CN (RA) Gladys Elena Medina Ochoa - TC. Milena Elizabeth Realpe Díaz
Ivonn Alexandra Niño Medina
Editoras

HACIA LA CONSTRUCCIÓN DEL CONCEPTO DE SEGURIDAD Y DEFENSA,

UN APORTE DESDE LA INVESTIGACIÓN FORMATIVA

Ediciones Escuela Superior de Guerra
Colombia

HACIA LA CONSTRUCCIÓN DEL CONCEPTO DE SEGURIDAD Y DEFENSA,

UN APORTE DESDE LA INVESTIGACIÓN FORMATIVA

CN. (RA) Gladys Elena Medina Ochoa
TC. Milena Elizabeth Realpe Díaz
Ivonn Alexandra Niño Medina
Editoras

Catalogación en la publicación Escuela Superior de Guerra
Hacia la construcción del concepto de seguridad y defensa, un aporte desde la investigación formativa / Editoras: Gladys Elena Medina Ochoa, Milena Elizabeth Realpe Díaz y Ivonn Alexandra Niño Medina – Bogotá.: Escuela Superior de Guerra "General Rafael Reyes Prieto", 2021.
1 volumen: 214 páginas, ilustraciones; 15x23,5 cm.
ISBN-E: 978-958-53101-5-5
1. Influencia del océano en la política nacional de Colombia. 2. La Amazonia colombiana: oportunidades y retos para el Ejército colombiano. 3. Implicaciones de una eventual competencia de la Corte Penal Internacional a la luz de los derechos de las víctimas en el marco de la Justicia Especial para la Paz. 4. Modelo de auditoría de seguridad cibernética aplicado a la Secretaria General de la Alcaldía de Bogotá. 5. Estrategia para la adopción de una cultura organizacional de ciberseguridad en la Alcaldía de Neiva.
Archivo descargable en formato PDF en: esdeguelibros.edu.co

Código THEMA: JWA Código DEWEY: 363.3

LIBRO RESULTADO DE INVESTIGACIÓN

Corrección de estilo: María del Mar Agudelo
Diagramación: José Vicente Gómez
Imagen de carátula: Freepik

Impreso por:
Área imprenta y publicaciones COGFM

Proceso de arbitraje:
Primer concepto
Evaluación: 20 de agosto de 2020

Segundo concepto
Evaluación: 16 de septiembre de 2020

CONTENIDO

PARTE III
MAESTRÍA EN CIBERSEGURIDAD Y CIBERDEFENSA

PRESENTACIÓN

El libro *Hacia la construcción del concepto de seguridad y defensa, un aporte desde la investigación formativa* compila las ponencias magistrales de magísteres en geopolítica y estrategia, derechos humanos y derecho internacional humanitario y ciberseguridad y ciberdefensa, en el marco del Seminario Virtual de Resultados de Investigación Formativa, realizado el 8 de mayo de 2020, a través de la plataforma virtual Blackboard AVAFP de la Escuela Superior de Guerra. Esta publicación reúne productos resultado de investigación de los siguientes proyectos de investigación: a) "Influencia del océano en la política nacional de Colombia", de la línea de investigación "Estrategia, Geopolítica y Seguridad Hemisférica", del grupo de investigación "Centro de Gravedad", reconocido y categorizado en (A1) por MinCiencias, registrado con el código COL0104976, vinculado a la Maestría en Estrategia y Geopolítica; b) "Esclarecimiento de la verdad histórica sobre la violencia estructural en Colombia, provocada al medio ambiente y a las víctimas del conflicto: aporte de las Fuerzas Militares en la reconstrucción del tejido social", de la línea de investigación "Memoria Histórica, Memoria Institucional,

Derechos Humanos y Derecho Internacional de los Conflictos Armados (DICA), del grupo de investigación "Memoria Histórica, Construcción de Paz, Derechos Humanos, DICA, Justicia", reconocido y categorizado en (C) por MinCiencias, registrado con el código COL0141423, vinculado a la Maestría en Derechos Humanos y Derecho Internacional de los Conflictos Armados, y c) "Gestión de riesgos en seguridad digital para la infraestructura crítica", de la línea de investigación "Seguridad Digital", del grupo de investigación "Masa crítica", reconocido y categorizado en (B) por MinCiencias, registrado con el código COL0123247, vinculado a la Maestría en Ciberseguridad y Ciberdefensa, todos los grupos anteriores adscritos y financiados por la Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia.

Mayor General Luis Mauricio Ospina Gutiérrez
Director de la Escuela Superior de Guerra "General Rafael Reyes Prieto"

INTRODUCCIÓN

Parte de la misión de la Escuela Superior de Guerra es formar líderes estratégicos militares y civiles nacionales e internacionales para afrontar los desafíos a la seguridad y la defensa nacionales, a través de sus diferentes maestrías. Así, bajo el liderazgo de la Maestría en Ciberseguridad y Ciberdefensa, se desarrolla el Seminario Virtual de Resultados de Investigación Formativa, con la participación de maestrantes que dan cuenta de la importancia de formar analistas en los diferentes escenarios que impactan directamente en el ámbito estratégico del país y, por supuesto, en la seguridad y la defensa.

A través de ponencias elaboradas como modalidad de grado, se observa la responsabilidad social de los maestrantes, quienes enmarcan problemáticas que se conciben dentro los nuevos retos que enfrenta el Estado colombiano. Tras un análisis exhaustivo, profesional, y desde el pensamiento crítico, han desarrollado productos de alta calidad académica.

Las dinámicas cambiantes que vive el Estado colombiano generan la necesidad de crear estrategias flexibles basadas en conocimientos

adquiridos, a través de la mirada crítica de asesores que se hayan profesionalizado para tal fin. Así, el Seminario Virtual de Resultados de Investigación Formativa presenta generalidades desde la estrategia y la geopolítica, los derechos humanos y el derecho internacional de los conflictos armados, así como desde la ciberseguridad y la ciberdefensa.

El presente documento se compone de cinco partes. La primera registra una búsqueda por evidenciar la necesidad de reconocer el potencial que tiene el país en los mares. Así, hace un llamado a la creación de estrategias, políticas económicas, sociales y educativas, con el fin de enmarcar un desarrollo sostenible y controlado de este recurso e impulsar, desde la academia, la participación del Estado en el fortalecimiento de los intereses marítimos.

La segunda parte se enfoca en las oportunidades y los retos que tiene el Ejército nacional en la Amazonia colombiana. Mediante un análisis desde el enfoque geopolítico y la incidencia de esta región en los intereses nacionales, da cuenta de los planes y de las acciones que ha realizado la fuerza militar, para así forjar estrategias claves, con variables medioambientales, de cooperación internacional y recursos, materializadas en ventajas estratégicas para Colombia.

La tercera parte presenta un análisis sobre las implicaciones de una eventual competencia de la Corte Penal Internacional, a la luz de los derechos de las víctimas, en el marco de la Justicia Especial para la Paz. Esto, teniendo en cuenta que esta corte se encarga de garantizar el reconocimiento de los derechos de las víctimas —en esta ocasión, del conflicto armado colombiano— y de supervisar el cumplimiento de las actividades establecidas dentro del acuerdo de paz firmado con las Fuerzas Armadas Revolucionarias de Colombia (FARC-EP).

La cuarta parte contextualiza la necesidad de implementar un modelo de auditoría de seguridad cibernética aplicado a la Secretaría General de la Alcaldía de Bogotá, Colombia, teniendo en cuenta los avances tecnológicos y los riesgos existentes que afectan la ciberseguridad de las entidades.

Finalmente, la quinta parte plantea adoptar una cultura organizacional de ciberseguridad en la Alcaldía de Neiva, Colombia, debido a

que para que exista seguridad cibernética, no es suficiente el empleo de tecnologías avanzadas, también deben existir buenas prácticas por parte de los usuarios.

Desde diferentes visiones de la academia, surgen estas *Memorias*, que alimentan diversas formas de observar, analizar, investigar y proponer estrategias de impacto nacional.

PARTE I

MAESTRÍA EN ESTRATEGIA Y GEOPOLÍTICA

CAPÍTULO I

INFLUENCIA DEL OCÉANO EN LA POLÍTICA NACIONAL DE COLOMBIA*

Teniente de Navío Nicolás Correa Ramos

* Ponencia resultado del proyecto de investigación titulado *Influencia del océano en la política nacional de Colombia*, de la Maestría en Estrategia y Geopolítica, de la línea de investigación *Estrategia, Geopolítica y Seguridad Hemisférica*, del grupo de investigación *Centro de Gravedad*. El grupo está categorizado en (A1) por Minciencias, registrado con el código COL0104976 y adscrito y financiado por la Escuela Superior de Guerra de la República de Colombia. La investigación fue presentada como opción de grado para optar por el título de magíster en Estrategia y Geopolítica de la Escuela Superior de Guerra "General Rafael Reyes Prieto".

Resumen

Colombia tiene un gran potencial para explotar sus mares, tanto en la región Caribe como en la región Pacífica. Así, es necesario buscar estrategias políticas, económicas, sociales y educativas para incentivar a los ciudadanos colombianos a que conozcan ese gran recurso que tienen al alcance, para un desarrollo marítimo sostenible y controlado. Históricamente, los países que han sabido utilizar la potencia que ofrece el mar en todos los ámbitos han percibido sus grandes beneficios, pues los intereses marítimos van muy ligados a los intereses de la nación. En el caso colombiano, existen muchas áreas de desarrollo y de explotación marítima donde se observa la falta de conocimiento y regulación por parte de la población y de sus gobernantes. De ahí la importancia de investigar sobre las capacidades de Colombia para lograr ser un país marítimo integral.

Palabras clave: desarrollo marítimo sostenible; explotación marítima; intereses marítimos; intereses de la nación; país marítimo integral.

Abstract

Colombia has great potential to exploit its seas, both in the Caribbean region and in the Pacific region. It is necessary to look for political, economic, social and educational strategies to encourage Colombian citizens to know such resource for a sustainable and controlled maritime

development. Historically, countries that have known how to develop their maritime potential in all its areas have perceived all its benefits, due to the link between the maritime interests and the interests of the nation. In Colombia, there are many areas of development and maritime exploitation where the lack of knowledge and regulation from the citizens and its governors is evident. For this reason, it is important to investigate the full capabilities of Colombia to become an integral maritime country.

Keywords: Interests of the nation; maritime development; maritime interests; maritime country; sustainable.

1. Introducción

El mar es el centro de la prosperidad y seguridad
de todas las naciones.
Geoffrey Till

Durante la conquista de Suramérica, y en especial la región que hoy es Colombia siempre se buscó el camino hacia el Dorado, a lo llevó que la colonización llegara a Bogotá en 1538. Esta, quedó establecida como la capital del país, pero los dos mares que rodean el territorio, y su potencial para el desarrollo marítimo (por encima de otros países de Suramérica), fueron desaprovechados.

Este capítulo expone el estado actual del ámbito marítimo en Colombia, así como las oportunidades que tiene el país para explotar sus capacidades al respecto. Desde la teoría hasta casos comparativos con otros países permiten observar que el problema puede estar en la voluntad del pueblo, en que quiera o no desarrollarse como país marítimo.

Desde los inicios del siglo XX, el *poder marítimo* ha sido una herramienta utilizada para beneficiar a un país, tanto en tiempos de paz como de guerra. El concepto abarca el sector industrial, el comercio exterior, las inversiones, las políticas y, por supuesto, las armadas (Mahan, 1890).

Ahora bien, Colombia es un país estratégicamente afortunado por contar con dos grandes océanos: el Atlántico, por intermedio del mar Caribe, y el Pacífico. Según esto, y siguiendo a Mahan (1890), para quien el desarrollo de un país depende de su proyección hacia el mar, Colombia debe enfocar sus esfuerzos en mirar de las costas hacia

afuera y proyectarse como una verdadera potencia marítima regional e internacional.

Para hacer un análisis geopolítico desde el punto de vista económico y lograr entender la infraestructura política y las riquezas de la sociedad, hay que tener en cuenta la geografía, los recursos naturales y los eventos históricos (Rosenberg, 2017). De ahí la importancia de aprovechar las oportunidades y de disminuir los obstáculos que se presentan, con el fin de plantear estrategias y políticas públicas que permitan una integración política, económica, social y militar de los actores públicos y privados que tengan impacto en el desarrollo marítimo de Colombia.

Se hace necesario entender la Política de Defensa y Seguridad vigente en Colombia, que impulsa el libre desarrollo del país a través de las fuerzas(Martínez Pachón, 2014). En el caso del aprovechamiento de los recursos marítimos y fluviales, es importante alinear los intereses nacionales con los intereses marítimos, en conexión con las instituciones públicas y privadas y las poblaciones costeras para realmente crear una conciencia oceánica nacional.

Las conclusiones permitieron plantear unos lineamientos estratégicos con base en todo el contexto investigado, para resaltar la oportunidad que tiene Colombia de potencializar sus capacidades en desarrollo marítimo e impulsar la economía mediante el apoyo político y de estrategias nacionales.

La presente investigación se llevó a cabo a través de un enfoque cualitativo y un carácter propositivo. Se utilizó un método deductivo, que permitió destacar el análisis de varias fuentes de información que muestran las estrategias marítimas emprendidas por el Gobierno colombiano. Incluyó la consulta de recursos académicos, políticas gubernamentales, artículos de revista y experiencias personales.

Desde la Independencia, en 1810, el país no ha desarrollado sus capacidades marítimas. Sin embargo, dado el creciente interés en proyectar a Colombia como potencia marítima, con el apoyo de varios sectores políticos, económicos y sociales, la pregunta que orienta esta investigación es la siguiente: ¿cómo Colombia, a través de su historia, ha alineado

sus políticas para aprovechar el mar y convertirse en una potencia marítima en el siglo XXI?

Lo anterior permite establecer como objetivo general analizar las estrategias implementadas por el Estado colombiano en relación con el aprovechamiento del mar y su impacto en la proyección geopolítica de Colombia. Esto requiere: 1) describir el desarrollo histórico que ha tenido el pensamiento político colombiano sobre el mar; 2) dar a conocer los conceptos estratégicos para el planteamiento de una política nacional marítima en Colombia; 3) evidenciar la posición actual de Colombia ante otros países, tomando en cuenta su proyección de poder marítimo; 4) analizar las políticas vigentes para el fortalecimiento del poder marítimo en Colombia.

Con esta investigación se buscó analizar las capacidades político-económicas para optimizar los procesos requeridos para un buen desarrollo marítimo del país. Se tomaron en cuenta las políticas del Departamento de Planeación Nacional, la Política Nacional del Océano y los Espacios Costeros, la Política de Defensa y Seguridad 2019, el CONPES 3990, entre otros documentos maestros, y un análisis de cuáles hacen falta para integrar y orientar las instituciones públicas y privadas hacia una cooperación efectiva en la ejecución de tareas y responsabilidades para que Colombia crezca como potencia marítima y amplíe su participación a escala regional.

La Comisión Colombiana del Océano caracteriza a Colombia como "potencia oceánica" porque tiene enormes capacidades de desarrollar su poder marítimo para el beneficio de la población y el crecimiento económico del país (Comisión Colombiana del Océano, 2017). Además, porque tiene 1) poder inteligente, 2) voluntad política de poder marítimo, 3) intereses marítimos nacionales y 4) posición oceánica y marítima. Con ello, se espera que los gobernantes tomen decisiones acertadas para el beneficio del país hacia el desarrollo marítimo y fluvial.

Lo expresado en el Plan Nacional de Desarrollo 2018-2022 ("diseñar el marco estratégico marítimo y fluvial para mejorar la gobernanza marino-costera y fluvial, ordenar el territorio marítimo y desarrollar el transporte, el turismo, la recreación y el comercio marítimo y fluvial"

[Departamento Nacional de Planeación, 2019]) debe ir alineado con las intenciones y estrategias del Gobierno para los siguientes años.

Es importante tener en cuenta que durante el curso de la historia las naciones han prosperado y fracasado por las políticas del Estado (Daron Acemoglu y Robinson, 2012). Por ello, es del interés de todos los ciudadanos su participación en la toma de decisiones y el establecimiento de sus intereses, pues la idea es que Colombia esté a la vanguardia de las estrategias para fomentar y fortalecer la actividad marítima y fluvial en todo el país, con la participación activa de todos los entes del Estado y del sector privado.

Siendo Colombia uno de los Estados de mayor tamaño e influencia en la región Caribe, su función, a modo de potencia mediana, es disuadir las iniciativas de otros Estados sobre el mar. Los gobernantes deben asumir la proyección del poder geopolítico como una necesidad para evitar las pérdidas de territorio o los desafíos al ejercicio del poder del Estado y controlar las actividades que suceden en su región (Esquivel Triana, 2015).

Otro aspecto que hay que traer a colación para el desarrollo marítimo es la industria de astilleros, como bien lo anuncia el señor presidente de la Corporación de Ciencia y Tecnología para el Desarrollo de la Industria Naval Marítima y Fluvial. En una entrevista reciente, manifestó que "El país debe reconocer la importancia de la industria astillero y atender sus necesidades" (Presidente de Cotecmar, comunicación oral, 2019). Así, acompañado por el Gobierno nacional y por las políticas emitidas, debe impulsar la economía y la integración de varios sectores nacionales —como los astilleros colombianos— hacia el fortalecimiento de la industria naval.

Vale destacar el conflicto que sufrió Colombia con las Fuerzas Armadas Revolucionarias de Colombia (FARC), puesto que muchos recursos se orientaron hacia la terminación del conflicto. Así, en esta época de transición hacia una paz, es cuando el país puede encaminar sus esfuerzos hacia el cumplimiento de las metas establecidas en el Plan Nacional de Desarrollo 2018-2022, mientras alimenta las buenas relaciones con sus países aliados, como los Estados Unidos (Rosenberg, 2017), y crece geopolítica y económicamente.

Por su parte, la Armada Nacional de Colombia, a través de su deber constitucional[1], ha sido muy proactiva en incentivar el desarrollo de la ciencia y las tecnologías para fomentar la economía nacional. Su posición regional en Ciencia, Tecnología e innovación (CTeI), junto con un astillero naval fortalecido, como lo es COTECMAR, ha abierto nuevas puertas hacia el desarrollo marítimo, contribuyendo a la defensa y generación de conocimiento nacional4 (Roncallo Torres et al., 2019).

2. Desarrollo histórico del pensamiento político colombiano sobre el mar

La República de Colombia, desde sus inicios en 1810, ha desconocido la explotación y el aprovechamiento del mar para el desarrollo y el crecimiento del país. La primera muestra de un interés en el poder naval fue cuando se creó la Comandancia General de Marina, pero no fue sino hasta el 24 de julio de 1823, después de la batalla naval de Maracaibo, que se marcaron en la historia naval las capacidades militares en el mar de Colombia.

La Escuela Náutica se creó en 1907, pero desafortunadamente fue clausurada años después, dejando a la nación sin un centro de entrenamiento de futuros marinos colombianos. No fue sino hasta en el conflicto con Perú, en 1932, que los gobernantes entendieron la necesidad de crear una fuerza naval, que posteriormente fue formalizada como Armada Nacional, en 1936, cuya misión era brindar una fuerza efectiva en el mar y en los ríos para la defensa y la protección del Estado (Armada Nacional, 2018).

Por otro lado, la Marina Mercante en Colombia no se había formado sino hasta 1946, y lastimosamente dejó de operar a finales del siglo XX, dejando un vacío enorme en las esperanzas de muchos colombianos, que

1 Art. 217: "La Nación tendrá para su defensa unas Fuerzas Militares permanentes constituidas 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 de Colombia, 1991).

veían aquella la oportunidad para fortalecer el poder marítimo del país ante las naciones (Becerra, 1986). Hay que destacar que esta institución tenía un impacto directo en la economía nacional y otros sectores productivos que se beneficiaban de ella, como los campesinos, los comerciantes y las industrias nacionales.

De acuerdo con Holmes (2019) y con el pensamiento de Mahan, se debe mantener una marina mercante nacional fuerte, y no dejarla a terceros o privatizarla, puesto que asegura un talento humano de gente de mar capacitada y lista al servicio del país, para atender situaciones en tiempos de paz y de conflicto. En otras palabras, en Colombia falta conciencia marítima, es decir, un conocimiento —individual y colectivo— sobre la influencia del mar y las oportunidades —políticas, económicas, sociales y militares— que brinda para convertir al país en una potencia marítima próspera (Terzago Cuadros, 2005).

3. Conceptos estratégicos para el planteamiento de una política nacional marítima en Colombia

El lenguaje de la estrategia marítima abarca diferentes conceptos —como *intereses nacionales, poder marítimo, desarrollo marítimo, estrategias marítimas* y *poder naval*—, cuyo entendimiento contribuye a la comprensión de esta investigación. Luego de presentar su definición, se expondrán las regulaciones marítimas vigentes y cómo estas afectan el desarrollo marítimo actual en Colombia.

Según Barceló (2008), el concepto de *talasocracia* se utiliza para describir a un país que muestra su interés en desarrollar su hegemonía naval, utilizando sus capacidades, su posición geográfica, su voluntad política y sus intereses políticos, económicos y militares. La antigua Roma y Estados Unidos —este ya en el siglo XX— son un ejemplo. En el segundo caso, las teorías del almirante Alfred Thayer Mahan, expuestas en su publicación *The Influence of Sea Power upon History, 1660-1783*, y la voluntad política del presidente de la época, Theodore Roosevelt,

lograron posicionar a ese país como una verdadera talasocracia moderna. Estos Estados se distinguen de los demás por explotar al máximo las capacidades del mar, así como por conducir todos los sectores políticos, económicos y sociales hacia el desarrollo de un poder marítimo sólido, acompañado de un fuerte poder naval.

> Dicho por el jefe de comando de la Armada de los EE.UU., Master Chierf Petty Officer Rick West en el año 2012, el futuro de la Armada debe regirse por la regla del 70-80-90 por ciento, en donde el 70 por ciento de la superficie de la tierra está cubierta por agua, 80 por ciento de la población mundial vive cerca del mar, y 90 por ciento del comercio mundial se mueve a través del mar. (Holmes, 2019, p. 48)

Entendiendo el concepto de *poder marítimo* como la interacción entre el poder naval y los intereses marítimos, impulsada por la consciencia marítima de una nación (Uribe Cáceres, 2015) y las oportunidades que ofrece la explotación del mar para el progreso y el posicionamiento del *status quo* de un país, Colombia no ha sido muy efectiva en promover el desarrollo de sus potencialidades marítimas a lo largo de la historia. Esto se puede otorgar al desconocimiento o a una falta de visión para utilizar el mar como herramienta y recurso fundamental para el desarrollo.

Esa falta de conocimiento sobre el mar se conoce como *ceguera marítima* (antónimo de *conciencia marítima*) o la dificultad que el público tiene para no entender el uso o la importancia del mar (Speller, 2014). En el caso colombiano, los políticos tienen también una visión limitada para proyectar políticas públicas hacia la misma.

Aunque muchos Estados han dado prioridad a la seguridad marítima para combatir los crímenes marítimos modernos, como la piratería, la trata de personas, delitos ambientales marítimos y narcotráfico (Bueger y Edmunds, 2017), esta es solo una parte de lo que debe tener un país si quiere convertirse en una potencia marítima.

En Colombia, uno de los factores que ha impedido su desarrollo como potencia marítima puede ser el hecho de que se instauró el Gobierno central en el interior del país, en las montañas, y no al lado de las costas, como en la gran mayoría de países del mundo. Según Rossman

(2017), "la ubicación de la capital con respecto al mar y el modelo de una relación tierra-mar también pueden desempeñar un papel importante en la definición de la diferencia entre los imperios terrestres y los imperios marítimos."

Según el doctor Geoffrey Till (2004), una nación debe tener claros sus intereses y, más aun, bien definidas sus políticas marítimas según sus capacidades navales, como lo expone la figura 1.1. Hoy en día, los intereses nacionales no son claros, y esto exige plantear unos lineamientos estratégicos para aunar esfuerzos hacia el desarrollo del país, especialmente en el ámbito marítimo.

Figura 1.1. Interrelación del poder marítimo

Fuente: Till (2004).

Según el Almirante Stavridis (2017), hay dos conceptos importantes que un país que se proyecte en el mar debe tener en cuenta (algo que aplicó muy asertivamente Estados Unidos): el *soft power* y el *hard power*. *Hard power* es el poder que tiene un Estado para aplicar su voluntad

contra otro Estado por medio de la fuerza, es decir, a través de su fuerza militar. *Soft power* es la capacidad de influir en el comportamiento de otros países por medios diplomáticos, económicos y políticos, sin la utilización de la fuerza. El balance entre los dos se denomina *smart power*, y es importante que Colombia tenga la capacidad de emplear de manera inteligente estos conceptos, para demostrar su hegemonía local ante los demás países de la región.

4. Proyección del poder marítimo

Con el fin de mejorar las capacidades político-económicas del país, se deben optimizar los procesos y los esfuerzos para un buen desarrollo marítimo.

Tomando en cuenta la situación actual, las políticas del Departamento de Planeación Nacional, la Política Nacional del Océano y los Espacios Costeros (PNOEC), la Política Nacional Ambiental para el Desarrollo Sostenible de los Espacios Oceánicos y las Zonas Costeras e Insulares de Colombia (PNAOCI) y la Política de Defensa y Seguridad 2019, entre otros documentos maestros, se observa la necesidad de integrar a las instituciones públicas y privadas hacia una cooperación efectiva en la ejecución de tareas y responsabilidades para que Colombia crezca como potencia marítima y amplíe su participación a escala regional.

