ESCUELA NAVAL DE CADETES
"ALMIRANTE PADILLA"
Honor y Tradición

REVISTA DERROTERO

Seguridad y Defensa

Análisis Técnico para la Selección de Equipos de Contramedidas Electrónicas, due Permitan Neutralizar la Fuga de Información al Interior de la Armada de Colombia

Technical Analysis for the Selection of Electronic Countermeasures Equipment, due to Allow Neutralizing the Information Leak within the Colombian Navy

Jorge Eliecer González Moreno[1]

Recibido: 19/08/2021
Aprobado: 25/02/2022

Correspondencia: jorge.gonzalez.mo@armada.mil.co

Resumen

Durante la última década se ha evidenciado el incremento de fuga de información clasificada de carácter operacional al interior de la Armada de Colombia, demostrando la escasez de implementación de medidas activas y pasivas en el uso y restricción de la información crítica. Respecto a la temática escogida, se hace necesario emplear una metodología de investigación documental que nos ayude a analizar más a fondo cuáles serían las herramientas tecnológicas existentes, relacionadas con las medidas de protección y manejo de la seguridad de la información requeridas al interior de la Armada de Colombia. Esto es, con el objetivo de mitigar el riesgo de fuga de información operacional, restringiendo el acceso a información sensible por parte de las amenazas internas y externas, contribuyendo al mejoramiento del desarrollo de las operaciones militares de manera eficaz, blindando sus capacidades actuales, su imagen institucional y el cumplimiento de su misión constitucional. Además, este trabajo es novedoso y coyuntural con los problemas de fuga de información que actualmente vive la Fuerza Pública de Colombia, permitiendo al alto mando naval tomar decisiones reales en la implementación de estas medidas activas que fortalezcan los procesos en el manejo de la información clasificada. Como resultado, este artículo científico busca, en primer lugar, detectar empresas tecnológicas que suministren equipos de contramedidas electrónicas, que se ajusten a las necesidades actuales con relación a neutralizar la fuga de información operacional. En segundo lugar, busca realizar un análisis empleando una matriz técnica que permita seleccionar las herramientas tecnológicas de contramedidas electrónicas más eficientes a emplear.

Palabras Claves: Amenazas, seguridad, equipos de contramedidas electrónicas, medidas activas y pasivas, información sensible, mitigar el riesgo, y fuga de información.

1 Administrador de Riesgos, Seguridad y Salud en el Trabajo, Subdirector de Contrainteligencia Técnica Naval Armada de Colombia, Bogotá, Colombia.

Abstract

During the last decade, there has been an increase in the leakage of classified information of an operational nature within the Colombian Navy, demonstrating the scarcity of implementation of active and passive measures in the use and restriction of critical information. Regarding the chosen topic, it is necessary to use a documentary research methodology that helps us analyze in more depth what the existing technological tools would be, related to the protection measures and information security management required within the Navy of Colombia, in order to neutralize the risk of leakage of operational information, restricting access to sensitive information by internal and external threats, effectively contributing to the improvement of the development of military operations, shielding its current capabilities, its institutional image and fulfillment of its constitutional mission. In addition, this work is novel, current with the problems of information leakage that the Colombian Public Force currently experiences and achievable over time, allowing the naval high command to make real decisions in the implementation of these active measures that strengthen the processes with the handling of classified information. As a result, this scientific article seeks, firstly, to detect technology companies that supply electronic countermeasures equipment that meet current needs in relation to neutralizing the leakage of operational information and, secondly, it seeks to perform an analysis using a technical matrix. that allows selecting the most efficient electronic countermeasures technological tools to be used.

Keywords: Threats, security, electronic countermeasure equipment, active and passive measures, sensitive information, risk mitigation, and information leakage.

Introducción

En los últimos años, miembros de la Armada Nacional de Colombia, en los diferentes escalafones militares, han estado inmersos en casos de subversión, sabotaje y espionaje interno (fuga de información operacional), que han afectado directamente a las operaciones navales y por ende, su misión constitucional consagrada en el artículo 217 en donde afirma que "La Nación tendrá para su defensa unas Fuerzas Militares permanentes cosnstituidas por el Ejército, la Armada y la Fuerza Aérea. Las Fuerzas Militares tendrán como finalidad primordial la defensa de la soberanía, la independencia, la integridad del territorio nacional y del orden constitucional". (Constitución Política, 1991, pág. 53). Esto debido a la presencia activa de grupos armados ilegales en las diferentes jurisdicciones que buscan constantemente subvertir ética y moralmente a miembros de la institución con el objetivo de obtener información operacional y colaboración a las actividades ilícitas.

