las actividades orientadas a la obtención de información, en base a los EEI y ONI recibidos, que se realiza mediante la explotación sistemática y ordenada de las fuentes con los medios y técnicas operacionales de acuerdo al Plan de Búsqueda, para su entrega posterior al órgano superior de colección que efectúa la evaluación primaria y remisión al órgano de procesamiento.

(b) Características

1 Previsión

Debe anticiparse a los acontecimientos, para ello es necesario planear y ejecutar oportuna y detalladamente las acciones de búsqueda, explotando sobre el mismo asunto, diversas fuentes y órganos.

2 Permanencia

La necesidad de disponer de inteligencia en todo momento impone un esfuerzo continuo en el tiempo para la búsqueda de la información.

3 Dinámica

La búsqueda de información debe realizarse con iniciativa y decisión, en función de la dinámica de los acontecimientos.

4 Reserva

La búsqueda de información solo debe ser conocida y divulgada entre el personal autorizado.

(c) Fuentes de información

1 Definición

Son todas aquellas personas, organizaciones, comunicaciones, infraestructuras, actividades o lugares de los que se puede obtener información útil para absolver los EEI y las ONI.

2 Clasificación

Las fuentes de información pueden ser clasificadas:

a Por su importancia

1) Fuente cerrada

Aquella que contiene la información requerida para absolver los EEI y las ONI, que se encuentra protegida, por lo que es necesario ejecutar actividades de infiltración para su acceso u obtención.

2) Fuente abierta

a) De acceso limitado

Aquella que administran órganos públicos o privados y a la que se accede siguiendo un procedimiento legal establecido. Por ejemplo, el secreto bancario, al secreto tributario, entre otros.

b) De acceso ilimitado

Aquella que está a libre disposición y ofrece información no clasificada. Por ejemplo, boletines informativos de medios de comunicación social, servicios de noticias, Internet, actividades públicas y académicas, entre otros.

b Por su origen

1) Fuente humana

Constituida por cualquier persona, conjunto de personas o sus actividades, de las que se obtiene información de interés para la seguridad nacional.

2) Fuente documental

Son los medios diversos en los que se encuentran registradas informaciones de interés para la seguridad nacional, como documentos, escritos, fotografías, mapas, cartas, gráficos, páginas web, audios, videos, entre otros.

3) Fuente electrónica y digital

Está constituida por cualquier información de interés para la seguridad nacional que está presente en el espectro electromagnético y en el ciberespacio.

4) Material y equipo

Compuesto por aquellos bienes materiales utilizados por el hombre, de los que se obtiene información de interés para la seguridad nacional.

5) Infraestructura física

Conformada por aquellos bienes materiales contruidos por el hombre, de carácter fijo, de los que se obtiene información de interés para la seguridad nacional.

6) Ambiente natural

Comprende los bienes o recursos, accidentes geográficos y fenómenos naturales y ambientales de los que se obtiene información de interés para la seguridad nacional.

(d) Órganos de búsqueda

1Definición

Son las personas y equipos de un órgano de inteligencia, que obtienen la información como consecuencia de la explotación de las fuentes correspondientes.

2Procedimientos de búsqueda

a Para fuente cerrada

Mediante Operaciones Especiales de Inteligencia

(OOEEI) que emplean a la infiltración con medios humanos y tecnológicos, como principal técnica operacional.

b Para fuente abierta

1) De acceso limitado

Mediante el cumplimiento de los procedimientos legales establecidos para acceder a dicha fuente.

2) De acceso ilimitado

Mediante la observación y examen detallado de la información existente en las fuentes de libre disponibilidad.

(e) Etapas para la búsqueda de información

La secuencia para las actividades de la búsqueda de información comprende cuatro etapas:

1Planeamiento

Consiste en determinar las fuentes, órganos y procedimientos a emplear en la colección.

Comprende las siguientes acciones:

- a** Evaluación y selección de las fuentes de información.
- b** Se realiza teniendo en cuenta priorizando la fuente por la información requerida.
- c** Evaluación, selección y asignación de tareas a los órganos de búsqueda.
- d** Se realiza teniendo en cuenta la proximidad y especialización del órgano con relación a la información requerida.
- e** Selección de los procedimientos de búsqueda.
- f** Se realiza mediante los procedimientos señalados en el

párrafo (d) numeral 2).

2Colección

Consiste en el conjunto de actividades orientadas a la explotación de las fuentes para la obtención, organización y evaluación de la información.

Comprende las siguientes acciones:

a Explotación de la fuente

Consiste en obtener la información de las fuentes empleando una o más técnicas operacionales.

b Organización de la información

Consiste en ordenar la información tanto por campos de inteligencia (político, económico, social, militar y policial) y otros ámbitos (científico, tecnológico, geográfico y ambiental, entre otros).

c Evaluación de la información

Se realiza para asegurar que la información sea la requerida, atendiendo criterios de importancia, pertinencia, objetividad y urgencia, priorizando la que requiere explotación inmediata.

3Formulación de la nota de agente

La nota de agente es un documento elaborado por elementos de los órganos de búsqueda de los componentes del SINA, para la transmisión de información objetiva y oportuna acerca de una persona, hecho, situación o evento, que sirve como insumo para el análisis de inteligencia.

La información debe responder a las siguientes preguntas:

qué, quién, cuándo, dónde y cómo, con relación a la misión recibida. Si es factible debe incluir otras informaciones de interés.

Si en el cumplimiento de la misión se obtuvieran informaciones sobre otros asuntos, se informan mediante otra u otras notas de agente.

4Distribución de la información obtenida

Consiste en transmitir las informaciones obtenidas y evaluadas por el órgano de búsqueda de la organización de manera oportuna (evaluación primaria de la información), a través de Notas de Información (NI) al órgano de procesamiento de la información.

(f) Evaluación de fuentes, órganos e informaciones

Es un conjunto de acciones que se realizan a nivel de órganos de búsqueda para determinar el grado de credibilidad de las fuentes y órganos de búsqueda, así como la exactitud de las informaciones, cuyo resultado es determinante para su empleo en la producción de inteligencia.

El proceso de evaluación es constante y consecuentemente los resultados pueden variar, la evaluación debe ser fundamentalmente objetiva dejando en el mínimo indispensable elementos subjetivos, de tal forma que todos los involucrados en ella apliquen los mismos criterios.

La evaluación se simboliza mediante el uso de un código alfanumérico, letras para la credibilidad de la fuente y el órgano de búsqueda, números para la exactitud del contenido

o información. Esta evaluación alfanumérica no limita la comunicación verbal entre colectores y analistas con el fin de obtener mayores detalles sobre el nivel de acceso de la fuente a la información, la forma de adquisición de la información y las referencias de informaciones anteriores dadas por la fuente, sin que ello signifique revelar la fuente o método empleado para la obtención de la información.

(3) Fase 3.- Procesamiento de Información

(a) Definición

Es la fase del PI que consiste en explotar la información obtenida, mediante su registro, evaluación, análisis y conclusión, para transformarla en un producto de inteligencia con alto grado de certeza o predicción.

(b) Etapas del procesamiento de información

El procesamiento de la información comprende las siguientes actividades: Registro, Evaluación, Análisis y Conclusión (REAC).

1El registro

Es la actividad a través de la cual la información recibida se reseña e inscribe, codifica y clasifica en un sistema, para facilitar su identificación y acceso para el análisis, así como su posterior archivo. Es un procedimiento continuo que comprende las acciones siguientes:

a Inscripción

Consiste en el registro resumido de la información en medios electrónicos, diarios, libros o cuadernos de trabajo, cartas de situación, álbumes, entre otros.

b Codificación y clasificación

Consiste en ordenar la información para asignarle códigos de acuerdo con criterios preestablecidos (espacio, tiempo, contenido, seguridad, entre otros) a fin de facilitar su archivo, control y acceso.

c Archivo

Es el almacenamiento de la información codificada y clasificada en medios electrónicos.

2La evaluación

Consiste en la revisión de la información obtenida, a fin de otorgarle una valoración final para su posterior análisis y explotación. Comprende los pasos siguientes:

a El examen de la información

Se realiza con el objeto de determinar su importancia, pertinencia, objetividad, urgencia y valor presente o futuro. Se efectúa sometiendo la información a las interrogantes siguientes:

¿Está relacionada con la situación estudiada o con los EEI y ONI?

