Importancia de implementar la Ciberdefensa en las Unidades Operativas Mayores del Ejército de Colombia

Andrés Mauricio Avilés Ramírez
Lewis Chaith Mahecha Ardila
Rafael Enrique Niño Zea
Ricardo Esleanny Ordoñez Ordoñez

Trabajo de grado para optar al título profesional:
Especialización en Seguridad y Defensa Nacionales

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

2017

TRABAJO DE GRADO

IMPORTANCIA DE IMPLEMENTAR LA CIBERDEFENSA EN LAS UNIDADES OPERATIVAS MAYORES DEL EJÉRCITO DE COLOMBIA

ANDRÉS MAURICIO AVILÉS RAMÍREZ
LEWIS CHAITH MAHECHA ARDILA
RAFAEL ENRIQUE NIÑO ZEA
RICARDO ESLEANNY ORDOÑEZ ORDOÑEZ

ESPECIALIZACIÓN EN SEGURIDAD Y DEFENSA NACIONAL
ESCUELA SUPERIOR DE GUERRA
COMANDO GENERAL DE LAS FUERZAS MILITARES
BOGOTÁ D.C.- 2017

IMPORTANCIA DE IMPLEMENTAR LA CIBERDEFENSA EN LAS UNIDADES OPERATIVAS MAYORES DEL EJÉRCITO DE COLOMBIA

ESPECIALIZACIÓN EN SEGURIDAD Y DEFENSA NACIONAL

ESCUELA SUPERIOR DE GUERRA

COMANDO GENERAL DE LAS FUERZAS MILITARES

BOGOTÁ D.C.- 2017

IMPORTANCIA DE IMPLEMENTAR LA CIBERDEFENSA EN LAS UNIDADES OPERATIVAS MAYORES DEL EJÉRCITO DE COLOMBIA

Trabajo de grado para optar el título de Especialista en Seguridad y Defensa Nacional

ESPECIALIZACIÓN EN SEGURIDAD Y DEFENSA NACIONAL

ESCUELA SUPERIOR DE GUERRA

COMANDO GENERAL DE LAS FUERZAS MILITARES

BOGOTÁ D.C.- 2017

IMPORTANCIA DE IMPLEMENTAR LA CIBERDEFENSA EN LAS UNIDADES OPERATIVAS MAYORES DEL EJÉRCITO DE COLOMBIA

Trabajo de grado para optar el título de Especialista en Seguridad y Defensa Nacional

ESPECIALIZACIÓN EN SEGURIDAD Y DEFENSA NACIONAL

ESCUELA SUPERIOR DE GUERRA

COMANDO GENERAL DE LAS FUERZAS MILITARES

BOGOTÁ D.C.- 2017

IMPORTANCIA DE IMPLEMENTAR LA CIBERDEFENSA EN LAS UNIDADES OPERATIVAS MAYORES DEL EJÉRCITO DE COLOMBIA

Andrés Mauricio Avilés Ramírez [1]

Lewis Chaith Mahecha Ardila [2]

Rafael Enrique Niño Zea [3]

Ricardo Esleanny Ordoñez Ordoñez [4]

Resumen

Este trabajo pretende determinar la importancia de implementar la ciberdefensa en las Unidades Operativas Mayores (en adelante: UOM) del Ejército Nacional a través de la estructura implementada en el Comando de la Fuerza para contrarrestar los diferentes ataques cibernéticos; de organizaciones criminales, como de amenazas transnacionales partiendo del resultado de analizar los diferentes ataques cibernéticos que el Ejército Nacional ha sufrido en la red informática desde el año 2015, posteriormente analizaremos los beneficios de implementar la ciberdefensa en las Unidades Operativas Mayores del Ejército Colombiano, para lo cual, se realizará un estudio de la situación actual de la ciberdefensa en las UOM y finalmente determinaremos las recomendaciones para mitigar las falencias en ciberdefensa de

[1] Mayor Ejército Nacional de Colombia, Escuela Superior de Guerra.
Correo: andresmar_76@hotmail.com
[2] Mayor Ejército Nacional de Colombia, Escuela Superior de Guerra.
Correo: lewischma@gmail.com
[3] Mayor Ejército Nacional de Colombia, Escuela Superior de Guerra.
Correo: renz7418@hotmail.com
[4] Mayor Ejército Nacional de Colombia, Escuela Superior de Guerra.
Correo: ricardo151979@hotmail.com

las UOM del Ejército de Colombia. Igualmente, para la organización, es fundamental tener claro su marco jurídico y el campo de acción en relación al contexto de la ciberdefensa en Colombia.

Palabras claves: Ciberdefensa – Red Informática – Ataques Cibernéticos

Abstract

This paper work intends to determinate the importance of implementing the sections of Cyber-defense in the Major Operatives Units (MOU on ahead) of the Colombian Army through the structure of Command, Control, support, communication and cyber-defensa implemented by the Command of the Colombian Army to counter different cyberattacks from the criminal organizations, starting from the analysis result of different cyber-attacks against Colombian Army computer network that it has suffered since 2015; Later, we will analyze the benefits of implementing the Cyber-Defense into the Colombian Army's MOU, for which we will do a study of the current Cyber Defense situation into the UOM will be carried out and finally we will determine the recommendations to mitigate the cyber-defense weaknesses into the MOU of the Colombian Army. Equally for the organization, it is essential to be clear about its legal framework and the action field into the context of the Cyber-defense in Colombia.

Keywords: Ciberdefensa - Computer Networking - Cyber Attacks.

Introducción

La ciberdefensa ha evolucionado durante el siglo XXI a nivel local, regional y global de manera trascendental, lo cual ha repercutido en la seguridad y defensa del Estado colombiano; el cual, a través de las Fuerzas Militares y en este caso del Ejército Nacional, debe contrarrestar el accionar de las diferentes amenazas de grupos delincuenciales y terroristas que pretenden atacar la red informática para obstaculizar los diferentes canales de comunicación con los cuales dispone la Fuerza para cumplir con su misión constitucional.

Este documento tiene por objeto determinar los beneficios de implementar la ciberdefensa en las Unidades Operativas Mayores del Ejército Nacional, a través de la estructura implementada en el Comando de la Fuerza para contrarrestar los diferentes ataques cibernéticos, para lo cual, en la primera parte del documento se hará una breve presentación del marco referencial de la investigación partiendo desde un ámbito general teórico, conceptual y jurídico de la ciberdefensa y los lineamientos generales estipulados en los documentos CONPES 3701 y CONPES 3854 del gobierno Nacional.

Posteriormente se abarcara, la ciberdefensa en otros países y en el Comando General de las Fuerzas Militares y la estructura de ciberdefensa que fue implementada por el Ejército Nacional desde el año 2016; así mismo, los diferentes ataques cibernéticos que el Ejército Nacional ha sufrido en la red informática desde dicho año, basados en la consolidación de los datos estadísticos que la Fuerza ha establecido y los beneficios que la ciberdefensa ha traído desde su implementación en el Ejército Nacional en concordancia con el cumplimiento de su misión constitucional y se profundizará a partir de la estructura organizacional de las Unidades

Operativas Mayores y la realización de una encuesta a los Oficiales de Comunicaciones de dichas Unidades determinar la situación actual de esta unidades en el área de ciberdefensa .

Finalmente, se presentan las recomendaciones para mitigar las falencias de las Unidades Operativas Mayores del Ejército de Colombia en el área de ciberdefensa determinando los beneficios de implementar la ciberdefensa en las Unidades Operativas Mayores del Ejército Nacional para contrarrestar los diferentes ataques cibernéticos que se presentan en la Fuerza para generar mejores prácticas en el empleo de los diferentes equipos y herramientas tecnológicas con las que cuentan para potencializar el poder defensivo en el espectro del ciberespacio, generando un cambio cultural en el recurso humano y el empleo de los sistemas de comunicación de forma segura a la par de los avances tecnológicos en un mundo cada día más globalizado.

Importancia de la ciberdefensa

Durante las últimas décadas, el crecimiento y desarrollo de las Tecnologías de la Información y las Comunicaciones (TIC), tanto a nivel internacional como a nivel nacional en los diferentes sectores públicos y privados han generado una dependencia de las TIC al cumplimiento de las diferentes misiones y de su funcionamiento, es así que en el caso de la seguridad y defensa para el caso de las Fuerzas Militares y en el Ejército Nacional no han sido la excepción razón por la cual las vulnerabilidades y los riesgos en relación a la información, las redes informáticas y la infraestructura cibernética siempre deben estar en continua transformación e implementación de medidas activas y pasivas, de ahí la importancia de la implementación efectiva de la ciberdefensa en las diferentes organizaciones y para la presente investigación el Ejército Nacional y las diferentes Unidades Operativas Menores.

Así mismo, las dimensiones de la guerra a nivel externo e interno han mutado "En los conflictos tradicionales normales existen fronteras y límites, mientras que en el ciberespacio no. El ciberespacio es un ambiente único, sin fronteras geográficas, anónimo, asimétrico y puede ser fácilmente clandestino". (Acosta, 2009), por ende, su conocimiento es complejo y requiere de la implementación y uso de medios y métodos tecnológicos adecuados y modernos para proteger el ciberespacio en materia de defensa y seguridad.

Es así, que la importancia de la ciberdefensa bajo en contexto de la seguridad y defensa nacional a nivel internacional y nacional ha ido evolucionando de manera sistemática teniendo en cuenta los nuevos escenarios de las guerras como lo es "La guerra cibernética ya hacía furor a finales de los años 90, pero se desvaneció desde el 11-S y con el terrorismo islámico." (Acosta, 2009).