Para lograr convertirse en una potencia marítima, es importante que un país tenga definida su estrategia marítima, expresada como creación, mantenimiento y empleo del poder marítimo por parte del Estado para promover los intereses marítimos (Uribe Cáceres, 2015).

Según Holmes (2019), la *estrategia marítima* es un arte y una ciencia que utiliza el poder para el cumplimiento de propósitos relacionados con el mar. Por su parte, para Mahan el objetivo de la estrategia marítima es asegurar el comercio, mediante medidas políticas y una fuerza naval. De aquí surge la importancia de la armonía de tres elementos esenciales: el comercio marítimo, la voluntad política y una fuerza militar que asegure el buen desarrollo de estos elementos.

Actualmente, lo que se puede acercar a una estrategia marítima en Colombia son las gestiones institucionales de la Comisión Colombiana del Océano, plasmadas en la Política Nacional de los Océanos y Espacios Costeros (PNOEC); la Dirección General Marítima, con sus políticas orientadoras para preservar la seguridad integral marítima; la Armada Nacional, con su Plan Estratégico Naval 2015-2018, y la Corporación de Ciencia y Tecnología para el Desarrollo de la Industria Naval Marítima y Fluvial (COTECMAR), a través de su astillero naval, el más grande de Colombia, para el desarrollo de la industria naval. La tabla 1.1 muestra cómo se articulan los diferentes factores del poder marítimo en Colombia que aportan a la estrategia marítima actual.

Hoy en día existen instituciones gubernamentales que impulsan los intereses marítimos, componentes importantes del poder marítimo de Colombia. Como lo contempla el documento de las Bases del Plan Nacional de Desarrollo 2018-2022:

> El DNP y MinAmbiente, con apoyo de la Comisión Colombiana del Océano (CCO), la Dirección General Marítima (DIMAR) y la Armada Nacional (ARC), construirán modelos de desarrollo regional sostenible que promuevan los océanos como activos estratégicos de la Nación y modelos de financiamiento innovadores que apalanquen su conservación e investigación. (Departamento Nacional de Planeación, 2019, p. 413)

La Armada Nacional (ARC) ha liderado la protección de los intereses marítimos y fluviales, salvaguardando la vida en el mar y velando por la correcta explotación de los recursos marinos. Gracias a la proyección de la institución en los escenarios internacionales, la ARC ha alcanzado un liderazgo y un reconocimiento en la región en áreas como delitos trasnacionales, las operaciones para contribuir a la seguridad de los océanos, la investigación científica, así como para apoyar el esfuerzo diplomático en concordancia con los objetivos nacionales (ARC, 2019). De igual manera, la inmensa inversión que hizo el Gobierno para potencializar las capacidades navales de Colombia, a través del Plan Orión, demuestra un interés nacional por el poder marítimo, a través del fortalecimiento del poder naval.

Tabla 1.1. Ejes articuladores de la estrategia marítima de Colombia

País	Territorio marítimo (extensión geográfica)	Intereses marítimos (fines)	Poder naval (medios)	Estrategia marítima (modos)
Colombia	La Constitución Política de Colombia (1991) señala, en el artículo 101, que la extensión geográfica marítima es de 928 660 km2, lo cual representa el 44,86 % de territorio total del país; de igual manera, posee arrecifes coralinos de 300 hectáreas y manglares de 378 939 hectáreas.	• Conciencia y apropiación territorial y cultura marítima. • Recursos ambientales, marinos y pesqueros. • Educación marítima. • Investigación científica, tecnológica y de innovación. • Poder naval. • Seguridad integral marítima. • Ordenamiento marítimo costero. • Transporte y comercio marítimo. • Turismo marítimo y recreación. • Industria naval y marítima. • Minería marina y submarina. • Pesca y acuicultura. • Soberanía e integridad del territorio marítimo nacional (CCO, 2017).	• La Armada Nacional de Colombia emplea el poder naval y se encarga de la seguridad marítima. Cuenta con la capacidad operacional y el espacio geográfico. • La Dirección General Marítima (DIMAR) contribuye a fortalecer el poder marítimo garantizando la seguridad integral marítima. • Desarrollo de industria naval a través de Coctemar.	**Plan Estratégico Naval 2015-2018** "Estrategias para el empleo y gestión sostenible del territorio marino-costero" Planes estratégicos 2030 a) Orión I – II: fortalecer capacidades; b) Puente: completar medios para una cobertura efectiva; c) Faro: renovación del material naval. **Estrategia Pentagonal** 1. Rol internacional. Operaciones de paz y ayuda humanitaria; presencia naval y ejercicios combinados. 2. Defensa y seguridad nacional. Soberanía, integridad territorial, combate al terrorismo y al narcotráfico, disuasión estratégica, manejo de crisis. 3. Seguridad marítima y fluvial. Protección de la vida humana en el mar, cumplimiento de la legislación interna e internacional, control tráfico marítimo, ayudas a la navegación. 4. Protección del medio ambiente. Protección de los mares y océanos, control del tráfico ilícito de especies, control de vedas, control de la contaminación. 5. Desarrollo marítimo. Protección y sostenibilidad de los recursos marítimos, investigación científica marina, servicio cartográfico e hidrográfico.

Fuente: Ramírez Benítez (2018).

La Dirección General Marítima (DIMAR), como autoridad marítima colombiana creada en 1971, es la que regula y vigila toda la normatividad marítima, cumpliendo los estándares internacionales emitidos por la Organización Marítima Internacional (OMI). La DIMAR permite fortalecer el conocimiento científico del territorio marítimo nacional y coadyuva esfuerzos con el gremio marítimo y con la Armada Nacional, de tal manera que pueda explotar al máximo las capacidades de sus buques de guerra para el ejercicio de control y defensa nacional; la protección de las líneas de comunicación marítima y de los principales puertos comerciales y turísticos del país, y el ejercicio de actividades marítimas, entre otras funciones (ARC, 2019).

Finalmente, la Comisión Colombiana del Océano (CCO), creada en 1969, como órgano intersectorial de asesoría, consulta, planificación y coordinación del Gobierno nacional con respecto al mar, encabezado por la Vicepresidencia de la República, lidera el Programa Antártico Colombiano. Por primera vez en la historia, un buque hecho en Colombia, el ARC "20 de Julio", llegó a la Antártida exitosamente, en el año 2015, para conducir investigaciones científicas bajo la protección de los intereses nacionales colombianos y de la humanidad. Este hito abre las puertas ante la comunidad marítima y científica como un ejemplo de desarrollo tecnológico y de la industria naval de Colombia. Asimismo, demuestra el interés de los gobernantes en invertir en el desarrollo marítimo (CCO, 2020).

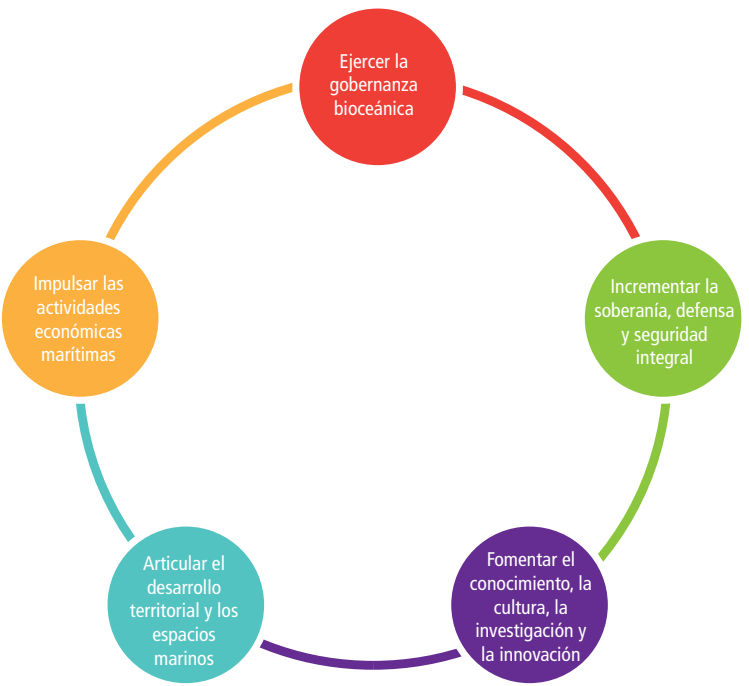
Adicionalmente, la CCO lideró la elaboración de la Política Nacional del Océano y de los Espacios Costeros (PNOEC), así como sus diferentes temas conexos, estratégicos, científicos, tecnológicos, económicos y ambientales relacionados con el desarrollo sostenible de los mares colombianos y sus recursos (Armada Nacional, 2019). Gracias al gran esfuerzo de esta institución, el 31 de marzo de 2020 el Gobierno Nacional aprobó el CONPES 3990, que integra un conjunto de estrategias para alinear a Colombia en una potencia bioceánica sostenible para el año 2030.

El CONPES 3990 está alineando con el Plan Nacional de Desarrollo (PND) 2018-2022 "Pacto por Colombia, Pacto por la Equidad", la

Política Nacional Ambiental para el Desarrollo Sostenible de los Espacios Oceánicos y las Zonas Costeras e Insulares de Colombia (PNAOCI) y la Política Nacional del Océano y los Espacios Costeros (PNOEC), documentos rectores que solidifican el compromiso nacional con una visión estratégica hacia los océanos y comprometen a varios actores necesarios para su desarrollo.

Es importante tener en cuenta que este documento abarca distintos sectores, como educación, industria y comercio, defensa, medio ambiente, trabajo, ciencia y tecnología, pesca, social, entre otros. Su objetivo general es "Proyectar a Colombia como potencia bioceánica para el año 2030, mediante el aprovechamiento integral y sostenible de su ubicación estratégica, condiciones oceánicas y recursos naturales para contribuir al crecimiento y desarrollo sostenible del país" (CONPES, 2020) (figura 1.2).

Figura 1.2. Objetivo general y objetivos específicos del CONPES 3990



Fuente: Elaboración propia con base en el CONPES 3990.

Hoy por hoy se están fortaleciendo las políticas nacionales en pro de articular varios sectores en el país, algo que antes no se percibía de manera tan notoria. Estas decisiones políticas siembran una semilla cuyos frutos se verán dentro de unos años, cuando la industria marítima crezca en Colombia y las personas empiecen a invertir y lograr aprovechar de las riquezas con que siempre han contado en el país.

5. Análisis actual de políticas vigentes para el fortalecimiento del poder marítimo en Colombia

Existen varios documentos que citan las actividades marítimas y fluviales para su buen manejo. El primero es el Plan Nacional de Desarrollo 2018-2022, específicamente el Pacto Región Océanos: Colombia, Potencia Bioceánica (2018), adelantado por el Consejo Nacional de Política Económica y Social (CONPES), la Política Nacional del Océano y los Espacios Costeros de la Comisión Colombiana del Océano (2017), la Política de Defensa y Seguridad (2019) del Ministerio de Defensa y el Plan Estratégico Naval 2015-2018 de la Armada Nacional (Ramírez Benítez, 2018).

El segundo es el CONPES 3990, Colombia Potencia Bioceánica Sostenible 2030. Estos documentos son un soporte para fortalecer el desarrollo marítimo del país y orientan a Colombia hacia una estrategia nacional, en cabeza del presidente de la República, con el fin de posicionar a Colombia con un poder marítimo[2].

Con estos antecedentes, se busca efectuar un análisis cualitativo con un carácter propositivo, para lograr proyectar, a través de varias fuentes de información, una estrategia para impulsar la participación del Estado colombiano en el desarrollo de los intereses marítimos.

2 Concepto explicado en el libro *Poder marítimo: una guía para el siglo XXI* (Till, 2004).

6. Conclusiones

Dentro del análisis se plantea una matriz DOFA (debilidades, oportunidades, fortalezas y amenazas) para explicar cuál ha sido la evolución y cuáles son los retos para Colombia en el siglo XXI, en busca de convertirse en una potencia marítima. Hay que destacar el esfuerzo de las instituciones estatales en su labor para construir un país marítimo seguro y confiable para todos (figura 1.3).

Figura 1.3. Conclusiones según la matriz DOFA

Fuente: Elaboración propia.

6.1. Debilidades

La falta de conciencia marítima como país a lo largo de la historia colombiana es el primer punto por destacar. La necesidad de contribuir a la promoción de una conciencia marítima nacional y de fomentar la construcción de un pensamiento marítimo se fortalece con la producción de los esfuerzos académicos resumidos en la presente ponencia. Su variedad de formas y contextos permiten un alcance de gran profundidad y cantidad, como lo evidencian las estadísticas de lectura de los textos y el alto número de países impactados.

Con miras a producir un interés y un conocimiento en torno al mar, los resultados presentados van no solo dirigidos a los miembros de la Armada Nacional encargados de "Proteger el azul de la bandera" y a

la gente de mar, sino a todos los colombianos, para que reconozcan en el mar una de las más importantes fuentes de desarrollo y de recursos sostenibles para la Nación (Santamaría, 2016). Hoy en día, Colombia se está "curando" de esa ceguera marítima, para dar paso hacia un camino próspero y consciente de sus capacidades en el mar como país bioceánico, título que lleva el CONPES 3990.

De acuerdo con lo aprobado en el CONPES 3990, se puede evidenciar el financiamiento a once años (tabla 1.2) que va a impactar a los diferentes sectores, dentro de los cuales se destacan la DIMAR y la Autoridad Nacional de Acuicultura y Pesca. Si bien es cierto que es un monto considerable, es necesario seguir buscando mayor inversión y oportunidades de emprendimiento en el sector marítimo, para impulsar su construcción y desarrollo.

Tabla 1.2. Costos indicativos por entidad*

Entidad	Costos
Autoridad Nacional de Acuicultura y Pesca	202.551
Departamento Administrativo Nacional de Estadística	56
Dirección General Marítima	107.522
Instituto Colombiano de Antropología e Historia	563
Ministerio de Ambiente y Desarrollo Sostenible	7.830
Ministerio de Ciencia, Tecnología e Innovación	363
Ministerio de Comercio, Industria y Turismo	974
Servicio Nacional de Aprendizaje	40.970
Unidad Administrativa Especial - Parques Nacionales Naturales de Colombia	9.705
Unidad Nacional para la Gestión del Riesgo de Desastres	260
Total general	**370.794**

* Cifras en millones de pesos (constantes en 2020)

Fuente: CONPES 3990.

6.2. Oportunidades

Las oportunidades de un desarrollo marítimo sustancial dependen mucho del compromiso de las instituciones con el seguimiento y el cumplimiento de las tareas, así como de un aprovechamiento responsable de los recursos oceánicos. Igualmente, requieren del desarrollo económico, pues muchos de los proyectos de inversión tendrían un retorno favorable para el país, como lo tuvo en su momento la Flota Mercante Grancolombiana.

Con tal nivel de compromiso y esfuerzo institucional, Colombia lograría un reconocimiento mundial por la comunidad marítima y por aquella dispuesta a invertir en el sector marítimo. El resultado se observaría a través de espacios de crecimiento social, la creación de empleos, la explotación sostenible de los recursos naturales marinos y un verdadero acercamiento hacia el mar como parte del propósito nacional definido por Bartholomees (2006) en la proyección de la estrategia nacional.

6.3. Fortalezas

Colombia tiene unas capacidades instaladas bastante desarrolladas, a través de sus políticas nacionales vigentes, como la PNOEC, la PNAOCI, el PND 2018-2022 y el CONPES 3990. Todos los documentos mencionados hacen énfasis en la importancia del activo más valioso que tienen los seres humanos en la tierra: el agua. Estas iniciativas dan a entender que el Gobierno tiene un gran interés por impulsar estas políticas a través de diferentes estrategias para proteger y aprovechar los intereses marítimos colombianos, plasmados en la PNOEC.

Paralelamente, la industria naval ha sido un factor determinante para dejar en alto el nombre de Colombia ante la comunidad internacional, evidenciado en la construcción de buques para la ARC con capacidad de sostener operaciones en aguas internacionales, como fue la expedición antártica en 2014-2015, la operación Atalante en el cuerno de África y la participación en ayudas humanitarias, cuando se llevó víveres a Haití

en 2016. Esta es una clara demostración del interés de los gobernantes en la construcción de buques nacionales para su participación activa en escenarios internacionales y, con ello, la proyección de la imagen y del poder marítimo colombiano.

6.4. Amenazas

Si bien es cierto que Colombia presenta una situación de conflicto interno desde mediados del siglo XX, que generó una importante inversión en recursos para afrontar las amenazas a la seguridad nacional, el mar siempre ha estado ahí para su explotación y para la creación de oportunidades de progreso, independientes de las actividades ilícitas que se presentaron a lo largo de más de sesenta años.

Otro factor de amenaza son los litigios internaciones, que desafían los intereses nacionales y, en particular, las fronteras marítimas, con lo cual afectan las actividades normales de explotación de los recursos naturales, como la pesca, el turismo y la investigación científica. Un ejemplo de esto es la disputa territorial con Nicaragua, que perjudica a la comunidad de los habitantes de San Andrés, Providencia y Santa Catalina y sus actividades ancestrales de pesca artesanal —más allá de las doce millas náuticas—. En ocasiones, autoridades nicaragüenses han sacado a los pescadores artesanales colombianos de las aguas colombianas a causa del conflicto jurídico que sigue vigente hoy en día.

Finalmente, lo que se evidencia en la investigación es que las políticas actuales van a crear una semilla de esperanza para las futuras generaciones en el desarrollo marítimo, y sus frutos se van a ver a lo largo de los años. Colombia se proyecta como potencia marítima, según sus capacidades y políticas exteriores, y ello involucra a la comunidad y a otros actores del sector público y privado para coadyuvar esfuerzos con el fin de crear un espacio de participación de las actividades marítimas para el beneficio de los colombianos.

7. Recomendaciones

Dada su importancia para el comercio, el desarrollo y la biodiversidad, se deben incluir los ríos como parte de la estrategia marítima en Colombia. Además de alimentar los océanos. forman parte de la conectividad de la infraestructura del país, junto con las carreteras y las vías férreas, fundamentales para el comercio de los productos desde el interior hacia los puertos marítimos y, finalmente, hacia destinos internacionales.

Hay que fortalecer los tanques de pensamiento estratégico en el ámbito marítimo. Un buen ejemplo es el de Deep blue, que tuvo como objetivo ubicar mentes brillantes para la formulación de estrategias particulares para la defensa, a causa de los ataques del 11 de septiembre en los Estados Unidos (Stavridis, 2019). Esto es aplicable a escala nacional, para afrontar el problema planteado en la presente investigación y resaltar la importancia de encaminar una estrategia marítima efectiva en Colombia.

Es importante tomar como ejemplo los países que han logrado un desarrollo marítimo admirable, como Panamá, Ecuador y Chile, en el ámbito regional, y Estados Unidos y la China, a escala global. Además de tener unas políticas más definidas hacia el mar, mediante la legislación, sus habitantes están convencidos del aprovechamiento excepcional del océano. Junto con Rusia, Estados Unidos y China se han interesado sobre la importancia geoestratégica de dominar el mar con unidades militares y de contar con una marina mercante fuerte que impulse la economía de esos países.

De igual manera, hay que incentivar a la comunidad académica y educativa nacional, desde los colegios hasta las universidades, para descubrir la importancia del mar. Estas estrategias darán frutos a largo plazo, pues las nuevas generaciones serán más conscientes del efecto que tiene el recurso marítimo en la economía del país, en el cuidado del medioambiente y en el sentido de pertenencia de la población.

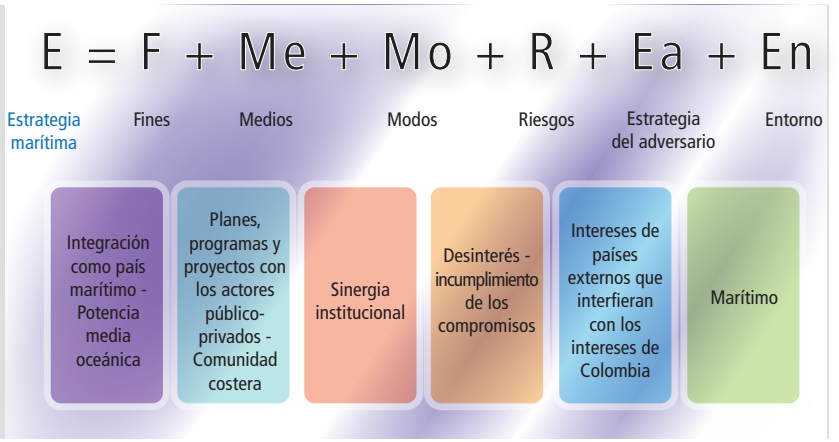
Se debe tener en cuenta el impacto estratégico que tiene para Colombia, a escala internacional entre la comunidad marítima, el fortalecimiento de sus políticas hacia una economía marítima, con el fin de

realzar la importancia de los mares y de los océanos como motores de la economía nacional. Por ende, desde el sector político se deben tomar medidas pertinentes para dar facilidad a los trámites que conlleven al desarrollo marítimo. Un ejemplo es el proyecto de "ley de abanderamiento", que agiliza los trámites para la matrícula de naves en Colombia. Así, el país se vuelve más atractivo para las empresas navieras del mundo, y esto le genera recursos a la nación.

Aparte de brindar a los colombianos la confianza de participar activamente en el desarrollo marítimo, hay que hacer campañas —centrales, regionales y locales— que den a conocer las oportunidades que ofrece el mar para un desarrollo sostenible, responsable e inteligente.

Para que las políticas nacionales actuales prosperen, se construyó una fórmula para la estrategia marítima, tomada del concepto de Holmes, planteado en el libro *En la mente de los estrategas* (Sánchez Hurtado, 2012). Esta construcción de la fórmula fue necesaria para entender los componentes esenciales de la ecuación hacia el resultado esperado, y es que Colombia sea una potencia marítima en el siglo XXI (figura 1.4).

Figura 1.4. Propuesta para una estrategia marítima



Fuente: Elaboración propia con base en Sánchez Hurtado (2012).

La frase "Pensar globalmente, actuar localmente" (Pierre, 2019) debe aplicarse a la realidad colombiana para enfrentar los retos del siglo XXI, sobre todo aquellos que buscan la preservación y conservación del medioambiente marino. Por tal razón, las estrategias que adopte el Estado deben estar alineadas con las políticas internacionales, como la economía azul, que busca el desarrollo sostenible del mar, siempre protegiendo los recursos marinos (López Cabia, 2018).

Como última recomendación, debe existir una amplia socialización y difusión de los avances en las gestiones políticas, de manera didáctica y de fácil acceso a la población, para generar confianza y transparencia respecto a las decisiones políticas. Hay que fortalecerlas de manera *bottom-up*, es decir, con la participación ciudadana en las decisiones políticas que afecten los sectores económicos y sociales.

De manera de prospectiva, los entes gubernamentales que asesoran al alto Gobierno deben hacerse estas preguntas para tener una visión más estratégica hacia dónde quieren posicionar a Colombia en un futuro deseado: ¿qué puede ocurrir? ¿Qué se puede hacer? ¿Qué se va a hacer? ¿Cómo se va a hacer? (Godet y Durance, 2011). Esto, con el fin de crear una estrategia proactiva hacia los posibles futuros, teniendo en cuenta los factores que puedan afectar el normal desarrollo de país en su visión de convertirse en una potencia marítima.

CAPÍTULO II

LA AMAZONIA COLOMBIANA: OPORTUNIDADES Y RETOS PARA EL EJÉRCITO COLOMBIANO*

Lisseth Paola Salazar Narváez

* Ponencia resultado del proyecto de investigación titulado *Influencia del océano en la política nacional de Colombia*, de la Maestría en Estrategia y Geopolítica, que forma parte de la línea de investigación *Estrategia, Geopolítica y Seguridad hemisférica*, del grupo de investigación *Centro de Gravedad*, reconocido y categorizado en (A1) por Minciencias, registrado con el código COL0104976, adscrito y financiero por la Escuela Superior de Guerra de la República de Colombia. Ponencia resultado de la investigación presentada como opción de grado para optar por el título de magíster en estrategia y geopolítica de la Escuela Superior de Guerra "General Rafael Reyes Prieto".

Resumen

El objetivo de la presente ponencia es presentar los resultados del análisis geopolítico de la Amazonia colombiana y mostrar sus características estratégicas y su valor dentro de los intereses nacionales. Así, este trabajo se centra en 1) dar un sustento teórico a la Amazonia como un interés nacional para Colombia, 2) describir los planes y las acciones realizadas por las Fuerzas Militares en la región, 3) finalizar con una propuesta estratégica para consolidar el Estado colombiano en la Amazonia y 4) destacar su relevancia para el país, dados sus recursos medioambientales, estratégicos y de cooperación internacional.

Palabras clave: Colombia; medioambiente; Amazonia.

Abstract

The objective of this paper is to present the results of the geopolitical analysis of the Colombian Amazon, showing its strategic characteristics and its value within the national interests. Thus, this work focuses on 1) giving a theoretical basis to the Amazon as a national interest for Colombia, 2) describing the plans and actions carried out by the Military Forces in the region, 3) concluding with a strategic proposal to reinforce the Colombian State in the Amazon, and 4) highlighting its relevance for the country, due to its environmental, strategic, and international cooperation resources.