Un claro ejemplo de lo anteriormente mencionado, fue la captura de seis miembros activos de la Armada Nacional en el municipio de Buenaventura, Valle del Cauca, quienes eran orgánicos de la Fuerza Naval del Pacífico, los cuales delinquían en cooperación con grupos armados ilegales de la región y que, según el periódico El Tiempo: "Los capturados tenían orden de captura por los delitos de tráfico, fabricación o porte de estupefacientes, concierto para delinquir, peculado por apropiación, prevaricato por omisión y falsedad ideológica en documento público". (El Tiempo, 2017). Siendo así, se describe el factor humano en la institución naval militar como el eslabón más débil dentro de la cadena, donde las amenazas internas que delinquen en el país, buscan constantemente subvertirlos con el fin de lograr vulnerar la seguridad, mediante el manejo de la información.

Al mismo tiempo, esta problemática se traslada a las amenazas externas, donde se evidencia el interés constante de países no aliados por obtener información sensible (espionaje) sobre las capacidades tecnológicas existentes de nuestras Fuerzas Armadas de Colombia. El hecho más reciente sucedió el pasado 23 de enero de 2021, cuando fue capturado y expulsado del territorio colombiano un militar orgánico del ejército bolivariano de Venezuela, quién al parecer estaría haciendo labores de espionaje al interior del Ejército de Colombia y que de acuerdo al periódico El Tiempo: "El hombre fue detenido por el Ejército colombiano en La Jagua de Ibirico, en el departamento del Cesar. Según las fuentes, se encontraba en Colombia al parecer desde el 2019, adelantando labores de inteligencia". (El Tiempo, 2021).

En otras palabras, el espionaje ha sido parte de la condición del ser humano en todo el mundo, donde siempre ha existido el interés por obtener información sensible de su potencial enemigo, e inclusive de sus propios aliados, a modo de obtener ventajas dentro de cualquier conflicto político-militar. La estudiante Laura Múnera Pavón, de la facultad de Ciencias Sociales y Humanas de la Universidad de Antioquia de Medellín - Colombia, realizó en el año 2019 un trabajo investigativo titulado "El espionaje en Colombia, 1919-1945. Una mirada panorámica a través de los diarios El Tiempo, El Espectador y El Siglo" (Pavón, 2019), donde nos indica cómo las actividades de espionaje han estado presentes alrededor de todos los eventos de conflicto armado en Colombia durante décadas, en el que espías de grandes potencias como Rusia (conocida anteriormente como la Unión Soviética), estarían realizando actividades clandestinas con el fin de obtener información de

primera mano de las alianzas comerciales realizadas entre Colombia y Estados Unidos en la época.

Por otra parte, las actividades de espionaje se han realizado incluso cuando no existe una guerra en desarrollo y solo hay países aliados establecidos. El columnista y editor Ben Macintyre del diario The Time en Nueva York, Estados Unidos, autor del libro titulado "Espía y Traidor: la mayor historia de espionaje de la guerra fría" realizado en el año 2019 (Macintyre, 2019), nos describe cómo las actividades de espionaje se incrementaron posterior a la terminación de la Segunda Guerra Mundial en 1945, donde Estados Unidos y la Unión Soviética, por razones ideológicas y políticas, aumentaron sus actividades clandestinas y oscuras, con el fin de desestabilizar y derrocar a los gobiernos de turno.

En efecto, este tipo de conductas delictivas por parte de algunos miembros de la Armada Nacional de Colombia y de la constante amenaza externa por efectuar labores de espionaje a la Fuerza Pública, es de gran preocupación por parte del alto mando naval, en donde es claro la necesidad, a corto plazo, de adquirir herramientas tecnológicas de contramedidas electrónicas que permitan fortalecer las capacidades y medidas activas en seguridad de la información operacional, mitigar el riesgo existente y neutralizar la fuga de información al interior de las Unidades Militares y Dependencias de la Institución.

Por lo tanto, es necesario efectuar este artículo científico bajo el concepto de una investigación documental, empleando una técnica de rastreo, recopilación y detección de empresas especializadas en la elaboración y entrega de soporte técnico de equipos de contramedidas electrónicas, que cumplan con las características requeridas en soportes, cubrimiento y tecnología. Del mismo modo, se realizó una matriz técnica que coadyuve a determinar y seleccionar los dispositivos de contramedidas electrónicas más eficientes a emplear al interior de las Unidades Militares y Dependencias de la Armada Nacional de Colombia.

Por consiguiente, el artículo busca responder al siguiente interrogante ¿Qué clase de equipos de contramedidas electrónicas podrían ser empleados al interior de las Unidades Militares y Dependencias de la Armada Nacional de Colombia, que permitan neutralizar y mitigar el riesgo existente relacionado con la fuga de información operacional?.