Países como Francia, Estados Unidos de América, Reino Unido, Alemania, España, Noruega, la Unión Europea, Rusia, China, India , entre otros han desarrollado diferentes estrategias para implementar de manera efectiva la ciberdefensa dentro de sus estructuras de defensa y seguridad, "La llegada de Barack Obama a la presidencia del país ha supuesto un aumento en la concienciación de la amenaza que supone el mundo cibernético para la seguridad nacional", (Acosta, 2009), enfocándose no solo al ámbito de una guerra regular sino profundizando en el ámbito del terrorismo y las nuevas amenazas como lo es el surgimiento del autodenominado Estado Islámico.

De igual forma se presentan casos como los acontecidos en Estonia:

> El mes de abril de 2007, el gobierno de Estonia sufrió el que es considerado el mayor ataque cibernético de la historia, en el cual se vieron afectados la presidencia, el parlamento, la mayoría de los ministerios, los partidos políticos y dos de sus grandes bancos. (CONPES, 2011).

Eventos que hacen que se cambie la dinámica en los diferentes países en la implementación de la ciberdefensa de manera más contundente.

Para el caso colombiano, a partir del CONPES 3701 del año 2011, se establecen unos lineamientos de la política para Ciberseguridad y ciberdefensa, orientado a "desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país". (CONPES, 2011). teniendo en cuenta el aumento del uso de las TIC a nivel nacional "en Colombia se ha incrementado considerablemente el uso de tecnologías de la información y las comunicaciones elevando su nivel de exposición a amenazas cibernéticas. El número de usuarios de internet aumentó en 354% entre el 2005 y el 2009". (CONPES, 2011).

De igual forma a partir del empleo de las TIC se han suscitado a nivel nacional diferentes ataques cibernéticos con el fin de destruir y obstaculizar el normal funcionamiento de las diferentes entidades del Estado:

> Un caso a resaltar fue el ocurrido durante el primer semestre de 2011, cuando el grupo "hacktivista" autodenominado anonymous atacó a los portales de la Presidencia de la República, el Senado de la República, Gobierno en Línea y de los Ministerios del Interior y Justicia, Cultura y Defensa, dejando fuera de servicio sus páginas web por varias horas, (CONPES, 2011).

Aspectos que hacen imperativo la adopción de estrategias más agresivas en la implantación de la ciberdefensa en las diferentes organizaciones tanto públicas como privadas del país y es lo que respecta a esta investigación en el Ejército Nacional dentro del cumplimiento de su misión en relación con la seguridad y defensa nacional.

Política Pública Nacional de Ciberseguridad y Ciberdefensa

En el 2011, el Gobierno Nacional expidió el Documento CONPES 3701 "Lineamientos de política para ciberseguridad y ciberdefensa", así mismo el documento CONPES 3854 "Política Nacional de Seguridad Digital", publicado en el año 2016; del último se destaca que "Las principales entidades ejecutoras de esta política son el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa Nacional, la Dirección Nacional de Inteligencia y el Departamento Nacional de Planeación", (CONPES 3854, 2016), y dicha política de ciberseguridad y ciberdefensa va enfocada a contrarrestar el incremento de las amenazas cibernéticas en relación a la defensa del país, la lucha contra el cibercrímen y la gestión del riesgo en el entorno digital, bajo un direccionamiento armónico social, económico y tecnológico

de crecimiento del país, generando un marco institucional de seguridad digital lo cual de acuerdo a lo que se establece en dicho CONPES fortalecerá la defensa y seguridad nacional en el entorno digital, a nivel nacional y transnacional, generando también mecanismos permanentes para impulsar la cooperación, la colaboración y la asistencia en materia de seguridad digital, a nivel nacional e internacional.

De igual forma se visualiza un crecimiento notable en el crecimiento global en el uso de las TIC aspecto que requiere cada día de políticas más activas y dinámicas en relación a ciberseguridad y ciberdefensa, crecimiento que va alineado con los diferentes campos de poder del Estado Colombiano y en el caso particular del sector de defensa y seguridad.

Proyecciones de algunos Indicadores de uso de las TIC a nivel global

Proyecciones	2015	2020	Incremento porcentual
Más usuarios de banda ancha móvil	3 mil millones	4 mil millones	33%
Más terminales conectados	16,3 mil millones	24,4 mil millones	49%
Más datos generados	8,8 zettabytes	44 zettabytes	400%
Más tráfico IP de red (mensual)	72,4 exabytes	168 exabytes	132%
Dispositivos (Internet de las cosas)	15 mil millones	200 mil millones[a]	1200%
Tamaño del mercado de la nube pública global	USD 97 mil millones	USD 159 mil millones	63%

Figura N. 1 Tics a nivel global. *Fuente:* CONPES 3854 (2016, p. 11)

Así mismo, el crecimiento en ataques informáticos ha crecido, razón por la cual la política de seguridad digital en relación a la ciberdefensa y ciberseguridad cada día debe ser más efectiva y eficaz ante el actuar de los diferentes factores y amenazas cibernéticas existentes a nivel nacional e internacional, toda vez que la respuesta a las mismas mitigara o no el accionar

de criminalidad de dichas amenazas y se evidencia en la presente tabla tabla un consolidado de algunos de los ataques cibernéticos a nivel mundial los cuales son un referente de la importancia en la planeación, estructuración, ejecución y evaluación de políticas de seguridad digital en Colombia.

Grandes casos de ataque cibernéticos en el mundo en el 2014

Organización afectada	Sector	Impacto
Snapchat	Red social	4,5 millones de nombres y numeros moviles comprometidos
Kickstarter	*Crowd funding*	5,6 millones de victimas
Korean Telecom	Telecomunicaciones	12 millones de suscriptores comprometidos
Heartbleed	*Software*	Primera de tres vulnerabilidades de fuente abierta
Ebay	Compras	Base de datos de 145 millones de compradores comprometida
PF chang's	Comidas	Más alta violación de información de alto nivel del mes
Energetic bear	Energia	Operación de ciberespionaje a la industria de energia
Cybervor	Tecnologia	1,2 billones de credenciales comprometidas
iCloud	Entretenimiento	Cuentas de celebridades comprometidas
Sandworm	Tecnología	Ataque cibernético a la vulnerabilidad de Windows
Sony Pictures	Entretenimiento	Más alta violación de alto nivel del año
Inception Framework	Sector publico	Operación de ciberespionaje a sector publico

Figura N. 2 Ataques cibernéticos en el Mundo *Fuente*: CONPES 3854 (2016, p. 12)

La ciberdefensa en el contexto internacional

Hace aproximadamente 2500 años, el famoso estratega Sunt Zut acuñó esta frase, "El supremo arte de la guerra es someter al enemigo sin combatir" (Biblioteca Virtual Universal, 2003).

Hemos podido ver que a lo largo de la humanidad la guerra ha sido combatida en diferentes formas con armas convencionales y sobre el terreno; hoy en día, hablamos de una

guerra distinta que no se combate físicamente, se combate tecnológicamente en un campo de batalla virtual pero real. Una guerra que ha sobrepasado los gobiernos porque no se sabe cómo controlarla, esta es la guerra cibernética la guerra del futuro. En el fondo la ciberguerra se parece a todas las demás guerras en cuanto que los gobiernos temen a las armas secretas del enemigo y por esta razón se recurre a los espías, pero en esta ocasión sin maletines, ni agentes a cubierta; por ende, los métodos cambian. Para el mundo ciber, las fronteras no existen ni mucho menos enemigos lejanos y cercanos.

A lo largo de los siglos, se han ido perfeccionando las técnicas de combate y el armamento, y cada vez se fueron inventando armas más precisas y sofisticadas para hacer la guerra en el terreno. Posteriormente, se implementa la fuerza naval como un segundo poder estratégico como dominio de la guerra, iniciando con botes a remo, luego las embarcaciones de propulsión a velas y en la edad media la artillería naval. Para el siglo XIX surge la propulsión a vapor como una revolución.

Posteriormente en el siglo XX aparece el submarino como poder contundente y decisivo, al igual que la táctica y estrategia naval han de evolucionar notablemente con la aviación naval, los misiles, las comunicaciones satelitales y la implementación de nuevas tecnologías de la época (Oyarzún, 2006). Solo hasta el siglo XX, el aire se convierte en un campo de batalla; hasta entonces sólo había sido el escenario de observación a distancia de objetivos en el campo terrestre.

Como en los casos anteriores, la evolución continua de la tecnología ha obligado a revisar y replantear los conceptos doctrinales que rigen el combate, los radares, los misiles y últimamente las aeronaves no tripuladas (López, 2002). A finales del siglo XX, las Fuerzas

Militares de las grandes potencias, centran la atención en el espacio implementado las comunicaciones satelitales para garantizar el mando, y control a las operaciones militares; como también para las operaciones de inteligencia para la obtención de información enemiga, apoyándose en los satélites de observación. Las potencias más avanzadas como Rusia y EEUU desarrollan capacidades para impedir el uso de estos medios al enemigo (Yagüe, 2009).

Ya para finales del XX y comienzos del siglo XXI, aparece el quinto dominio de la guerra: el Ciberespacio. Siendo este un medio, en el que como los anteriores, se puede combatir para defender los intereses propios de un Estado del enemigo. El Ciberespacio, puede tener gran influencia en los otros cuatro dominios pero que tiene unas grandes peculiaridades que lo hacen completamente diferentes a los otros dominios (Tecnología, 2010).