Keywords: olombia; environment; Amazonia.

1. Introducción

El anarquismo vigente, expuesto y sustentado por varios autores del área de las relaciones internacionales sobre el sistema internacional, permite hablar sobre una interdependencia de las naciones sustentada en lo que podría llamarse "egoísmo nacional". Los Estados reconocen la necesidad de otros países para alcanzar sus objetivos, sin dejar de actuar en favor de sus intereses. En palabras del profesor Baños (2017), "la geopolítica actual podría definirse como la actividad que se desarrolla con la finalidad de influir en los asuntos de la esfera internacional, entendiendo este ejercicio como la aspiración de influencia a escala global evitando, al mismo tiempo, ser influidos" (p. 14). En resumen, la supervivencia de los Estados radica en conocer su entorno y actuar acorde a los beneficios que puedan percibir.

Este preludio expresa que ningún fenómeno que afecte los intereses nacionales es netamente local. El análisis contextual permite entender la influencia externa en las circunstancias internas y, con ello, aprovechar los escenarios internacionales con el fin de lograr no solo la supervivencia del Estado, sino también su proyección como posible potencia.

Dentro de este panorama sobresalen temáticas y ejes que el país puede aprovechar, como la cooperación internacional para la inmersión en nuevos mercados, la Alianza del Pacífico, el posicionamiento del territorio en el Caribe y la consolidación del Estado en la Amazonia. Dada la importancia de esta para el mundo actual y el peligro al que se está enfrentando por el cambio climático, el país debe proteger aquellos recursos que permitan su subsistencia, como el agua, el oxígeno y la biodiversidad de la región.

El Estado colombiano debe reconocer el valor geopolítico de la Amazonia, dados sus recursos estratégicos y su incidencia en la esfera internacional, en el marco de los Objetivos del Desarrollo Sostenible y la protección del medio ambiente. Colombia puede aprovechar esta coyuntura para convertirse en un líder regional al respecto, y por esta razón vale preguntarse ¿cuáles son los componentes que debe tener la estrategia de las Fuerzas Militares de Colombia para mitigar los efectos de la minería ilegal en la Amazonia y, con ello, lograr consolidar al Estado como una potencia en la región?

Reconocer la Amazonia y su valor geopolítico, teniendo en cuenta las amenazas que la afectan o la vulneran, así como las acciones realizadas por las Fuerzas Militares en favor de la consolidación del Estado en la región es clave para poder proponer los lineamientos que apunten a dicho objetivo.

El entramado de variables que plantea este trabajo de investigación otorga al Estado colombiano la definición de una estrategia económica y de seguridad contra la amenaza transnacional que tome en cuenta las potencialidades negativas y positivas de la región Amazónica como Hinterland colombiano.

El aislamiento se manifiesta en varios aspectos, como el político, social, marginalización comercial y económica de la región. Sin embargo, este último aspecto puede ser aún más grave en el mediano y en el largo plazo, cuando se terminen los corredores que unen a Brasil con el Pacífico y con el Caribe, en particular si se tiene en cuenta la precariedad de la infraestructura vial, la infraestructura portuaria y la ausencia de un sistema férreo en Colombia (Chaves, 2016). Este aislamiento se puede agravar frente a la relativización total de la Comunidad Andina (CAN) y la atracción que ejerce el Mercosur hacia los socios reticentes que aún quedan de este acuerdo de integración (Chaves, 2016).

La generación de alternativas económicas en el territorio amazónico que permitan solventar las necesidades básicas de la región no debe impactar de forma drástica el modelo económico tradicional de sus habitantes, con sus productos propios (con potencialidad económica) y experiencia en procesos productivos documentados. Dichos procesos

deben enlazarse en cadenas productivas para que se puedan establecer los canales de comercialización necesarios, ya que este es el principal cuello de botella para el mercadeo de los productos generados en la región Amazónica (Luis Eduardo Acosta, 2014).

2. Importancia geopolítica de la región

El primer análisis de la Amazonia se centra en los fundamentos teóricos que permiten sustentar el interés nacional en esta región y su importancia geopolítica para el país. Al respecto, podemos determinar que

> el papel determinante que desempeñan los fenómenos naturales en la explicación de los fenómenos sociales, preocupada por las interrelaciones hombre-medio y naturaleza-sociedad, aseguraba que una de las características del ser humano civilizado era su adscripción a un marco jurídico y la construcción de lógicas de coerción permitidas por el cuerpo social. (Ratzel, 1885, citado en Bilbao, 2015, p. 66)

Así, el espacio, como escenario donde habita la población, y los elementos que lo constituyen forman parte de la construcción del Estado, lo cual, se complementa con los argumentos de Ratzel (2014) citado en Talledos Sánchez, quien menciona que la

> necesidad de los Estados nación de un *Lebensraum*, espacio vital para poder desarrollarse. Esta propuesta representó una intersección entre la ciencia política, la geografía política, la estrategia militar y la teoría jurídica del Estado, la cual fue determinante en la geografía política del siglo XX, puesto que una variedad de autores la homologaron con la geopolítica. (p. 25)

La noción de *Lebensraum* es aplicable en la actualidad, si se considera la necesidad —para la supervivencia— del territorio y de un adecuado desarrollo de la población respecto a ubicación geoestratégica relevante y recursos de gran valor. Dado que la Amazonia colombiana cumple con estos requisitos, el país debe asegurarla como espacio vital,

considerando las múltiples amenazas que se presentan en el escenario mundial y los intereses de las distintas naciones.

Según Ratzel (2011, citado en Trigal, 2011), existe un

> papel determinante que desempeñan los fenómenos naturales en la explicación de los fenómenos sociales, preocupada por las interrelaciones hombre-medio y naturaleza-sociedad. Desde estudiosos clásicos (Aristóteles, Estrabón, Ibn Khaldun) y modernos (Montesquieu) se venía ya observando la influencia decisiva del medio ambiente en las manifestaciones sociales y humanas, culminando en los principios del evolucionismo de Darwin que influirá de manera notoria en las ciencias sociales, desde las posiciones ideológicas más opuestas, en una interpretación que enfatiza las leyes naturales y la causalidad en la evolución de la sociedad y su adaptación al medio ambiente (darwinismo social). (p. 159)

Desde la geopolítica, el entorno tiene dimensiones profundas que lo consolidan como un componente indispensable para la supervivencia de sus habitantes. Por esta razón se le considera un elemento de interés nacional y geopolítico, dado que permite a los Estados su proyección regional.

Para explicar la importancia de la geopolítica para esta investigación, se retoman las palabras de Laureano (2012):

> La *Geopolitik* de Kjellén es síntesis de una serie de planteamientos conceptuales, en principio separados en tiempo y espacio, pero conectados finalmente por el vocablo. Es una fórmula sencilla y fácil de entender, y que podemos sintetizar en la siguiente función: Política = f (Geografía), en donde el término "política" es la variable dependiente, y se define en función de los factores geográficos del Estado. (p. 62)

La complejidad misma del territorio colombiano, por su diversidad de valles, montañas, páramos, llanos, ríos, mares, océanos y selva, tiene un gran valor estratégico y geopolítico, y esto aumenta el poder que pueda llegar a tener el Estado y su relevancia para asegurar el bienestar de todos los ciudadanos[1].

1 "Habría que proceder de esta forma porque la naturaleza del Estado sería, ante todo, poder, y la ley debería estar subordinada al mismo. El edificio de la ciencia política que diseña Kjellén se compone

El análisis geopolítico se enfoca en el punto fronterizo entre Leticia y Tabatinga, con miras a establecer las ventajas geoestratégicas de la región —aprovechables por sus diferentes amenazas— y una matriz comparativa que permita analizar la correlación sistémica que existe entre las constantes geoestrategia, fronteras dinámicas y factores de inestabilidad.

Una vez realizado el ciclo exploratorio, la investigación brinda una serie de resultados útiles para contextualizar los diferentes parámetros que convierten la región mencionada en un imperativo geopolítico para los diferentes actores económicos que la proyectan como un pivote estratégico para nuestro país.

Un gran desafío está en el plano geopolítico, militar y estratégico. Para Colombia es fundamental el control de su territorio frente a los grupos insurgentes y a los carteles criminales transnacionales. Al respecto, la porción de la Amazonia colombiana está en peligro, y esto afecta el desarrollo de la región. La ausencia de soberanía puede provocar una acción de parte de un actor externo con las capacidades militares para llevarla a cabo, y esto puede representar una amenaza para el Estado colombiano (Vélez, 2012).

La hipótesis planteada en esta investigación es que se podría sufrir un aislamiento político y una marginalización de las corrientes comerciales y económicas regionales, si el Estado colombiano no define una estrategia económica y de seguridad contra la amenaza transnacional, que tome en cuenta las potencialidades negativas y positivas de la región amazónica como Hinterland colombiano y posible territorio estratégico para la proyección de Colombia en la región. Esta última posibilidad puede ser aún más grave en el mediano y en el largo plazo, cuando se terminen los corredores que unen a Brasil con el Pacífico y con el Caribe, en particular si se tiene en cuenta la precariedad de la infraestructura vial, la infraestructura portuaria y la ausencia de un sistema férreo en Colombia (Chaves, 2016).

---

de cinco campos de estudio, que son, de mayor a menor importancia: la *Geopolitik*, que se ocupa del estudio de la organización política del territorio del Estado; la *Demopolitik*, que estudia la población del Estado; la *Oekopolitik*, que examina los recursos económicos del Estado; la *Sociopolitik*, que investiga la estructura social del Estado, y la *Kratopolitik*, cuyo objeto es la constitución y la organización gubernamental". (Cairo, 2012, p. 337. Las cursivas son del editor)

Esta investigación busca establecer un paradigma analítico que permita determinar cuál es el impacto y la influencia de los factores de inestabilidad que convierten a la región de la Amazonía (límite entre Leticia y Tabatinga) en un imperativo geopolítico para los distintos actores armados ilegales que interactúan sobre dicho espacio geográfico.

Para establecer un referente teórico que guiara la investigación hacia la consolidación del objetivo general, se empleó la teoría de las fronteras dinámicas de Karol Gernshmain y el concepto teórico correlacionado con las fortalezas geopolíticas descritas por Jakub Grygiel. Asimismo, se buscó diagnosticar la situación actual asociada con la evolución constante de los diferentes factores de criminalidad, a fin de identificar los métodos de financiación empleados por distintos actores armados ilegales.

3. Comprensión de la Amazonia colombiana

En términos geográficos, la Amazonia se extiende hacia el interior del país, como un corredor para el tránsito de diferentes especies de fauna. Las figuras 2.1 y 2.2 representan la magnitud de este ecosistema con respecto a Colombia y al mundo.

La Amazonia cubre siete países del continente. Ubicado a los lados del río más caudaloso del planeta, este ecosistema nace en la cordillera de los Andes y cuenta con múltiples y valiosos recursos. En Colombia, seis departamentos, que representan casi el 20 % de la superficie total del territorio, forman parte de este ecosistema y están conectados con los demás ecosistemas del territorio.

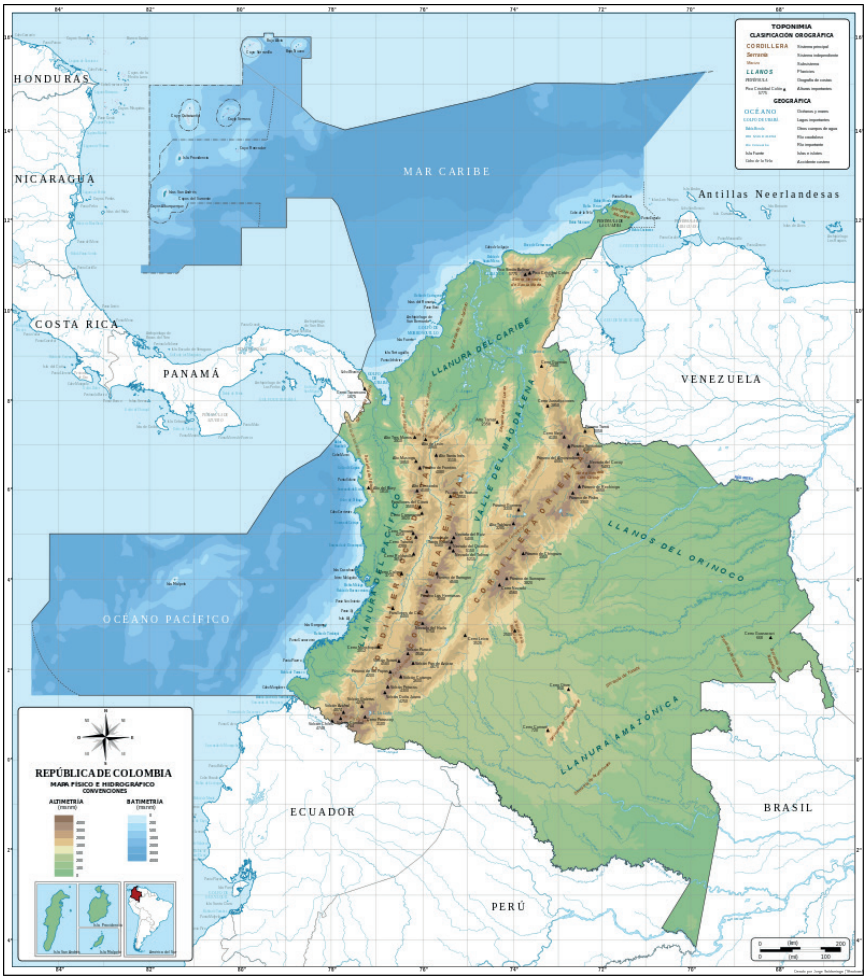
Como se puede observar en la figura 2.2, la Amazonia está conectada con los llanos del país, pero se corta con las cordilleras. Si bien esto ha implicado una problemática de conexión relevante porque es en estas cordilleras donde se concentra el poder del Estado, existe una diversidad de medios que pueden concretar esta conectividad de una forma multimodal.

Una vez descrito el objeto de estudio, un estudio de caso en la región permite comprender cuáles son las amenazas que afectan el territorio en observación.

Figura 2.1. Ubicación geografía de la región Amazónica

Fuente: Instituto Geográfico Agustín Codazzi (2017).

Figura 2.2. Mapa geográfico de Colombia



Fuente: Instituto Geográfico Agustín Codazzi (2017).

3.1. Amenaza transnacional

Para comprender las amenazas que afectan la región, es importante determinar el enfoque desde el que se han podido identificar. Para el caso de esta investigación, se hace referencia a la *seguridad multidimensional*. Este concepto, según el cual el objeto de protección no es solo el Estado, sino también la sociedad, representada en cada una de las personas, ofrece una serie de ventajas al intentar superar los retos impuestos por el sistema.

Para poder aplicar de manera apropiada el modelo de la multidimensionalidad de la seguridad, se deben analizar los siguientes problemas que afectan a nuestro país y a la región:

- No se ha logrado interiorizar la seguridad como un bien público fundamental.
- El enfoque ha sido represivo y no preventivo.
- Se pueden considerar como acelerantes de la inseguridad los siguientes fenómenos: drogas, tráfico de armas, pandillas, debilidades de los gobiernos y las sociedades para repartir equitativamente los ingresos, fallas estructurales en los Estados, como la corrupción.
- La falta de conexión entre el Gobierno y el sector productivo.
- La convergencia de actores criminales y la asimetría en sus medios y modos.

Estos problemas llevan a adoptar un modelo de seguridad inteligente que incentive la cultura de la evidencia basada en el conocimiento que se obtiene a través de diagnósticos en el campo. Esto permite diferenciar los problemas internos y externos y, con ello, adaptar respuestas efectivas según las amenazas. Es decir, utilizar como herramienta la inteligencia, definida por González (2012) como "el empleo de la información y el conocimiento más adecuado para atender una necesidad específica orientada a la toma de decisiones y a la acción por parte de un determinado individuo o grupo" (p. 10).

El diseño de una estrategia de seguridad y defensa por parte del Estado colombiano ha pasado por una serie de problemas, como la

incapacidad de diferenciar lo externo de lo interno. Los dos últimos gobernantes, Álvaro Uribe y Juan Manuel Santos, intentaron formular una estrategia, pero esta aún estaba centrada en los aspectos internos e ignoraba las amenazas internacionales.

En la construcción del concepto de *seguridad* combina insumos teóricos y evidencias empíricas, y con ello permite que procesos que se desarrollan en el Sistema Internacional se materialicen a partir de contextos precisos, representando elementos fundamentales que configuran realidades locales y afectan la concepción de seguridad que tienen los individuos y Estados.

Lo anterior significa que lo que las sociedades construyen como concepto de *seguridad* está ligado con la no existencia o disminución de amenazas a sus intereses vitales. Su visión, objetiva y subjetiva, se materializa en la ausencia de temor ante la afectación de dichos intereses.

En Colombia, el concepto de seguridad ha estado ligado a la visión de las élites gobernantes en cuanto a amenazas internas, y los intereses de estas élites han estado por encima del interés común. Incluso en la Independencia, la búsqueda de la liberación de los españoles se vio motivada por los intereses de una clase criolla que buscaba favorecer a un pequeño sector de la población.

Una vez finalizada la Independencia, el concepto de seguridad se relacionó con la percepción de amenazas internas, situación que se reflejó en las innumerables guerras civiles iniciadas entre las élites que querían imponer, por un lado, un sistema centralista y, por el otro, uno federalista. La seguridad se comprendió como defensa del territorio y dio poca o ninguna importancia a los acontecimientos que ocurrían en la región y que podían ser una amenaza para nuestro país. Hasta nuestros días, esta situación no ha cambiado.

Los nuevos desafíos de las amenazas hemisféricas, afectan la seguridad regional, preocupando a los actores estatales en la construcción de escenarios que permitan un despliegue a nivel global donde el comercio y la presencia del estado no se vea afectado por los negocios ilícitos, ni el terrorismo impartido desde los grupos al margen de la ley, permitiendo que la seguridad sea imperativa en la región.

3.2. Crimen transnacional

Los Estados latinoamericanos se ven enfrentados al fenómeno del *crimen trasnacional organizado*, término que genera una discusión académica en torno a la evolución y perfeccionamiento de la "delincuencia común". El crimen organizado interfiere en los intereses del Estado; rebasa los controles gubernamentales; establece líneas especiales de operaciones basadas en un sistema complejo para la delegación de hechos delictivos, y persigue, por medio de acciones violentas, la obtención del poder económico y social de un territorio (Rojas, 2008).

El crimen organizado tiene objetivos económicos, y para esto emplea la extorsión y la violencia. Esta característica es la que representa el mayor peligro para las sociedades de la región latinoamericana. Lo que busca este fenómeno es la influencia y la capacidad de decisión sobre los agentes del Estado, sin importar su ideología. Es una empresa ilegal, aunque, por lo común, penetra empresas legítimas (Rojas, 2008).

Entre sus actos criminales figuran el tráfico de personas, la piratería, el fraude, el tráfico de drogas y el secuestro. Se habla de la "transnacionalización" de este tipo de crimen porque cruza las fronteras y sus acciones se relacionan con los distintos tipos de amenazas de carácter global (Rojas, 2008).

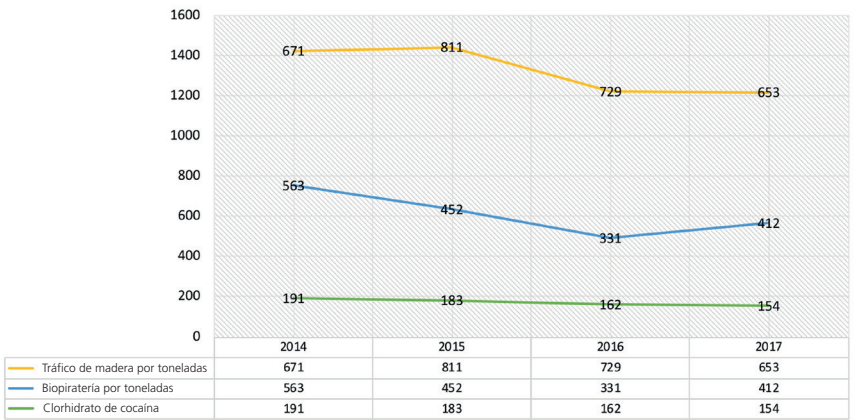
Sus actos de delincuencia son una forma de violencia premeditada y sistemática, perpetrada contra objetivos no combatientes, como forma de influir y generar tensión en un sector de la población (Laqueur, 2003, p. 24). Estos actos se llaman terrorismo.

Es muy importante observar en la figura 2.1 que la incautación de sustancias y elementos ajenos al orden legal no es creciente, pero sí constante. A raíz de este fenómeno, Sandino y Fernando (2012) argumentan que el crecimiento de los índices de pobreza multidimensional y el deceso de las constantes favorables para la optimización del Índice de Desarrollo Humano (IDH) colombiano son inevitables.

Por otro lado, y en pro de ilustrar y contextualizar al lector, es indispensable reconocer que la mayoría (un 72,5 %) de las toneladas de clorhidrato de cocaína, piedras preciosas ilegales (salida y entrada) y madera

en la jurisdicción amazónica ingresa y sale desde dos puntos limítrofes ya reconocidos: Tabatinga y la isla de Santa Rosa (triple frontera conformada por Colombia, Brasil y Perú). Por tal razón, y según los resultados del trabajo, puede decirse que el aumento del tráfico y del microtráfico, ya establecido en la región por diferentes grupos delictivos, es uno de los mayores problemas en nuestra Amazonia, y más en la zona fronteriza (figura 2.3).

Figura 2.3. Estadísticas de incautación de cocaína, piedras preciosas y madera en la frontera colombo-brasileña



	2014	2015	2016	2017
Tráfico de madera por toneladas	671	811	729	653
Biopiratería por toneladas	563	452	331	412
Clorhidrato de cocaína	191	183	162	154

3.3. La minería ilegal como una amenaza

La minería en Colombia se ha proyectado como una oportunidad de crecimiento económico en los últimos diecisiete años. Durante el gobierno del presidente Juan Manuel Santos (2010-2018), este aspecto fue una de las "locomotoras" del desarrollo, pues con esta se buscaba generar un crecimiento paulatino en la economía desde el sector minero energético, pues diferentes multinacionales han demostrado su interés por explotar los recursos naturales del suelo colombiano (González, 2014).

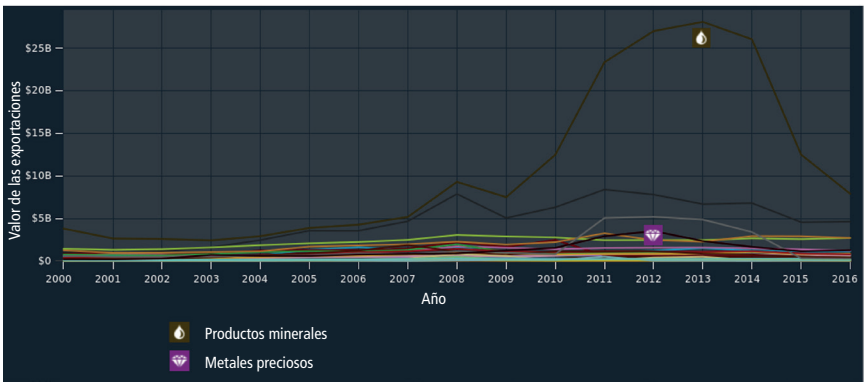
A pesar de ese interés, las decisiones del Gobierno para conceder los permisos de exploración y extracción de recursos naturales necesarios

a dichas multinacionales no han sido acogidas por una gran parte de la población. Diferentes sectores sociales encabezados por organizaciones ambientalistas han manifestado su preocupación por el modelo extractivo (dependiente del sector primario) que ha adoptado el Gobierno. Si bien dichas preocupaciones tienen un profundo sentido ambiental, se identifican claramente con intereses políticos y económicos.

Dada la extracción de productos minerales, el sector primario mostró un crecimiento importante desde la década de los noventa. En 1995, superó al sector agrícola y se convirtió en el principal motor económico. Según el Observatorio de Complejidad Económica (2016), para 2016 los productos minerales contaron con una participación en las exportaciones del 48 %, seguidos de los productos vegetales, con el 16 %; productos químicos, con el 6,3 %, y el sector referente a la extracción de metales preciosos, con el 4,6 %.

La figura 2.4 muestra el crecimiento sistemático de dos sectores de la economía extractiva: productos minerales y extracción de metales preciosos.

Figura 2.4. Crecimiento de las exportaciones de productos minerales y metales preciosos (2000-2016)



Fuente: Observatorio de Complejidad Económica (2016).

Estos sectores presentan un crecimiento sistemático desde 2002 y alcanzaron su tope más alto en 2012. A partir de este año hubo una

reducción sistemática en las exportaciones, debido a la caída del precio del petróleo y, con ello, al aumento del precio del dólar.

Dichos lineamientos son el punto de partida para la reconfiguración y la organización de la minería legal en Colombia, con miras a posicionar al sector como un pilar de desarrollo de la economía. Por otro lado, y acorde con las dinámicas sociales, la legalización de la explotación minera no solo propenderá a fortalecer al Estado, sino que además presenta para el Gobierno una oportunidad de crecimiento social, aspecto que en teoría mejoraría la gobernabilidad en esos territorios.