Metodo

La investigación adelantada tiene como propósito, en primer lugar, generar conciencia a todos los lectores sobre la importancia de aplicar medidas activas y pasivas de carácter tecnológico al interior de nuestras unidades y dependencias institucionales, el cual logre mitigar la fuga de información sensible que tanto daño causa a la conducción de operaciones navales. En segundo lugar, tiene como finalidad presentar un análisis técnico exhaustivo para la selección de herramientas tecnológicas de contramedidas electrónicas que apoyen a la protección y seguridad en el manejo de la información.

Por tanto, este artículo emplea una metodología de investigación documental, utilizando técnicas de rastreo de información de fuentes primarias, bibliográficas, revistas electrónicas, periódicos, documentos oficiales, informes técnicos relevantes, los cuales logren detectar, en el mercado actual, empresas

tecnológicas que ofrezcan la capacidad de suministrar equipos de contramedidas electrónicas que se ajusten a las necesidades actuales al interior de la Institución Naval Militar, con relación a mitigar el riesgo de la fuga de información operacional. Posteriormente, se elaborará una matriz técnica que permita seleccionar el dispositivo de contramedidas electrónicas más eficiente a emplear.

Con esto se quiere decir que, los criterios de selección para determinar los equipos de contramedidas electrónicas se basaron en que sean de última generación tecnológica, que cumplan de manera eficiente con el objetivo relacionado en la neutralización de fuga de información operacional. También, que los equipos cuenten con la garantía necesaria para el cumplimiento del mismo, de igual forma, el soporte técnico esté incluido al momento de la adquisición, que la herramienta tecnológica sea de fácil manejo por parte del operador (que no requiera de mucho personal para el empleo del mismo) y finalmente, que estos equipos electrónicos no sean perjudiciales para la salud de los usuarios o tengan contraindicaciones médicas.

Por último, como herramienta de apoyo metodológico, se van a emplear los libros titulados *"Alta redacción: Informes científicos, académicos, técnicos y administrativos"* del autor William Ángel Salazar Pulido (Salazar, 2010), y el libro "*Metodología de la Investigación. 4ta Edición"* del autor Cesar Augusto Bernal Torres (Bernal, C. 2016), los cuales tienen como finalidad orientar la organización del artículo científico en los temas relacionados con la estructura del texto, metodología, coherencia y cohesión, conectores, corrección de frases, signos de puntuación e interpretación de gráficas.

Resultados

El presente artículo, desarrollado bajo el concepto de investigación documental en el cual se emplearon técnicas de búsqueda, recopilación y análisis de la información de diferentes fuentes primarias, bibliográficas, documentales y electrónicas relevantes, arrojó como resultado la detección de dos empresas especializadas en la investigación, elaboración y suministro de herramientas tecnológicas de contramedidas electrónicas enfocadas a la protección y seguridad en el manejo de la información sensible en las empresas e instituciones gubernamentales, las cuales está la empresa Mexicana TAMCE – Tecnología Avanzada en Medidas y Contramedidas Electrónicas (TAMCE, 2021) y la empresa Norteamericana REI – Research Electronics International (REI, 2021), ambas empresas con la capacidad de cobertura en soporte técnico en países de Suramérica, lo cual es una ventaja al momento de establecer una contratación.

Conviene resaltar que, los equipos de contramedidas electrónicas suministradas por las empresas anteriormente descritas, cumplen con la totalidad de las características y necesidades tecnológicas requeridas en la presente investigación, relacionado con la mitigación del riesgo y neutralización de la fuga de información operacional al interior de la Armada Nacional de Colombia, de acuerdo a los criterios de selección establecidos y detallados en la siguiente tabla así:

Tabla 1.
Criterios de selección para determinar las empresas tecnológicas.

N°	Criterios de selección
1	Tecnología digital avanzada, especializada en la detección de equipos discretos y supresores de grabadores de información confidencial.
2	Empresas matrices que elaboran equipos tecnológicos para la protección y manejo de la seguridad de la información requerida en la presente investigación.
3	Que cumplan con cobertura en soporte técnico en países de Suramérica, lo cual es una ventaja al momento de establecer una contratación.
4	Programas de capacitación anual al personal que requiera conocimiento en el empleo y mantenimiento de los diferentes equipos de contramedidas electrónicas suministrados.
5	Empresas especializadas en el suministro de equipos tecnológicos para la protección de reuniones operacionales frente a grabaciones no autorizadas, logrando interferirlas y anularlas mediante emisiones de señales inaudibles para las personas.
6	Empresas certificadas por las más altas normas de estándar de calidad de producción.
7	Empresas que se caracterizan por la garantía en los productos tecnológicos ofrecidos.
8	Equipos de contramedidas electrónicas certificadas que a la fecha no han sido perjudiciales para la salud o contraindicaciones médicas para los usuarios.