Una de sus peculiaridades es que lo hace completamente infinito, que no tiene fronteras definidas y en el que se emplean técnicas y armas de batalla completamente diferentes a los que se emplean en los campos tradicionales, no existe ningún tipo de control armamentístico, ni definición de grupos u organizaciones, como de individuos aislados, tienen capacidad potencial de hacer daño y en algunos casos unos daños muy graves contra la seguridad y defensa de un estado. A esto se le suma una ausencia una notable carencia del marco legal con el cual, se pueda ejercer el debido control quedando en evidencia la falta de autoridad legal beneficiando del agresor. Este es un dominio, del cual no es ajena ninguna entidad y/o actividad del Estado debido a que todas estas, se apoyan y/o dependen en pequeña o gran medida del ciberespacio. Transportes, comunicaciones, producción y distribución de energía, el comercio, la sanidad, los medios de comunicación social, inclusive el deporte y el ocio.

Lo más transcendental de todo lo anterior, es que pone en primera línea de combate el corazón de una nación. Desafortunadamente no hay ninguna herramienta técnica o específica que se pueda emplear en el ciberespacio en el ámbito militar. Y así como en los otros dominios de la guerra, el armamento está en poder de los ejércitos, en el ciberespacio, son muchos los actores quienes son poseedores de estas armas; muchos de ellos no son militares quienes hacen daño motivados bajo intereses personales o de alguna organización criminal, pero que en razón a la existencia de este campo complicado y difuso, las Fuerzas Militares de las grandes potencias vieron la necesidad de crear los Comandos Conjuntos de Ciberdefensa con el fin de ejercer la acción militar en el ciberespacio, con un ámbito principal de acción de protección y defensa para las redes telemáticas, de sistemas y comunicaciones de las fuerzas armadas. En segundo lugar, la protección y defensa a otras redes y sistemas que afecten la seguridad y defensa nacional.

Estos Comandos Conjuntos están conformados con personal altamente capacitado y equipados de tierra, mar y aire con la misión principal de proteger las redes telemáticas, de sistemas y de comunicaciones; pero en determinadas circunstancias pueden actuar y responder contra ciberamenazas y ciberagresiones que atenten a la seguridad nacional. Una de las misiones asignadas a estos Comandos Conjuntos de Ciberdefensa de estas grandes potencias, es la defensa y restauración de los sistemas de las Fuerzas Militares, pero no como única restricción, sino que también a otros sistemas que afecten la seguridad y defensa de la nación. Como principal responsabilidad, la obtención, análisis y explotación de información de posibles ciberataques a los sistemas que afecten los intereses nacionales y la seguridad y defensa de la nación.

Otra responsabilidad es la respuesta oportuna y proporcionada ante ciberataques o ciberagresiones.

Dirigir y coordinar las actividades de los diferentes centros de todas las fuerzas armadas.

Representar al Ministerio de defensa liderando la cooperación con otros organismos nacionales e internacionales en materia de ciberdefensa

Las Fuerzas Militares son los responsables, de concientizar, de dirigir y coordinar, la formación y entrenamiento especializado en ciberdefensa al personal de las fuerzas armadas concientizar (Nacional, 2013)

Estructura de ciberdefensa actual del Ejército Nacional

En relación al tema organizacional de ciberdefensa adicional a lo establecido por el gobierno nacional en el CONPES 3701 "Lineamientos de política para ciberseguridad y ciberdefensa", del 2011 y el CONPES 3854 "Política Nacional de Seguridad Digital", del 2016; el Ejército Nacional dentro de su proceso de transformación y estructuración y en especial en su nueva organización incluye la ciberdefensa dentro de su organización estratégica como parte del Comando de Apoyo Operacional de Comunicaciones y ciberdefensa perteneciente a la Jefatura de Estado Mayor de Operaciones del Ejército Nacional, lo cual se evidencia en las estructuras organizacionales que se presentan a continuación.

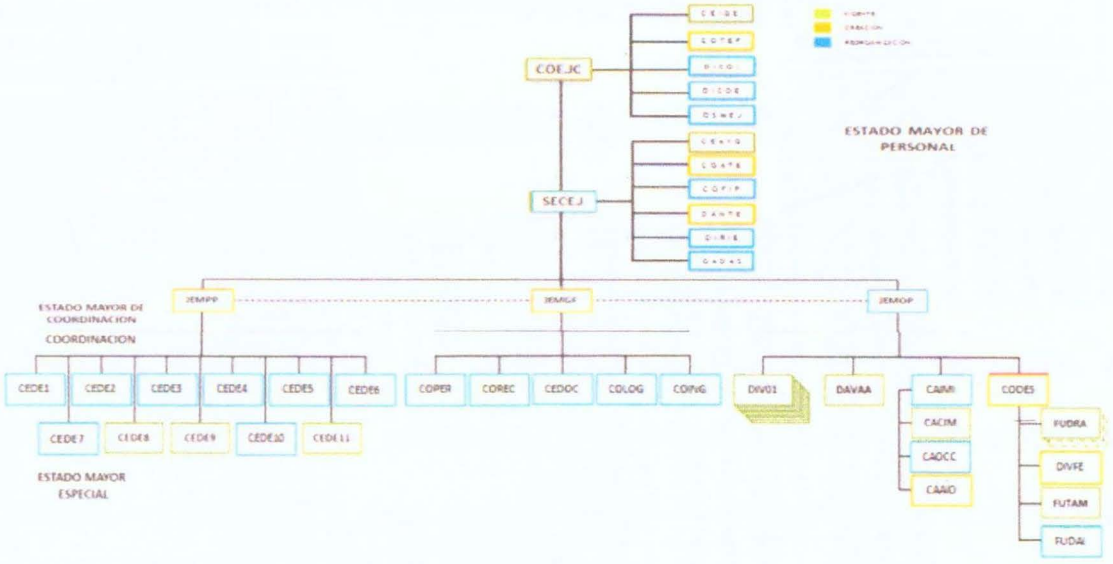


Figura N. 3 Organización actual del Comando del Ejército Nacional. *Fuente:* CAOCC EJC (2016)

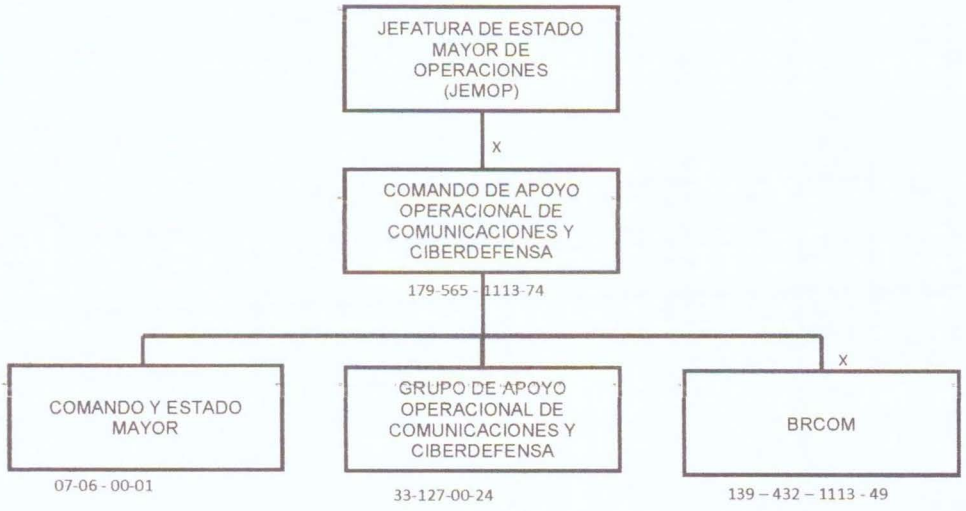


Figura N. 4 Organización del Comando de Apoyo Operacional de Comunicaciones y Ciberdefensa CAOCC. *Fuente:* CAOCC (2016)

Es así, como la ciberdefensa quedó inmersa dentro de la estructura estratégica organizacional del Ejército Nacional en el Grupo de Apoyo Operacional de Comunicaciones y ciberdefensa (en adelante: GAOCC) y este a su vez quedó organizado de la siguiente forma:

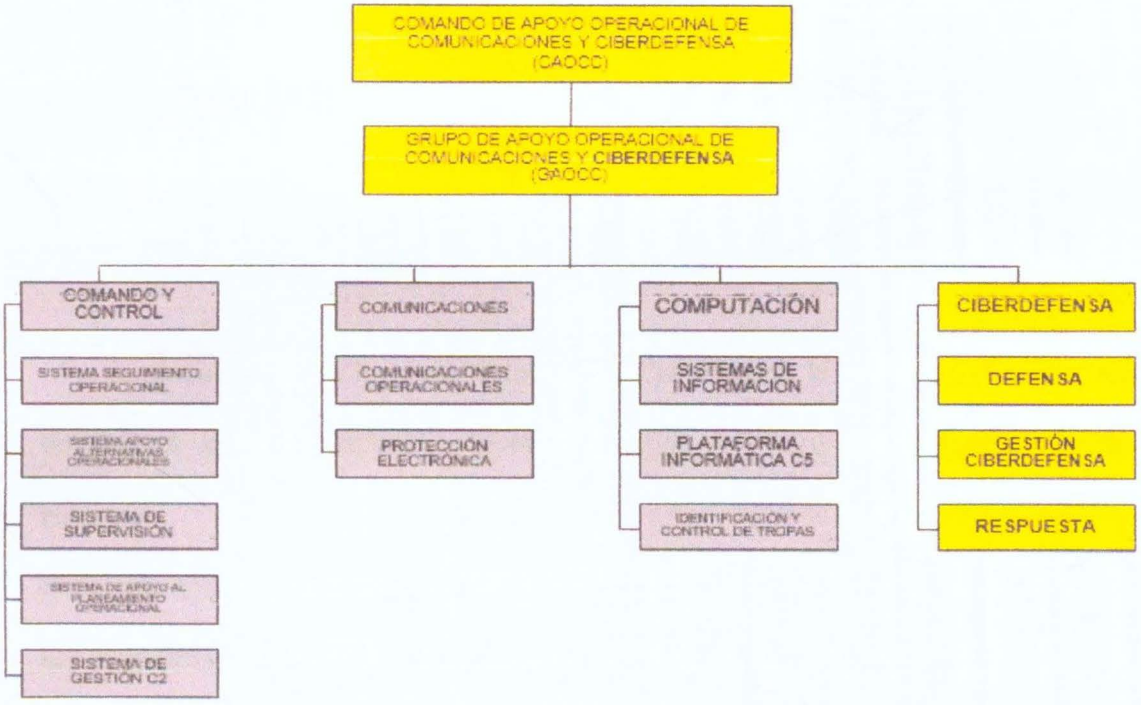


Figura N. 5 Organización del Grupo de Apoyo Operacional de Comunicaciones y Ciberdefensa GAOCC. *Fuente:* CAOCC EJC (2016)

Es así como la sección de ciberdefensa del Comando del Ejército (Visualizada en color amarillo) quedó establecida en la organización del GAOCC descrito como en el organigrama aparece y cumpliendo la misión de "defender el dominio cibernético y ejecutar acciones relativas a la ciberdefensa para la protección de la infraestructura crítica digital del Ejercito Nacional" (GAOCC, 2017).