¿Cubre todos los requerimientos planteados en los EEI y las ONI?

¿Obliga a un procesamiento urgente? Si es así, ¿a quién le interesa principalmente?

¿Tiene valor presente o futuro? Si es así, ¿para quién lo tiene?

Si la información no está relacionada o no satisface los requerimientos de los EEI y ONI, debe hacerse de conocimiento del órgano de búsqueda para que lo amplíe.

b La valoración final de la información

Consiste en determinar el valor final de la información que ha pasado el examen anterior, en función de su exactitud así como de la credibilidad de la fuente y el órgano, utilizando los mismos criterios empleados en la Fase de Búsqueda de Información (Fase 2), con la finalidad de determinar la continuación o interrupción de su procesamiento.

La valoración de la información puede prescindir de la evaluación de la fuente y el órgano cuando los componentes del SINA actúan como órganos en la producción de inteligencia del más alto nivel.

Como resultado de la valoración de la información se procederá a su análisis correspondiente.

Este proceso de valoración también sirve para mejorar el control de la eficacia de las fuentes y órganos.

3El análisis

Consiste en examinar las informaciones evaluadas y las disponibles sobre un determinado hecho, empleando métodos y operaciones intelectuales continuas para determinar su significado en el marco de la situación que se está estudiando o en función de los requerimientos de inteligencia del usuario, con la finalidad de producir conocimiento y/o adelantar un pronóstico sobre su evolución más probable. Comprende:

a La disgregación

Consiste en descomponer toda la información disponible y tomar de ella aquellos elementos que tengan relación

con la situación en estudio o con los requerimientos de inteligencia del usuario, los que se someten a un examen minucioso con la finalidad de interrelacionarlos en función de su coincidencia y complementariedad, a fin de constituir elementos de juicio para la comprensión y determinación de su significado.

En determinados casos no es necesario descomponer la información en sus elementos para comprenderla.

b La integración

Consiste en combinar los elementos de juicio determinados en la disgregación con la inteligencia básica o enciclopédica y otras informaciones confirmadas y/o disponibles, a fin de obtener un conjunto unificado de informaciones que permitan validar o replantear la hipótesis sobre un escenario de riesgo. En este último caso se procede a la reorientación del esfuerzo de búsqueda mediante la formulación de nuevos EEI y ONI.

c La interpretación

Es el entendimiento de lo que nos quiere decir la hipótesis ya validada, determinando las causas, elementos, dinámica e intereses que concurren sobre un escenario de riesgo.

4La conclusión

Es la etapa final del procesamiento de información, que consiste en la elaboración de las conclusiones para la formulación del producto de inteligencia, que contienen el conocimiento útil que sirve para satisfacer los requerimientos

del usuario.

De ser necesario, se considerarán los probables cursos de evolución de los escenarios de riesgos (proyecciones), empleando para ello los principios y métodos de la predicción en inteligencia.

(4) Fase 4.- Difusión y Utilización de Inteligencia

(a) Definición

Es la fase del PI que consiste en la entrega del producto de inteligencia a los usuarios autorizados -internos y externos- de manera oportuna, apropiada y a través de un canal seguro. También se le conoce como distribución o diseminación.

(b) Procedimientos

Se efectúa empleando, entre otros, los siguientes:

- 1** Contacto personal
- 2** Documentos de Inteligencia
- 3** Redes electrónicas de información seguras
- 4** Otros

Estos procedimientos de difusión de inteligencia se seleccionarán en función de diversos factores (por su oportunidad, importancia del asunto, naturaleza del problema, medios disponibles, nivel de órgano productor u otros).

3. ACTIVOS CRÍTICOS NACIONALES³

Todo con lo que cuenta el Estado para desarrollar y mantener las capacidades nacionales, con la finalidad de lograr los objetivos nacionales

³DINI. FUNDAMENTOS DOCTRINARIOS. 14 FEBRERO 2014.

y garantizar la seguridad de la nación y la supervivencia del Estado. Se clasifican en las siguientes categorías:

- Personal
- Información
- Procesos, actividades y operaciones
- Infraestructura física
- Infraestructura cibernética
- Ambiente y recursos naturales.

4. DEFENSA NACIONAL

Instrumento para alcanzar la Seguridad Nacional. Conjunto de recursos que un Estado, a través del Gobierno, puede utilizar para prevenir, neutralizar o eliminar las amenazas que pongan en riesgo la soberanía, independencia e integridad nacional.

5. PRODUCCIÓN DE INTELIGENCIA⁴

Conjunto de actividades que se realizan en los órganos de inteligencia para producir y difundir la inteligencia.

La producción de inteligencia debe responder a una misión o finalidad específica a fin de que los procesos correspondientes se desarrollen en forma coherente y con una orientación precisa.

Sin embargo, en ausencia de una misión o finalidad específica, la producción de inteligencia no debe detenerse, sino realizarse tomando como marco general de referencia los objetivos y las necesidades de inteligencia de los organismos del Sistema de Defensa Nacional.

6. SEGURIDAD NACIONAL

⁴DINI. FUNDAMENTOS DOCTRINARIOS. 14 FEBRERO 2014.

Situación en la que el Estado tiene garantizada su existencia, la integridad de su patrimonio, sus intereses así como su soberanía e independencia, para actuar con plena autoridad y libre de toda subordinación frente a todo tipo de amenazas.

7. SISTEMA DE INTELIGENCIA NACIONAL⁵

Conjunto de principios, normas, procedimientos, técnicas, instrumentos, organismos y órganos del Estado funcionalmente vinculados, que bajo la dirección y coordinación de la Dirección Nacional de Inteligencia – DINI como ente rector, producen Inteligencia Nacional, Inteligencia Militar e Inteligencia Policial y ejecutan medidas de contrainteligencia en las áreas de su responsabilidad.

8. SOBERANIA NACIONAL

Poder que tiene el Estado sobre su territorio, la cual está enmarcada en nuestra constitución y permite ser un territorio independiente e inviolable.

9. TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES

Conjunto de servicios, redes, software y aparatos que tienen como fin la mejora de la calidad de vida de las personas dentro de un entorno, y que se integran a un sistema de información interconectado y complementario.

Esta innovación servirá para romper las barreras que existen entre cada uno de ellos.

Las TIC son herramientas teórico conceptuales, soportes y canales que procesan, almacenan, sintetizan, recuperan y presentan información de la forma más variada.

⁵DINI. FUNDAMENTOS DOCTRINARIOS. 14 FEBRERO 2014.

CAPITULO III: DESARROLLO DEL TEMA

3.1 Antecedentes

El uso de las tecnologías de la información y de la comunicación se ha incorporado de forma general a la vida cotidiana de la gran mayoría de países del mundo. Este nuevo escenario facilita un desarrollo sin precedentes en el intercambio de información y comunicaciones, pero, al mismo tiempo, conlleva serios riesgos y amenazas, como son las actividades de países u otros actores que afectan la soberanía nacional.

Varios son los factores que contribuyen a la proliferación de acciones delictivas en el ciberespacio. La rentabilidad que ofrece su explotación en términos económicos, políticos o de otro tipo, la facilidad y el bajo costo del empleo de las herramientas utilizadas para la consecución de ataques, y la facilidad de ocultación del atacante hacen posible que estas actividades se lleven a cabo de forma anónima y desde cualquier lugar del mundo, con impactos transversales sobre los sectores público y privado y los propios ciudadanos.

El ciberespacio está considerado como el quinto dominio; éste está constituido por hardware, software, internet, servicios de información y sistemas de control que garantizan la provisión de aquellos servicios esenciales para la actividad socio-económica de cualquier nación.

Los distintos perfiles de atacantes que explotan las vulnerabilidades tecnológicas con el objeto de recabar información, sustraer activos de gran valor y amenazar los servicios básicos, pueden afectar al normal funcionamiento del país. El disfrute pacífico de ciertos derechos fundamentales consagrados en nuestra Constitución y en el ordenamiento

jurídico internacional puede verse seriamente comprometido como consecuencia de este tipo de acciones.