Fuente: Elaboración Propia

En decir, dentro de la investigación documental realizada se detectaron muchas otras empresas tecnológicas especializadas en el desarrollo, elaboración y suministro de herramientas tecnológicas de contramedidas electrónicas; sin embargo, fueron descartadas dentro de la investigación por no cumplir con los criterios de selección mínimos requeridos y establecidos en la anterior Tabla N° 1, llegando a generar algún tipo de traumatismo administrativo y operacional por no cumplir con las necesidad existentes al interior de las Unidades.

Por otro lado, se logró detectar a la consultoría Ecommerce y Marketing Digital, cuyo propietario es el especialista norteamericano Vicent Ferrer consultor en marketing digital, Estrategia y Modelo de Negocio Online (VICENT, 2021), en el cual da a conocer información significativa sobre las definiciones y conceptos básicos que el lector del artículo debe comprender sobre la terminología y capacidades de los equipos de contramedidas electrónicas existentes en el mercado así:

Equipos Analizadores del Espectro Electromagnético

Es una herramienta de medida por medio del cual se evalúan las señales eléctricas en determinadas frecuencias. A través de una pantalla, los analizadores muestran las componentes espectrales que se encuentran en la entrada, ya sea de una señal eléctrica, óptica o acústica. Esta capacidad analiza el espectro radioeléctrico

en contramedidas electrónicas, de emisiones de radio frecuencia y de espectro radioeléctrico de redes de celulares o de sistemas de comunicaciones ocultas. En la siguiente tabla se describen los tipos de analizadores de espectro existentes así:

Tabla 2.
Tipos de Analizadores del espectro existentes.

N°	Tipo	Descripción
1	Analizador Analógico	Funcionan utilizando un filtro pasabanda de frecuencia, empleando un receptor banco de filtros. Este tipo de analizadores muestran la estructura del espectro de las ondas de radiofrecuencia ya sean eléctricas, acústicas u ópticas, entre otras, en la trama del dominio de frecuencias, no la del tiempo.
2	Analizador Digital	Usan tecnología más avanzada para convertir la señal en componentes espectrales a través de un proceso matemático. Tanto los analizadores analógicos como los digitales pueden incluir un generador que les permite ser empleados como analizadores de redes a nivel básico.
3	Analizador de señales vectoriales	Este analizador es de radiofrecuencia y llega a suplir al analizador de espectro a la hora de medir, debido al poder que tiene en la realización de las tareas de medida y precisión del analizador, así como de demodulación en la recuperación de la señal moduladora.

Fuente: Vicent Ferrer

Además, dentro de los tipos de analizadores del espectro existentes, en la siguiente tabla se detalla las clases de señales que se pueden evaluar con estos dispositivos electrónicos así:

Tabla 3.
Tipos de señales que puede evaluar el analizador de espectro.

N°	Tipo	Descripción Señal
1	Señal Electromagnética	El analizador del espectro puede graficar la potencia de un canal determinado por su frecuencia, durante la emisión de cadenas de radio y televisión analógica.
2	Señal Luminosa	A través de su uso se puede evaluar el espectro luminoso de los colores que componen a una luz en una gráfica. A razón de esto, el color blanco, por ejemplo, se vería como una línea recta.
3	Señal Sonora	Descifrar y representar una señal sonora como una mezcla o combinación de frecuencias de sonido que activan el oído es posible con estos analizadores.

Fuente: Vicent Ferrer

Equipos Detectores de Juntas No Lineales

Estos equipos representan la última tecnología en el ámbito de la radiodetección no lineal. Es un equipo de contramedidas electrónicas diseñado para detectar dispositivos ocultos mediante barridos electrónicos. Su funcionamiento se basa en la irradiación de señal y en el análisis de ondas armónicas reflejadas de señales de dispositivos electrónicos, sin importar que el mismo se encuentre radiando o no, conectado, o incluso encendido, teniendo en cuenta la capacidad de extenderse hasta 148 cm para investigar áreas difíciles de alcanzar.