Así mismo de acuerdo a lo informado por el GAOCC del Ejército es la sección encargada del "empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales", (GAOCC, 2017).

De igual forma según información suministrada por el GAOCC dispone de las siguientes capacidades:

1. Correlación de los activos informáticos del Ejército Nacional, logrando auditar el comportamiento y tráfico que se presentan en las redes informáticas del Ejército Nacional.
2. Monitoreo constante de las redes informáticas, para lograr la anticipación y prevención de ataques cibernéticos contra la infraestructura crítica e información del Ejército Nacional.
3. Detección y contención de amenazas cibernéticas, obteniendo como resultado mantener la integridad de las redes informáticas y la información del Ejército Nacional.
4. Análisis de las amenazas, ataques e incidentes cibernéticos, logrando distinguir los factores comunes dando como resultado el bloqueo de amenazas persistentes dentro de la infraestructura informática del Ejército Nacional.
5. Y por último asesorar y prevenir al personal de seguridad informática de las unidades Operativas Mayores sobre amenazas o vulnerabilidades cibernéticas que atenten contra la seguridad de las redes informáticas de las mismas.

Ataques, incidentes o amenazas cibernéticas que el Ejército de Colombia ha sufrido en la red informática desde el año 2016

En relación a los ataques cibernéticos que el Ejército de Colombia ha sufrido, de acuerdo a información presentada por el GAOCC, se presentan las siguientes estadísticas y comparativos en relación con incidentes, amenazas, ataques, entre otros eventos relacionados con la

ciberdefensa en el Ejército Nacional de igual forma se clarifican conceptos en relación a cada estadística.

Malware malicious software

"Término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento". (GAOCC, 2017).

II SEMESTRE 2016

NOMBRE TÉCNICO	CAUSAS	ALERTAS DETECTADAS	ALERTAS CONTENIDAS
Worm.Jenxcus (malware)	Vulneración de contraseñas.	216.758	100%
Trojan.Zbot (malware)	Roba información.	22.626	100%
Backdoor.H-WORM (malware)	Tener acceso al sistema de un computador.	12.274	100%
InfoStealer.Magovel.A (malware)	Descarga software malicioso.	2.203	100%
Backdoor.APT.Xtreme RAT (malware)	Software diseñado para infectar ordenadores y robar dinero.	1.881	100%
Worm.Email.Brontok (malware)	Desactiva software del antivirus.	340	100%
PWS.Win32.Magovel. A (malware)	Descarga software malicioso.	227	100%
Trojan.Generic (malware)	Roba información.	125	100%
DTI.Callback (malware)	Tener acceso al sistema de un computador.	103	100%
Exploit.Kit.Malvertise ment (malware)	Vulneración de contraseñas.	63	100%
Trojan.Sality (malware)	Roba información.	48	100%
Exploit.Kit.Rig (malware)	Descarga software malicioso.	44	100%

Trojan.DorkBot (malware)	Roba información.	27	100%
Trojan.Downloader.Gamarue.A (malware)	Descarga software malicioso.	24	100%
TOTAL		**256.743**	

Figura N. 6 Estadistica Ciberdefensa GAOCC. *Fuente:* Información estadística GAOCC EJC (2017)

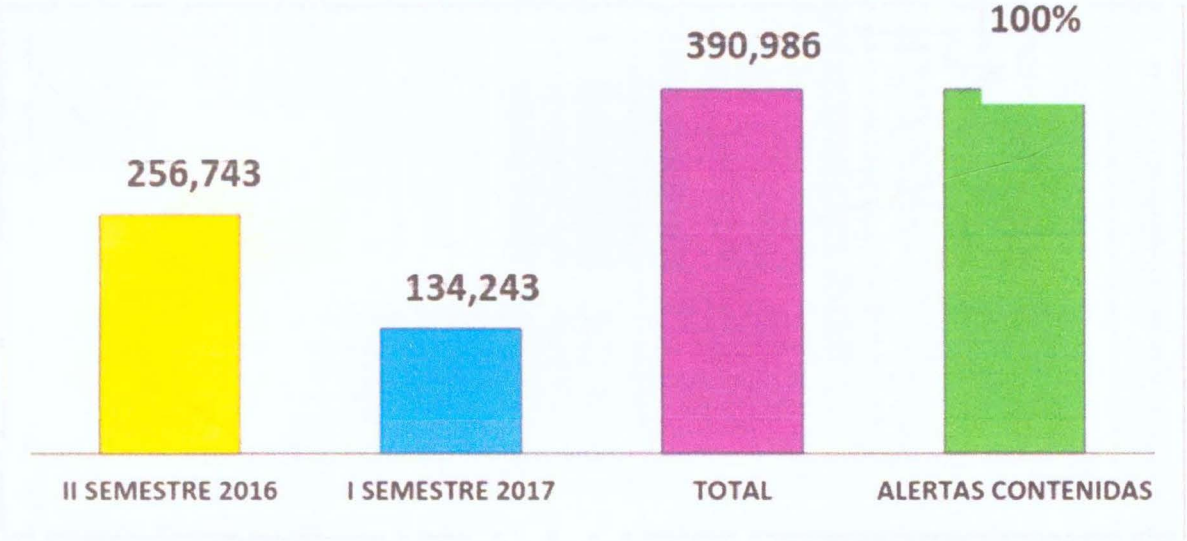
Alertas detectadas

I SEMESTRE 2017

NOMBRE TÉCNICO	CAUSAS	ALERTAS DETECTADAS	ALERTAS CONTENIDAS
Backdoor.H-WORM (malware)	Tener acceso al sistema de un computador.	74.280	100%
Trojan.Zbot (malware)	Roba información.	30.350	100%
Worm.Jenxcus (malware)	Vulneración de contraseñas.	18.038	100%
Trojan.Xtrat (malware)	Software diseñado para infectar ordenadores y robar dinero.	9.195	100%
Worm.Email.Brontok (malware)	Desactiva software del antivirus.	1.523	100%
Trojan.Downloader (malware)	Descarga software malicioso.	541	100%
Trojan.Generic (malware)	Roba información.	69	100%
DTI.Callback (malware)	Tener acceso al sistema de un computador.	82	100%
Malware.Binary.exe (malware)	Descarga software malicioso.	35	100%
Mal/Banker-BB (malware)	Roba información.	34	100%
PUP.Mysearch (malware)	Redirecciona a páginas sospechosas.	30	100%
Malware.archive (malware)	Descarga software malicioso.	29	100%
PUP.Agent (malware)	Desactiva software del antivirus.	21	100%
Trojan.KWW.DNS (malware)	Roba información.	16	100%
TOTAL		**134.243**	

Figura N. 7 Estadística Ciberdefensa GAOCC. *Fuente:* Información estadística GAOCC EJC (2017)

Comparativo alertas detectadas contenidas



Gráfica N. 8 Estadística Ciberdefensa GAOCC. *Fuente:* Información estadística GAOCC EJC (2017)

Equipos bloqueados por políticas de seguridad

En relación a este punto es preciso indicar las políticas de seguridad que para el GAOCC generan bloqueo de los cuales se destacan las siguientes:

- Incorrecta identificación del equipo
- No instalación del antivirus institucional
- Instalación de software no autorizados
- Navegación a páginas con contenidos no autorizados

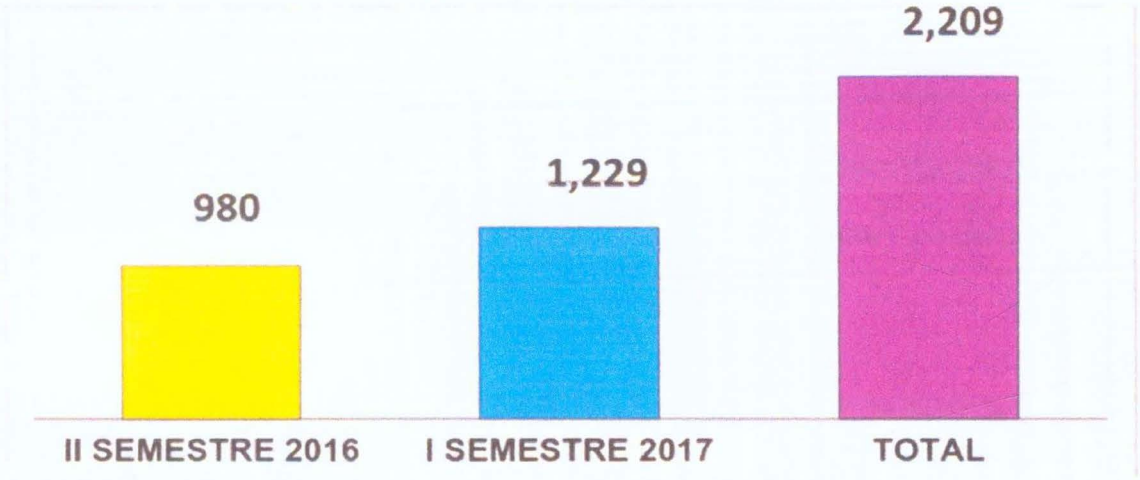


Figura N. 9 Estadistica Ciberdefensa GAOCC. *Fuente:* Información estadística GAOCC EJC (2017)

Comparativo semestral de incidentes detectados

En relación a este punto se recalca el concepto de incidente cibernético como " Un incidente cibernético es la violación o amenaza inminente a la violación de una política de seguridad de la información (confidencialidad, integridad y disponibilidad).", (GAOCC, 2017) y algunos de los incidentes que de acuerdo a la sección de ciberdefensa del GAOCC se presentan en el Ejército Nacional, como lo son: acceso no autorizado, robo de contraseñas, robo de información, denegación de servicio, no instalación y/o actualización del antivirus institucional.