Sin embargo, son varios los obstáculos que no le han permitido al sector minero alcanzar sus objetivos. En los últimos diecisiete años, el cambio climático ha sido uno de los protagonistas en las agendas de los diferentes gobiernos, puesto que se ha convertido en una prioridad disminuir el impacto de las actividades económicas en el medioambiente, aspecto que claramente es contradictorio, en tanto que la actividad del sector minero energético produce daños permanentes, sin importar los esfuerzos para mitigarlos. Según la Defensoría del Pueblo (2015), el daño de la minería legal, además de generar conflictos sociales, también causa problemas irreversibles en el medioambiente, debido a que contamina fuentes hídricas aledañas con cianuro y mercurio.

> El mayor número de títulos es para los materiales de construcción, con 3711; le siguen los sectores oro, plata y platino, con 2261 (2.854.487 hectáreas); luego el carbón, con 1534 (1.057.133 hectáreas). Las esmeraldas y el níquel tienen menos asignación de títulos, con 354 (82.501 hectáreas) y 13 (91.351 hectáreas), respectivamente. (p. 142)

A pesar de estas cifras, el fenómeno de la minería ilegal ha adquirido fuerza porque se ha convertido en una alternativa laboral para las comunidades pobres y para otros actores como las bandas criminales y los grupos armados (2015). Una explicación para este fenómeno es que la carencia de un marco regulador conforme a las particularidades y dinámicas propias sociales en los departamentos ha impulsado la presencia de economías ilícitas de grupos armados (2015).

4. Lineamientos estratégicos para proteger la Amazonia y consolidar la proyección de Colombia en la región

Para poder determinar aquellos lineamientos que el Estado colombiano debe contemplar para consolidarse en la Amazonia y proteger esta región, se deben precisar y analizar los planes y los proyectos que se han desarrollado hasta el momento, con el fin de puntualizar las fortalezas y aquellas condiciones que deben mejorarse.

4.1 Análisis de las políticas vigentes para la protección de la Amazonia colombiana

Este análisis contempla los diferentes niveles de la estrategia para proteger la Amazonia en Colombia y busca comprender la importancia de esta región para el país. De este modo, se estudian los postulados que al respecto contiene la Constitución, como fuente principal de los intereses del Estado, y el Plan Nacional de Desarrollo actual, que analiza el contexto y busca proteger dichos intereses, dependiendo de las circunstancias. Al final, se analizan las estrategias que las Fuerzas Militares del país al elaborado al respecto, pues en algunas circunstancias son la única representación del Estado en muchas regiones del país.

Según el artículo 2 de la Constitución Nacional de Colombia, entre los intereses nacionales están la protección de la soberanía y la integridad del territorio; el propio contenido de ese articulado tiene un enfoque ecológico, regionalista y promotor de la cooperación, evidenciándose que dentro de la Constitución que existe un enfoque entre los mandatos constitucionales y la protección de la Amazonia como parte del territorio nacional por su valor ecológico.

El actual Plan Nacional de Desarrollo, que para esta investigación es el correspondiente al mandato del presidente Iván Duque, bajo el nombre "Pacto por Colombia, Pacto por la Equidad, 2018-2022", ha representado un antes y un después dentro de las políticas de Gobierno y de Estado, al ser el primero en generar pactos específicos para temas de gran relevancia, como los océanos, la innovación y las regiones. En el

caso de estas, el Plan ha permitido un reconocimiento de aquellas zonas del territorio que no han sido debidamente reivindicadas, y la Amazonia forma parte de estas. La figura 2.5 describe los objetivos y las metas que se esperan alcanzar con dicho Plan de Desarrollo.

La figura 2.5 expresa el interés del Estado por la Amazonia y el reconocimiento de su relevancia para el desarrollo del país, dados su valor ecológico y su biodiversidad. Incluso expone uno de los principales requerimientos para el desarrollo de esta región, como lo es la conectividad.

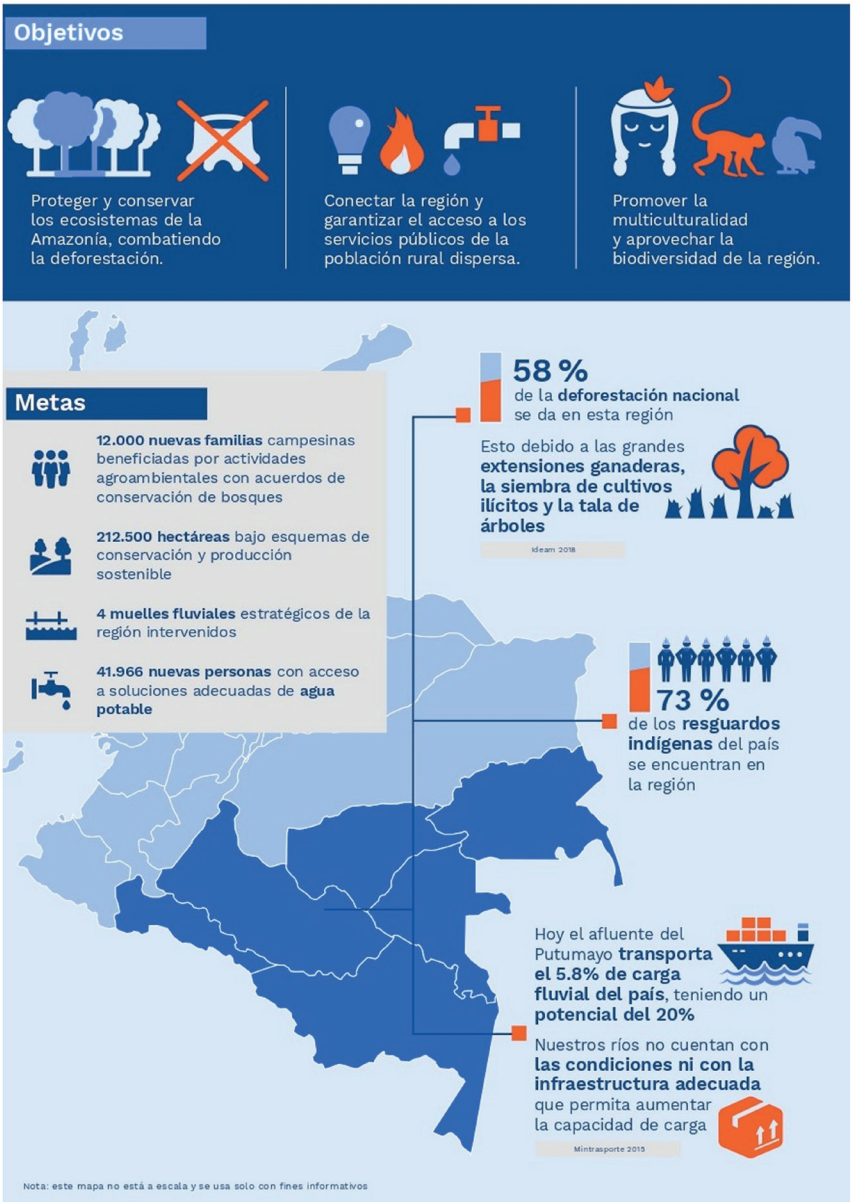
Por su parte, la Política de Defensa y Seguridad (2018) nacional consigna lo siguiente:

> Finalmente, Colombia es potencia mundial en biodiversidad y agua, además de ser uno de los países privilegiados que comparte la selva Orinoco-Amazónica. Tales riquezas constituyen un activo estratégico de la Nación y deben ser objeto de protección especial y defensa activa. Las amenazas a dichos recursos provienen de su devastación para actividades ilícitas, pero también de la escasez global de esos recursos que se vislumbra en el futuro. El sector velará especialmente por la protección y defensa de tales recursos. (p. 37)

Dentro de los objetivos políticos que rigen la estrategia de las Fuerzas Militares, la Amazonia ha adquirido un gran realce. Los siguientes son los aspectos que necesitan un impulso para poderse cumplir.

- Afectación a la seguridad territorial: control del tráfico de migrantes, garantizando la salud, la integridad y la vida de la región Amazónica.
- Contribución al desarrollo del país.
- Contrarresto de la delincuencia organizada transnacional favorecida por la porosidad de las fronteras.
- Inestabilidad regional por crisis económicas y sociales.
- Insostenibilidad de los ecosistemas derivada de los efectos de las economías ilícitas (degradación de las fuentes hídricas, deforestación y contaminación ambiental).

Figura 2.5. Pacto por la Amazonia



Fuente: Plan Nacional de Desarrollo Sostenible (2018).

4.2. Cooperación internacional

Una cooperación bilateral con Brasil está encaminada a contrarrestar las amenazas transnacionales y a promover el desarrollo y la consolidación del Estado nación. A diferencia de Colombia, Brasil es un Estado que ha determinado sus intereses de defensa y seguridad nacionales. Para este, la defensa es el conjunto de medidas y acciones del Estado, con énfasis en la expresión militar, para la defensa del territorio, la soberanía y los intereses nacionales contra amenazas preponderantemente externas, potenciales o manifiestas (Republica Federativa Do Brasil, 2012).

La estrategia nacional de defensa es inseparable de la estrategia nacional de desarrollo. Es el vínculo entre el concepto y la política de independencia nacional, por un lado, y las Fuerzas Armadas para resguardar esa independencia, por el otro. La base de la defensa nacional es la identificación de la Nación con las Fuerzas Armadas y de las Fuerzas Armadas con la Nación (2012).

El concepto de *seguridad* para Brasil es una condición que permite al país la preservación de la soberanía y la integridad territorial, la realización de sus intereses nacionales, libre de presiones y amenazas, y la garantía a los ciudadanos del ejercicio de sus derechos y deberes constitucionales (2012).

Para la República Federativa de Brasil, la Amazonia representa más que la vasta extensión de tierra sobre la que el Estado ejerce su poder. Para Colombia, este territorio significa uno de los focos de mayor interés en términos de defensa, dado el abandono en el que ha estado. Lo que se denomina Pan-Amazonia, que equivale a la totalidad de la Amazonia en América del Sur, tiene, en números aproximados, el 40 % del área sudamericana y detiene un 20 % de la disponibilidad mundial de agua dulce. La mayor parcela de extensión amazónica pertenece a Brasil, con alrededor del 70 %. Brasil afirma su incondicional soberanía sobre la Amazonia brasileña, que tiene más de 4 millones de km2, reservas minerales de distintos órdenes y la mayor biodiversidad del planeta.

La cooperación de Brasil con los demás países que tienen territorio en la Pan-Amazonia es esencial para la preservación de esas riquezas naturales (2012). Así, busca promover acercamientos y alianzas para

enfrentar las problemáticas que amenazan la sobrevivencia de dicha región y afinar estrategias que fortalezcan las acciones dirigidas al cuidado integral de la vida en ella.

Brasil se ha detenido a luchar por la recuperación y la defensa de este territorio frente a la intervención de políticas cuyas lógicas productivas y de acumulación del capital la amenazan y la degradan. En el caso de Colombia, lo hacen las actividades propias de la explotación minero-energética, las fumigaciones aéreas, el conflicto armado, la ganadería extensiva, la agroindustria, la biotecnología y la construcción de infraestructura vial (Foro Social Amazónico, 2017).

Brasil ejerce una completa y exclusiva soberanía sobre su territorio, su mar territorial y el espacio aéreo sobreyacente y no acepta ninguna forma de intromisión externa en sus decisiones. El Estado brasileño trabaja en pro de acciones que fortalezcan el acercamiento y la confianza entre los Estados, ya que la valorización y la explotación representan un aporte para la prevención de conflictos capaces de potenciar amenazas para la seguridad nacional (Republica Federativa Do Brasil, 2012).

En el ámbito social, es necesario desarrollar una acción de protección de los derechos humanos de la población que cohabita la frontera entre Tabatinga y los sectores aledaños a la isla de Santa Rosa. Ambas naciones deben trabajar al respecto, teniendo en cuenta que durante 2012 los grupos al margen de la ley de la zona fueron responsables de 141 asesinatos en cercanías a los puntos limítrofes. De las 141 muertes mencionadas, 59 correspondían a colombianos que habitaban la frontera. De las 59, 32 fueron en territorio colombiano (ISRT, 2016).

En 2015, acorde con las cifras de Muñoz (2017) citadas por Montero et al. (2018) fueron taladas 812 hectáreas de bosque en los puntos geográficos y limítrofes que ambas poblaciones comparten. La deforestación produjo el desplazamiento de 315 colombianos hacia departamentos aledaños (Putumayo) y de 139 brasileños hacia el interior del país. De esta manera, se observa que esta actividad ilícita, propia de los grupos dedicados al crimen trasnacional, atenta contra el artículo 4 de la Declaración Universal de los Derechos Humanos: “Derecho a vivir en un medioambiente sano”.

5. Conclusión

Colombia debe implementar una estrategia de cooperación, que potencie el accionar y el alcance jurídico de las operaciones militares sobre la frontera entre Colombia y Brasil. Para consolidar este objetivo, es dispensable que esta estrategia vaya de la mano con la estructuración de tres componentes clave. El primero está relacionado con el factor militar y la configuración de un comité de análisis internacional que permita intercambiar información, desarrollar operaciones conjuntas y establecer un marco normativo integral que garantice la legitimidad de las operaciones por desplegar. El segundo, el social, debe diseñar una burbuja (*think tank*) que prevenga la extracción ilegal de recursos naturales estratégicos, el daño medioambiental generado por la deforestación, y la violación de los derechos humanos relacionados con la protección de los entornos ambientales aptos para la existencia humana. El tercero, el factor económico, debe garantizar la inversión pública en la zona fronteriza y en la región Amazónica para prevenir y desarticular factores de inestabilidad producto de la ineficacia de las políticas públicas, la invisibilidad del Estado y la pérdida de control entre el centro del poder y las regiones periféricas.

PARTE II

MAESTRÍA EN DERECHOS HUMANOS Y DERECHO INTERNACIONAL DE LOS CONFLICTOS ARMADOS

CAPÍTULO III

IMPLICACIONES DE UNA EVENTUAL COMPETENCIA DE LA CORTE PENAL INTERNACIONAL A LA LUZ DE LOS DERECHOS DE LAS VÍCTIMAS EN EL MARCO DE LA JUSTICIA ESPECIAL PARA LA PAZ*

Nelson Eduardo Jiménez Valencia

* Ponencia resultado del proyecto de investigación titulado *Esclarecimiento de la verdad histórica sobre la violencia estructural en Colombia, provocada al medio ambiente y a las víctimas del conflicto: aporte de las Fuerzas Militares en la reconstrucción del tejido social*, de la Maestría en Derechos Humanos y Derecho Internacional de los Conflictos Armados, de la línea de investigación Memoria Histórica, Memoria Institucional, Derechos Humanos y Derecho Internacional de los Conflictos Armados (DICA), del grupo de investigación *Memoria Histórica, Construcción de Paz, Derechos Humanos, DICA, Justicia*, reconocido y categorizado en (C) por Minciencias, registrado con el código COL0141423, adscrito y financiado por la Escuela Superior de Guerra de la República de Colombia. Ponencia resultado de la investigación presentada como opción de grado para optar por el título de magíster en derechos humanos y derecho internacional de los conflictos armados "General Rafael Reyes Prieto".

Resumen

En los escenarios de los conflictos armados internacionales, se vulneran los derechos humanos y se desconocen los derechos de las víctimas a la verdad, la justicia, la reparación y la no repetición. Los países viven tiempos de justicia transicional, atendidos por los tribunales penales internacionales mixtos y *ad hoc*, que, debido a su naturaleza jurídica, dan un tratamiento particular a las víctimas y al posconflicto. Esta situación requiere plantear el alcance del Estatuto de Roma y de la Corte Penal Internacional, en el marco de la reparación y la atención a las víctimas de crímenes conocidos por esta Corte y su competencia frente a los países que forman parte del Estatuto, como es el caso de Colombia. Aquí, junto con la Jurisdicción Especial para la Paz y el Sistema Integral de Verdad, Justicia, Reparación y no Repetición, se han consolidado el marco normativo y los mecanismos para la reparación integral de las víctimas. Sin embargo, pese a los esfuerzos realizados por el Estado, continúa existiendo en el país una violación a los estándares internacionales de protección de los derechos humanos frente a crímenes de guerra acaecidos durante el conflicto.

Palabras clave: víctimas; derechos humanos; justicia transicional; Corte Penal Internacional; conflicto armado.

Abstract

In the context of the different scenarios of international armed conflicts, human rights are violated and victims' rights to truth, justice, reparation, and non-repetition are unknown. Countries live in times of transitional justice, addressed by the mixed and *ad hoc* international criminal courts, which, due to their legal nature, brings particular treatment to the victims and the post-conflict. This situation requires examining the scope of the Rome Statute and the International Criminal Court, within the reparation and attention to victims of crimes framework that are known by this court and its competence vis-à-vis the countries that are part of the Statute, like Colombia. Together with the Special Jurisdiction for Peace and the Comprehensive System of Truth, Justice, Reparation and Non-Repetition, the regulatory framework and mechanisms for the integral reparation of victims have been consolidated. However, despite the efforts made by the State, there is still a violation in the country of the international standards for the protection of Human Rights against war crimes that occurred during the conflict.

Keywords: victims; human rights; transitional justice; International Criminal Court; armed conflict.

1. Introducción

La existencia del conflicto armado en Colombia y la ejecución de un acuerdo que busca el establecimiento de una paz duradera, luego de décadas de vulneración a los derechos humanos, genera diversas reacciones desde los ámbitos nacional e internacional frente a la terminación del conflicto y, luego, a la etapa del posconflicto, por medio de una justicia transicional y restaurativa.

Un análisis de esta coyuntura requiere, primero, considerar los antecedentes históricos y las normas internacionales que son aplicables en los Estados que pretenden poner fin al conflicto armado interno. Segundo, tener en cuenta la posición de las víctimas y la importancia del reconocimiento de sus derechos a la verdad, a la justicia y a la reparación y no repetición. Tercero, examinar el compromiso de los actores del conflicto de poner fin a las actuaciones que vulneraron los derechos humanos y la verdadera intención de negociar y propender por una paz estable.

Todo lo anterior, en el marco del Estatuto de Roma (ER), instrumento internacional que determina el funcionamiento de la Corte Penal Internacional (CPI), con el fin de buscar no solo la penalización de los crímenes que se encuentran bajo su competencia, sino también de dar protagonismo a las víctimas directas e indirectas de un conflicto interno. Por tal motivo, un Estado que forme parte de la CPI debe garantizar la debida aplicación y reconocimiento del ER como organismo complementario a su jurisdicción interna.

Es tal la importancia de las víctimas en el derecho internacional, que la CPI cuenta con el Sistema de Asistencia de las Víctimas. Creado por el ER, tiene el objetivo de privilegiar a las víctimas de crímenes de guerra, de lesa humanidad y de genocidio, reconociendo su derecho a participar en los juicios directamente o por medio de sus representantes legales y a obtener reparaciones por daños sufridos a causa de estas conductas.

En este contexto, en los casos concretos investigados por la CPI, en el marco de la terminación de los conflictos armados con carácter internacional, el ER ha establecido límites claros frente a la solución de estos, resaltando tres puntos principales: 1) la exigencia de no impunidad en los casos investigados y los juicios, 2) las penas adecuadas para los responsables de las conductas y 3) la consecución de una justicia transicional y restaurativa que garantice los derechos de las víctimas. Hasta la fecha, la CPI nunca ha intervenido ningún proceso de negociación ni acuerdos de paz firmados que hayan terminado un conflicto. Sin embargo, en el momento en que se active la competencia de la CPI de acuerdo con lo establecido en el ER, Colombia puede llegar a ser el primer país intervenido por el organismo internacional.

Lo anterior demuestra la importancia que han tenido las víctimas en el proceso del posconflicto, pues la garantía de sus derechos a la verdad, a la justicia, a la reparación y la no repetición se convirtió en el eje central del ER y, luego, de los acuerdos de paz firmados en los Estados, específicamente del que dio origen a la Justicia Especial para la Paz (JEP) y al Sistema Integral de Verdad, Justicia, Reparación y no Repetición, que debe cumplir con los estándares internacionales de protección de los derechos humanos. Solo queda esperar que en la práctica se cumplan todos los objetivos y las acciones que permitan la verdadera reparación de las víctimas del conflicto. De no ser así, es posible que la Corte intervenga el país.

2. La situación de las víctimas a la luz de los tribunales penales internacionales mixtos y *ad hoc*, conforme a lo dispuesto en la jurisprudencia de la Corte Penal Internacional

La creación de un tribunal penal internacional mixto depende del acuerdo y la cooperación entre el Estado y las Naciones Unidas. Estos dos componentes son las fuentes de energía necesarias para que el mecanismo de justicia cooperativa funcione en su totalidad, "con el fin de lograr la reconstrucción del sistema judicial interno; en su defecto cuando es impuesto la óptica cambia y lo que se observa es la creación de un sistema judicial exclusivo para cada conflicto" (Swinnen, 2016, p. 110). De tal forma, a este tipo de tribunal pertenecen los siguientes: la Corte Especial para Sierra Leona, las Salas Extraordinarias de las Cortes de Camboya, los paneles internacionales en Kosovo, entre otros.

En consecuencia, los derechos de las víctimas nunca fueron reconocidos dentro de estos tribunales internacionalizados ni se implementó un procedimiento que permitiera a las víctimas reclamarlos ante el gran Tribunal, pues solo podían hacerlo bajo los mandatos de las leyes nacionales y acudir a la jurisdicción nacional. Es decir, no existió la posibilidad de que internacionalmente se les reconocieran derechos y, menos, reparaciones ni compensaciones de ninguna categoría.

Se puede tomar como ejemplo la Corte Especial para Sierra Leona (CESL), que a pesar de que fue creada después del Estatuto de Roma, no se incorporaron disposiciones relativas a los derechos de las víctimas para participar en los procedimientos o reclamar y recibir reparaciones. Al igual que en el Tribunal Penal Internacional de las Naciones Unidas para la ex Yugoslavia (TPIY) y que en el Tribunal Penal Internacional de Ruanda (TPIR), las "víctimas no cuentan con el derecho a participar en los procedimientos y no existen disposiciones que permitan a las víctimas solicitar reparaciones ante la Corte Especial. La compensación solo se puede obtener mediante las cortes y la legislación nacionales" (Federación Internacional por los Derechos Humanos, 2007, p. 1).

Otro ejemplo se puede tomar de las Salas Extraordinarias de las Cortes de Camboya, que respecto a los derechos de las víctimas establecen que el procedimiento debe ser acorde con el derecho camboyano. Cuando el derecho nacional no considere un tema particular, o donde existan dudas respecto la interpretación o "la aplicación de una norma en particular del derecho interno, o cuando exista una pregunta respecto el uso consistente de dicha norma respecto a estándares internacionales, se podrá hacer uso de las reglas procesales a nivel internacional al respecto" (Organización de las Naciones Unidas, 2003, p. 1).

En este sentido, los tribunales penales internacionales *ad hoc* han sido un importante antecedente en la lucha contra los crímenes cometidos en contra de los derechos humanos. Por lo tanto, fueron creados con el fin de perseguir las conductas que desconocen al ser humano como principal objetivo de protección de un Estado, razón por la cual el Consejo de Seguridad de las Naciones Unidas establece este tipo de tribunales con una competencia específica, la cual es desarrollada igualmente en un tiempo determinado.

En consecuencia, se creó el TPIY —con sede en La Haya— con el objetivo de investigar y llevar a juicio a personas que hubieran cometido crímenes de guerra, crímenes de lesa humanidad y genocidio en el territorio de la antigua Yugoslavia a partir de 1991. Siguiendo la línea temporal, el mismo Consejo de Seguridad creó el Tribunal Penal Internacional para Ruanda, con el fin de perseguir a los individuos que cometieron los mismos delitos ocurridos en el caso de Yugoslavia, solo que en este caso se trataba de aquellos desarrollados en el territorio ruandés o en Estados vecinos durante 1994. Las salas de primera instancia del TPIR se encuentran en Arusha, Tanzania, mientras que la Sala de Apelaciones se encuentra en la ciudad de La Haya.

Para Swinnen (2016), "este modelo de justicia presenta algunas debilidades como […] las dificultades de orden político y la reticencia a cooperar, que terminan influyendo, en gran medida, en la lentitud con la que actúan estos tribunales" (Swinnen, 2016, p. 111). Además, desde su creación, los derechos de las víctimas no fueron tenidos en cuenta y los apartaron de todos los procesos judiciales que se llevaran a cabo,

con el argumento de que, de acuerdo con las resoluciones del Consejo de Seguridad, la misión consistía en asegurar el enjuiciamiento de los responsables de estas atrocidades, y solo el preámbulo de la resolución que establece el TPIY contiene una referencia a las víctimas.

Las Reglas de Procedimiento y Pruebas (RPP) del TPIY y del TPIR contienen una definición muy limitada del concepto de *víctima*. Bajo la regla 2(A), una víctima es "aquella persona en contra de quien se comete un crimen sobre el cual el tribunal tiene jurisdicción". "El requisito de que el crimen sea perpetrado en contra de la víctima implica que aquellos que han sufrido a consecuencia del crimen, pero que no han sido atacados específicamente, no sean reconocidos como víctimas" (Federación Internacional por los Derechos Humanos, 2007, p. 26).