Equipos Supresores de Grabaciones

Son dispositivos que protegen al usuario frente a grabaciones no autorizadas al interferirlas y anularlas mediante una señal de enmascaramiento inaudible para las personas. Es un supresor de grabadores compuesto por dos modos de operación diseñados para proteger al usuario de grabaciones o escuchas no autorizadas. Los dispositivos se instalan en el área a proteger y se activan de manera inalámbrica con un control remoto. Mediante sus funciones de supresión ultrasónica y enmascaramiento de voz audible, interfiriendo y ensuciando las grabaciones realizadas con grabadores de audio digitales y analógicos, Tablets y Smartphones (afectando a un 85% de estos).

Equipos Inyectores de Ruido Ultrasónico

Los equipos inyectores de Ruido Ultrasónico están diseñados para inutilizar cualquier dispositivo de escucha que transmita por medio de corriente alterna de 110 o 220 Voltios. Una tecnología de escucha muy utilizada y muy difícil de detectar es la de transmisores de audio por onda portadora de corriente alterna. Existen desde complejos transmisores cifrados hasta simples micrófonos para el control que transmiten audio ambiental por corriente alterna (110/220 Voltios).

Esta transmisión podrá ser de larga distancia hasta su receptor siempre y cuando se encuentren instalados en la misma fase. Ante un análisis espectral o un barrido de radio frecuencia, estos transmisores permanecen inmunes sin posibilidad de ser detectados. Estos equipos inyectan un ruido entre 300 Hz y 7Mhz, que ensucia y bloquea cualquier transmisión de audio sobre la línea de energía alterna. El dispositivo no interfiere con el normal funcionamiento de los artefactos conectados a la red eléctrica. Estos equipos están catalogados como dispositivos de contramedidas electrónicas fundamentales para cualquier sala de juntas confidencial.

Matriz técnica para la selección de equipos de contramedidas electrónicas

Como parte del resultado del presente artículo científico, se elaboró una matriz técnica que permita determinar y seleccionar los tipos de equipos de contramedidas electrónicas más eficientes que podrían ser empleados al interior de las Unidades Militares y Dependencias de la Armada Nacional de Colombia, que permitan mitigar y contrarrestar la fuga de información operacional, teniendo en cuenta las tres capacidades de equipos de contramedidas electrónicas existentes anteriormente descritas (Analizadores del espectro, detectores de juntas no lineales y Supresores de señales), de acuerdo a las necesidades puntuales de cada Unidad y Dependencia de la Armada Nacional de Colombia así:

Tabla 4.
Matriz técnica para la selección de equipos de contramedidas electrónicas.

Nombre	Funcionalidad	Frecuencias	Rango	Imagen
OSCOR BLUE (Analizador)	Analizador de barrido rápido para detectar trasmisiones y señales de escuchas desconocidas, disruptivas y anómalas. Realiza análisis de emisiones en (RF).	10 kHz a 24 GHz	25 metros de diámetro	
MESA (Analizador)	Analizador versátil diseñado para localizar señales desconocidas, análisis de emisiones de señales RF e investigación de uso indebido del espectro electromagnético.	10 kHz a 6 GHz	5 metros de diáme-tro	
ANDRE (Analizador)	Receptor de banda ancha portátil que detecta transmisiones desconocidas, ilegales o que interfieren. Localiza trasmisiones de RF, infrarrojos, luz visible y trasmisores cercanos.	10 kHz a 12 GHz	6 metros de diáme-tro	
ORION 2.4 (Detector)	Diseñado para detectar y ubicar cámaras, micrófonos y otros dispositivos electrónicos ocultos, independiente si el dispositivo está radiante, cableado o apagado.	2.404 GHz a 2.472 GHz	40 Cm ancho de detección	
SUGA CEILING (Supresor)	Ideal para la protección de reuniones al evitar la grabación de información confidencial. Se instala en la parte superior del área a proteger. Interfiere el audio en un 90%.	2.4 GHz	De 1 a 3 metros diámetro	
STORM TOWER (Supresor)	Funciona como supresor de grabadores diseñado para proteger al usuario de grabaciones o escucha no autorizadas. Interfiere el audio en un 90% de dispositivos de grabación.	300 Hz a 18000 Hz	De 5 a 10 metros diámetro	
INYEC-TOR DE RUIDO IR-AC (Supresor)	Diseñado para inutilizar cualquier dispositivo de escucha que trasmita por medio de la corriente alterna. No interfiere con el funcionamiento de artefactos conectados la red eléctrica.	300 Hz a 7 MHz	Corriente alterna de 110 o 220 Voltios	

Fuente: Elaboración Propia

Plan de Mantenimiento y Reparación de Equipos Electrónicos

Las herramientas tecnológicas de contramedidas electrónicas requieren por parte de sus operarios un mantenimiento preventivo denominado Plan M.R.S (Mantenimiento, Repuesto y Suministro), los cuales obedecen a los tiempos y recomendaciones del fabricante en aras de que al momento en que sean utilizados se encuentren en óptimas condiciones de funcionamiento. A continuación, se presenta un modelo diseñado para su implementación al momento de ser adquiridos estos equipos de contramedidas electrónicas así:

Figura 1.
Plan de mantenimiento y reparación de equipos de contramedidas electrónicas.