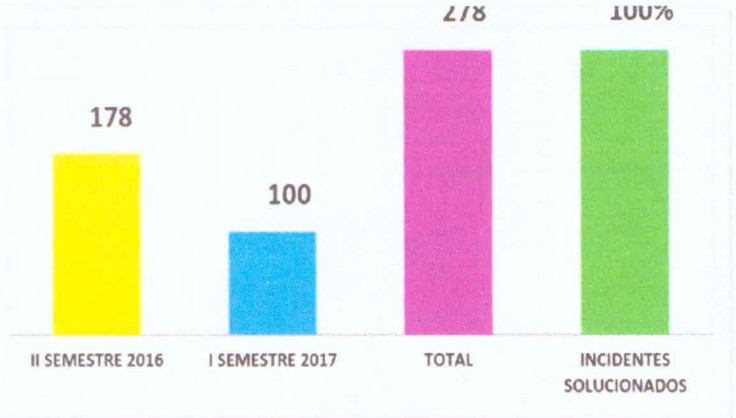


Figura N. 10 Estadistica Ciberdefensa GAOCC. *Fuente:* Información estadística GAOCC EJC (2017)

Es preciso indicar que el Ejército Nacional en el año 2015 dispuso de recursos económicos y humanos para la creación e implementación de la ciberdefensa en el Ejército Nacional a nivel estratégico, inversión y resultados que se ven en las estadísticas que son muy dicientes de la reducción en el número de ataques que la infraestructura del Ejército a nivel estratégico recibió.

Sin embargo, no se tiene información clara y específica de los ataques que recibieron las Unidades Operativas Mayores que integran el Ejército Nacional de forma discriminada por unidad, razón por la cual la información que se relacionó anteriormente corresponde a todo el Ejército Nacional como Fuerza.

Así mismo, es de aclarar que cada Unidad Operativa Menor tiene una jurisdicción diferente, una misión particular para cada unidad, una información referente a cada jurisdicción y unos activos informáticos que de una u otra forma requieren de una mayor visualización a nivel División y no a nivel Comando del Ejército, con el fin de mitigar riesgos en relación a ciberdefensa.

La Ciberdefensa actual en las Unidades Operativas Mayores del Ejército

En relación a la inclusión de la ciberdefensa en las Unidades Operativas Mayores del Ejército partimos de lo dispuesto en la doctrina actual del Ejército Nacional de acuerdo al Manual de Estado Mayor 3-50, en el cual se visualiza la organización del Estado Mayor de División, en el cual encontramos la sección G-10 (Comunicaciones) que es la que está asumiendo la responsabilidad de ciberdefensa en cada Unidad, sin embargo en la organización no se evidencia que exista como tal la sección de ciberdefensa dentro de la estructura organizacional del G-10 en la cual aparece: centro de mensajes y laboratorio divisionario.

Es de aclarar que en relación a la doctrina actual y la organización actual del Ejercito Nacional difieren ya que a nivel Ejercito ya se tiene organizo y el funcionamiento el departamento de comunicaciones CEDE6, sin embargo, en relación a las UOM todavía se mantiene la organización establecida en el manual de estado mayor 3-50 ya que la nueva organización de las UOM no ha sido aprobada por parte del comando superior y por ende no se ha implementado la nueva organización en dicho nivel.

Así mismo, el CEDE6 no es el que tiene a cargo la ciberdefensa del Ejercito Nacional ya que su función se enmarca en relación a planeamiento, políticas y estandarización del C5, las funciones de ciberdefensa están a cargo del GAOCC perteneciente al CAOCC como se mencionó anteriormente, organización que difiere en las UOM donde el G10 debe cumplir con todo lo relacionado con comunicaciones.

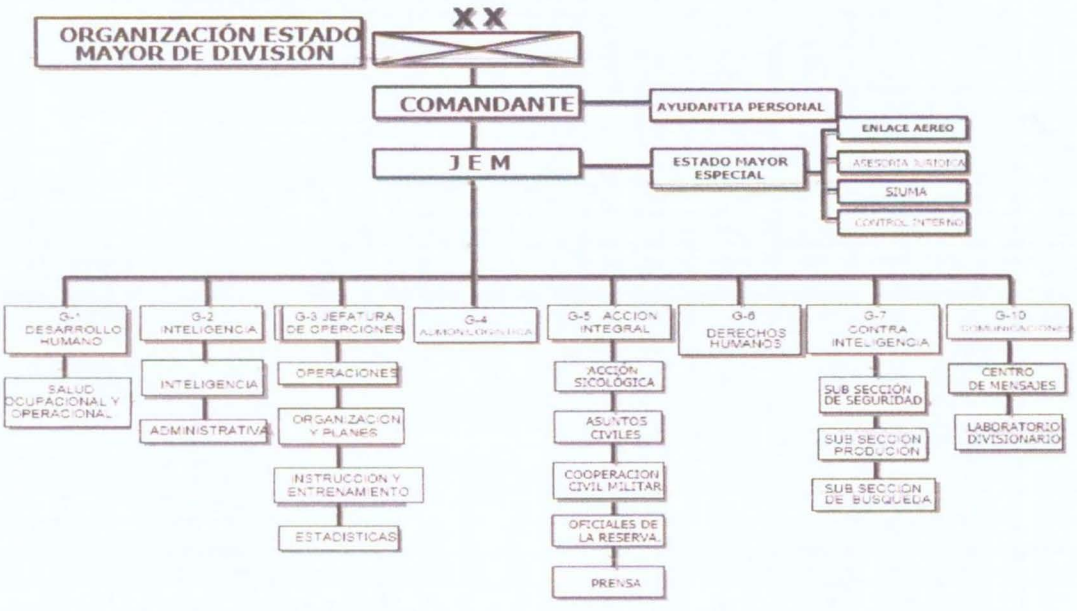


Figura N. 11 Organización Estado Mayor de División. *Fuente:* Manual de Estado Mayor 3-50 EJC (2013)

De igual forma, es preciso indicar que las funciones de ciberdefensa se vienen cumpliendo de forma parcial por parte de Oficiales y Suboficiales de cada UOM, a pesar de no estar organizados como se encuentra el GAOCC a nivel Ejército y que no cuentan con la organización, infraestructura, personal y presupuesto suficiente para desempeñar las acciones y labores de ciberdefensa.

Aunado a lo anterior y con el fin de tener una mayor percepción de la situación actual de las actividades de ciberdefensa que se están desarrollando las UOM que integran en Ejercito Nacional y su situación actual, se elaboró una encuesta enviada a los Oficiales de Comunicaciones de la Nueve Divisiones del Ejército Nacional encargados del proceso de ciberdefensa en cada una de las UOM, de la cual se anexan los resultados al presente documento, obteniendo resultados de percepción muy disientes en relación a la importancia de la ciberdefensa en las UOM, así mismo algunos tópicos que reflejan el estado actual y la importancia que se le está dando a la ciberdefensa en las unidades donde se realizó dicha encuesta como lo es el tema de conocimientos o preparación en ciberdefensa donde solo el 56,6% de los encuestados manifestó tener dichos conocimientos, al igual que los subalternos de comunicaciones en cada UOM, donde solo el 33,3% considera tener dicha capacitación.

Así mismo se evidencia que el 100% de los encuestados consideran que la ciberdefensa en sus unidades del Ejército Nacional es importante, pero cuando se preguntó si tiene un sistema de ciberdefensa actualmente su unidad, solo el 77,8% manifestó tenerlo en su UOM.

De igual forma cuando se preguntó a los encuestados de las UOM, si su unidad está preparada para contrarrestar un incidente cibernético y solo el 22,2 % manifiesta estar preparados, siendo muy disiente del grado de alistamiento para afrontar ataques cibernéticos y

sobre todo para evitarlos o contenerlos, aspecto que va relacionado con el presupuesto que las UOM destinan para ciberdefensa, donde solo el 11,1 % de los encuestados manifiestan tener presupuesto para la ciberdefensa en las UOM, los resultados de dicha encuesta en forma detallada y cada uno de los tópicos que se abarcaron se anexan al final del documento.