En estos tribunales, a las víctimas no se les reconocía el derecho a participar como parte en los procesos judiciales (no existían disposiciones legales que lo permitieran), y menos a reclamar algún tipo de reparación por los daños sufridos. Las víctimas quedaban supeditadas a la voluntad del fiscal, a si este consideraba tenerlas en cuenta o no, y el fiscal tampoco tenía la obligación de notificarlas ni de justificar los fundamentos de sus decisiones sobre la participación en el juicio. Si por alguna razón las víctimas lograban participar en una audiencia, era por voluntad de alguna de las partes, pero sus derechos procesales no eran respetados. Estas personas podían ser atacadas por los abogados, sin tener la oportunidad de defenderse. Tampoco tenían derecho a contar con un abogado que las representara efectivamente cuando presentaban sus testimonios, no tenían acceso a las pruebas ni podían exigir un informe sobre los procesos de su interés personal.

En resumen, el concepto de víctima y su participación como parte en un proceso judicial era muy limitado en las disposiciones legales. Aunque existiera la posibilidad remota de su participación, todo dependía de la voluntad de los particulares, pues ni los magistrados podían oír directamente las historias de los hechos contadas por las víctimas del conflicto.

En cuanto al derecho a la reparación de las víctimas, ninguno de los dos tribunales contiene disposiciones legales que lo garanticen, pues

el argumento principal se fundamenta en que en las resoluciones del Consejo de Seguridad de las Naciones Unidas se determinó que estos tribunales fueron creados para "perseguir responsables" de delitos, es decir, que la justicia impuesta es la retributiva. La resolución que establece el TPIY hace referencia a la reparación en su preámbulo, pero solo para mencionar que "el trabajo del Tribunal Internacional deberá ser llevado a cabo sin perjuicio a los derechos de las víctimas de buscar, por medio de mecanismos adecuados, la compensación por daños resultados de las infracciones del derecho internacional humanitario" (Naciones Unidas, Consejo de Seguridad, Resolución 827 de 1993).

Esta resolución se refiere a la reparación solo en el caso de que la propiedad haya sido "tomada ilegalmente". Esta es devuelta a sus propietarios por orden oficiosa del Tribunal o por solicitud del fiscal como ha sido establecido en el Estatuto del TPIY, artículo 24; Estatuto del TPIR, artículo 23 (CICR, s. f.). Además, las víctimas no llegan a ser compensadas por daños físicos o morales. Aunque exista algún procedimiento para reclamar cierta reparación que compense los daños, este nunca fue reclamado por ningún afectado, debido a que no se garantizaba un acceso a la justicia de manera efectiva ni eficiente.

Lo anterior se puede contrastar con la jurisprudencia de la CPI. Así, el reconocimiento de las víctimas "en los procesos de la CPI se convierte en un factor novedoso, pues la Corte estableció diferentes clasificaciones de víctimas como titulares de derechos, teniendo en cuenta tanto las personas naturales como las jurídicas, y las víctimas directas e indirectas" (Val, 2011, p. 87). Con esto, permitió que participen activamente, interviniendo en cualquier fase procesal cuando consideren que sus derechos están siendo vulnerados y provocando el equilibrio entre las partes procesales. "En consecuencia, se les otorga un lugar de independencia frente a la Corte" (Abogados sin Fronteras Canadá, 2018, p. 1). Aunque el Estatuto de Roma, en su artículo 75, no define concretamente el concepto de víctima, sí expresa el derecho de esta a ser reparada.

A partir de la clasificación, se establece el tipo de reparación para cada una. Así, "como las personas jurídicas se limitan a las organizaciones e instituciones que tengan como objetivo la prestación de servicios

comunitarios, las víctimas directas son aquellas que sufrieron daños por la conducta del condenado por la CPI" (McKay, 2008, p. 4). Estas son reparadas por la CPI, a través de la imposición de la condena como resultado del proceso penal desarrollado ante la Corte. Mientras tanto, "las víctimas indirectas sufren daños o vulneraciones debido a la comisión de los delitos que se encuentran bajo la competencia de investigación de la CPI" (Federación Internacional por los Derechos Humanos, 2007, p. 24) y son reparadas por medio del Fondo Fiduciario en Beneficio de las Víctimas.

El tratamiento de las víctimas por parte la de la CPI demuestra el verdadero compromiso con la defensa de los DD. HH., pues no solo pretende condenar a los responsables de la ejecución de crímenes, sino también atender de "manera eficaz a quienes han sufrido por las conductas criminales, las cuales son cometidas por los miembros de grandes estructuras, que son investigadas y procesadas por la CPI, persiguiendo siempre a los líderes y responsables más importantes de estas estructuras" (Val, 2011, p. 84).

Por tal razón, la actividad jurisprudencial desarrollada por la Corte inició con el juicio de Thomas Lubanga. La sentencia, expedida el 7 de agosto de 2012 por la Sala de Primera Instancia de la CPI, marcó un hito en el desarrollo jurisprudencial de las reparaciones del Derecho Penal Internacional. Lubanga, jefe militar líder de la guerra del Congo, fue condenado por graves violaciones a los DD.HH., como el reclutamiento de menores e innumerables masacres. La Fiscalía inició la investigación en agosto de 2006 y terminó con el juicio el 12 de marzo de 2012, que declaró a Lubanga culpable de crímenes de guerra y de alistar, reclutar y utilizar niños para participar activamente en "las hostilidades en la República Democrática del Congo entre los años 2002 y 2003. Los niños eran utilizados como guardias, porteadores y esclavos sexuales. Esta sentencia se consideró un hecho histórico en los años de funcionamiento de la CPI" (López, 2013, p. 210).

> La Sala, dentro del desarrollo de la sentencia, indicó un gran número de principios, de los cuales se pueden destacar, en primer lugar, el dar un trato justo y equitativo a todas las víctimas, teniendo en cuenta sus necesidades y características; en segundo lugar, los principios que refieren a que la

> reparación debe ser apropiada, adecuada y pronta; en tercer lugar, las reparaciones. En el caso concreto, deben tener en cuenta la violencia sexual de las posibles víctimas, las condiciones personales y sus posibles necesidades. Además, complementa que para ser considerado víctima, en el caso concreto se debe demostrar la relación entre el daño sufrido y la conducta criminal por la cual la persona es condenada, atendiéndose siempre con prelación a las víctimas más vulnerables. (Gutiérrez, 2017, p. 12)

En esta sentencia proferida por la Corte, por primera vez se hace referencia a la relevancia que tiene la reparación para las víctimas, y por primera vez se establecen los principios y los procedimientos como directrices que serán utilizadas en el tratamiento de las mismas, buscando siempre la verdad, la justicia y la reparación. Sin embargo, es necesario aclarar que la Sala determinó que los principios anteriores no aplican para otros casos que se presenten en el futuro; es decir, la sentencia de reparaciones del caso de Thomas Lubanga no "constituye jurisprudencia futura sobre el tema. De esta manera, en las futuras sentencias de la CPI nuevamente se tendrá que esperar por los principios (distintos a los de la primera sentencia) que la CPI aplicará en relación con las reparaciones" (Gutiérrez, 2017, p. 13).

En sentencia de primera instancia, la Corte decidió condenar a Lubanga a reparar a sus numerosas víctimas, fijando por ello un enfoque colectivo: "como medidas de reparación, las establecidas en el artículo 75 del Estatuto de Roma, como la restitución, compensación y rehabilitación; además de la sentencia condenatoria y la publicación de la misma" (Gutiérrez, 2017, p. 13).

Sin embargo, Thomas Lubanga se declaró indigente, y la Corte decidió que debido a esta situación solo podía contribuir a las reparaciones que se decretaran con carácter no monetario. Por su parte, la Sala señaló que su participación sería simbólica y cuando él estuviera de acuerdo (Amnistía Internacional, 2012, p. 1)

En consecuencia, la Sala de Apelaciones de la Corte, conforme a lo establecido por el artículo 75 del Estatuto de Roma, afirmó que

> […] una orden de reparación debe contener como mínimo cinco elementos: primero, debe estar dirigida contra la persona condenada; segundo: debe

> establecer la responsabilidad de la persona condenada con relación a las reparaciones consagradas en la orden; tercero: debe especificar y justificar los tipos de reparaciones establecidos, sean individuales, colectivos o mixtos; cuarto: debe determinar cuál fue el daño causado a las víctimas, que debe ser el resultado de los crímenes cometidos por las personas condenadas, así como la determinación de las modalidades de reparación ordenadas, y quinto: debe identificar a los beneficiarios de las reparaciones, o al menos los criterios para determinar su elegibilidad, teniendo en cuenta el nexo causal entre el daño y los crímenes de la persona condenada. (Gutiérrez, 2017, p. 15)

Hay evidencia de que en la jurisprudencia de la CPI se ha buscado la protección y la reparación de las víctimas, situación que debería ser igual o semejante con las víctimas del Estado colombiano, que son una muestra clara de la vulneración y el desconocimiento de los derechos humanos, la dignidad humana y los intereses colectivos. Este tipo de situaciones interesa a los entes internacionales, quienes ven en la justicia internacional la posibilidad de no solo juzgar a los responsables de crímenes atroces, sino también la oportunidad de lograr una reparación integral de todos los afectados de estas conductas.

Tanto en los conflictos internacionales, como en los conflictos internos con carácter internacional, el origen de los enfrentamientos ha sido la lucha por el poder y, con esta, la deshumanización de las partes en conflicto.

En consecuencia, la comunidad internacional atendió en su momento la crisis mundial por los conflictos armados que conllevaban la vulneración de los derechos humanos. Así, a mediados del siglo XIX se empezó a responsabilizar a los particulares por los crímenes de guerra y los crímenes de lesa humanidad (en aquel tiempo no se usaban esos términos, pues el responsable de estas conductas siempre era el Estado, aunque los crímenes fueran cometidos por sus súbditos o por sus ciudadanos).

De acuerdo con los antecedentes históricos que motivaron la creación de los Tribunales Penales Internacionales —como la Primera y la Segunda Guerra Mundial, los juicios de Núremberg, la creación de las Naciones Unidas, la Guerra de la antigua Yugoslavia, la Masacre de Ruanda, el conflicto de Sierra Leona, entre otros—, se puede colegir

que siempre estuvieron motivados por alcanzar el poder. Como factores determinantes de la guerra estuvieron las ideologías religiosas y políticas, así como los niños utilizados como soldados y la raza. La sociedad civil de todas las edades fue la más afectada.

3. La Corte Penal Internacional en el contexto colombiano y la Justicia Especial para la Paz a la luz de la situación de las víctimas en el marco del conflicto armado

La CPI es un tribunal permanente, con vocación universal, de carácter complementario respecto de las jurisdicciones nacionales, creado por el Estatuto de Roma. Adoptado el 17 de julio de 1998, con sede en La Haya, Holanda, tiene la competencia para juzgar a los individuos responsables de haber cometido genocidio, crímenes de lesa humanidad y crímenes de guerra. Para formar parte del Estatuto de Roma, Colombia debió reformar la Constitución Política, mediante el "acto legislativo" 02 de 2001, que adicionó el artículo 93 de la Norma Superior, en los siguientes términos: el Estado colombiano puede reconocer la jurisdicción de la CPI en los términos previstos en el Estatuto de Roma.

A partir de esta disposición constitucional, Colombia reconoce el Estatuto de Roma mediante la Ley 742 de 2002, declarada exequible por la Corte Constitucional mediante su sentencia C-578 del mismo año. El 5 de agosto de 2002 ratificó el Estatuto de Roma. Asimismo, también forma parte del Acuerdo sobre Privilegios e Inmunidades de la CPI (Ley 1180 de 2007) e introdujo las reglas de procedimiento y prueba y los elementos de los crímenes del Estatuto de Roma de la CPI (Ley 1268 de 2008).

Colombia ha apoyado, desde su creación, la labor de la CPI. Además de introducir en su legislación interna los instrumentos internacionales legales mencionados, Colombia ha promovido el debate y el conocimiento público sobre la CPI, ha presidido el Grupo de Amigos de la

CPI y ha contribuido voluntariamente al Fondo Fiduciario de Víctimas.

Respecto al conflicto colombiano, la Fiscalía General de la Nación ha recibido por parte de la Fiscalía de la CPI informes de los crímenes cometidos en el territorio colombiano, que son competencia de la Corte en particular: asesinatos, violaciones y otras formas de violencia sexual, "traslados forzosos de población, privaciones graves de libertad física, torturas y desapariciones forzadas. Se han presentado acusaciones de ataques dirigidos contra defensores de los derechos humanos, funcionarios públicos, sindicalistas y profesores, así como miembros de comunidades indígenas y afrocolombianas" (CPI, 2012a, p. 2).

Asimismo, la Corte halló importantes avances en el sistema judicial colombiano frente a las investigaciones de los responsables de crímenes que son de su competencia. Las autoridades nacionales han llevado a cabo acciones judiciales pertinentes contra los que parecen ser los máximos responsables de los crímenes más graves entre "los miembros de las FARC y el ELN. Según la información disponible, numerosos miembros de las FARC y del ELN, incluidos líderes superiores, han sido objeto de acciones judiciales en el marco del sistema de justicia penal ordinaria de Colombia" (CPI, 2012a, p. 2). Fueron acusados por delitos perpetrados en contra de civiles, defensores de derechos humanos, pueblos indígenas y afrodescendientes y personas que no formaban parte del conflicto pero que resultaron seriamente afectadas. Así, violaron los Derechos Humanos (DD. HH.), el DIH y, en general, el derecho internacional de los derechos humanos.

Teniendo en cuenta la evolución internacional del reconocimiento de los derechos de las víctimas —en cuanto a la reparación, la justicia, la verdad y la no repetición—, según lo establecido en el Estatuto de Roma, y luego de hacer referencia a los atroces acontecimientos internacionales, se llega al caso colombiano, que no se diferencia en nada de los demás descritos en la historia mundial.

La Justicia Especial para la Paz nació en Colombia, en una etapa en la que el país vivía momentos críticos de vulneración a los derechos humanos: secuestros, homicidios, torturas, tomas guerrilleras, reclutamiento de niños, genocidios, terrorismo, etc., razón que llevó al Gobierno

y el grupo subversivo de las FARC a unos diálogos que permitieran su acercamiento para acordar una paz duradera y estable.

Así, se iniciaron los diálogos, protegidos por un esquema de seguridad y la veeduría de países garantes, y amparados en los mandatos constitucionales y los acuerdos internacionales ratificados por Colombia, hasta llegar al "Acuerdo Final de Terminación del Conflicto y la Construcción de una Paz Estable y Duradera". Dado que una de las grandes preocupaciones de las víctimas era que "los delitos cometidos en el marco del conflicto quedaran impunes, […] en el acuerdo quedó estipulado que el Estado se encargaría de investigar y juzgar, por medio de un nuevo modelo de justicia, a quienes cometieron graves crímenes" (Congreso de Colombia, Acto Legislativo 01, 2017).

Como resultado de ese acuerdo, firmado en la Habana, Cuba, el 24 de agosto de 2016, se creó la JEP, como una entidad autónoma del orden nacional, con personería jurídica, autonomía administrativa, presupuestal y técnica, sujeta a un régimen legal propio y con la capacidad de administrar justicia en Colombia de manera transitoria. La JEP se convirtió en la instancia judicial que busca cerrar el conflicto armado, obligando a comparecer a los exmiembros "de las FARC-EP, los miembros de la fuerza pública que hayan cometido delitos en el desarrollo del conflicto armado, y los civiles que hayan participado en una forma determinante en la comisión de graves violaciones dentro del conflicto" (Congreso de Colombia, Acto Legislativo 01, 2017).

En virtud de todo esto, la JEP, como organismo de justicia transicional, con su competencia, jurisdicción y estructura, tiene un eje fundamental: las víctimas del conflicto. Estas incluyen mujeres, indígenas, afrodescendientes y demás representantes de otras estructuras sociales. Por esta razón, todas las discusiones del Acuerdo se centraron en el reconocimiento de los derechos de las víctimas, así como en su reparación, y se creó, en el Acto Legislativo 01 de 2017, un Sistema Integral de Verdad, Justicia, Reparación y No Repetición (SIVJRNR), con el cual el Estado garantiza a todas las víctimas su reparación integral y todos los derechos procesales de acceso a la justicia, equidad e imparcialidad en las decisiones.

Las funciones de este Sistema contemplan los principios de reconocimiento de los ciudadanos víctima del conflicto, de la responsabilidad de sus actores y el derecho que tienen las víctimas a la verdad, la justicia, la reparación y la no repetición. Esto hace que se alcance el mayor nivel de complacencia de los derechos de las víctimas y garantiza la seguridad jurídica de aquellos que deciden participar en el Sistema con el objetivo de aportar a la convivencia, la reconciliación y la no repetición. Por esta razón, el Sistema tiene como medida principal la aplicación de medidas restaurativas y reparadoras, es decir, pretende optar por una justicia alternativa, y no solo por sanciones retributivas, como paradigma de la JEP.

El Gobierno colombiano, con la Ley Estatutaria 1957 de 2019, reafirma la garantía de los derechos de las víctimas, la prevención de nuevos hechos de violencia y el alcance de una paz duradera. Esto se debe alcanzar a través del SIVJRNR, justificando la autonomía que tiene el Estado para crear sistemas jurídicos o jurisdicciones especiales de acuerdo con lo establecido en la Carta de las Naciones Unidas, la Constitución Política, los principios del Derecho Internacional Humanitario, el Derecho Internacional de los Derechos Humanos y el Derecho Penal Internacional.

Con base en lo señalado, resulta pertinente establecer el alcance de la competencia de la CPI ante la JEP respecto a los derechos de las víctimas, partiendo de lo establecido en el preámbulo y en los artículos 1, 17, 18, 19 y 20 del Estatuto de Roma. Este afirma que la competencia de una corte penal internacional de carácter permanente, independiente y vinculada al sistema de Naciones es juzgar los crímenes más graves de trascendencia internacional y complementar las jurisdicciones penales de cada nación.

En este sentido, el principio de complementariedad (que no es de subsidiaridad, como algunos autores lo han descrito), es desarrollado en el Estatuto de Roma, con fundamento en un sistema jurisdiccional compartido entre la CPI y la jurisdicción nacional, justificando que todos los Estados tienen el deber de ejercer su propio sistema penal. Así, la CPI se convierte en un organismo de última ratio, que solo puede activarse cuando se compruebe la falta de disposición o de capacidad judicial de un Estado para promover las investigaciones y los enjuiciamientos.

En cuanto a la competencia de la CPI en el Estado colombiano, esta fue ratificada por la Ley 742 de 2002, que la faculta para que ejerza su jurisdicción para judicializar los crímenes de genocidio, de guerra, de agresión y de lesa humanidad que sean cometidos en el territorio colombiano, por lo que debe ser aplicada a los hechos cometidos en el conflicto armado.

Sin embargo, es importante aclarar que esa jurisdicción y su competencia tienen un carácter complementario a la jurisdicción penal ordinaria interna, como lo afirma el artículo 1 de la ley mencionada. Por este motivo, Colombia tiene la facultad de poner en acción su jurisdicción interna, para buscar un acuerdo en el cual esas conductas establecidas en el Estatuto de Roma sean investigadas y juzgadas mediante una justicia especial y restaurativa.

Igualmente, la sentencia C-578 de 2002, con la cual se realiza el control de constitucionalidad al Tratado y a la Ley 742 de 2002, afirma que la jurisdicción de la CPI es complementaria al sistema penal interno en cuanto a la sanción, la reparación y el restablecimiento de los derechos de las víctimas, en el momento en que los responsables no hayan podido ser juzgados por el Estado colombiano. Esto significa que prima el ordenamiento interno.

En consecuencia, Colombia debe garantizar la efectividad de la Justicia Especial para la Paz y el cumplimiento de los objetivos del SIVJRNR, con el fin de que la Corte no tenga la necesidad de investigar.

El exfiscal de la CPI, Luis Moreno Ocampo, expone en una entrevista que, a partir del Estatuto de Roma de 1998, la CPI intentó crear una "justicia global basada en acuerdos de Estados". Esto supuso un paso importante en las relaciones internacionales, pues los Estados que forman parte del Estatuto están aceptando la competencia de una corte penal internacional que impartirá justicia cuando en aquellos la misma falle. De esta manera, puede quedar a un lado el interés nacional, y al juzgar a individuos, los Estados reconocen la responsabilidad individual en temas penales, con el fin de garantizar los derechos de las víctimas.

De lo anterior, se puede decir que el conflicto colombiano no ha cambiado de manera sustancial con los hechos históricos que se han

mencionado. Para la comunidad nacional y para la internacional es clara la cruda situación que vivió Colombia durante un conflicto que se extendió por décadas, destruyendo familias y estructuras sociales importantes, cobrando miles de vidas inocentes y, al igual que en Sierra Leona, utilizando niños como soldados.

En consecuencia, Colombia creó su propio tribunal amparado en el acuerdo de paz, de carácter nacional y por un periodo determinado. La JEP, aunque tiene similitudes con los tribunales internacionales, es exclusivamente nacional, razón por la cual se vive un momento de reconstrucción, de posconflicto, de fortalecimiento del Estado de Derecho y de respeto de los derechos humanos.

4. Conclusiones

El juzgamiento de la violación a los derechos humanos a causa de los conflictos armados vividos en la historia de la humanidad siempre será la preocupación de los entes internacionales y nacionales que administran la justicia, pues desde el momento de su creación, su principal propósito ha sido no solo la condena de los responsables, sino también dar a las víctimas la oportunidad de satisfacer su derecho a la verdad, la justicia y la reparación integral de sus derechos. Por tal razón, de acuerdo con la evolución del derecho internacional, se encuentran cuatro tipos de jurisdicciones que, con sus beneficios y críticas, con mayor o menor rendimiento, han logrado o intentado judicializar los crímenes para que estos no queden impunes: los Tribunales Penales *ad hoc*, los Tribunales Penales Mixtos, la CPI y, en el caso colombiano, la JEP.

El Sistema Penal Internacional ha presentado importantes avances respecto a la judicialización de los responsables de crímenes graves, gracias a la aprobación del ER por parte de varios países. Esto permitió establecer la responsabilidad individual de los máximos líderes de estructuras organizadas, garantizando todos los derechos procesales de los acusados y permitiendo el acceso a la justicia de todas las partes

involucradas en los casos concretos. De tal forma, el ER se convierte en el garante de los derechos humanos y del derecho internacional humanitario más importante a escala internacional, pues sus mandatos superaron toda soberanía y límite territorial.

Los conceptos de *verdad, justicia, reparación* y *no repetición* son principios fundamentales de todo proceso de paz, con los cuales se protegen los derechos de las víctimas. Deben ser garantizados no solo por la CPI, sino también por todos los gobiernos que deseen finalizar un conflicto que está violando derechos humanos y el derecho internacional humanitario. La CPI se ha encargado de que así se cumpla. El caso Lubanga representó un hito en la historia: la Corte intervino y condenó al máximo responsable, no solo privándolo de la libertad, sino también obligándolo a reparar a sus víctimas.

Según lo anterior, la CPI avala y apoya la creación de la JEP, considerando que con esta se garantiza el reconocimiento de los derechos de las víctimas, así como la persecución y condena de los responsables. Sin embargo, es responsabilidad del Estado colombiano continuar con el ejercicio judicial, legislativo y ejecutivo, para permitir que las actividades planteadas en el acuerdo de paz firmado con las FARC-EP se continúen garantizando. De no ser así, la CPI tendría motivos suficientes para intervenir el país, y esto causaría un ambiente político desfavorable para Colombia con sus vecinos, debido a que las relaciones internacionales estarían permeadas por la desconfianza. Asimismo, quedaría en duda la efectividad del sistema judicial del país y la falta de cooperación de todos sus sectores.

Los hechos históricos confirman que nunca en la aplicación del derecho penal internacional se había creado un sistema integral que estuviera compuesto por mecanismos de tipo judicial y extrajudicial que buscara la máxima satisfacción de los derechos de las víctimas. Por esto, la JEP significa un precedente para la solución de otros conflictos.

Ahora bien, activar la competencia de la CPI para que intervenga en Colombia tendría una trascendencia política frente a los países de la región, pues se convertiría en el primer país investigado por dicha corte, por no tener la capacidad de enfrentar la terminación de un conflicto

respecto a la investigación, judicialización y reparación integral de las víctimas, en la ejecución de un proceso de paz. Además, quedaría como precedente el protagonismo de las víctimas en la negociación del conflicto, pues es esta la premisa de la CPI en el marco de la terminación de los conflictos armados.

En el hipotético caso de que el acuerdo de paz en Colombia no continúe el desarrollo de sus objetivos, el conflicto seguiría siendo un factor que desestabiliza la región y las relaciones internacionales en todo el continente. En un caso tal, la Corte tendría que aplicar el ER, sin abstenerse de judicializar a los responsables de los crímenes de su competencia.