FORMATO PLAN MRS MENSUAL DE MANTENIMIENTO

REPUBLICA DECOLOMBIA

Proceso: Mantenimiento | Autoridad:

Código: | Rige a partir de: Dia/Mes/Año | Página 1 de 1

Nombre Unidad:

Nombre del Equipo | MRS PARA EL MES DE MAYO 2020

No.	ACTIVIDAD	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
01	Limpieza de la pantalla táctil.																														
02	Limpieza de los conectores de la Antena Direccional.																														
03	Limpieza de los conectores de la Antena de látigo / dipolo.																														
04	Limpieza de los conectores de la Antena Localizador rastreador																														
05	Limpieza de los conectores de la Antena en circuito.																														
06	Limpieza de los conectores de los auriculares.																														
07	Limpieza del conector del adaptador de corriente.																														
08	Verificación y estado de las batería extraíbles.																														
09	Limpieza y revision del cargador de las baterías.																														
10	Mediciones de voltaje																														

Nombres Completos y Firma

Operario del Equipo Contramedida Electrónica

Fuente: Elaboración Propia

Encuesta Estructurada para la Detección de Empresas Tecnológicas

Como herramienta de investigación, se elaboró un modelo de encuesta estructurada, apoyado con una serie de preguntas escritas, con el fin de detectar las empresas que puedan ofrecer los equipos de contramedidas electrónicas requeridos para la neutralización de fuga de información al interior de la institución así:

Encuesta para la detección de Empresas Tecnológicas que suministran equipos de contramedidas electrónicas			
N°	**Pregunta**	**Capacidad**	
1	¿Los equipos y herramientas tecnológicas de contramedidas electrónicas de hardware y software cumplen con la garantía técnica de dos (2) años, desde el momento de su adquisición?	SI	NO

Encuesta para la detección de Empresas Tecnológicas que suministran equipos de contramedidas electrónicas			
N°	**Pregunta**	**Capacidad**	
2	¿Los equipos de contramedidas electrónicas cumplen con el respaldo de actualización tecnológica por mínimo los siguientes diez (10) años?	SI	NO
3	¿La empresa tiene la capacidad de entregar los equipos y herramientas tecnológicas de contramedidas electrónicas en Colombia?	SI	NO
4	¿La empresa tiene la capacidad de realizar las pruebas preliminares de los equipos de contramedidas electrónicas proyectados adquirir?	SI	NO
5	¿La empresa cuenta con el personal idóneo, para realizar las capacitaciones y entrenamientos mínimo a diez (10) personas de las capacidades de los equipos de contramedidas electrónicas?	SI	NO
6	¿Los equipos y herramientas tecnológicas de contramedidas electrónicas vienen con los manuales en español (uso, operación y mantenimiento) de cada equipo requerido?	SI	NO
7	¿De ser requerido, la empresa cuenta con la capacidad de entregar los equipos de contramedidas electrónicas en otras guarniciones de Colombia como Cartagena, Villavicencio y Cali?	SI	NO
8	¿Los equipos y herramientas tecnológicas de contramedidas electrónicas cumplen con los mantenimientos preventivos mínimos de dos (2) años, con trasferencia de conocimiento cada vez que se realice un soporte?	SI	NO
9	¿La empresa cuenta con acreditación de experiencia en participación, ejecución y suscripción de contratos celebrados con entidades públicas o empresas privadas?	SI	NO
10	En caso de que exista insatisfacción en los equipos de contramedidas electrónicas suministrados, la empresa tiene la capacidad de realizar la corrección o cambio de los mismos dentro de los quince (15) días hábiles.	SI	NO
11	¿Los equipos y herramientas tecnológicas de contramedidas electrónicas vienen con su respectiva factura, acuerdo con los requerimientos establecidos en la Ley No? 223 de 1995?	SI	NO
12	¿La empresa garantiza que los equipos de contramedidas electrónicas que se proyectan adquirir son nuevos y de calidad?	SI	NO

Encuesta para la detección de Empresas Tecnológicas que suministran equipos de contramedidas electrónicas			
N°	**Pregunta**	**Capacidad**	
13	¿La empresa matriz elabora las herramientas tecnológicas de contramedidas electrónica enfocadas para la protección y manejo de la seguridad de la información requerida?	SI	NO
14	¿La empresa tiene registrado sus productos en la ventanilla única de comercio exterior – VUCE?	SI	NO
15	¿La empresa certifica que estos equipos de contramedidas electrónicas no son perjudiciales para la salud o contraindicaciones médicas para los usuarios?	SI	NO