Recomendaciones para mitigar las falencias de las Unidades Operativas Mayores del Ejército de Colombia en el área de Ciberdefensa

Teniendo como precedente los argumentos presentados anteriormente y lo evidenciado en la organización actual del Ejército Nacional de acuerdo a la Doctrina DAMASCO, la organización de las Unidades Operativas Mayores de acuerdo al Manual de Estado Mayor 3-50, lo cual está en proceso de actualización, los diferentes incidentes, amenazas o eventos que de acuerdo a las estadísticas que el GAOCC a través de su sección de ciberdefensa ha consolidado los resultados de las encuestas realizadas a los oficiales de comunicaciones de las diferentes Unidades Operativas Mayores que integran la Fuerza, se presentan las siguientes recomendaciones:

Con base en la misión que cumplen las diferentes Unidades Operativas Mayores, la jurisdicción que cada una tiene asignada, los activos informáticos de los cuales disponen para cumplir dicha misión el ambiente y entorno Volátil, Incierto, Complejo y Ambiguo (en adelante: VICA) que cada día deben enfrentar para contrarrestar las diferentes amenazas y factores de inestabilidad que convergen en cada una de las regiones del país, se recomienda que se implementen las secciones o departamentos de ciberdefensa en cada una de las Operativas Mayores dependiendo organizacionalmente del Departamento de Comunicaciones de cada Unidad.

Como segundo aspecto se recomienda que dicha organización sea similar a la que actualmente tiene el Comando del Ejército Nacional a través del GAOCC en relación al área de ciberdefensa ya que a nivel estratégico es quien viene desarrollando dicha labor, que podría fortalecerse con una participación más dinámica y activa por parte de las Unidades Operativas Mayores, toda vez que en temas de tecnología y en especial de redes informáticas las amenazas e intereses nacionales y extranjeros que circundan son cada día cambiantes y se transforman con el desarrollo tecnológico, por lo tanto se requieren organizaciones cibernéticas más robustas en el nivel de las Unidades Operativas mayores para afrontar los retos venideros de forma más eficaz y efectiva.

Como tercer punto, teniendo en cuenta el ambiente operacional en el que se encuentra cada División, la información de la cual hacen uso para el cumplimiento de cada una de sus misiones y la infraestructura crítica digital que cada una de las Unidades Operativas Mayores tiene, es de vital importancia incrementar las capacidades de monitoreo para mitigar riesgos de vulnerabilidades en ciberdefensa, siendo más efectivos en la ejecución de la defensa activa y/o pasiva a nivel de hardware y/o software.

Como cuarta recomendación es de vital importancia generar una concientización masiva y capacitación en relación a lo que es ciberdefensa, cuál es su finalidad e importancia, no solo al personal que tiene a cargo la responsabilidad de comunicaciones y ciberdefensa en las Unidades Operativas Mayores, sino a todo el personal de Oficiales, Suboficiales, Soldados y Civiles que integran cada una de las Unidades y que de una u otra forman tienen o hacen uso de los diferentes activos informáticos del Ejército Nacional.

Como quinta recomendación, la implementación de la ciberdefensa en las unidades operativas mayores del Ejército Nacional a través de la estructura implementada en el Comando de la Fuerza es de vital importancia para contrarrestar los diferentes ataques cibernéticos que pueden llegar a presentar tal como ha sucedido en varios países

Así mismo es preciso indicar que dicha implementación de la ciberdefensa en las Unidades Operativas Mayores no se puede lograr solo con cambios organizacionales en las Divisiones, se requiere de esfuerzos adicionales en capacitación del personal de forma permanente, ampliación del recurso humano para que labore en ciberdefensa y la asignación de recursos para su buen funcionamiento, de igual forma se debe interiorizar en cuál es el costo de no tener fortalecida la ciberdefensa en las unidades, cual es el beneficio y qué capacidades se adquieren con el fortalecimiento de la ciberdefensa en las Divisiones .

Como última recomendación, es de vital importancia entender el entorno cibernético en el que nos encontramos en un mundo cada día más globalizado donde la tecnología en tópicos informáticos avanza cada día, por lo cual las capacidades técnicas y operativas que el Ejército Nacional y las Unidades Operativas Mayores que la integran en materia de ciberdefensa deben ir a la vanguardia de los nuevos retos y desafíos.

Conclusiones

PRIMERA: Es de vital importancia implementar la ciberdefensa en las Unidades Operativas Mayores del Ejército Nacional de acuerdo a la estructura implementada en el Comando de la Fuerza a través del GAOCC con el fin de contrarrestar los diferentes ataques, amenazas o incidentes cibernéticos, dicha implantación permitirá fortalecer la labor y las capacidades que el Comando del Ejército ha venido desarrollando bajo el liderazgo del Comando de Apoyo Operacional de Comunicaciones y ciberdefensa. Dicha implementación deberá llevar consigo una inclusión en el Sumario de Ordenes Permanentes (SOP) de cada unidad, para que de esta forma se pueda desarrollar y aplicar la ciberdefensa en los diferentes niveles y unidades del Ejército.

SEGUNDA: Es prioritario generar una concientización masiva y una capacitación en relación a que es ciberdefensa, capacidades, vulnerabilidades y normas sobre el manejo de información cibernético digital, no solo al personal de comunicaciones o que tiene a cargo la responsabilidad de ciberdefensa, sino a todo el personal de Oficiales, Suboficiales, Soldados y Civiles que integran las diferentes Unidades Operativas Mayores y hacen uso de la infraestructura digital del Ejercito Nacional. En el desarrollo de dicha concientización se debe hacer un énfasis especial en los niveles más altos del mando, mostrando con hechos y las estadísticas actuales, las consecuencias que puede traer el saltarse o ignorar las instrucciones en el área de ciberdefensa, en especial por el manejo y control de la información que estos niveles del mando manejan. La información como fuente de poder, y de valor estratégico dentro de los intereses de posibles enemigos y la importancia de proteger los activos estratégicos institucionales y del Estado deben ser una prioridad.

TERCERA: La implementación de la ciberdefensa en las Unidades Operativas Mayores requiere no sólo de cambios organizacionales, sino de capacitación al personal asignado en dicha labor, asignación de presupuesto para poder funcionar y comprometimiento del personal de toda la División.

CUARTA: Dentro de la estructura organizacional del Ejército Nacional, se debe proyectar la creación de una sección que maneje todos los aspectos relacionados al ciberespacio, tal como lo hace el Ejército de Estados Unidos, el cual maneja el CEMA (CYBER ELECTROMAGNETIC ACTIVITIES), cuya misión recita "Tiene como objetivo explotar las ventajas sobre el enemigo en el ciberespacio y en el espectro electromagnético a la vez que, de forma simultánea, le deniega su uso y protege al sistema de mando y control de la misión" (FM 3-38, 2014). Pero para poder llevar a cabo dicha proyección se debe tener una política institucional muy clara de ciberdefensa, con la cual no se cuenta todavía. La sección CEMA en alineación de la nueva doctrina DAMASCO y en cumplimiento de los parámetros de OTAN.

QUINTA: La ciberdefensa como herramienta de prevención, se debe considerar de vital importancia dentro de la organización de los Estados Mayores y Planas Mayores de las distintas unidades de la Fuerza, hecho que obliga a los comandantes de las mismas a utilizar el personal de comunicaciones para los fines que éstos están destinados, maximizando el recurso humano dentro de las posibilidades que la disponibilidad del mismo facilite este proceso. Todos los cargos tienen responsabilidades, pero dentro del actual ambiente ciber, los hombres de comunicaciones toman una relevancia en su misión que los comandantes deben tomar muy en cuenta y es la de salvaguardar y sostener los medios que garanticen el Mando Tipo Misión, como

base fundamental del Comando y Control que todo comandante debe ejercer sobre sus hombres y recursos disponibles.

SEXTA: Considerar como opción la ubicación y organización de un Centro de Operaciones de Seguridad (SOC por sus siglas en inglés Security Operations Center), en tanto se da cumplimiento a la organización de la sección de ciberdefensa en las unidades, esto con el fin de poder garantizar unas condiciones mínimas para el uso, seguimiento y verificación de las herramientas disponibles en la Fuerza, de tal forma que se pueda realizar trabajos coordinados con el CAOCC y el GAOCC respectivamente.

Referencias bibliográficas

Acosta, P. R. (octubre de 2009). Seguridad Nacional y Ciberdefensa. Cuaderno. Madrid: Fundación Rogelio Segovia para él.

Artiles, N. G. (2011). Situación de la Ciberseguridad en el ámbito internacional y en la OTAN. Cuadernos de estrategia, (149), 165-214.

Ambos, K. (2015). Responsabilidad penal internacional en el ciberespacio. U. Externado de Colombia.

Barrios Rubio, A. (2009). Los jóvenes y la red: usos y consumos de los nuevos medios en la sociedad de la información y la comunicación. Signo y pensamiento.

Biblioteca Virtual Universal. (2003). *https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiN6fippc_TAhUDKiYKHSZaDL0QFgghMAA&url=http%3A%2F%2Fwww.biblioteca.org.ar%2Flibros%2F656228.pdf&usg=AFQjCNGWmzL6kt0xo2WOXHb1iWO1DrHKuw&sig2=fDbClbleAR2AuaiObV6rPw*. Recuperado de http://www.biblioteca.org.ar/libros/656228.pdf

Bueno, A. (Abril de 2017). Redes Informáticas. Recuperado de http://www.indibaamparooltra.com/Toni/Redes/Ud_4_redes_V1_c.pdf.

Cano, J. J. (2011). Ciberdefensa y Ciberseguridad: dos tendencias emergentes en un contexto global.

Camacho García, J. D. (2016). Evolución de la ciberdefensa y la seguridad de la información en Colombia (Bachelor's thesis, Universidad Militar Nueva Granada).

Colombia, Ejercito Nacional, (2017) Información de comando CAOCC, Reservado.

Colombia, U.E. (Ed.). (s.f.). (11). Recuperado de: http://revistas.uexternado.edu.co/index.php/Deradm/article/view/3831/4087.