La Dirección de Inteligencia del Ejército, es el ente rector de la producción de inteligencia en el Ejército Peruano, por tal motivo, es de nuestro interés conocer si esta Dirección utiliza y aplica los instrumentos que el ciberespacio y la ciberinteligencia proporcionan a fin de mejorar y optimizar los procedimientos empleados en el proceso de producción de inteligencia.

La Dirección de Inteligencia del Ejército está organizada en 05 Sub – direcciones; la Subdirección de Frente Externo, Subdirección de Frente Interno, Subdirección de Contrainteligencia, Subdirección de Personal, Subdirección de Inteligencia Técnica.

Estas Subdirecciones reciben informaciones de los órganos de inteligencia subordinados de todas las guarniciones del Ejército del Perú; insumo que luego de sufrir un procesamiento y análisis se convierte en inteligencia, insumo útil para el proceso de la toma de decisiones por el comando del Ejército y para el Sistema de Inteligencia Nacional.

3.2 Descripción

De acuerdo a lo observado y verificado durante la ejecución del trabajo de campo se pudo determinar que en la Dirección de Inteligencia del Ejército, la Subdirección de Inteligencia Técnica, es la encargada de producir inteligencia en el campo tecnológico, vale decir por imágenes, señales y audio, la misma que se obtiene con los escasos medios tecnológicos con que cuentan tanto los órganos subordinados como los medios propios que ella posee, notándose una carencia en la nueva cultura de amenazas cibernéticas, su conocimiento y su necesidad de neutralización, debiendo ser necesario que en la producción de inteligencia de la Dirección de Inteligencia del Ejército se deba

implementar una nueva herramienta que sería la ciberinteligencia en el proceso de producción de inteligencia, de lo contrario la amenaza de actividades de países u otros actores que afecten la soberanía nacional se multiplicaría aún más y la obtención de la información en el cumplimiento de la producción de inteligencia resultaría innecesario provocando ineficiencia en la labor, potenciación de la amenaza y una ineficacia para controlar el riesgo que ello conlleva al país y al ejército; por lo tanto cabe preguntarnos, ¿ Es necesario implementar una nueva Subdirección en la Dirección de Inteligencia del Ejército que se encargue de producir inteligencia cibernética que permita potenciar la Producción de Inteligencia en la Dirección de Inteligencia del Ejército.

De no utilizar las bondades que el ciberespacio proporciona, en materia de inteligencia y seguridad, el producto final a entregar al decisor no sería el más adecuado y se convertiría en una vulnerabilidad que podría ser aprovechada por actores hostiles en contra de nuestros activos críticos nacionales atentando contra la seguridad y defensa nacional.

La nueva doctrina que ha sido elaborada por todos los componentes del SINA, será de vital importancia en el presente trabajo, ya que podremos verificar si estos nuevos conceptos que se encuentran en los manuales están vigentes y son aplicables al contexto actual.

La importancia del presente trabajo de investigación radica en que permitirá demostrar que actualmente los órganos de inteligencia del Ejército, para el Proceso de Inteligencia, se valen del ciberespacio y todos sus componentes para lograr obtener de manera oportuna la inteligencia más útil que permita al decisor la correcta toma de decisiones.

Con el desarrollo del presente trabajo, se entregará una propuesta que permita enriquecer la Doctrina de Inteligencia, de modo tal que los futuros integrantes del Sistema de Inteligencia del Ejército consoliden los nuevos

conceptos doctrinarios que están vigentes en la actualidad y que permitan optimizar las diferentes fases del proceso de producción de inteligencia a fin de entregar al decisor una información adecuada y oportuna.

Con la finalidad de lograr el cumplimiento de los objetivos trazados se va realizar entrevistas al personal de analistas de la Dirección de Inteligencia del Ejército que tengan mayor experiencia en el uso del ciberespacio y la tecnología en el proceso de inteligencia; así mismo realizaremos un análisis documental de la doctrina y bibliografía que le sirven de marco doctrinario al personal de analistas en su labor diaria.

3.3 Propuesta de innovación

Se adjunta un Plan de Acción donde se materializan las recomendaciones efectuadas.

PLAN DE ACCIÓN

A. FUNDAMENTOS

El Estado garantiza el bien común, a través del Bienestar General y la Seguridad Nacional. La Seguridad Nacional, es la situación en la que el Estado garantiza su integridad y su soberanía, utilizando como instrumento la Defensa Nacional.

El Ejército del Perú es una institución de las Fuerzas Armadas, dependiente del Ministerio de Defensa, responsable de organizar y preparar la fuerza para disuadir amenazas y proteger al Perú de agresiones, con el fin de contribuir a garantizar la independencia, soberanía e integridad territorial de la República.

Dentro de su organización cuenta como Órgano de Planeamiento y Asesoramiento al Estado Mayor General, dentro del cual se encuentra la Dirección de Inteligencia del Ejército.

La Dirección de Inteligencia, es el ente rector de la inteligencia dentro del Ejército y como tal es el encargado de proporcionarle al Comandante General del Ejército la mejor información procesada y convertida en conocimiento útil para que como decisor tome la decisión más adecuada. La Dirección de Inteligencia del Ejército, como parte del SINA, debe adecuarse a la nueva doctrina recientemente aprobada y difundir a todos sus elementos subordinados estos nuevos conceptos con la finalidad de fortalecer y mejorar el proceso de inteligencia, para lo cual debe valerse de las nuevas herramientas que el avance tecnológico nos proporciona, como es la ciberinteligencia.

Con la publicación del Decreto Legislativo N° 1141, “Fortalecimiento y Modernización del Sistema de Inteligencia Nacional – SINA y de la

Dirección Nacional de Inteligencia – DINI”, del 12 de diciembre del 2012, se establecen las normas para llevar a cabo la reforma del Sistema de Inteligencia Nacional; el mismo que fue reglamentado el 14 de Febrero del presente año con el Decreto Supremo 016-2014-PCM.

Así mismo a mediados del presente año se aprobó la nueva doctrina para el SINA, la cual está siendo difundida a todos los componentes con la finalidad de enriquecerla con las experiencias de sus integrantes y utilizarla en los diferentes procesos que realiza el sistema para el cumplimiento de sus objetivos.

De acuerdo a los resultados de la entrevistas realizadas se ha podido determinar que el personal de la Dirección de Inteligencia del Ejército desconoce y no se encuentra debidamente capacitado en los nuevos conceptos doctrinarios de Inteligencia, particularmente en lo referente a Ciberinteligencia y sus herramientas; así mismo los recursos humanos, recursos materiales e infraestructura que actualmente cuenta la Dirección de Inteligencia del Ejército, no es la más adecuada; por lo que el presente Plan de Acción reviste una gran importancia porque permitirá revertir dicha situación en beneficio del Proceso de Inteligencia que realiza este componente del SINA.

B. FINALIDAD

Optimizar la aplicabilidad de la Ciberinteligencia en el Proceso de Inteligencia en la Dirección de Inteligencia del Ejército, con la creación de la Subdirección de Ciberinteligencia.

C. ALCANCE

El presente Plan de Acción compromete a todo el personal integrante de todas las Subdirecciones de la Dirección de Inteligencia del Ejército, como

a todos los integrantes de los componentes del Sistema de Inteligencia del Ejército (SIDE).

D. OBJETIVOS Y METAS

1. OBJETIVOS

- a. Creación de la Subdirección de Ciberinteligencia en la Dirección de Inteligencia del Ejército.
- b. Difusión a todos los miembros integrantes de la Dirección de Inteligencia del Ejército; así como a los integrantes de los elementos subordinados los nuevos conceptos doctrinarios establecidos en la doctrina aprobada el presente año.
- c. Implementación y modernización de los recursos materiales existentes en la Dirección de Inteligencia del Ejército.

2. METAS

Objetivo a

- a. Solicitar al Comando del Ejército la aprobación de la norma legal que cree la Subdirección de Ciberinteligencia.
- b. Modificar el Cuadro de Asignación de Personal, el Manual de Organización y Funciones y el Manual de Procedimientos de la Dirección de Inteligencia del Ejército.
- c. Solicitar al Comando de Personal del Ejército el personal de Oficiales, Técnicos y suboficiales establecidos en el nuevo Cuadro de Asignación de Personal.

Objetivo b

- a. Incorporar la enseñanza de la nueva Doctrina de Inteligencia Nacional en la malla curricular de la Escuela de Inteligencia del

Ejército para todos los Cursos de Formación, Perfeccionamiento y Especialización.