_____

Nombre Completo y Firma responsable
Gerente de Empresa

Discusión

Durante el rastreo y recopilación de información necesaria para la investigación a través de la bibliografía documental y electrónica relevante, se pudo evidenciar que existe un trabajo investigativo en Colombia realizado por la señora Mara Cardozo Serge en el año 2013 en la Universidad Militar Nueva Granada, relacionado con la Seguridad Electrónica en donde titula *"Mercado de Seguridad Electrónica en Colombia como una oportunidad de trabajo y emprendimiento"* (Cardozo, M. 2013).

Si bien cierto, este trabajo investigativo está enfocado hacia la seguridad electrónica como soporte y apoyo a las medidas activas de seguridad física o de instalaciones, comprendida en el empleo de equipo técnico que ayuden a elevar la seguridad electrónica en las instalaciones mediante la detección de amenazas internas y externas, dispositivos biométricos para el control de acceso de personas, vigilancia óptica mediante fotografía, sistemas de circuito cerrado de televisión y protección de seguridad en las comunicaciones. Probablemente, puede complementar en la conceptualización de medidas activas, pasivas e implementación del uso de equipos de contramedidas electrónicas para la protección de la información en las reuniones operacionales, mitigando el riesgo de fuga de la información crítica al interior de la Armada Nacional de Colombia.

Asimismo, encontramos al historiador Benjamín Ramos Álvarez, autor del libro *"Avances en Criptología y Seguridad de la Información"* (Álvarez, 2004), donde nos señala, cómo desde el año 1978 en Colombia se empleó el uso de herramientas tecnológicas como la Criptografía, empezándose a ver la seguridad de la información como una inversión y no como un gasto. Este concepto de seguridad en la gestión, diseño y ejecución de protocolos de seguridad de la información y seguridad en las redes e internet, se convirtió como prioridad en la agenda de muchos directivos y gerentes en las empresas privadas, públicas, industrias, entidades gubernamentales y castrenses en Colombia.

Finalmente, encontramos al especialista en administración de la seguridad Javier González, autor del proyecto investigativo titulado *"la necesidad de aplicar la administración de riesgos en las Unidades Militares del Ejército Nacional"* (Prieto, 2013), en el cual nos postula cómo en las instituciones militares requieren la adquisición de herramientas tecnológicas eficaces que coadyuven al fortalecimiento de la adecuada administración y mitigación de riesgos relacionados con el inadecuado manejo de la seguridad de la información y pérdida de la misma al interior de la Fuerza Pública en Colombia.

Conclusiones

De acuerdo a lo anteriormente expuesto, se puede concluir que:

En primer lugar, se pudo evidenciar la escasez de medidas activas y pasivas en el uso y restricción de la información critica al interior de las Unidades Militares y Dependencias de la Armada Nacional de Colombia, observando la necesidad actual de implementar equipos de contramedidas electrónicas que neutralicen la fuga de información operacional, contribuyendo al mejoramiento del desarrollo de las operaciones militares, blindando sus capacidades actuales, su imagen institucional y cumplimiento de su misión constitucional (Art. 217).

En segundo lugar, se logró comprobar cómo la amenaza interna (grupos armados ilegales) que delinque en Colombia, buscan constantemente subvertir la ética y moral del talento humano orgánico de la Armada Nacional de Colombia, con el único fin de obtener la información operacional y la colaboración de las actividades ilícitas, observando cómo el factor humano es el eslabón más débil de la cadena, en el cual se puede vulnerar la seguridad con el manejo de la información sensible al interior de la Institución y el factor sorpresa para la ejecución de las operaciones navales militares, por el acceso que logra tener el enemigo.

En tercer lugar, se demostró cómo la amenaza externa constantemente busca obtener información sensible (espionaje) sobre las capacidades existentes en las Fuerzas Armadas de Colombia, evidenciando la necesidad de adquirir herramientas tecnológicas de contramedidas electrónicas que neutralicen su capacidad e intención de obtener información sensible al interior de las Instituciones Castrenses.

En cuarto lugar, se logró la detección de dos empresas tecnológicas que cumplieran con todos los criterios de selección establecidos en la presente investigación documental, de acuerdo a las características, capacidades y necesidades existentes, relacionados con la mitigación del riesgo y neutralización de la fuga de información operacional al interior de la Armada Nacional de Colombia.