MAESTRÍA EN CIBERSEGURIDAD Y CIBERDEFENSA

CAPÍTULO IV

MODELO DE AUDITORÍA DE SEGURIDAD CIBERNÉTICA APLICADO A LA SECRETARÍA GENERAL DE LA ALCALDÍA DE BOGOTÁ*

María del Pilar Niño Campos

* Ponencia resultado del proyecto de investigación titulado *Gestión de riesgos en seguridad digital para la infraestructura crítica*, de la Maestría en Ciberseguridad y Ciberdefensa, de la línea de investigación *Seguridad Digital*, del grupo de investigación *Masa crítica*, reconocido y categorizado en (B) por Minciencias, registrado con el código COL0123247, adscrito y financiado por la Escuela Superior de Guerra de la República de Colombia. Ponencia resultado de la investigación presentada como opción de grado para optar por el título de Magíster en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto".

Resumen

Este capítulo presenta un modelo de auditoría cibernética que permita 1) identificar, enumerar y describir las diversas vulnerabilidades que pueden identificarse en una revisión exhaustiva de procesos y tecnología, y 2) determinar el nivel de ciberseguridad de una entidad, de forma que esta se convierta en una herramienta estratégica para el área de seguridad de la información y riesgos. Así, puede ser útil para el equipo auditor interno de una entidad o como herramienta de control para las auditorías externas de validación.

Este modelo se basa en un lenguaje común para gestionar riesgos de ciberseguridad, pues maneja un enfoque priorizado, flexible, repetible y neutral, basado en las necesidades de la entidad distrital. Permite a los responsables identificar, catalogar y gestionar los riesgos de ciberseguridad, estableciendo criterios y métricas para el control y la correspondiente emisión de una opinión objetiva e independiente del estado de ciberseguridad auditado.

El modelo propuesto gira en torno a seis ejes temáticos principales, que se unen e interrelacionan entre sí como las fuerzas de un átomo. El núcleo de este átomo es la información que reposa en la entidad y que forma parte esencial del negocio. Los ejes temáticos serán calificados con base en quince indicadores por cada uno, para un total de noventa preguntas. Aquellos tendrán una calificación de inicial, maduro y avanzado, con lo cual los hallazgos identificados tendrán una parte cuantitativa (numérica) y otra cualitativa (descriptiva) en la calificación. Para completar el set de cien preguntas, existen diez extra que interrelacionan los ejes temáticos.

Palabras clave: Auditoría de ciberseguridad; modelo de auditoría cibernética; riesgos cibernéticos; aseguramiento de ciberseguridad; controles de ciberseguridad; auditoria interna y externa cibernética.

Abstract

This chapter presents a model of cyber security audit that allows 1) describe and list vulnerabilities that can be identified in a comprehensive review of processes and technology. And 2) Determinate the level of cybersecurity of an entity. Thus, it becomes a strategic tool for the information, security, and risk areas, this model can also be useful for internal audit teams or as a control tool for external validation audits.

This model uses common language to manage cybersecurity risks, as it handles a prioritized, flexible, repeatable, and neutral approach, based on the needs of the district entity. It allows the person who is using this model identify, catalog, and manage cybersecurity risks, establishing criteria and metrics for control, and creating an objective, professional, and independent opinion of the audited cybersecurity status.

The proposed model goes around six main thematic points, which are related to each other like the forces of an atom. The nucleus of this atom is the information sitting in the entity, which is essential part of the business. The thematic points will be qualified based on 15 indicators for each one, for a total of ninety questions. These indicators will have a qualification of initial, mature, and advanced. Therefore, the found results will have a quantitative (numerical) and a qualitative (descriptive) segment. To complete the set of hundred, there are ten extras question that are connected to the thematic points.

Keywords: Cybersecurity audit; cyber audit model; cyber risks; cybersecurity assurance; cybersecurity controls; internal and external cyber audit.

1. Introducción

El hiperconectividad al ciberespacio es tal vez uno de los productos más visibles de la cuarta revolución industrial. Está beneficiando el nacimiento de nuevos ecosistemas complejos que proporcionan información en tiempo real y posibilitan las interacciones autónomas entre máquinas, sistemas, objetos y cosas.

Estos ecosistemas digitales permiten sacar el máximo partido y rendimiento a la internet de las cosas (IoT), a la nube, al *big data* y a la analítica de datos; tendencias de consumo del tipo *Bring Your Own Device* (BYOD), las aplicaciones de última generación, redes inalámbricas de sensores WSN (Wireless Sensor Networks), impresión 3D, robótica avanzada, realidad aumentada y ciberseguridad, entre otros.

En mundo cada vez más interconectado, la trasmisión de mensajes de datos, de acuerdo con la Ley 527 de 1999, se ha convertido en una necesidad para la gran mayoría de los colombianos, que encuentran en la internet la mejor herramienta para realizar sus actividades laborales y de esparcimiento personal: tareas, búsquedas de información, envío de correos electrónicos, compra y venta de artículos y acceso a redes sociales.

En una sociedad caracterizada por la explosión de las redes sociales y el uso de la internet de las cosas, la interconexión digital a escala global es un hecho, como también lo es la vulnerabilidad de los ciudadanos virtuales. Si bien hay aspectos positivos, como la socialización y el intercambio de información, hay riesgos que pueden trascender del mundo virtual al mundo real, y este es el principal estímulo de los ciberdelincuentes.

En los últimos años, los ciberataques contra los sistemas de información del sector público, de las empresas e instituciones de interés estratégico o de aquellas poseedoras de importantes activos de propiedad intelectual e industrial —y, en general, contra todo tipo de entidades y ciudadanos— se han venido incrementando en número, tipología y gravedad. Esto, según los informes presentados por la Asociación Bancaria y de Entidades Financieras de Colombia (Asobancaria). Según esta, los ciberataques en Colombia crecieron el 28 % en 2018.

Ante este panorama de riesgos cibernéticos que provienen de la amenaza continua a los activos digitales, las operaciones y la información corporativa, se requirieron directrices que permitieran afrontar dicha situación. Una de estas fue el CONPES 3701 de 2011, por medio del cual se dictan los lineamientos de política para la ciberseguridad y la ciberdefensa. Tales lineamientos buscan fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra la seguridad y la defensa en el ámbito cibernético, creando un ambiente propicio para la protección en el ciberespacio.

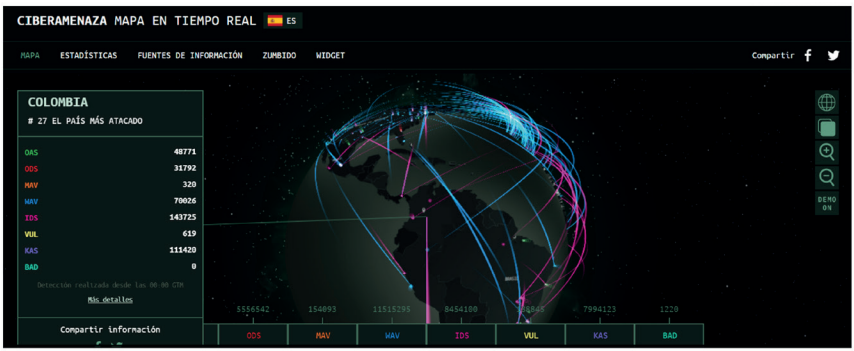
2. Antecedentes para comprender el riesgo cibernético

De acuerdo con los mapas de ciberamenzas en tiempo real, dispuestos por firmas como Kaspersky Lab (figura 4.1), y que pueden ser consultados en internet, se puede evidenciar que en promedio cien países son víctimas de ataques cibernéticos, en periodos menores a un minuto.

Los objetivos de los ciberdelincuentes varían según sus propios intereses o de terceros, y dentro de las múltiples razones esgrimidas se encuentran: la rentabilidad que ofrece su explotación, la producción de un deterioro económico directo a una compañía, el sabotaje a infraestructuras críticas, activismo político, la facilidad y el bajo costo de las herramientas utilizadas para la consecución de ataques, delitos informáticos, la sustracción de información corporativa estratégica —como la relativa a la propiedad industrial o intelectual—, robo de datos personales de

clientes y empleados, y ataques específicos a plataformas de e-commerce y redes financieras —como las relacionadas con criptomonedas. Esto se suma a una variable que genera descompensa respecto a las actividades lícitas y las contrarias a la ley en el ciberespacio, como lo es la facilidad que tiene el atacante de ocultarse. Su trazabilidad y seguimiento resulta sumamente complejo.

Figura 4.1. Mapa de amenazas en tiempo real



Fuente: Kaspersky (2019).

Por la naturaleza misma del ciberespacio, donde la conexión entre diferentes sistemas es intrínseca, cualquier sistema que dependa de una u otra manera de dicho entorno se encuentra conectado y, con esto, vulnerable a un ataque (Refsdal et al., 2015).

Si bien el término *ciberespacio* suele confundirse con el término *internet*, hay una diferencia: la expresión ciberespacio se refiere a los objetos y los recursos que coexisten en una red informática; es decir, los fenómenos que ocurren en la internet ocurren en el ciberespacio, y no en el espacio geográfico donde los cibernautas se encuentran físicamente. Así, entenderemos el ciberespacio como "un mundo no físico, el cual no tiene límites y donde cualquier persona puede estar interconectada con una conexión a la red de tal manera que pueda interactuar con el mundo entero sin barreras" (Facultad de Informática de la Universidad Complutense de Madrid, 2017a).

En el ciberespacio, el eslabón más débil de la cadena de seguridad de la información son las personas que interactúan allí, hecho que se refleja en las cifras proporcionadas por el CAI Virtual de la Policía Nacional, con corte a septiembre de 2019. Según estas, hubo un total de 7879 denuncias por hurto a través de medios informáticos.

Con corte al mes de septiembre del año 2019, se habían presentado en promedio 7800 denuncias específicamente por el Delito de Hurto por medios informáticos y semejantes, tal como lo exponen las cifras de la policía nacional.

Asimismo, hay un aumento de estos delitos a escala corporativa debido al uso extendido de la internet, que genera un mayor nivel de exposición y superficie de ataque para los cibercriminales. Además, en la mayoría de los casos no existen medidas de protección adecuadas y efectivas.

Entre otras, estas razones explican por qué el ciberespacio representa el quinto dominio de las Fuerzas de Ley. De igual manera, cualquier suceso que ocurra en el ciberespacio podría tener efectos en los mundos físico y virtual, pues da lugar a nuevas ciberamenazas que atentan contra la seguridad nacional, el Estado de derecho, la prosperidad económica, el bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas. De ahí que el ciberespacio tenga un carácter de escenario estratégico, operacional y táctico (XIX Conferencia de Directores de Colegios de Defensa Iberoamericanos, 2018).

Khuel (2009), por ejemplo, se refiere al ciberespacio como un "espacio operacional donde los humanos y sus organizaciones hacen uso de las tecnologías necesarias para actuar o crear efectos, los cuales pueden ser en el mismo ciberespacio o sobre otros dominios, operaciones o elementos del poder" (p. 29). El planteamiento de este autor nos permite comprender cómo el ciberespacio es similar a los otros cuatro dominios que existen (tierra, mar, aire y espacio), en la medida en que nace como otro dominio operacional por ser un elemento del poder dentro del cual opera la seguridad nacional. Esta característica le permite influir en los acontecimientos que surgen en todos los ambientes operativos.

Por último, vale la pena mencionar el *Informe de Riesgos Globales 2017*, publicado por el Foro Económico Mundial en su duodécima edición, donde se menciona que el riesgo cibernético emerge como uno de los diez principales riesgos por ser considerados en el entorno global, debido al aumento de su frecuencia y de su severidad por la internet de las cosas. El sinnúmero de conexiones entre personas y máquinas que esta ha provocado ha generado una ciberdependencia que aumenta las probabilidades de un ciberataque, con alto potencial de efecto dominó a través del ciberespacio (World Economic Forum, 2017).

Esta reflexión, aportada por el Foro Mundial de Economía, es muy valiosa y nos lleva a pensar que los temas que se refieren a la administración y a la contención de los riesgos asociados a las Tecnologías de información y Comunicaciones (TIC) y las tecnologías de Operación (TO) cobran en adelante un nivel de complejidad mayor, toda vez que la amenaza cibernética tiene múltiples aspectos y, sin lugar a dudas, es potencialmente peligrosa.

Sobre esto, Gastón Sack y Ierache (2015) llaman la atención sobre las características asimétricas que tiene el ciberespacio y que lo convierten en algo más complejo de definir y de defender:

> 1. la inteligencia y el engaño son aspectos críticos en el ciberespacio;
> 2. el ciberespacio es extenso, y es fácil esconderse en el mismo;
> 3. los efectos que producen los ataques son desproporcionados de cara a las herramientas que se utilizan para producirlos (pp. 3-5).

3. Riesgos de la seguridad digital

De acuerdo con lo publicado en el documento *Ciberseguridad: una guía de supervisión*, del Instituto de Auditores Internos de España (2016, pp. 9-10), los principales riesgos cibernéticos a los que se exponen todos los usuarios del ciberespacio pueden clasificarse como lo expone la tabla 4.1.

Tabla 4.1. Riesgos de la seguridad digital

Riesgo cibernético	Descripción
Fraude financiero	Es uno de los principales objetivos de los ciberdelincuentes.
Robo de información	La información de carácter personal o los documentos clasificados son algunos de los principales activos de información que deben ser especialmente protegidos. La filtración pública o la pérdida de la información confidencial tienen un riesgo elevado, cuyos impactos o pérdidas pueden resultar significativos.
Indisponibilidad de servicios	Es la interrupción puntual o prolongada de los servicios ofrecidos en línea, como correos, pagos financieros, cobro de impuestos, registros públicos, entre otros.
Sabotaje de infraestructuras	Son los ataques contra los servicios o las infraestructuras críticas de un país o Estado. Provocan desabastecimientos, interrupciones de las comunicaciones, etc., con el objetivo de provocar una paralización puntual o prolongada de aquellos.
Pérdida de reputación	Es una de las principales consecuencias de las agresiones cibernéticas y el objetivo de gran parte de los ciberataques, cuyos efectos pueden resultar altamente significativos.

Fuente: Adaptación propia con base en datos del Instituto de Auditores Internos de España (2016).

Desde sus inicios, estos riesgos han sufrido una evolución tecnológica y operacional, ya que los ciberdelincuentes se han adaptado a los cambios y están al acecho de las debilidades de nuestros sistemas de información.

Específicamente en los ámbitos laborales, dichas debilidades se convierten en vulnerabilidades por la ausencia o la ineficiencia de algún tipo de control de seguridad, ya sea de tipo procedimental, tecnológico, etc. En otras palabras, la ausencia de control aumenta de forma significativa la probabilidad de que se produzca un incidente de seguridad y que el impacto sea mayor.

Por lo anterior, y con base en los autores citados, entenderemos *ciberriesgo* como aquella posibilidad de que una amenaza proveniente del ciberespacio ataque la información administrada, almacenada, procesada, comunicada y transmitida de la entidad.

3.1. Agentes generadores de ciberriesgos internos

Un *agente generador de riesgo* puede definirse como una persona o una cosa que produce una falla. En el caso de las personas que laboran para las entidades, por ejemplo, la falta de formación y de concientización, el descontento laboral, la impericia, la ausencia de políticas y de procedimientos o la ausencia de mecanismos de disuasión son causas habituales y suficientes para facilitar un incidente de fuga de información.

Para el caso particular de los agentes generadores de ciberriesgo a escala interna, está la falta de clasificación de la información con base en su nivel de confidencialidad y en función de diversos parámetros, como el valor que tiene para la organización, el impacto público que puede generar su difusión, su nivel de sensibilidad o si se trata de información de carácter personal o no.

3.2. Agentes generadores de riesgos externos

Son aquellos originados por terceros ajenos a la propia red o sistema y que consiguen acceder a información no autorizada, modificar o interferir el propio funcionamiento del sistema, mediante la explotación de sus vulnerabilidades.

Medios nacionales como el periódico *El Tiempo* han hablado de una "profesionalización del cibercrimen", basados en criterios como el conocimiento experto de los atacantes (Medina, 2016). De igual manera, se manifiesta en informes periciales dispuestos en revistas de la Policía Nacional que los ciberdelincuentes cuentan con recursos humanos, técnicos y financieros a su libre disposición, cuando de realizar ataques gubernamentales se trata (*Semana*, 2017).

En el mercado hay múltiples amenazas capaces de infiltrarse en los sistemas y obtener información. A continuación, se exponen algunas de ellas, con base en el informe presentado por Symantec (2019).

Ataque de denegación de servicio (DOS): es un intento de hacer que un recurso deje de estar disponible para sus usuarios. Un ataque de denegación de servicio distribuido (DDoS) se produce cuando varios atacantes lanzan ataques simultáneos DoS contra un solo objetivo.

Ataques de inyección de código: son técnicas de ataque contra aplicaciones web, como la inyección SQL, *cross-site scripting* (XSS), la solicitud a través del sitio de la falsificación (CSRF), etc. Utilizando este tipo de técnicas, se persigue extraer los datos, robar credenciales o tomar el control del servidor web.

Botnet: son un conjunto de ordenadores comprometidos que están bajo el control de un atacante. Se les llama *zombies*, y estos se comunican con el sistema maestro que los puede dirigir.

Drive-by Exploits: se basa en la inyección de código malicioso en el código HTML de sitios web que explotan vulnerabilidades en los navegadores web de usuario.

Exploit kits: son paquetes de *software* creados para "automatizar" delitos informáticos. Descargan código malicioso en sitios web comprometidos.

Falsos antivirus: son cualquier tipo de *software* falso que los ciberdelincuentes distribuyen con el fin de infectar los equipos a través de falsas alertas de seguridad.

Gusanos: son programas maliciosos con capacidad de replicarse y redistribuirse mediante la explotación de las vulnerabilidades de los sistemas de destino.

Troyanos: son programas maliciosos que se inyectan sigilosamente en los sistemas de los usuarios. Pueden tener capacidades de puerta trasera, es decir, permiten que un usuario remoto pueda acceder al equipo infectado (como los troyanos de acceso remoto [RAT]) y robar datos de usuario y credenciales.

Spam: uso abusivo de correos electrónicos para saturar los buzones del usuario con mensajes no solicitados.

La evolución de estas amenazas y sus combinaciones marcó el panorama de los ataques en 2018 y 2019. La aparición de los *cryptoworms*, un tipo especializado de *ransomware* que elimina la necesidad del elemento humano, se basa en el lanzamiento de campañas de *ransomware* a través de la red, de forma autopropagada. Se considera el más peligroso, pues tiene el potencial de acabar con la internet, según los investigadores de amenazas de Cisco.

Por esto, es clave entender la evolución de estas capacidades desarrolladas por los ciberdelincuentes. Para estos personajes, la motivación para lanzar este tipo de ataques no es solo el dinero —como fuese el pago de un rescate—, sino también la eliminación de sistemas y de datos, como lo demostró Nyetya —*malware* de borrado disfrazado de *ransomware*.

Los ciberataques permiten destruir las comunicaciones y la coordinación de las ciberinfraestructuras; asimismo, crean confusión, desinformación, desorganización, caos, casos de espionaje, robo de información, entre otros problemas.

Respecto a la clasificación de los ciberdelincuentes, la empresa Arkavia Networks listó los tipos de *hackers* con sus principales características (*24 horas*, 2017).

Black hat: son los *hackers* con malas intenciones. Usan sofisticadas técnicas para acceder a sistemas, apoderarse de ellos, destruir y vender los datos.

White hat: son *hackers* éticos, que trabajan asegurando y protegiendo sistemas de tecnologías de la información (TI). Usualmente se desempeñan en empresas de seguridad informática y dan cuenta de las vulnerabilidades de las empresas para poder tomar medidas correctivas.

Grey hat: es un híbrido, ya que a veces actúa de manera ilegal, aunque con buenas intenciones. Puede penetrar sistemas y divulgar información de utilidad al público general y, con ello, acusar con pruebas a grandes compañías por la recopilación no autorizada de datos de los usuarios.

Dentro de la clasificación específica de los *black hat* existe una descripción presentada por la empresa Malware Bytes, entre la cual se mencionan los siguientes perfiles:

Carder: experto en fraudes con tarjetas de crédito. Genera números falsos y códigos de acceso que violan exitosamente los sistemas de control para robar y clonar tarjetas.

Cracker: persona que *rompe* y penetra un sistema informático con el fin de robar o destruir información valiosa, realizar transacciones ilícitas o impedir el buen funcionamiento de redes informáticas o computadoras. Puede estar motivado por una multitud de razones, desde fines de lucro y protesta hasta un simple desafío.

Defacer: busca *bugs* de páginas web en internet para poder infiltrarse en ellas y, así, modificarlas.

Lammers: son aquellos que aprovechan el conocimiento adquirido y publicado por los expertos. Si el sitio web que intentan vulnerar los detiene, su capacidad no les permite continuar más allá. Generalmente, son despreciados por los verdaderos *hackers*, que los desestiman por su falta de conocimientos y herramientas propias. Muchos de los jóvenes que hoy en día se entretienen en este asunto forman parte de esta categoría.

Pharmer: se dedica a realizar ataques de *phishing*, a través de los cuales el usuario cree que está entrando a un sitio real e introduce sus datos en uno creado por el *hacker*. Posteriormente, usa las credenciales obtenidas para robar fondos de las cuentas de sus víctimas.

Phreaker: es una persona con amplios conocimientos en telefonía. Puede construir equipos electrónicos artesanales para interceptar y ejecutar llamadas desde aparatos telefónicos celulares, sin que el titular se percate de ello.

Piratas informáticos: este apelativo se atribuye a las personas que usan *software* creado por terceros, a través de copias obtenidas ilegalmente, es decir, sin permiso o licencia del autor. Al *software* no original se le denomina "copia pirata", pero en términos reales y crudos debe llamarse "*software* robado".

Script-kiddie: es un tipo de ciberdelincuente que se limita a recopilar información, herramientas de *hacking* gratuitas y otros programas para probar sus efectos en posibles víctimas. Más de alguna vez terminan comprometiendo sus propios equipos.

Spammer y diseminador de *spywares*: hay empresas que le pagan por

la creación de *spams* de sus principales productos. También se lucra con publicidad ilegal.

Trasher: recientemente relacionado con los delitos informáticos, este ciberdelincuente obtiene información secreta o privada a través de la revisión no autorizada de la basura descartada por una persona, una empresa u otra entidad, con el fin de utilizarla en actividades delictivas.

War driver: es un *hacker* que sabe aprovechar las vulnerabilidades de todo tipo de redes de conexión móvil (*24 horas*, 2017).

Estas definiciones han surgido en diferentes espacios de discusión, como ponencias, páginas web y foros relacionados con el crimen cibernético, pero para la investigación se tomaron las mencionadas en el *Boletín Criminológico n.º 11* (Instituto de Criminoloxía, Universidad Santiago de Compostella, 2009, pp.10-19).

Todos estos personajes son cada vez más expertos en evasión y en usar como armas los servicios de la nube y otras el *sandboxing*, un mecanismo para ejecutar programas con seguridad y de manera separada (en el caso particular, para ejecutar código nuevo o *software* de dudosa confiabilidad proveniente de terceros). Los sistemas de SandBoxing, se consideran un entorno controlado, donde el área TI, puede, entre otras, ejecutar tareas de revisión de *software*, programas, códigos, todo asegurando que este no va a generar daños en los ambientes productivos.

En esta amalgama de ciberdelincuentes, es característico el uso y la adopción del cifrado para evitar la detección, así como el ocultamiento de su dirección original de navegación, con el fin de cubrir actividades de comando y control. Esto les brinda más tiempo para operar e infligir daños.

3.3. Clasificación de las ciberamenazas

Las ciberamenazas se pueden clasificar en dos: contra la información y contra la infraestructura TIC, como se muestra en la tabla 4.2 (Instituto de Auditores Internos de España, 2016, pp. 10 y 11).

Tabla 4.2. Descripción de las ciberamenazas

Ciberamenaza	Descripción	Ejemplos
Contra la información	Las materializaciones de estas ciberamenazas provocan pérdida, manipulación, publicación o uso inadecuado de la información.	• Espionaje (de Estado o industrial). • Robo y publicación de información clasificada o sensible (datos personales, datos bancarios). • Robo de identidad digital. • Fraude.
Contra la infraestructura de tecnologías de la información y las comunicaciones	Son aquellas cuya materialización puede provocar la interrupción temporal, parcial o total de determinados servicios o sistemas.	• Ataques contra infraestructuras críticas. • Ataques contra redes y sistemas. • Ataques contra servicios de internet. • Ataques contra sistemas de control y redes industriales. • Infecciones con *malware*. • Ataques contra redes, sistemas o servicios a través de terceros.

Fuente: Elaboración propia con base en información del Instituto de Auditores Internos de España (2016).

4. Estado de los delitos cibernéticos nacionales e internacionales

Se consideran delitos en el ciberespacio aquellos que están tipificados en la Ley 1273 de 2009 y que se han convertido en un negocio (*cybercrime as a service*). En la actualidad, es posible contratar, a través de la *deep-web*, la realización de un ataque de DoS, *spam*, *phishing*, el alquiler de una *botnet* o los servicios de un *hacker*.

De acuerdo con el Índice de Tendencias Ciber de la empresa consultora Deloitte, en su informe Ciber Riesgos y Seguridad de la Información en América Latina & Caribe, Tendencias 2019 Reporte Colombia (Deloitte, 2019):

- 4 de cada 10 organizaciones sufrieron un incidente de ciberseguridad en los últimos 24 meses.
- El 70 % de las organizaciones afirma no tener certeza de la efectividad de su proceso de respuesta ante incidentes de ciberseguridad.
- Solo el 3 % realiza simulaciones para probar sus capacidades efectivas de respuesta ante una amenaza *ciber*.