CONPES. (14 de Julio de 2011). CONPES 3701. Lineamientos de Política para Ciberseguridad Y Ciberdefensa. Colombia.

Criado, M. Á. (2016). Redes sociales y ciberterrorismo. Las TIC como herramienta terrorista.

Eduardo, L. (2016). Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia.

Ferrero, J. A. (2013). La Ciberdefensa, Génesis y Evolución. Revista General de Marina, 83-84.

Fragoso, S. (2001). Espacio, ciberespacio, hiperespacio. Razón y Palabra.

Giudici, D. E. (2013). Lineamientos para la seguridad cibernética en Teatro de Operaciones.

Hoyos Buiron, V. A. (2016). ¿Qué tal esta Colombia en cuestión de ciberseguridad? (Bachelor's thesis, Universidad Militar Nueva Granada).

Justribó, C. (2014). Ciberdefensa: una visión desde la UNASUR. In VII Congreso del IRI/I Congreso del CoFEI/II Congreso de la FLAEI (La Plata, 2014).

López, J. A. (2002). *El poder aéreo, instrumento.* España: (c) Consejo Superior de Investigaciones Científicas.

Moreno Forero, F. A. (2016). Ciberseguridad: nuevo enfoque de las Fuerzas Militares en Colombia (Bachelor's thesis, Universidad Militar Nueva Granada).

Nacional, G. d. (Abril de 2013). *https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwi9ouTIrs_TAhVJVyYKHUDiCgAQFggpMAE&url=http%3A%2F%2Fwww.defensa.gob.es%2Fceseden%2FGalerias%2Fealede%2Fcursos%2FcurDefNacional%2Fficheros%2FCiberseguridad_nuevo_re.* Recuperado de http://www.defensa.gob.es/ceseden/Galerias/ealede/cursos/curDefNacional/ficheros/Ciberseguridad_nuevo_reto_del_siglo_XXI_Guerra_cibernetica_aspectos_organizativos.pdf

Oyarzún, E. S. (Abril de 2006). *https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjH1O-6qs_TAhVITCYKHRUHD0gQFgghMAA&url=http%3A%2F%2Frevistamarina.cl%2Frevistas%2F2006%2F4%2Fsolis.pdf&usg=AFQjCNHuCcyDrLpRDrh4i4n-laRXYFAWQw&sig2=Zj0YlfG0ArzPlHvi.* Recuperado de http://revistamarina.cl/revistas/2006/4/solis.pdf

Tecnología, N. C. (10 de Octubre de 2010). *https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&cad=rja&uact=8&ved=0ahUKEwi9ouTIrs_TAhVJVyYKHUDiCgAQFghEMAU&url=http%3A%2F%2Fwww.cubadebate.cu%2Fnoticias%2F2010%2F10%2F18%2Fel-ciberespacio-ya-es-un-nuevo-dominio-de-guerra-afirma-subsecr.* Recuperado de

http://www.cubadebate.cu/noticias/2010/10/18/el-ciberespacio-ya-es-un-nuevo-dominio-de-guerra-afirma-subsecretario-de-defensa-de-eeuu/

Vargas Vargas, E. M. (2014). Ciberseguridad y ciberdefensa: ¿qué implicaciones tienen para la seguridad nacional? (Bachelor's thesis, Universidad Militar Nueva Granada).

Yagüe, D. (17 de Julio de 2009). *https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0ahUKEwiWpZC9rc_TAhUC5yYKHbExB8MQFggvMAI&url=http%3A%2F%2Fwww.20minutos.es%2Fnoticia%2F478620%2F0%2Fcarrera%2Fespacial%2Fguerra-fria%2F&usg=AFQjCNFUmcNYd9rGeB7KmC4lkUKsH.* Recuperado de http://www.20minutos.es/noticia/478620/0/carrera/espacial/guerra-fria/

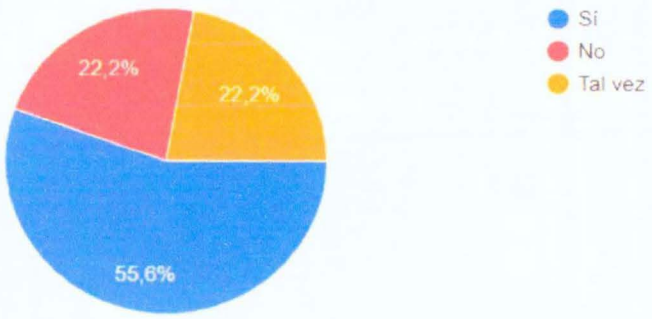
Índice de cuadros, tablas, gráficas y figuras

Anexos

Anexo

Resultados encuesta dirigida a oficiales de comunicaciones UOM

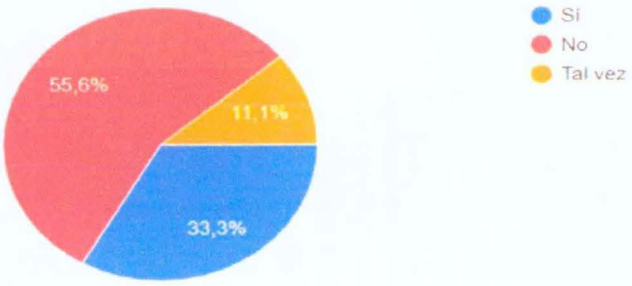
1. ¿Usted tiene conocimientos o preparación en el tema de ciberdefensa?



Nota: Figura Nº 12 Elaboración propia tomada a partir de encuesta realizada a Oficiales de comunicaciones de las Divisiones del Ejército. (2017)

Se evidencia que solo el 55,6 % de los oficiales de comunicaciones encargados del proceso de ciberdefensa en las Unidades Operativas Mayores (en adelante: UOM) encuestados manifiesta tener conocimiento o algún tipo de preparación en relación al área de estudio.

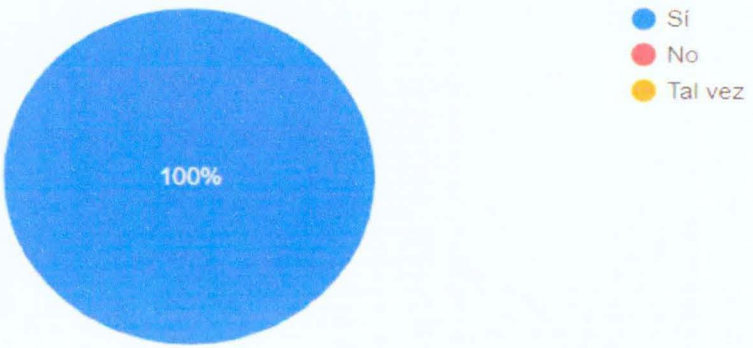
2. ¿Sus subalternos tienen conocimiento o preparación sobre ciberdefensa



Nota: Figura Nº 13 Elaboración propia tomada a partir de encuesta realizada a Oficiales de comunicaciones de las Divisiones del Ejército. (2017)

En relación a esta pregunta el escenario de capacitación, conocimiento y preparación es más diciente ya que los oficiales y suboficiales que son subalternos en cada una de las UOM de acuerdo a la percepción del jefe del área de ciberdefensa solo el 33,3 % cumple con el perfil que deberían tener en ciberdefensa.

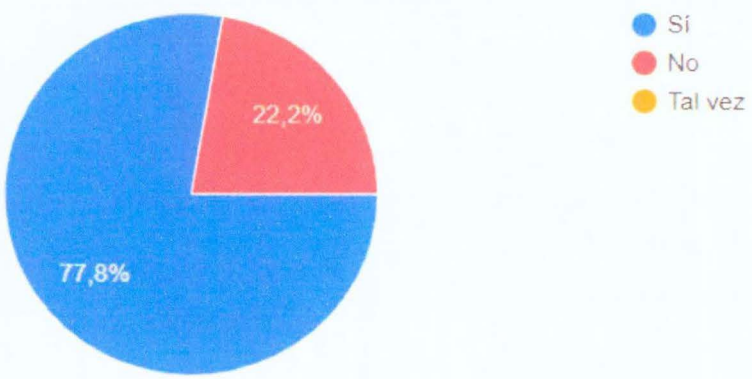
3. ¿Indíquenos por favor si usted considera importante la ciberdefensa en las unidades del Ejército Nacional?



Nota: Figura Nº 14 Elaboración propia tomada a partir de encuesta realizada a Oficiales de comunicaciones de las Divisiones del Ejército. (2017)

En esta pregunta se evidencia que el 100 % de los encuestados en las UOM son conscientes de la importancia de la ciberdefensa en sus unidades.

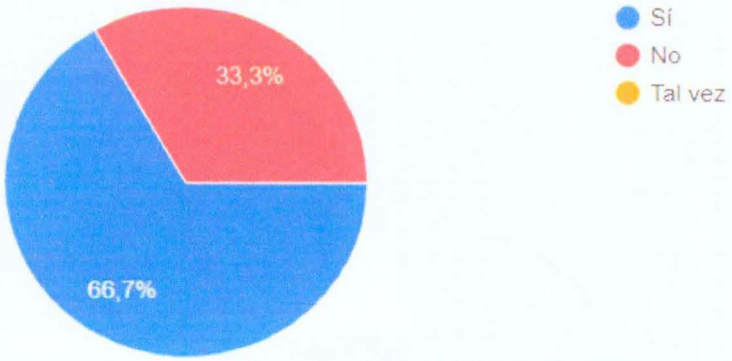
4. ¿Nos podría por favor informar si tiene sistema de ciberdefensa actualmente su unidad?



Nota: Figura Nº 15 Elaboración propia tomada a partir de encuesta realizada a Oficiales de comunicaciones de las Divisiones del Ejército. (2017)

En esta pregunta se evidencia que solo el 77,8 % de los encuestados consideran que tienen en su unidad sistema de ciberdefensa, a pesar de no estar contemplado en la organización de las Unidades Operativas Mayores de acuerdo a doctrina. Esto es un índice que no se tiene claro la organización y subordinación de la ciberdefensa en las unidades.