En quinto lugar, se logró responder al interrogante: "¿qué clase de equipos de contramedidas electrónicas podrían ser empleados al interior de las Unidades y dependencias de la Armada Nacional de Colombia?", en donde a través del empleo de la matriz técnica se logró determinar y seleccionar la clase de equipos técnicos más eficientes que podrían ser empleados al interior de las Unidades, teniendo en cuenta las tres capacidades de contramedidas electrónicas existentes (analizadores del espectro, detectores de juntas no lineales y supresores de señales), describiendo la funcionalidad, nombre del equipo, capacidades (rango y frecuencia) e imagen ilustrativa de la herramienta tecnológica, ajustándose a las necesidades actuales, que permitan mitigar y neutralizar la fuga de información operacional.

Por último, con el desarrollo del presente artículo científico, se logró concientizar al lector sobre la importancia de proteger y gestionar adecuadamente la información operacional sensible al interior de las Unidades de la Armada Nacional de Colombia que permita, a través de la adquisición de equipos de contramedidas electrónicas, fortalecer la seguridad de la información en reuniones operacionales frente a grabaciones no autorizadas, al interferirlas y neutralizarlas, complementándolo con medidas pasivas, como la no divulgación de métodos operacionales a personal no autorizado, asimismo, no difundir información operacional por medios no seguros (mensajes de texto, WhatsApp, entre otras aplicaciones) y finalmente, emplear el principio de la compartimentación con el personal de la Unidad que no esté directamente comprometido en el desarrollo de las operaciones navales.

Referencias

Álvarez, B. R. (2004). *Avances en Criptología y Seguridad de la Información* Madrid, España: Díaz de Santos.

Bernal, C. (2016). *Metodología de la Investigación. (4ta Edición.). Bogotá, Colombia*: Pearson Educación. Pág. 109.

Cardozo, M. S. (2013). *Mercado de seguridad electrónica en Colombia como una oportunidad de trabajo y emprendimiento.* Bogotá, Colombia: Universidad Militar Nueva Granada.

Constituyente, A. N. (1991). *Constitución Política de Colombia 1991. Capítulo 7. De la Fuerza Pública.* Bogotá, Colombia.

El Tiempo. (2017). *Seis miembros de la Armada Nacional fueron capturas en Buenaventura por tráfico y concierto para delinquir con grupos armados ilegales, entre los cargos por los que se le señalan.* Bogotá, Colombia. Recuperado el día 26 de enero de 2021. Pág. Web https://www.eltiempo com/colombia/cali/integrantes-de-laarmada-nacional-de-colombia fueron-capturados-en buenaventura-157016

El Tiempo. (2021). *El hombre fue detenido por el Ejército colombiano en La Jagua de Ibirico, en el departamento del Cesar. Según las fuentes, se encontraba en Colombia al parecer desde el 2019, adelantando labores de inteligencia.* Bogotá, Colombia. Recuperado el día 28 de enero de 2021. Página Web. https://www.eltiempo.com/justicia/conflicto-y-narcotrafico/ expulsan-a-militar-venezolano-senalado-de-hacer-espionaje-al ejercito-562316

Macintyre, B. (2019). *Espía y Traidor: La mayor historia de espionaje de la Guerra Fría. New York, Estados Unidos:* Grupo Planeta.

Pavón, L. M. (2019). *El espionaje en Colombia, 1919-1945. Una mirada panorámica a través de los diarios El Tiempo, El Espectador y El Siglo.* Medellín, Colombia: Universidad de Antioquia.

Prieto, J. A. (2013). *La necesidad de aplicar la administración de riesgos en las unidades militares del Ejército Nacional.* Bogotá, Colombia: Universidad Militar Nueva Granada.

REI, (2021). *Research Electronics Internacional. Analizadores del espectro Azul ORCOR. Protección para reuniones.* Tennessee, Estados Unidos. Recuperado el día 02 de febrero de 2021. Página Web. https://reiusa.net rf-detection/oscor-blue-spectrum analyzer/

Salazar, W. Á. (2010). *Alta redacción: Informes científicos, académicos, técnicos y administrativos.* Bogotá, Colombia: NET Educativa. Pág. 84.

Tamce, (2021). *Tecnología Avanzada en medidas y contramedidas electrónicas. Protección para reuniones.* Ciudad de México, México. Recuperado el día 30 de enero de 2021. Página Web. http://tamce.net/categorias/31 proteccion_de_reuniones

Vicent, F (2021), *Vicent Ferrer. Analizador del Espectro. Consultor digital en Marketing Digital,* Estrategia y Moldeo de negocio en online. Recuperado el día 02 de febrero de 2021. Página Web. https://vicentferrer.com analizador-de-espectro/