Otro dato relevante frente al impacto de la materialización de un ciberataque se relaciona directamente con las pérdidas económicas que se ocasionan en la entidad, dato que no suele ser fácil de estimar. Calcular el perjuicio económico debido a un incidente de ciberseguridad es una tarea compleja, dada la multiplicidad de tipos de ataques, actores y factores. (Se debe destacar que frente a la materialización de un incidente de ciberseguridad pueden ser muchos los servicios afectados, y esto complica el cálculo de las pérdidas totales).

Dentro de los costos involucrados a la hora de determinar el impacto en la entidad, debemos contemplar como mínimo si existe la necesidad de pagar por el rescate de la información, por la pérdida de los datos y por las demandas judiciales. Asimismo, hay que considerar los costos que pueden afectar la reputación de la entidad, el deterioro de la confianza de los usuarios en un servicio, la pérdida de la propiedad intelectual o la disminución de la ventaja tecnológica frente a los competidores, entre otros.

La llamada "seguridad digital" nos exige fortalecer no solo las capacidades técnicas, tecnológicas y operativas, sino también los esfuerzos civiles orientados a lograr un ciberespacio más seguro y confiable para todas las entidades públicas y privadas, y para la sociedad en general.

El esfuerzo interinstitucional está encabezado por el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT). Este coordina aspectos sobre ciberseguridad, como la protección de infraestructuras críticas, y sobre cooperación, como la gestión y el intercambio de información a escalas nacional e internacional.

Por su parte, el Comando Conjunto Cibernético (CCOCI) está conformado por las unidades cibernéticas de las Fuerzas Militares de Colombia, que son la Armada Nacional, la Fuerza Aérea y el Ejército

Nacional. Aquellos proporcionan la defensa del país mediante la creación y puesta en marcha de las estrategias que permiten prevenir y contrarrestar toda clase de ataque de naturaleza cibernética que ponga en riesgo los valores y los intereses nacionales.

Finalmente, el Centro Cibernético de la Policía (CCP) tiene entre sus funciones apoyar en ciberseguridad el territorio colombiano, ofreciendo investigación y judicialización ante los delitos cibernéticos. Para ello, incorporó dentro de su infraestructura el llamado CAI Virtual, donde los ciudadanos podemos denunciar todo tipo de delitos informáticos.

Países como Chile y España han determinado que es hora de intervenir en el mercado, y están utilizando regulaciones o leyes para exigir que ciertos sectores identifiquen, evalúen y corrijan las deficiencias en sus sistemas de seguridad. Los sectores regulados incluyen: servicios eléctricos, servicios financieros, atención en salud, transporte y telecomunicaciones.

Entre tanto, la Unión Europea (UE) impuso un enfoque especial en las infraestructuras críticas y operadores de servicios esenciales, mediante la adopción de un reglamento titulado *Directiva de Seguridad de las Redes y de la Información* (NIS, por sus siglas en inglés) (Parlamento Europeo, Consejo de la Unión Europea, 2016). Este documento comprende los aspectos del mercado interior, justicia y política exterior relacionados con el ciberespacio.

La estrategia de ciberseguridad y la propuesta de la directiva sirven de apoyo a la Agenda Digital para Europa, cuyo objetivo es ayudar a los ciudadanos y a las empresas europeas a aprovechar al máximo las tecnologías digitales. Guía a las empresas para que estas adopten las medidas oportunas para gestionar los riesgos que enfrentan en seguridad y notificar a las autoridades nacionales competentes los incidentes que tendrían un efecto perturbador significativo. Además, propone la creación de una red de cooperación entre todos los Estados miembro.

Esta directiva es un referente internacional y ha sido un derrotero para un sinnúmero de implementaciones de medidas de ciberseguridad. Cuenta con una serie de requisitos comunes en materia de:

- despliegue de capacidades;
- planificación;

- intercambio de información;
- cooperación;
- requisitos comunes de seguridad.

De la directiva NIS, resaltamos el establecimiento de reglas de seguridad cibernética que deben ser implementadas por las empresas que suministran servicios y que están clasificadas como esenciales. Los servicios cubiertos por la regulación incluyen energía; transporte; banca; finanzas; servicios públicos como el agua, la electricidad y la salud; servicios digitales como los mercados en línea (eBay, Amazon, Best Buy, Etsy, entre otros); motores de búsqueda (Google, Bing, YouTube, entre otros), y proveedores de servicios en la nube (Amazon, Google, Microsoft, entre otros).

La directiva requiere la notificación de la autoridad nacional pertinente sobre cualquier incidente cibernético grave del cual sea víctima. Este enfoque obliga a la rendición de cuentas e implica la reducción del riesgo cibernético porque la industria debe tomar medidas para reducir las vulnerabilidades y aumentar la resiliencia cibernética de las infraestructuras que administra.

Estados Unidos se ha abstenido de adoptar un enfoque regulatorio en esta materia, y, por el contrario, ha recomendado a la industria que invierta de forma voluntaria en estrategias que reduzcan el riesgo cibernético que enfrentan las infraestructuras y los servicios críticos del país. Esto, posiblemente porque el Gobierno estadounidense planea la creación de un centro encargado de proteger bancos, compañías de electricidad y otra infraestructura clave de ataques cibernéticos, una amenaza que ahora excede el peligro de un ataque físico por un grupo hostil extranjero, de acuerdo con lo dicho por la secretaria de Seguridad Nacional Kirstjen Nielsen (2018).

Si bien estamos frente a una institucionalidad definida, las cifras demuestran que los ataques son cada vez más complejos, por lo que las entidades de gobierno deben generar estrategias para contrarrestarlos. La ciberseguridad en un reto complejo que comprende diversos aspectos de gobernanza, operativos, técnicos y jurídicos.

El presente modelo de auditoría de seguridad cibernética aborda, organiza y prioriza dichos aspectos, recurriendo a modelos, marcos,

buenas prácticas y otras referencias existentes, que proveen un enfoque homogéneo para reducir el riesgo cibernético vinculado a las amenazas en el ciberespacio. Por medio de indicadores, permite el seguimiento continuo de este tipo de riesgo, a fin de robustecer los mecanismos existentes en las entidades y a mitigar el impacto de aquel.

5. Marco general de auditoría y de gestión de riesgos

En este acápite se repasan las metodologías de auditoría disponibles en el mercado de la ciberseguridad. Aunque algunos marcos se adaptan a ciertos tipos de organizaciones, no existe una única alternativa utilizada por todas las empresas. Si bien son un buen comienzo, la clave para agregar valor es ajustar las buenas prácticas a la necesidad de la entidad, con un enfoque basado en la gestión del riesgo en ciberseguridad, alineado a la estrategia de seguridad de la empresa y enmarcado siempre en función de los clientes, de la actividad principal de la entidad y del sector del mercado que representa.

Según la Unión Internacional de Telecomunicaciones (UIT, 2010), la *ciberseguridad* es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno.

De acuerdo con las metodologías existentes, para medir el nivel de riesgo se deben implementar ciertos pasos de manera organizada, con el fin de detectar qué tan seguro es el sistema de información y los riesgos y frecuencias que se pueden presentar. Estos procedimientos permiten determinar, con datos reales, las acciones por tomar para mitigar la materialización de dichos riesgos.

Los modelos conocidos de ciberseguridad y de auditoría están basados comúnmente en la gestión de riesgos conocidos. Por tanto, se hace un énfasis especial en este acápite para determinar la

articulación existente entre la gestión del riesgo y la auditoría de seguridad cibernética.

El proceso de gestión de riesgos es crítico para proteger de forma adecuada los activos de información de la entidad. Para ello, se requiere identificar la criticidad de dichos activos, las potenciales amenazas y las vulnerabilidades a las que están expuestos, además de los riesgos que con mayor probabilidad e impacto pueden afectan los procesos estratégicos, misionales y de apoyo de la entidad.

La gestión de riesgos permite tener un panorama actualizado de las posibles pérdidas en confidencialidad, integridad y disponibilidad de los activos de información. Este proceso es fundamental en la estructura del gobierno corporativo, puesto que implica la aplicación sistemática de políticas, procedimientos y prácticas que permitan:

1. identificar y analizar el riesgo, con el fin de establecer el contexto para las decisiones basadas en aquel;
2. evaluar el riesgo;
3. Tratar al riesgo una vez determinado;
4. Monitorear el riesgo de forma continua, utilizando comunicaciones organizacionales efectivas y un circuito de retroalimentación para la mejora continua de las actividades relacionadas con los riesgos de las organizaciones.

La gestión del riesgo es una actividad multidisciplinaria que requiere la participación de toda la organización, desde la alta gerencia —que proporcione la visión estratégica, las metas y los objetivos institucionales— hasta los líderes de nivel medio —que planifiquen, ejecuten y administren proyectos—, pasando por el recurso humano que apoya y opera los sistemas de información de la organización (National Institute of Standards and Technology, 2011, pp. 6-9).

Las tablas 4.3-4.5 exponen las metodologías de gestión del riesgo más conocidas y rescatan los criterios en los cuales se apoyará este modelo de auditoría.

Tabla 4.3. Metodología CRAMM

Nombre de la norma	Method CRAMM (CCTA Risk Analysis and Management Method)
Versión actual	5.0
Año de expedición	1985
Empresa	Central Computer and Telecommunications Agency del Reino Unido, gestionada por Insight Consulting Limited (Grupo Siemens).
Alcance	CRAMM utiliza métodos cualitativos y cuantitativos para identificar riesgos y amenazas. Para ello, usa una matriz cuyas filas representan los diferentes activos de información, y las columnas, los riesgos que amenazan la integridad, la confidencialidad y la disponibilidad de estos activos. Integridad es la precisión de información, así como su validez, de acuerdo con ciertas expectativas, confidencialidad, protección de la información contra la divulgación no autorizada y la disponibilidad de esta cuando sea requerida. Es distribuida de forma gratuita en idioma inglés.
Beneficios que aporta	Como resultado final de la aplicación de la metodología de CRAMM, se obtiene una matriz de análisis de riesgos y un reporte que establece como objetivo principal la gestión y el análisis del riesgo.
Enlace de interés	https://managementmania.com/en/cramm-ccta-risk-analysis-and-management-method

Fuente: Elaboración propia con base en la metodología CRAMM (Central Computer and Telecommunication Agency Risk Analysis and Management Method).

Tabla 4.4 Metodología MAGERIT

Nombre de la norma	Metodología MAGERIT
Versión actual	3
Año de expedición	1996
Empresa	Consejo Superior de Administración Electrónica
Alcance	MAGERIT implementa el proceso de gestión de riesgos dentro de un marco de trabajo útil para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de las tecnologías de la información. Esta metodología usa medios electrónicos, informáticos y telemáticos, por los beneficios que estos brindan para los empleados y los ciudadanos, pero también hace un llamado sobre sus posibles riesgos, que se tienen que minimizar.
Beneficios que aporta	El ciclo de MAGERIT inicia con la identificación de los activos de información, luego de las amenazas lógicas y del entorno. Estima las frecuencias y el impacto, para inmediatamente pasar a las salvaguardas y gestionar el riesgo residual. MAGERIT considera como activos de información el *hardware*, el *software*, la información electrónica, las personas, las instalaciones, los medios de soporte y los elementos de comunicación de datos.
Enlace de interés	https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Fuente: Elaboración propia con base en la metodología MAGERIT – versión 3.0 (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método).

Tabla 4.5. Estándar ISO 31000

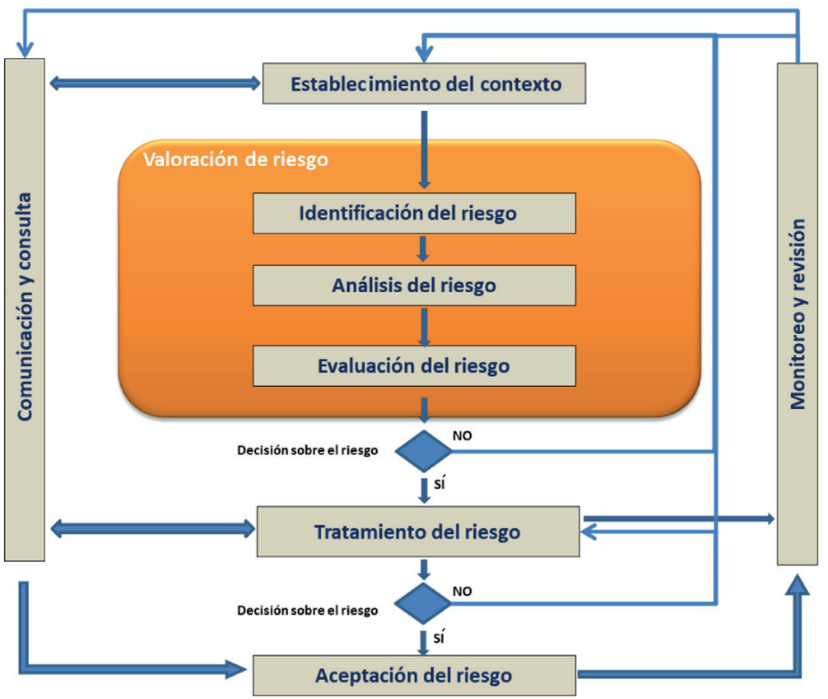
Nombre de la norma	Norma ISO 31000
Versión actual	ISO 31000:2009 - Gestión de riesgos - principios y directrices
Año de expedición	2009
Empresa	International Organization for Standardization
Alcance	La norma ISO 31000 incluye los principios del riesgo como factor clave del éxito en el diseño, implementación, operación, mantenimiento y mejora de un sistema de decisión de riesgos. Es importante aclarar que esta norma no tiene un propósito de certificación, ya que más bien aporta ciertas directrices para la implementación de una cultura organizacional. Puede utilizarse por cualquier empresa pública, privada o social, asociación, grupo o individuo. Por lo tanto, no es específica de una industria o sector concreto.
Beneficios que aporta	Incluye la valoración del riesgo, que contempla las fases de identificación, análisis, evaluación y tratamiento del riesgo. Todo ello, enmarcado en la comunicación y la consulta, así como en el monitoreo y la revisión, de lo cual se obtiene el reporte y el registro, necesarios para el Sistema de Gestión. Se aplica a metodologías que permitan hacer seguimiento sistemático de las políticas, los procedimientos y las diferentes prácticas que se han diseñado y dimensionado en el marco de referencia.
Enlace de interés	https://www.isotools.org/2018/10/15/resumen-nueva-norma-iso-31000-gestion-riesgos/

Fuente: Elaboración propia con base en la norma ISO 31000:2009 - Gestión de riesgos - principios y directrices.

El manejo que se le da a la gestión del riesgo en las entidades del distrito forma parte de un proceso estructurado y alineado con la gestión de riesgos sugerida por el Departamento Administrativo de la Función Pública (DAFP); la propuesta del *Modelo Nacional de Gestión de Riesgos de Seguridad Digital* del MinTIC; metodologías como ISO 27005, ISO 31000 y MAGERIT, y el *Documento metodológico guía 4: gestión de riesgos de la información*, publicado por la Alta Consejería Distrital de TIC.

La figura 4.2 describe las etapas de la gestión de riesgos que deben ser aplicadas en la entidad para buscar una mejora continua de la seguridad digital, en concordancia con lo establecido por el MinTIC, la función pública y las mejores prácticas internacionales, como la ISO/IEC 27001 y la ISO 31000.

Figura 4.2. Modelo de gestión de riesgo



Fuente: ISO 31000 (2018).

Los modelos vigentes de auditoría y los que estén relacionados —de manera transversal— con la ciberseguridad se basarán en una gestión de riesgos con un enfoque principalmente reactivo.

1. Inventario de sistemas de información.
2. Revisiones de configuración de seguridad de los sistemas (parches y actualizaciones).
3. Revisión de *logs* y registros de eventos.
4. Cumplimiento de los estándares de calidad.

Estos modelos de auditoría, en su mayoría, se realizan por exigencias de cumplimiento; se les dedica escasos recursos económicos y de personal, y no aportan en el proceso de concientización sobre el riesgo cibernético al que está expuesta la entidad.

6. Marco conceptual

La propuesta del Modelo de Auditoría de Seguridad Cibernética busca contemplar los dominios de ciberseguridad desde una visión holística y transversal de la gestión de riesgos que asegure que los procesos de auditoría de seguridad cibernética permitan reducir los riesgos de pérdida, alteración, manipulación y fuga de información corporativa. Busca, además, que lo que hasta hoy se conoce como "auditorías de seguridad de la información" —que mantienen un enfoque reactivo— maduren, dado el contexto actual, y que se implementen auditorías en seguridad cibernética que permitan identificar, de manera anticipada, los riesgos y una gestión continua de las amenazas. Ahí es fundamental la colaboración de la alta dirección.

En otras palabras, dicho modelo permite evolucionar de la actual cultura reactiva a una de prevención ciberresiliente, que se ajusta rápidamente a las demandas del entorno y permite detectar, de forma anticipada, las vulnerabilidades y las amenazas en el ciberespacio, con una respuesta proactiva.

Con la implementación de este modelo, se pueden medir las propiedades de seguridad de los activos de la organización y de los usuarios

contra los riesgos de seguridad en el ciberespacio. Las propiedades de seguridad analizadas dentro del modelo incluyen:

- disponibilidad;
- integridad —que incluye la autenticidad y el no repudio;
- confidencialidad.

Este modelo también incluye un apartado relacionado con la resolución de incidentes de ciberseguridad, como lo menciona Bartnes (2017). Este autor explica por qué es tan importante la colaboración interdepartamental entre varias categorías de personal y dice que para lograrlo con éxito se requiere la capacitación de todos en el tema en cuestión.

Es importante resaltar que las condiciones para la realización de las auditorías basadas en este modelo deben estar alineadas a los requerimientos específicos plasmados en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y demás planes mencionados en el Decreto 612 de 2018, expedido por el DAFP, o a lo requerido internamente, de acuerdo con el Modelo Estándar de Control Interno (MECI), por el que se regula el modelo estándar de control interno en el ámbito de la administración pública.

Esta propuesta de modelo de auditoría de seguridad cibernética es una herramienta de apoyo a la gestión del oficial de seguridad de la información y permite a las áreas de planeación y riesgos cumplir la política de seguridad digital requerida por el DAFP y el Decreto 2106 de 2019, expedido por la función pública. De este, específicamente el capítulo 2, artículo 16. "Gestión documental electrónica y preservación de la información", parágrafo 1, en el cual se requiere que las entidades dispongan de una estrategia de seguridad digital, al convertirse en una herramienta para el seguimiento de la misma.

El modelo se basa en procesos sistemáticos, independientes y documentados para obtener evidencias y evaluarlas de manera imparcial, con el fin de determinar el grado de madurez de los controles cibernéticos aplicados en la entidad. Así, permite a esta adoptar los controles oportunos para subsanar las deficiencias de su sistema de seguridad y atender las observaciones del equipo auditor.

El equipo auditor propuesto en este modelo tiene la potestad para definir el alcance de la auditoría (autoevaluación o formal), pues se adapta a sistemas con diferentes requisitos de seguridad.

7. Premisas contempladas en el modelo de auditoría de seguridad cibernética

Con el fin de lograr el éxito en la implementación del modelo de auditoría de seguridad cibernética en una entidad vinculada a la Alcaldía de Bogotá, se debe garantizar la implementación de los siguientes prerrequisitos:

1. Compromiso de la alta dirección

   Se establece como actividad previa, pues garantiza que la gestión del riesgo sea oportuna, verificada y progresiva en el tiempo y, con ello, mejorada continuamente.

   Este compromiso se materializa a través del establecimiento de políticas, guías y procesos que aporten los recursos financieros, de personal y demás necesarios para que el proceso sea exitoso y adecuado para la entidad.
2. Identificación de roles y responsabilidades para gestionar los riesgos de seguridad digital.

   Este proceso deberá ser dirigido y comunicado por la alta dirección, en razón de la importancia, para la entidad, de determinar quién debe realizar cada actividad. Para ello, se propone crear un equipo auditor.

   Frente al alcance de la auditoría, se debe aclarar que son las unidades o las oficinas de control interno (auditoría interna o quien haga sus veces) las encargadas de medir y evaluar la eficiencia, eficacia y economía de los controles por ejecutar en la entidad. Para ello, asesoran a la dirección en la continuidad del proceso administrativo, la reevaluación de los planes establecidos y la introducción de los correctivos necesarios para el cumplimiento de

los objetivos previstos. Por ello, deben estar al tanto del alcance propuesto por la alta dirección y ser actores primordiales en la implementación del modelo de auditoría.

Este modelo propone que el equipo auditor disponga de la siguiente serie de cualidades a la hora de aplicar los conocimientos y las habilidades en la entidad:

- Objetividad
- Imparcialidad
- Orientación al objetivo
- Discreción y confidencialidad
- Capacidad para informar con veracidad y exactitud
- Capacidad de aplicación de la debida diligencia
- Juicio experto al auditar de forma ética
- Mente abierta para considerar ideas y puntos de vista alternativos
- Diplomacia y tacto en el trato con las diferentes personas
- Alta capacidad de observación

Para implementar este modelo, el equipo auditor debe estar conformado por un conjunto de profesionales interdisciplinarios. La tabla 4.6 presenta la propuesta de roles y responsabilidades.

Tabla 4.6. Roles y responsabilidades específicas para auditoría

Rol	Responsabilidades
Auditor de seguridad de la información	Verificar la implementación y el cumplimiento de las políticas, normas y procedimientos que fortalezcan la seguridad de la información.
	Implementar el modelo de auditoría de seguridad cibernética.
	Presentar los informes de auditoría de seguridad cibernética, incluyendo las principales novedades.
	Estar al tanto del desempeño del sistema de gestión de seguridad de la información y de cualquier necesidad de mejora.
	Estar al tanto de los inventarios de los nuevos activos digitales de información y de los riesgos cibernéticos asociados.
	Estar en contacto con grupos especializados en seguridad digital, con el fin de estar documentado acerca de los nuevos métodos y herramientas de auditoría.
Auditor de protección de datos personales	Auditar la política de datos personales.
	Garantizar el cumplimiento del procedimiento de custodia de la aceptación de uso y almacenamiento de datos personales que realicen los ciudadanos.
Líder del proceso de auditoría	Vigilar el seguimiento a las no conformidades, el estado de las acciones correctivas y las quejas, los reclamos y las sugerencias sobre la auditoría de seguridad cibernética.
	Verificar los informes de auditorías realizadas a la seguridad cibernética y velar porque se apliquen las acciones correctivas identificadas y las recomendaciones entregadas por los auditores.
	Realizar el análisis de riesgos detectados en la auditoría de seguridad cibernética y coordinar el plan de tratamiento con el líder o responsable de ciberseguridad.
	Organizar las reuniones del equipo de auditoría de seguridad cibernética y convocar, cuando las circunstancias lo requieran, a uno de sus miembros.
	Validar las evidencias pertinentes para verificar los criterios de auditoría, cuya evaluación constituirá los hallazgos en que se basarán las conclusiones recogidas en el informe de auditoría.

Fuente: Elaboración propia con base en experiencias del autor.

Con el fin de crear dichos roles, la alta gerencia debe considerar las siguientes actividades de manera previa:

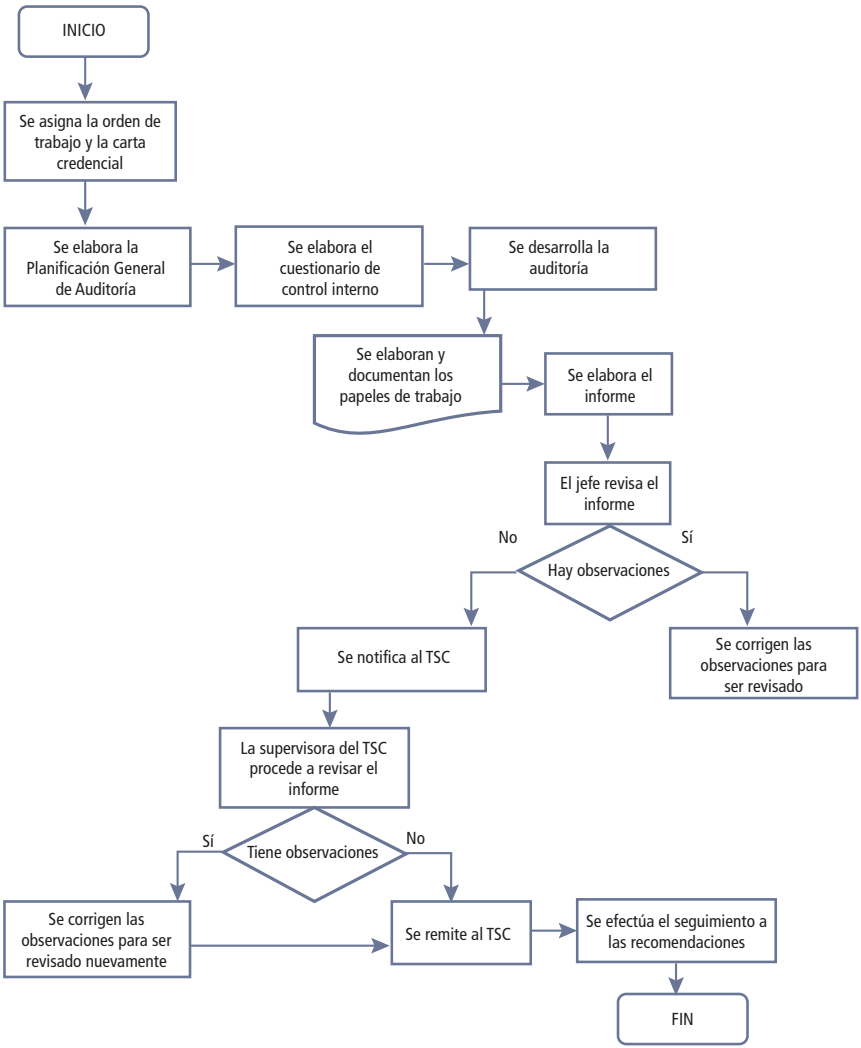
1. Identificar si existe información previa donde se describan los roles y las responsabilidades de auditoría de la entidad para procesos tecnológicos.
   La información se puede identificar en:
   - manuales de seguridad de la información o seguridad digital;
   - documentación de perfiles y funciones de los cargos de los servidores públicos;
   - políticas definidas en la entidad sobre la gestión de riesgos;
   - metodologías de gestión de riesgos que tenga actualmente la entidad.
2. Definir en el comité institucional de gestión y desempeño, de acuerdo con el Decreto 1499 de 2017 —o quien haga sus veces— los roles y las responsabilidades para la auditoría de seguridad cibernética. De ser posible, validar, mediante acto administrativo, si existe una norma jurídica que mencione el cargo.
3. Tener en cuenta la propuesta de roles y responsabilidades del equipo auditor desarrollada.