- b. Realizar conferencias y charlas a nivel nacional para difundir el dominio cognoscitivo de la Ciberinteligencia, sus herramientas y los nuevos conceptos doctrinarios.
- c. Solicitar a los miembros del sistema que han sido capacitados en la nueva doctrina difundir sus conocimientos en todos los estamentos del SIDE.

Objetivo c

- a. Elaborar los presupuestos adecuados para la modernización de las computadoras y redes informáticas existentes en la Dirección de Inteligencia del Ejército.
- b. Solicitar la cobertura presupuestal que permita la modernización e implementación de la infraestructura informática en la Dirección de Inteligencia del Ejército.
- c. Programar los procesos de selección adecuados que permitan adquirir los bienes y servicios necesarios para mejorar y modernizar la infraestructura informática.

E. LÍNEAS DE ACCIÓN

1. Creación de la Subdirección de Ciberinteligencia

Presentar los documentos que permitan la creación de esta nueva subdirección y paralelamente realizar las modificaciones de los documentos normativos que establecen las funciones, procedimientos y personal necesario para el adecuado funcionamiento.

2. Difusión de la nueva doctrina

Se empleará todo el personal capacitado, los recursos materiales y los medios necesarios que permitan difundir a nivel nacional a todos los

integrantes de la Dirección de Inteligencia del Ejército y sus elementos subordinados los nuevos conceptos doctrinarios.

3. Elaboración del presupuesto para la implementación y modernización

Se elaborara los presupuestos, se solicitará la cobertura presupuestal y se ejecutaran los procesos de selección que permitan adquirir los bienes y servicios que aseguren la implementación y modernización de la Dirección de Inteligencia del Ejército.

F. AGENDA

1. Prioridades y Estrategias

a. Potenciar el capital humano como garante de una nueva cultura de inteligencia.

(1) Instruir a los agentes y analistas en el significado de optimizar los productos de inteligencia, en los siguientes aspectos:

(a) Inteligencia para las operaciones militares.

(b) Identificar amenazas contra la Seguridad Nacional.

(c) Proteger los Activos Críticos Nacionales, a cargo del Ejército.

(2) Proporcionar conocimiento oportuno y útil para la toma de decisión del Comandante General del Ejército.

b. Consolidar los principios de la nueva cultura de inteligencia.

Los integrantes de la Dirección de Inteligencia del Ejército, internalizaran los principios establecidos en la ley de fortalecimiento y modernización del SINA, como son la legalidad, legitimidad, control democrático, pertinencia, circulación restringida, especialidad, planificación y especialidad.

- c. Valorar la Especialidad de Inteligencia.
 - (1) La capacitación en doctrina conllevará al conocimiento de la profesión de inteligencia, la cual es de carácter secreto y de alto riesgo.
 - (2) Inculcar en el personal la adopción de procedimientos y medidas de seguridad, en el ámbito personal y profesional.

2. **Movilización de Recursos**

La aplicación del Plan de Acción compromete la movilización de los recursos siguientes:

a. **Recursos Humanos**

- (1) Profesionales
 - (a) Instructores
 - (b) Catedráticos
 - (c) Administrativos
- (2) Integrantes de los Cursos de Formación, Capacitación, Especialización y Perfeccionamiento.
 - (a) Oficiales Superiores del EP
 - (b) Oficiales Subalternos del EP
 - (c) Técnicos y suboficiales del EP
 - (d) Alumnos de la EIE

b. **Recursos Institucionales**

- (1) Ente Rector
 - Dirección Inteligencia del Ejército
- (2) Órganos de Inteligencia del Ejército del Perú
 - (a) Divisiones de Ejército

(b) Brigadas del Ejército

(c) Unidades del Ejército

c. Recursos Tecnológicos

(1) Medios de comunicación

(2) Computadoras

(3) Retro proyector

(4) Filmadoras

(5) Videotecas

d. Recursos Económicos

Las Subdirecciones involucradas de la Dirección de Inteligencia del Ejército formularán su presupuesto específico para atender los gastos que irrogue su participación en el presente Plan de Acción.

G. SEGUIMIENTO Y EVALUACIÓN

Para el cumplimiento de los objetivos previstos, así como la consecución y efectividad de las medidas realizadas, se prevé el seguimiento y la evaluación del presente Plan de Acción, que se realizará a través de los Órganos de Control de la Dirección de Inteligencia del Ejército.

H. RETROALIMENTACIÓN

Sobre la base de los resultados que se obtengan de la evaluación al Plan de Acción, se diseñará otras estrategias de retroalimentación para superar las limitaciones que pudieran afectar la optimización de los procesos.

Chorrillos, 24 de Abril del 2018

JORGE ENRIQUE LEÓN PINEDO

43271470

CONCLUSIONES

1. La falta de conocimiento de los nuevos conceptos de ciberinteligencia y las bondades que esta posee por parte del personal de analistas de la Dirección de Inteligencia del Ejército; no permite que la ciberinteligencia contribuya en la recolección de datos e información en el Proceso de Inteligencia que esta Dirección ejecuta.
2. El personal de analistas que actualmente labora en la Dirección de inteligencia del Ejército, no se encuentra debidamente capacitado en los nuevos conceptos de ciberinteligencia y las herramientas que esta nos proporciona, lo cual motiva que la metodología que propicia la ciberinteligencia en el análisis de la información en el Proceso de Inteligencia en la Dirección de Inteligencia del Ejército no sea el más adecuado, eficiente y eficaz.
3. El desconocimiento de los nuevos conceptos de Ciberinteligencia y de las herramientas que este nuevo dominio nos ofrece, hace que el nivel de diseminación de la información en el Proceso de Inteligencia a cargo de la Dirección de Inteligencia del Ejército hacia sus elementos subordinados sea muy bajo.
4. La infraestructura relacionada a recursos materiales como, computadoras, sistemas y redes; existente en la Dirección de Inteligencia del Ejército, no es de última generación, y teniendo la necesidad de estar acorde con la modernidad y la tecnología, en vista del valioso trabajo que esta Dirección debe realizar, es necesario mejorarla.
5. El Proceso de Inteligencia, en la Dirección de Inteligencia del Ejército no es óptimo debido a la serie de factores limitantes y carencias, tanto en recursos humanos debidamente capacitados como recursos materiales en infraestructura y equipamiento tecnológico.

RECOMENDACIONES

1. Que el señor General de Ejército, Comandante General del Ejército; disponga las siguientes acciones:
 - a. Creación de la Subdirección de Ciberinteligencia en la Dirección de Inteligencia del Ejército.
 - b. Que el COEDE, formule las mallas curriculares para que los nuevos conceptos doctrinarios sean difundidos a todo el personal de Oficiales, Técnicos y Suboficiales integrantes del SIDE, en las Escuelas de Formación y Perfeccionamiento.
 - c. Solicitar la cobertura presupuestal con la finalidad de asegurar la implementación y modernización de la Dirección de Inteligencia del Ejército con equipos y tecnología de última generación.

REFERENCIAS BIBLIOGRAFICAS

1. DECRETO LEGISLATIVO 1134 (2012). **“Aprueba la Ley de Organización y funciones del Ministerio de Defensa”**. Lima – Perú: Diario Oficial El Peruano, promulgada el 10 diciembre de 2012.
2. DECRETO LEGISLATIVO 1137 (2012). **“Ley del Ejército del Perú”**. Lima – Perú: Diario Oficial El Peruano, promulgada el 10 diciembre de 2012.
3. DECRETO LEGISLATIVO 1141 (2012). **“Fortalecimiento y Modernización del Sistema de Inteligencia Nacional – SINA y de la Dirección Nacional de Inteligencia –DINI”**. Lima – Perú: Diario Oficial El Peruano, promulgada el 11 diciembre de 2012.
4. DECRETO LEGISLATIVO 1142 (2012). **“Ley de bases para la modernización”**. Lima – Perú: Diario Oficial El Peruano, promulgada el 10 diciembre de 2012.
5. DEPARTAMENTO DE SEGURIDAD NACIONAL (2013) **“Estrategia de Ciberseguridad nacional”**. España
6. DINI (2014). **“Fundamentos Doctrinarios”**. Lima – Perú: Dirección Nacional de Inteligencia, promulgada el 14 de Febrero del 2014.
7. ORGANIZACIÓN DE ESTADOS AMERICANOS (2014) **“Tendencias de Seguridad Cibernética en América Latina y el Caribe”**. EEUU
8. SAMUEL CESAR DA CRUZ JUNIOR (2013) **“Seguridad cibernética Brasil”**
PDF -Brasil
9. SIN (1997). **“Manual de Inteligencia Estratégica, Escuela de Inteligencia Nacional”**. Lima – Perú, 1997.