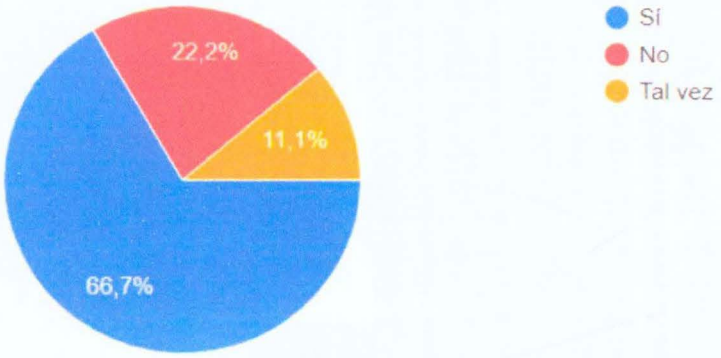
5. ¿En su unidad existe una dependencia encargada de la ciberdefensa?



Nota: Figura Nº 16 Elaboración propia tomada a partir de encuesta realizada a Oficiales de comunicaciones de las Divisiones del Ejército. (2017)

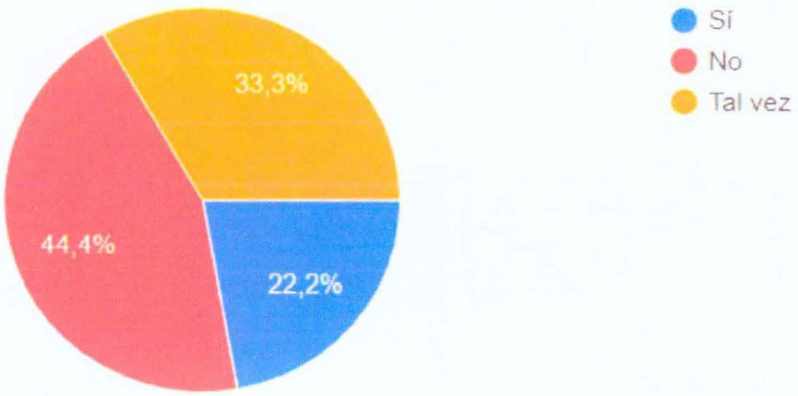
En relación con esta pregunta a pesar de no estar autorizado en la doctrina del Ejército hasta la presente fecha la creación de las secciones o dependencias de ciberdefensa en las Unidades Operativas Menores, se evidencia que un 66,7% de los encuestados considera que tiene una dependencia de ciberdefensa en su unidad.

6. ¿Su unidad ha implementado políticas y medidas técnicas de ciberdefensa para proteger los sistemas de información críticos?



Nota: Figura Nº 17 Elaboración propia tomada a partir de encuesta realizada a Oficiales de comunicaciones de las Divisiones del Ejército. (2017)

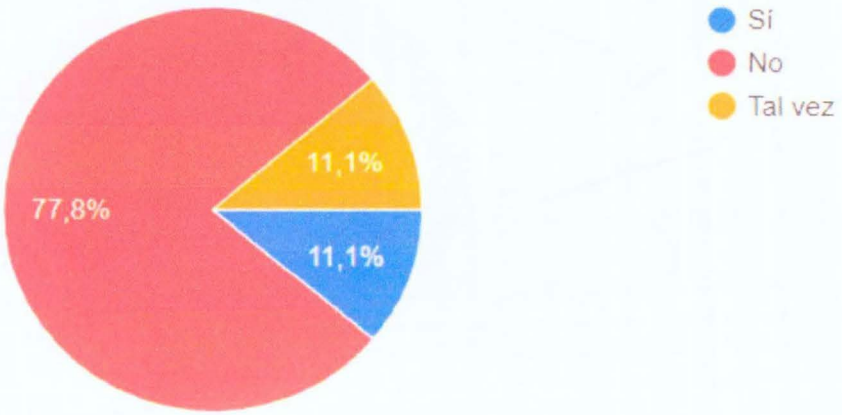
7. ¿Su unidad está preparada para contrarrestar un incidente cibernético?



Nota: Figura Nº 18 Elaboración propia tomada a partir de encuesta realizada a Oficiales de comunicaciones de las Divisiones del Ejército. (2017)

A esta pregunta la percepción positiva de los encuestados ante la preparación de sus unidades para afrontar algún tipo de incidente cibernético es solo del 22,2 % siendo muy disiente del grado de alistamiento para afrontar ataques cibernéticos y sobre todo para evitarlos o contenerlos. Por otra parte, la duda o negativa ante la pregunta muestra el alto nivel de duda y preparación para afrontar riesgos cibernéticos.

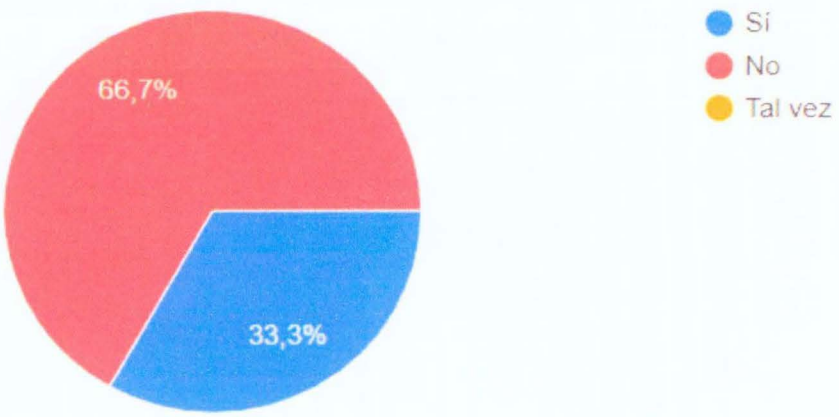
8. ¿Hay presupuesto para la ciberdefensa en su unidad?



Nota: Figura Nº 19 Elaboración propia tomada a partir de encuesta realizada a Oficiales de comunicaciones de las Divisiones del Ejército. (2017)

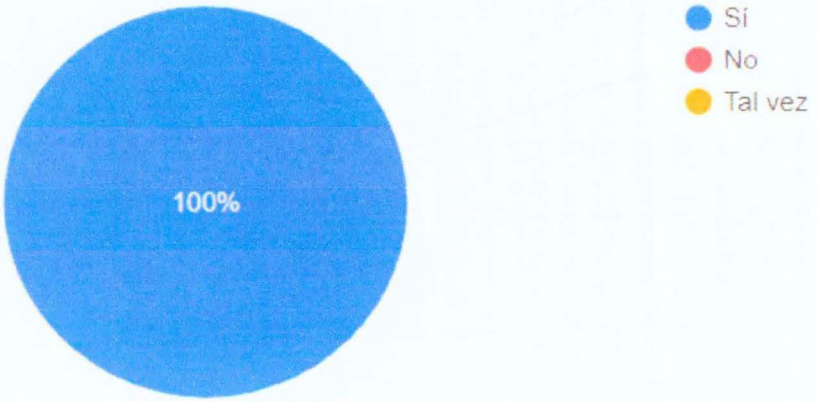
En relación a esta pregunta se evidencia una carencia de presupuesto en relación a la inversión en ciberdefensa en cada una de las Unidades Operativas Mayores presentándose solo un 11,1 % de los encuestados que manifiestan tener presupuesto para esta área.

9. ¿Las entidades de ciberdefensa en Colombia han prestado servicio o soporte en su unidad?



Nota: Figura Nº 20 Elaboración propia tomada a partir de encuesta realizada a Oficiales de comunicaciones de las Divisiones del Ejército. (2017)

10. ¿Le gustaría que el Ejército Nacional implemente sistemas de ciberdefensa en su unidad?

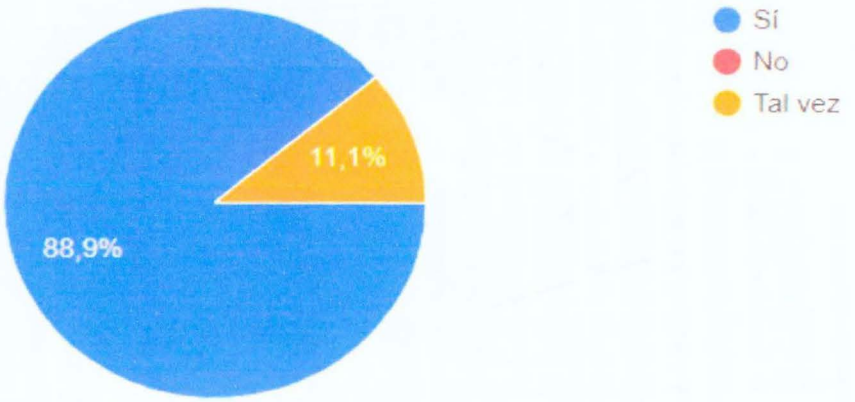


Nota: Figura Nº 21 Elaboración propia tomada a partir de encuesta realizada a Oficiales de comunicaciones de las Divisiones del Ejército. (2017)

11. ¿Usted considera que el sistema de ciberdefensa que tiene el Ejército Nacional debe mejorar?

Nota: Figura Nº 22 Elaboración propia tomada a partir de encuesta realizada a Oficiales de comunicaciones de las Divisiones del Ejército. (2017)

12. ¿Usted considera que los incidentes cibernéticos contra la infraestructura se están incrementando?



Nota: Figura Nº 23 Elaboración propia tomada a partir de encuesta realizada a Oficiales de comunicaciones de las Divisiones del Ejército. (2017)