ANEXOS

- A. Informe profesional
- B. Guía de Entrevista
- C. Resultado de entrevistas, tablas y gráficas.

ESCUELA MILITAR DE CHORRILLOS CORONEL FRANCISCO BOLOGNESI



“Alma Mater del Ejército del Perú”

ANEXO A: INFORME PROFESIONAL PARA OPTAR
EL TÍTULO PROFESIONAL DE LICENCIADO EN CIENCIAS MILITARES

1. DATOS PERSONALES:

1.01	Apellidos y Nombres	LEON PINEDO JORGE ENRIQUE
1.02	Grado y Arma / Servicio	CRL ING
1.03	Situación Militar	RETIRO
1.04	CIP	112625300
1.05	DNI	43271470
1.06	Celular y/o RPM	996381456
1.07	Correo Electrónico	jorgeleonpinedo@hotmail.com

2. ESTUDIOS EN LA ESCUELA MILITAR DE CHORRILLOS:

2.01	Fecha_ ingreso de la EMCH	20 de Marzo de 1,981
2.02	Fecha_ egreso EMCH	12 de Diciembre de 1,984
2.04	Fecha de alta como Oficial	01 de Enero de 1,985
2.05	Años_ experiencia de Oficial	30 años
2.06	Idiomas	ESPAÑOL

3. SERVICIOS PRESTADOS EN EL EJÉRCITO

Nº	Año	Lugar	Unidad / Dependencia	Puesto Desempeñado
3.01	2015	LIMA	COADNE	JEFE OFICINA ADMINISTRATIVA DE

				PROYECTOS
3.02	2014	LIMA	COADNE	JEFE DPTO ASUNTOS CIVILES Y MILITARES
3.03	2013	IQUITOS	V DE	JEFE DPTO PERSONAL
3.04	2012	IQUITOS	RMO	JEFE DPTO RELACIONES PUBLICAS
3.05	2011	LIMA	ACMP	JEFE DPTO SSGG

4. ESTUDIOS EN EL EJÉRCITO DEL PERÚ

Nº	Año	Dependencia y Período	Denominación	Diploma / Certificación
4.01	2014	DINI	INTELIGENCIA ESTRATEGICA	DIPLOMA
4.02	2007	ESCUELA INTELIGENCIA	CURSO SUPERIOR	DIPLOMA
4.03	1998	ESCUELA SUPERIOR DE GUERRA	CCEM	DIPLOMA
4.04	1993	ESCUELA INGENIERIA	CURSO AVANZADO	DIPLOMA
4.05	1991	ESCUELA INTELIGENCIA	CURSO BASICO	DIPLOMA

5. ESTUDIOS DE NIVEL UNIVERSITARIO

Nº	Año	Universidad y Período	Bachiller - Licenciado
5.01			
5.02			

6. ESTUDIOS DE POSTGRADO UNIVERSITARIO

Nº	Año	Universidad y Período	Grado Académico (Maestro – Doctor)
6.01			
6.02			

7. ESTUDIOS DE ESPECIALIZACIÓN

Nº	Año	Dependencia y Período	Diploma o Certificado
7.01			
7.02			

8. ESTUDIOS EN EL EXTRANJERO

Nº	Año	País	Institución Educativa	Grado / Título / Diploma / Certificado
8.01				
8.02				

JORGE ENRIQUE LEON PINEDO
DNI N° 43271470



ANEXO B: GUÍA DE ENTREVISTA – DIE
(Con fines eminentemente académicos)

=====

=====

INFORMACIÓN GENERAL

ENTREVISTADO:

.....

.....

CARGO :

.....

.....

=====

=====

INSTRUCCIONES

Se agradece por anticipado su respuesta concreta y objetiva que contribuirá a optimizar el nivel de desempeño del Personal EP que labora en la Dirección de Inteligencia del Ejército.

=====

Según su opinión:

1. ¿Según su opinión. En qué nivel se encuentra capacitado en Ciberinteligencia el personal que trabaja en la Dirección de Inteligencia del Ejército?

Muy alto Alto Medio Bajo Muy Bajo

2. La Dirección de Inteligencia del Ejército cuenta dentro de su organización con una subdirección donde se produce inteligencia en el campo del Ciberespacio y la Ciberinteligencia?

Si

No

3. ¿Para la ejecución de su trabajo en la Dirección de Inteligencia del Ejército, se aplica las ventajas que ofrece la Ciberinteligencia y el Ciberespacio?

Siempre

Algunas veces

Nunca

4. En qué nivel contribuye la Ciberinteligencia en la recolección de información dentro del proceso de producción de inteligencia en la Dirección de Inteligencia del Ejército?

Muy alto

Alto

Medio

Bajo

Muy Bajo

5. ¿Para la recolección de datos e información durante el proceso de inteligencia en la Dirección de Inteligencia del Ejército se apoya en la Ciberinteligencia? Fundamente su respuesta.

Si

No

6. ¿Cuál es la metodología que usted emplea para el análisis de la información en el Proceso de Inteligencia en la Dirección de Inteligencia del Ejército?

7. Para la diseminación de la información obtenida en el Proceso de Inteligencia a cargo de la Dirección de Inteligencia del Ejército ¿En qué nivel se vale de la Ciberinteligencia?

Bajo

Medio

Alto

8. En base a su experiencia que innovaciones considera Ud. se pueden implementar en la Dirección de Inteligencia del Ejército, para la diseminación de la Información.

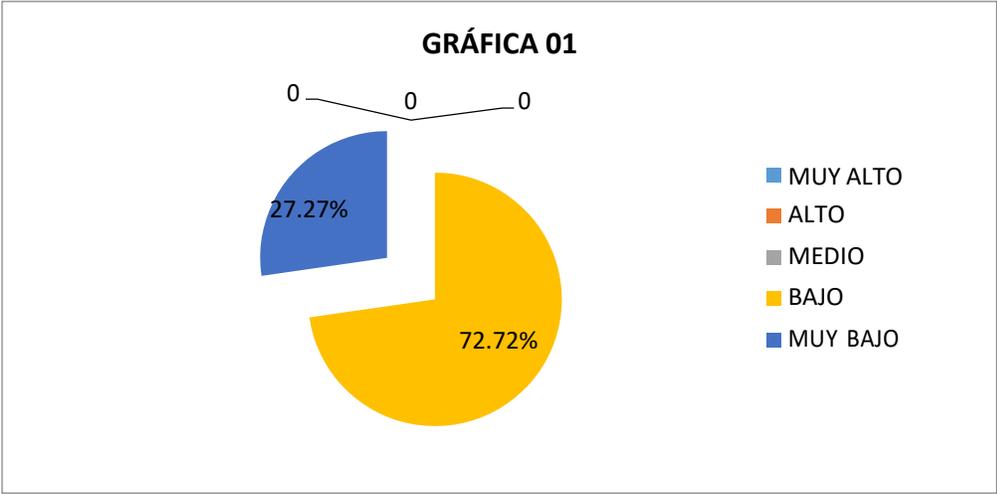
MUCHAS GRACIAS

ANEXO C: TABLA N° 01

ITEM	MUY ALTO	ALTO	MEDIO	BAJO	MUY BAJO	TOTAL
Según su opinión. ¿En qué nivel se encuentra capacitado en Ciberinteligencia el personal que trabaja en la Dirección de Inteligencia del Ejército?	0	0	0	8	3	11
	0	0	0	72.72%	27.27%	100%

FUENTE: ELABORACION PROPIA

El 72.72 % de la muestra opina que el nivel de capacitación en Ciberinteligencia del personal que trabaja en la Dirección de Inteligencia del Ejército es bajo; y el 27.27 % considera que el nivel de capacitación es muy bajo. Lo que evidencia que es necesario capacitar en estos nuevos conceptos al personal de la Dirección de Inteligencia del Ejército.



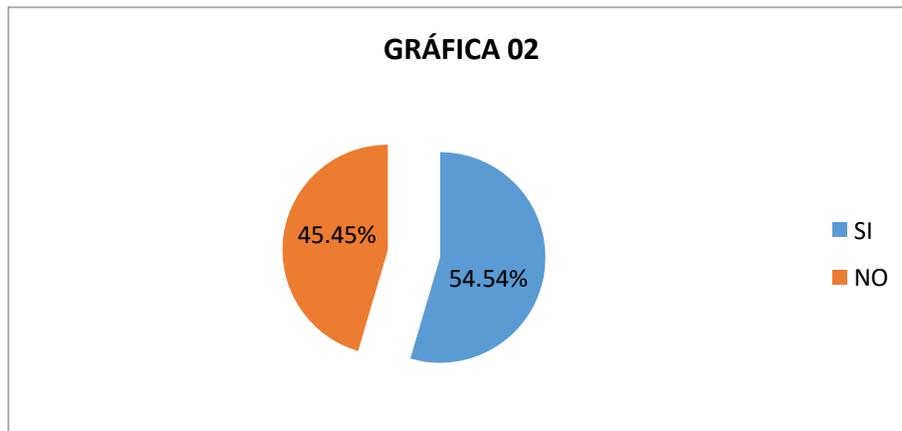
FUENTE: ELABORACION PROPIA

TABLA N° 02

ITEM	SI	NO	TOTAL
¿La Dirección de Inteligencia del Ejército cuenta dentro de su organización con una subdirección donde se produce inteligencia en el campo del Ciberespacio y la Ciberinteligencia?	6 54.54%	5 45.45%	11 100%

FUENTE: ELABORACION PROPIA

El 54.54 % de la muestra opina que en la Dirección de Inteligencia del Ejército dentro de su organización existe una Subdirección donde se produce inteligencia en el campo del Ciberespacio y la Ciberinteligencia; y el 45.45 % considera que no se cuenta con esta Subdirección. Lo que evidencia que el personal confunde la Oficina de Informática y redes con una Subdirección de Ciberinteligencia.



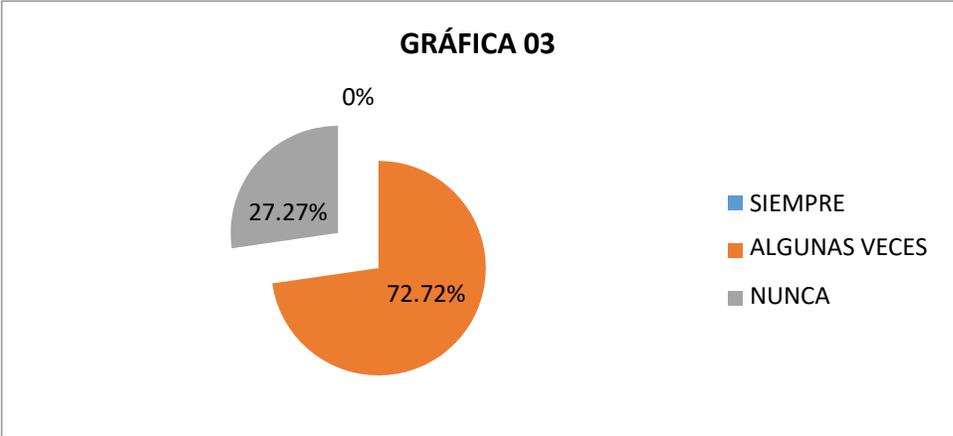
FUENTE: ELABORACION PROPIA

TABLA N°03

ITEM	SIEMPRE	ALGUNAS VECES	NUNCA	TOTAL
¿Para la ejecución de su trabajo en la Dirección de Inteligencia del Ejército, se aplica las ventajas que ofrece la Ciberinteligencia y el Ciberespacio?	0 0	8 72.72%	3 27.27%	11 100%

FUENTE: ELABORACION PROPIA

El 72.72 % de la muestra opina que para la ejecución de su trabajo en la Dirección de Inteligencia del Ejército aplica algunas veces las ventajas que ofrece la Ciberinteligencia y el Ciberespacio; y el 27.27 % considera que en la aplicación de su trabajo nunca se aplican las ventajas de la Ciberinteligencia y el Ciberespacio. Lo que evidencia que es necesario capacitar al personal que labora en la Dirección de Inteligencia del Ejército en las ventajas que ofrece la Ciberinteligencia.



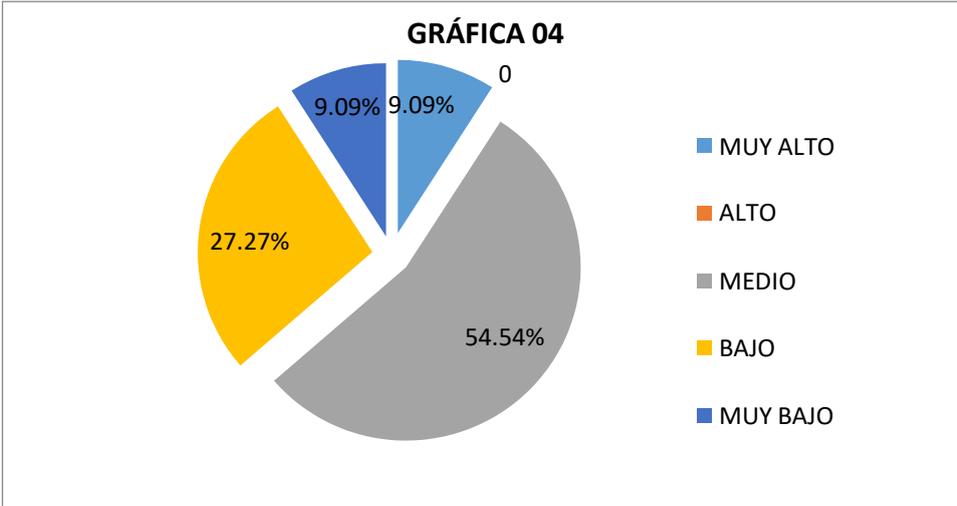
FUENTE: ELABORACION PROPIA

TABLA N° 04

ITEM	MUY ALTO	ALTO	MEDIO	BAJO	MUY BAJO	TOTAL
¿En qué nivel contribuye la Ciberinteligencia en la recolección de información dentro del proceso de producción de inteligencia en la Dirección de Inteligencia del Ejército?	1 9.09%	0 0	6 54.54%	3 27.27%	1 9.09%	11 100%

FUENTE: ELABORACION PROPIA

El 54.54 % de la muestra opina que la Ciberinteligencia contribuye en la Recolección de Información dentro del Proceso de Inteligencia en la Dirección de Inteligencia del Ejército en un nivel medio; el 27.27 % considera que el nivel en que contribuye la Ciberinteligencia es bajo; el 9.09 % considera que el nivel en que contribuye la Ciberinteligencia es muy alto y el 9.09 % de la muestra considera que la Ciberinteligencia contribuye en un nivel muy bajo en la Recolección de Información. Lo que evidencia que es necesario capacitar en estos nuevos conceptos al personal de la Dirección de Inteligencia del Ejército para que optimice el empleo de estas nuevas herramientas.



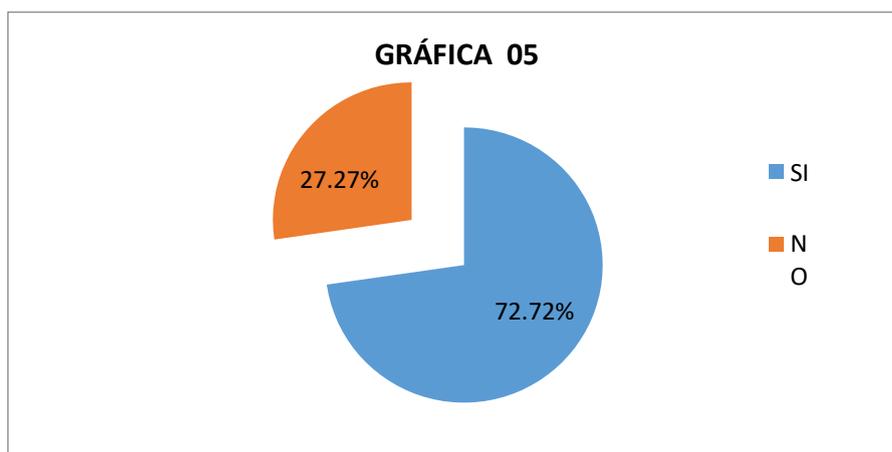
FUENTE: ELABORACION PROPIA

TABLA N° 05

ITEM	SI	NO	TOTAL
¿Para la recolección de datos e información durante el proceso de inteligencia en la Dirección de Inteligencia del Ejército se apoya en la Ciberinteligencia? Fundamente su respuesta.	8 72.72%	3 27.27%	11 100%

FUENTE: ELABORACION PROPIA

El 72.72 % de la muestra opina que para la recolección de datos e información durante el Proceso de Inteligencia en la Dirección de Inteligencia del Ejército se apoya en la ciberinteligencia; y el 27.27 % considera que no se apoya. Lo que evidencia que es necesario capacitar en estos nuevos conceptos al personal de la Dirección de Inteligencia del Ejército.



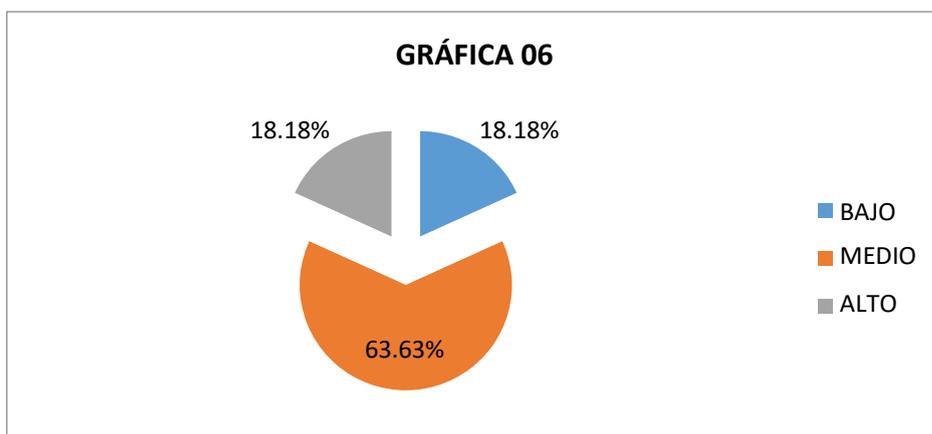
FUENTE: ELABORACION PROPIA

TABLA N° 06

ITEM	BAJO	MEDIO	ALTO	TOTAL
Para la disseminación de la información obtenida en el Proceso de Inteligencia a cargo de la Dirección de Inteligencia del Ejército ¿En qué nivel se vale de la Ciberinteligencia?	2	7	2	11
	18.18%	63.63%	18.18%	100%

FUENTE: ELABORACION PROPIA

El 63.63 % de la muestra opina que el nivel que se vale de la Ciberinteligencia para la disseminación de la información obtenida en el proceso de inteligencia a cargo de la Dirección de Inteligencia del Ejército es medio; el 18.18 % considera que el nivel que se vale de la Ciberinteligencia es alto y el 18.18 % considera que el nivel que se vale de la Ciberinteligencia es bajo. Lo que evidencia que es necesario capacitar en estos nuevos conceptos al personal de la Dirección de Inteligencia del Ejército.



FUENTE: ELABORACION PROPIA

RESULTADO DE ENTREVISTAS

TABLA N° 07

ENTREVISTADO	Según su opinión. ¿En qué nivel se encuentra capacitado en Ciberinteligencia el personal que trabaja en la Dirección de Inteligencia del Ejército?
Tco. JUAREZ José Percy Jefe Departamento Telemática de la SD IT - DIE	“El personal se encuentra en proceso de capacitación para desarrollar sistemas informáticos, pero no en las técnicas para poder ser empleados como auditores informáticos”
Tco. 1ra. QUINTANA PALOMINO Hernán Jefe Departamento	“El personal se encuentra capacitado de acuerdo a sus necesidades”
Tco. 2da. QUISPE TORRES Julio CIBERDEFENSA	“No opina”
PORTOCARRERO RIOS Fredy Inteligencia Técnica	“Falta capacitación”
ORDINOLA MORALES Honorato Administrativo	“Se encuentra en un nivel bajo, por falta de capacitación”
Tco. 3ra CASTRO YAULI Telemática	“No se encuentra capacitado”
OSORIO CASTEÑEDA Marco	“No opina”
GONZALES TINEO Freddy Departamento de Telemática	“No opina”
NINA CUSACANI Jhon Departamento Telemática	“Falta de capacitación en Ciberdefensa y Ciberataque”
SO3. QUINTANA MARQUEZ Gary CIBERDEFENSA	“Baja. No existen las capacitaciones progresivas”
	“Bajo. Por falta de capacitación en

RAMOS ANTON Jack REDES	Ciberinteligencia, la mayoría desconoce del concepto”
---------------------------	----------------------------------------------------------

FUENTE: ELABORACION PROPIA

Las opiniones coinciden casi en su totalidad, indicando que falta capacitación, que el nivel de capacitación del personal que labora en la Dirección de Inteligencia del Ejército es bajo o que no se encuentran capacitados. Los agentes que tienen mayor experiencia si manifiestan estar algo capacitados. Por lo que se infiere que es necesario capacitar en estos nuevos conceptos al personal de la Dirección de Inteligencia del Ejército.

TABLA N° 08

<p>ENTREVISTADO</p>	<p>¿Para la recolección de datos e información durante el proceso de inteligencia en la Dirección de Inteligencia del Ejército se apoya en la Ciberinteligencia?. Fundamente su respuesta</p>
<p>Tco. JUAREZ José Percy Jefe Departamento Telemática de la SD IT – DIE</p>	<p>“En internet podemos encontrar fuentes de información que nos ayudan a cumplir con el ciclo de inteligencia, particularmente durante el procesamiento de la información”</p>
<p>Tco. 1ra. QUINTANA PALOMINO Hernán Jefe Departamento</p>	<p>“Si, se apoyó a corto alcance”</p>
<p>Tco. 2da. QUISPE TORRES Julio CIBERDEFENSA</p>	<p>“Se apoya en la Ciberinteligencia en un 25%, por obtención de fuentes abiertas cibernéticas, por ser más económicos”.</p>
<p>PORTOCARRERO RIOS Fredy Inteligencia Técnica</p>	<p>“La información es recopilada por la internet”</p>
<p>ORDINOLA MORALES Honorato Administrativo</p>	<p>“Porque a través de internet podemos encontrar las herramientas necesarias para el cumplimiento del ciclo de inteligencia”</p>
<p>Tco. 3ra CASTRO YAULI Telemática</p>	<p>“No se realiza por no contar con personal capacitado en Ciberinteligencia”</p>
<p>OSORIO CASTENEDA Marco</p>	<p>“No opina”</p>
<p>GONZALES TINEO Freddy Departamento de Telemática</p>	<p>“No opina”</p>
<p>NINA CUSACANI Jhon</p>	<p>“La información que se procesa en su</p>

Departamento Telemática	mayoría de fuente abierta”
SO3. QUINTANA MARQUEZ Gary CIBERDEFENSA	“Para la recolección de datos usamos la internet para procesar información”
RAMOS ANTON Jack REDES	“Si, porque navegamos en la nube para la veracidad de información y extraer o aumentar la veracidad de la información”

FUENTE: ELABORACION PROPIA

La mayoría de los entrevistados coinciden en su respuesta al manifestar que para la recolección de datos e información recurren al internet, pero desconocen el resto de herramientas que ofrece la ciberinteligencia. Por lo que se infiere que es necesario difundir la nueva doctrina y capacitar en el empleo de las nuevas herramientas que ofrece la Ciberinteligencia al todo el personal de la Dirección de Inteligencia del Ejército.

TABLA N° 09

<p>ENTREVISTADO</p>	<p>¿Cuál es la metodología que usted emplea para el análisis de la información en el Proceso de Inteligencia en la Dirección de Inteligencia del Ejército?</p>
<p>Tco. JUAREZ José Percy Jefe Departamento Telemática de la SD IT - DIE</p>	<p>“Se emplea el internet como herramienta de trabajo para procesar o contrarrestar la información que se ha obtenido con la finalidad de obtener una buena inteligencia resultante durante el análisis”</p>
<p>Tco. 1ra. QUINTANA PALOMINO Hernán Jefe Departamento</p>	<p>“No Opina”</p>
<p>Tco. 2da. QUISPE TORRES Julio CIBERDEFENSA</p>	<p>“Determinación de la información; qué, cuándo, dónde y cómo, veracidad mediante cruces de información. Evaluar y analizar según el interés; determinar los EEI y ONI y difundir la información oportuna”</p>
<p>PORTOCARRERO RIOS Fredy Inteligencia Técnica</p>	<p>“Por la internet, confrontando la información”</p>
<p>ORDINOLA MORALES Honorato Administrativo</p>	<p>“Se emplea el internet para analizar la información obtenida”</p>
<p>Tco. 3ra CASTRO YAULI Telemática</p>	<p>“Actualmente, no realizo análisis de la información en el proceso de inteligencia”</p>
<p>OSORIO CASTEÑEDA Marco</p>	<p>“Por el campo de empleo y desempeño no realizo análisis”</p>
<p>GONZALES TINEO Freddy</p>	<p>“Ante una información, el proceso que</p>

Departamento de Telemática	se realiza es la verificación utilizando el internet, el cual nos brinda una amplia constatación de la información obtenida”
NINA CUSACANI Jhon Departamento Telemática	“Se realiza análisis de información mediante el uso de internet para contrastar la información”
SO3. QUINTANA MARQUEZ Gary CIBERDEFENSA	“La internet para confrontar y luego procesar la información”
RAMOS ANTON Jack REDES	“La internet para seguir el ciclo de inteligencia”

FUENTE: ELABORACION PROPIA

El personal de agentes que realiza el análisis de la información coincide en que para realizar su trabajo recurren como metodología al internet para contrastar la información obtenida con la que circula en los medios de fuente abierta. Por lo que se puede inferir que el personal desconoce las demás herramientas que nos ofrece la Ciberinteligencia las cuales adecuadamente aprovechadas por nuestro personal permitiría optimizar su metodología de trabajo

TABLA N° 10

<p align="center">ENTREVISTADO</p>	<p>En base a su experiencia que innovaciones considera Ud. se pueden implementar en la Dirección de Inteligencia del Ejército, para la diseminación de la Información.</p>
<p>Tco. JUAREZ José Percy Jefe Departamento Telemática de la SD IT – DIE</p>	<p>“Paralelamente a la diseminación que efectúa la sección criptográfica esta debería ser complementada con una base de datos. Asimismo, capacitar al personal en sistemas de información para que puedan desarrollar software que complementen o innoven la actual diseminación que se efectúa, paralelamente se debe implementar con equipos informáticos de última generación”</p>
<p>Tco. 1ra. QUINTANA PALOMINO Hernán Jefe Departamento</p>	<p>“Crear un departamento con personal capacitado dedicado a la diseminación de informaciones”</p>
<p>Tco. 2da. QUISPE TORRES Julio CIBERDEFENSA</p>	<p>“Crear un departamento con personal capacitado en sistemas, en base de datos, administración de redes y ciberseguridad con la finalidad de crear nuestro software según nuestras necesidades. Asimismo dotar de equipos de última generación”</p>
<p>PORTOCARRERO RIOS Fredy Inteligencia Técnica</p>	<p>“Una constante preparación al personal”</p>
<p>ORDINOLA MORALES Honorato Administrativo</p>	<p>“Que se capacite al personal periódicamente en sistemas, base de</p>

	datos y redes, así como la implementación de equipos informáticos de última generación”
Tco. 3ra CASTRO YAULI Telemática	“Actualmente la disseminación de información se realiza a través de nuestra red interna. Se podría considerar utilizar un software de cifrado interno de modo que la información sea guardada en claro”
OSORIO CASTEÑEDA Marco	“Si, porque sería o complementaría las fases y proceso de inteligencia”
GONZALES TINEO Freddy Departamento de Telemática	“Que se implemente en la adquisición de computadoras de última generación, asimismo en la capacitación de personal en el área de TICD (Tecnología de información y comunicaciones)”
NINA CUSACANI Jhon Departamento Telemática	“Capacitación del personal en el área de tecnología de información y comunicación; y computadoras de última generación”
SO3. QUINTANA MARQUEZ Gary CIBERDEFENSA	“Capacitación constante y motivación al personal”
RAMOS ANTON Jack REDES	“La inteligencia en informática va con la tecnología, se puede implementarla tanto en tecnología como capacitación a personal que tenga la vocación en informática”

FUENTE: ELABORACION PROPIA

Las respuestas son diversas, entre las que se puede destacar las siguientes innovaciones; capacitación del personal de la Dirección de Inteligencia del Ejército que intervienen directamente en el proceso de inteligencia en Ciberinteligencia y todas las herramientas que este nuevo dominio se vale.

Paralelamente, mejorar la infraestructura relacionada a equipamiento de última generación y tecnología de punta, a fin de maximizar el empleo de las herramientas que nos ofrece la ciberinteligencia.

Por lo que se puede inferir que con personal altamente capacitado, con la infraestructura en recursos humanos, recursos materiales adecuados y de última generación vamos a optimizar la aplicación de la Ciberinteligencia en el Proceso de Inteligencia en la Dirección de Inteligencia del Ejército haciéndola más eficiente y eficaz.



ESCUELA MILITAR DE CHORRILLOS
“CORONEL FRANCISCO BOLOGNESI”

DEPARTAMENTO DE INVESTIGACION Y DOCTRINA

**FORMATO DE AUTORIZACION PARA LA PUBLICACION EN EL
REPOSITORIO DIGITAL DE LA EMCH “CFB”**

Formato de autorización para la publicación electrónica en la página web del Repositorio Institucional Digital de la Escuela Militar de Chorrillos “Coronel Francisco Bolognesi” de conformidad con el Decreto Legislativo N° 822, sobre la Ley de los Derechos Autor, Ley N° 30035 del Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso y Reglamento del Registro Nacional de Trabajos de Investigación para optar grados académicos y títulos profesionales – RENATI.

Datos del autor

Apellidos y Nombres	León Pinedo Jorge Enrique
DNI N° 43271470	Teléfono : 996381456
Correo electrónico	jorgeleonpinedo@hotmail.com

1. Datos Académicos

Título: APLICACIÓN DE LA CIBERINTELIGENCIA EN EL PROCESO DE INTELIGENCIA EN LA DIRECCIÓN DE INTELIGENCIA DEL EJÉRCITO DEL PERÚ
Tipo de obra: Trabajo de suficiencia profesional
Cantidad de páginas: 72
Asesor: Trabajo de Suficiencia Profesional
Fecha de sustentación: Trabajo de Suficiencia Profesional
Año de publicación: 2018

2. Declaraciones:

El autor declara que:

- **La obra es original y de mi propia y exclusiva creación, realizándose**

sin violar u usurpar derechos de autor de terceros

- Con la obra no se ha quebrantado ningún derecho moral o patrimonial del autor.
- No contiene declaraciones difamatorias contra terceros y respeta el derecho a la imagen, intimidad, buen nombre y demás derechos constitucionales de las personas.
- Soy titular de los derechos patrimoniales sobre la obra, y no pesa ningún gravamen sobre ella.
- La información en ella contenida tiene carácter confidencial.

Por tanto, todo lo señalado en el presente formato, en especial lo descrito en el numeral dos, ostenta la condición de Declaración Jurada. Por ello, me comprometo a salir en defensa de LA ESCUELA MILITAR DE CHORRILLOS “Coronel Francisco Bolognesi” ante cualquier reclamación de terceros que al respecto pudiere sobrevenir. Para todos los efectos LA ESCUELA MILITAR DE CHORRILLOS “CFB” actúa como tercero de buena fe.

3. Publicación de su investigación en el Repositorio Digital RENATI de la SUNEDU.

TIP DE ACCESO A SU INVESTIGACION

Acceso abierto

Acceso restringido

JUSTIFICACION

Personal

En señal de conformidad

JORGE LEON PINEDO
DNI N° 43271470