La figura 4.3 expone la estructura del proceso de auditoría que se adelanta en la entidad vinculada a la Alcaldía Mayor de Bogotá.

Si bien esta metodología está aprobada, no tiene en cuenta la gestión del riesgo cibernético ni involucra trabajo conjunto entre áreas de la entidad.

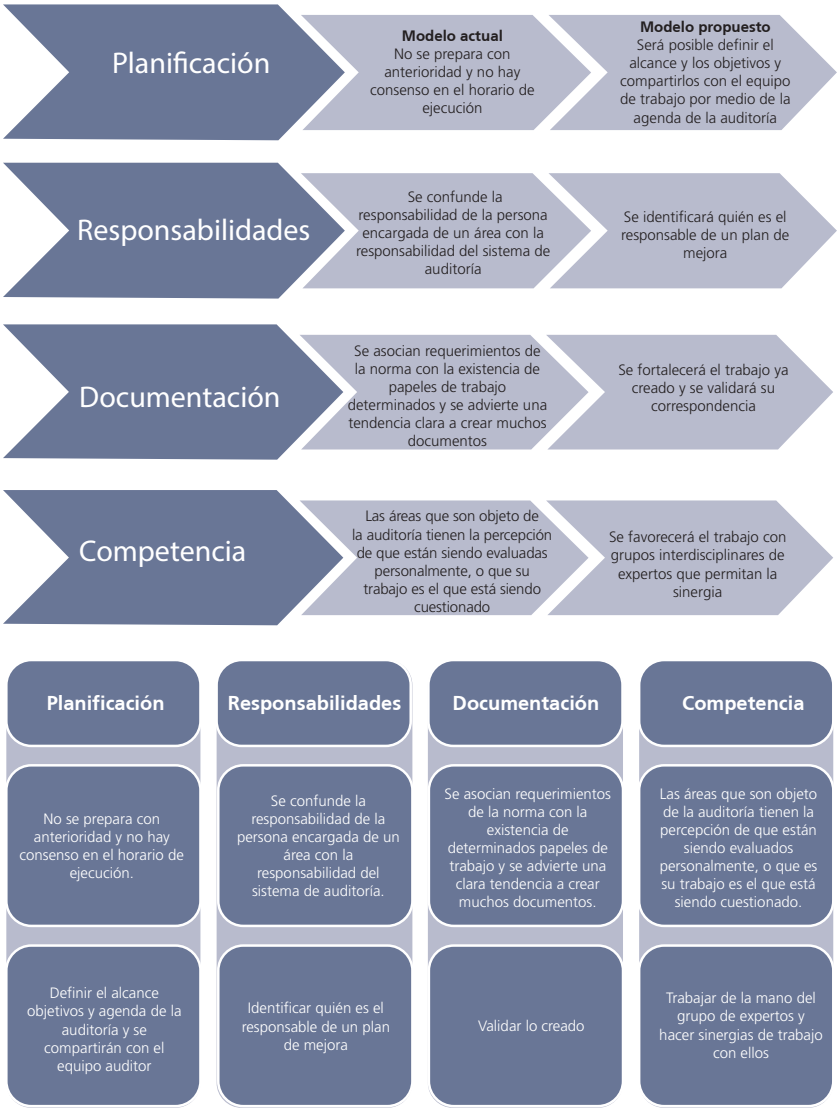
En la actualidad, el modelo implementado tiene dificultades con la comunicación entre auditado y auditor, ya que el hecho de que un auditor comience a profundizar en temas específicos, y que para ello requiera una mayor cantidad de evidencias físicas del tema, normalmente genera una reacción negativa, y en la mayoría de los casos se evidencia la falta de compromiso del auditado. La figura 4.4 ejemplifica los beneficios del modelo propuesto.

Figura 4.3. Modelo de auditoría interna



Fuente: Proceso de auditoría de entidad vinculada a la Alcaldía Mayor de Bogotá.

Figura 4.4. Puntos críticos en el modelo de auditoría actual



Fuente: Elaboración propia con base en la experiencia del autor.

Todo esto nos lleva a concluir que la metodología propuesta con el modelo de auditoría es mucho más amigable, pues convierte a los auditados en expertos, cerrando con esto la barrera cultural frente a la auditoría.

8. Metodología

Para adelantar el proceso de auditoría con base en la propuesta de un modelo de seguridad cibernética, se utilizará la metodología Delphi. Esta se basa en la suposición de que los juicios en grupo son más válidos que los juicios individuales (Reguant y Torrado, 2016).

Esta es una técnica netamente cualitativa, que permite tratar con algún grado de precisión problemas técnicamente complejos. Mediante un ciclo de entrevistas, permite recoger las ideas y las opiniones más cualificadas en el ámbito de la auditoría de seguridad cibernética. Dentro de los puntos que serán juzgados por los expertos, se tratarán temas como:

- Valoración de activos
- Gestión de riesgos
- Manejo de incidentes
- Identificación de amenazas e impactos

Lo primero que se solicita para iniciar con el modelo de auditoría de seguridad cibernética son los resultados de la auditoría anterior, para desarrollar este ejercicio a partir de un escenario inicial. La idea es que permita una adecuada recapitulación e identificación de los problemas que existen actualmente.

El uso de la metodología Delphi asegura que, en la implementación del modelo de auditoría de seguridad cibernética, el riesgo de que los auditores no detecten debilidades en el diseño o en la implementación de los controles de seguridad de las TIC se reduzca con base en las interacciones adelantadas con el grupo de expertos.

Esta metodología se propone porque si llegan a existir debilidades en los controles de ciberseguridad dispuestos por la entidad, y estos se

convierten en una vulnerabilidad, existe la posibilidad de tener un efecto adverso en las operaciones, activos o personas de la entidad y provocar la pérdida de confidencialidad, integridad o disponibilidad de la información.

El procedimiento se adelanta de la siguiente manera:

1. Definir el Tema, para este caso será lo relacionado con el modelo de auditoría
2. Hacer el cuestionario: Se prepara un cuestionario con los temas cuya valoración se desea conocer. Este punto es crítico para el éxito de los siguientes pasos. Por esta razón, el modelo de auditoría de seguridad cibernética propuesta gira en torno a seis ejes temáticos principales, que se unen e interrelacionan entre sí como las fuerzas de un átomo. Estos se ven con mayor detalle en el capítulo siguiente.
3. Definir los expertos: Se distribuye entre los sujetos que tienen una opinión relevante sobre el tema por investigar. Se recomienda que este personal forme parte del equipo de tecnología de la entidad, como el jefe de área, los administradores de sistemas de información y bases de datos, web master, coordinadores de plataformas web, personal de infraestructura y redes, oficiales de seguridad de la información, directores de protección de datos y personal de las áreas funcionales clave en la ejecución de procesos que tengan apalancamiento tecnológico.
4. Informar a los expertos su papel: Explicando que deberán de acuerdo a su experticia aplicar los cuestionarios a la vida practica enmarcado en los procesos de la entidad.
5. Distribuir los cuestionarios: El cuestionario deberá rellenarse de forma anónima para que no se puedan ver afectados los resultados, además antes de hacerlo se recomienda informar a los expertos de los objetivos que se persiguen con dicho cuestionario.
6. Tabular respuestas y analizar resultados: Con las respuestas recibidas, se prepara un histograma por cada eje temático,

indicando cuántos entrevistados se descartarán por cada nivel de valoración. Esto, con el fin de obtener unos resultados más acertados y rendir un informe de auditoría alineado y ajustado a la realidad técnica de la entidad. Si hay una clara concentración de respuestas en torno a un único valor, el proceso ha acabado: hay un claro consenso en el valor buscado. Esto demostraría que el valor obtenido de forma cuantificable se ajusta a la realidad técnica de la entidad, aunque parta de una calificación cualitativa. Si hay diferencias importantes de opinión, se remite de nuevo el mismo cuestionario en cada uno de los ejes temáticos que sean foco de desacuerdo, pero esta vez acompañado del histograma. Si se han apreciado ambigüedades en el primer cuestionario, deben aclararse en esta segunda ronda. A los entrevistados expertos de las áreas técnicas se les debe preguntar si consideran que deben mantener su primera opinión o si prefieren modificarla, con el fin de buscar consenso en las respuestas.

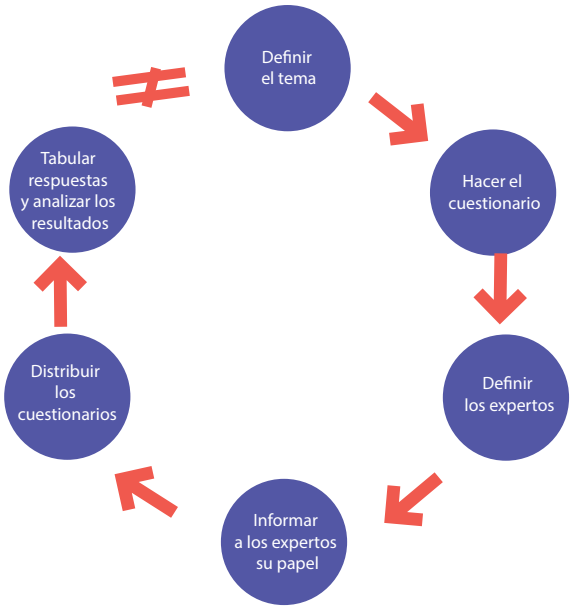
Si el histograma de esta segunda ronda sigue sin mostrar una respuesta clara, se recomienda convocar a los entrevistados a una reunión conjunta para llegar a un consenso entre el grupo de expertos de la entidad y el equipo auditor.

Es importante tener en cuenta que en el caso de que exista un histograma disperso, siempre hay que rectificar si se ha hecho la pregunta correcta a las personas correctas, si la pregunta estaba claramente expresada o si, por el contrario, se debe volver a empezar con nuevas preguntas o nuevos entrevistados. En el caso de que se requiera, se deben ajustar las preguntas, pues este modelo es evolutivo.

Después de existir un consenso entre las áreas en cada uno de los seis ámbitos, se procede, por parte del equipo auditor, a realizar el informe de auditoría, que se sustentará en los cuestionarios, los histogramas y las calificaciones cuantitativas y cualitativas del estado de la entidad frente a las medidas de seguridad cibernética implementadas.

Finalmente, se presenta el informe de auditoría (figura 4.5).

Figura 4.5. Paso a paso de la metodología Delphi aplicada al modelo



Fuente: Elaboración propia.

Buscando la evolución del modelo, se sugiere que, al terminar el proceso, si existe dispersión y hay diferencias entre el grupo de expertos, se inicie nuevamente el ciclo, ajustando las preguntas del cuestionario.

9. El informe de auditoría

El informe de auditoría deberá contener información suficiente para justificar, como mínimo:

- la fecha y el lugar en el que se ha realizado la auditoría;
- los ejes temáticos cubiertos por la auditoría de seguridad cibernética;
- las personas que han formado parte del equipo auditor —deben aparecer el nombre, los apellidos y la figura que ocupa dentro del equipo;

- el grupo de expertos evaluadores del modelo;
- el análisis de los resultados de las auditorías de seguridad cibernéticas previas;
- comentarios sobre el cumplimiento e integración del sistema de gestión de seguridad de la información y sobre si existe una referencia a la versión de la declaración de aplicabilidad;
- los hallazgos que se han identificado con el modelo de auditoría de seguridad cibernética —se recomienda que queden evidenciados y claramente numerados, para así realizar un seguimiento de estos;
- conclusiones sobre el sistema de gestión de seguridad y privacidad de la información;
- observaciones y recomendaciones.

El informe de auditoría resultante de la implementación del modelo debe contar con las características descritas en la tabla 4.7.

Tabla 4.7. Características del informe de auditoría

	Característica	Descripción
1	Claridad	Expresar las ideas de forma sencilla, legible y entendible para quien las lea.
2	Confiabilidad	Esperar confianza y fiabilidad de la información que reporta el auditor.
3	Brevedad	Expresar las ideas y los conceptos con el menor número de palabras.
4	Sencillez	Expresar con naturalidad las ideas y los conceptos.
5	Temporalidad	Presentar el informe en los tiempos requeridos.
6	Conexión	Llegar a las conclusiones con respecto a lo que reporta el informe, a través de un nexo lógico de pruebas y procedimientos.

	Característica	Descripción
7	Precisión	Redactar el informe utilizando solo conceptos completos, sin agregar datos innecesarios.
8	Exactitud	Narrar los hechos tal y como se presentaron.
9	Coherencia	Cuidar que lo que se esté reportando corresponda con lo que en realidad esté sucediendo.
10	Imparcialidad	Actuar de forma equitativa en el cumplimiento del trabajo, tratando de ser justo, honesto y razonable.
11	Objetividad	Describir las ideas y los conceptos con base en la realidad que ve el auditor.
12	Utilidad	Procurar que la lectura del informe sea útil y ágil, de tal forma que se entienda de inmediato lo que el auditor quiere decir.

Fuente: Elaboración propia con base en la Red Global de Auditores Auditool (2016).

10. Ejecución del modelo de auditoría de seguridad cibernética

Las actividades de auditoría normalmente son llevadas a cabo en una secuencia definida. Esta secuencia puede sufrir modificaciones para ajustarse a las circunstancias de auditorías específicas. Las siguientes son premisas que el equipo auditor debe contemplar al inicio de la auditoría, pues con esto se aseguran resultados positivos con la implementación del modelo.

- A fin de realizar de forma correcta la auditoría de seguridad cibernética, es necesario que la entidad en la que se lleve a cabo facilite la mayor cantidad de información pertinente para realizar los trabajos respectivos.

- Siempre que se pretenda determinar un hallazgo, este deberá estar respaldado por evidencias.
- Se deberán adoptar, por parte de las áreas responsables, las medidas oportunas para subsanar los hallazgos y atender las observaciones del equipo auditor, todo con miras a una mejora continua.
- Las recomendaciones de mejora que se desprendan de la implementación del modelo de auditoría de seguridad cibernética deberán tener en cuenta las eventuales limitaciones derivadas del ordenamiento jurídico.

10.1. Desarrollo argumental del planteamiento

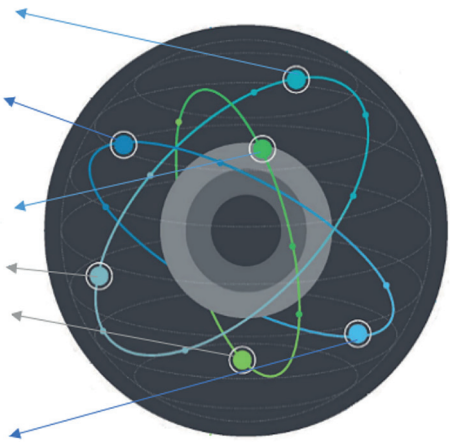
Este modelo propone incluir áreas funcionales de la entidad y al grupo de expertos del área de Tecnología, y presentar un modelo unificado y adaptable para la planificación y la realización de auditorías de seguridad cibernética, alineando metodologías existentes y requisitos regulatorios que permitan aportar un criterio técnico, administrativo y jurídico sobre la problemática planteada con un alto nivel de objetividad como herramienta de gestión de la seguridad digital de la entidad.

La idea del modelo de auditoría es mostrar el estado real de la entidad. Por lo tanto, no debe ser tomado como base para cuestionamientos, sino para tomar medidas proactivas, en caso de tener una calificación que se aleje de lo esperado en cado uno de los seis ejes temáticos.

El modelo propuesto gira en torno a seis ejes temáticos principales, que se unen e interrelacionan entre sí como las fuerzas de un átomo. El núcleo de este átomo es la información que reposa en la entidad y que forma parte de la actividad principal de la entidad (figura 4.6).

Figura 4.6. Propuesta de temas valorados por eje temático de tipo átomo

EJE	TEMAS VALORADOS EN EL EJE TEMÁTICO
1	Seguridad, protección y resiliencia de los sistemas de información, redes y telecomunicaciones que soportan las infraestructuras tecnológicas.
2	Capacidades de prevención, detección, gestión, respuesta, investigación y coordinación frente a los incidentes cibernéticos; y fomento del intercambio de información sobre ciberamenazas.
3	Conocimientos, habilidades experiencia y capacidades tecnológicas necesarias para alcanzar los objetivos de ciberseguridad establecidos en la estrategia de seguridad digital.
4	Activos de información, riesgos cibernéticos y planes de mitigación.
5	Gobernanza estratégica, arquitectura TI y marcos regulatorios y jurídicos.
6	Formación y concienciación en materia de ciberseguridad, con el fin de contribuir a la creación de una cultura de ciberseguridad.



Fuente: Elaboración propia.

Los ejes temáticos se definieron en seis grupos según los temas relacionados (tablas 4.8-4.13).

10.2. Ejes temáticos

Tabla 4.8. Eje temático número 1

Número de eje temático	Temas desarrollados
1	Seguridad, protección y resiliencia de los sistemas de información, redes y telecomunicaciones que respaldan las infraestructuras tecnológicas. **Pertinencia entre temas.** La seguridad, la protección y la resiliencia forman parte de este grupo porque permiten conocer el estado actual de seguridad cibernética al que están expuestos los activos de información de la entidad. Ante todo, se busca reconocer claramente las vulnerabilidades y las posibles brechas en la cadena de valor de la entidad, incluyendo infraestructuras, *cloud*, dispositivos móviles y, en general, los activos de información que forman parte del centro del negocio. También se evalúa la capacidad de la empresa para garantizar la continuidad de su negocio; es decir, si tiene los recursos humanos y tecnológicos necesarios para afrontar, con flexibilidad y fortaleza, las situaciones de ciberriesgo y para sobreponerse a ellas, minimizando y absorbiendo sus consecuencias negativas.

Tabla 4.9. Eje temático número 2

Número de eje temático	Temas desarrollados
2	Capacidades de prevención, detección, gestión, respuesta, investigación y coordinación frente a los incidentes cibernéticos; y fomento del intercambio de información sobre ciberamenazas. **Pertinencia entre temas.** Estos temas tratan del manejo de los incidentes que se puedan presentar por la afectación de los activos de información debido a una ciberamenaza. Este eje temático fue pensado para ayudar a los directores de tecnología de la información (TI) y oficiales de seguridad de la información de las entidades, quienes deben desarrollar un informe de incidentes de seguridad cibernética que no requiera un análisis de causa raíz, pero que amerite una investigación profunda, ágil y eficiente.

Tabla 4.10. Eje temático número 3

Número de eje temático	Temas desarrollados
3	Conocimientos, habilidades, experiencia y capacidades tecnológicas necesarias para alcanzar los objetivos de ciberseguridad establecidos en la estrategia de seguridad digital. **Pertinencia entre temas.** Se vincularon los temas referidos a los procesos de capacitación en este eje temático, con el fin de identificar la brecha de cumplimiento frente a los objetivos institucionales y de cara a la estrategia de seguridad digital que busca implementar el MinTIC. En este eje temático, se busca determinar la necesidad de desarrollar nuevas estrategias de capacitación para los funcionarios del área tecnológica sobre ciberseguridad, de acuerdo con las directrices de la Alta Consejería Distrital de las TIC, y que tales estrategias permitan potenciar la creación, difusión y aplicación de las mejores prácticas en materia de ciberseguridad en la Alcaldía Mayor de Bogotá.

Tabla 4.11. Eje temático número 4

Número de eje temático	Temas desarrollados
4	Activos de información, riesgos cibernéticos y planes de mitigación. **Pertinencia entre temas.** Se busca validar el estado de las estructuras de seguridad con las que cuentan los activos de información; en particular, los que manejan información clasificada o del centro del negocio que se encuentra almacenada, manejada o transmitida en las infraestructuras tecnológicas de la entidad. Esto, con el fin de validar el ámbito —físico y digital— de los riegos cibernéticos. Para ello, se evaluará la inclusión de las medidas de ciberseguridad oportunas en los distintos planes que se establezcan en la entidad.

Tabla 4.12. Eje temático número 5

Número de eje temático	Temas desarrollados
5	Gobernanza estratégica, arquitectura TI y marcos regulatorios y jurídicos. **Pertinencia entre temas.** Estos temas se vincularon de forma que se pueda evaluar la existencia y la pertinencia de un marco de gestión de ciberseguridad en los ámbitos técnico, operativo y jurídico. Se han integrado con el marco legal colombiano sobre delitos informáticos y con lo referido en el convenio de Budapest, con el fin de integrar soluciones a los problemas relacionados con la ciberseguridad. Esto, para determinar los tipos penales y el trabajo mancomunado de los departamentos competentes, tanto en la entidad como con terceros involucrados, y asegurar la coordinación de estas capacidades con las entidades policiales.

Tabla 4.13. Eje temático número 6

Número de eje temático	Temas desarrollados
6	Formación y concienciación en materia de ciberseguridad, con el fin de contribuir a la creación de una cultura de ciberseguridad. **Pertinencia entre temas.** Aquí se les evaluarán a los funcionarios de la entidad las actividades de sensibilización y desarrollo de programas de concienciación en ciberseguridad concernientes a vulnerabilidades, ciberamenazas e información sobre cómo proteger mejor su entorno tecnológico, no solo internamente, sino también en colaboración con agentes de los sectores público y privado.

Los ejes temáticos serán calificados con base en quince indicadores por cada uno, para un total de noventa preguntas, según "inicial", "maduro" y "avanzado". Con esto, los hallazgos identificados tendrán una parte cuantitativa (numérica) y otra cualitativa (descriptiva) en la calificación. Para completar el set de cien preguntas, existen diez extra, que tienen una interrelación entre los ejes temáticos (tablas 4.14-4.16).

Tabla 4.14. Calificación asignada al indicador

Indicador	Valor cualitativo	Valor cuantitativo	Definición
Pregunta número 1 a 15	Rojo	0	*En el nivel rojo de madurez:* no cumple con los requisitos mínimos de seguridad cibernética. Tiene conocimiento del requisito. La actividad no existe o no se está haciendo. Puede que el proceso exista, pero no se gestiona. El éxito o fracaso de la actividad depende de la competencia, no de la buena voluntad de las personas, y es difícil prever la reacción ante una situación de emergencia. Es impredecible el resultado, si se dan circunstancias nuevas. Existe un riesgo significativo de materialización de un ciberriesgo.
	Amarillo	1	*En el nivel amarillo de madurez*: cumple parcialmente. Dicha actividad se está haciendo de manera parcial, se está haciendo diferente, no está documentada en todas las ocasiones o se definió y aprobó, pero no se gestiona. Se ejerce un mantenimiento regular y el funcionamiento de los procesos está bajo control (con técnicas manuales o esporádicas).
	Verde	2	*En el nivel verde de madurez:* cumple satisfactoriamente. Existen actividades gestionadas y se cumple con la tarea solicitada. El indicador está documentado, es conocido y aplicado por todos los involucrados en la entidad. Dichas actividades se centran en la evolución continua de los procesos, con mejoras tecnológicas incrementales e innovadoras. Se establecen objetivos cuantitativos de mejora, se revisan continuamente para reflejar los cambios en los objetivos del negocio y se utilizan como indicadores en la gestión del perfeccionamiento de los procesos. En este nivel, la entidad es capaz de mejorar el desempeño de los sistemas a partir del progreso continuo de los procesos (con base en los resultados de las medidas e indicadores).
	Azul	N/A	El control no es aplicable para la entidad. En el campo, se observa la necesidad de indicar la justificación respectiva de su no aplicabilidad.

La sumatoria de la puntuación dada a cada uno de los indicadores en los seis ejes temáticos permitirá determinar el estado del avance en cada área. La calificación de cada indicador dependerá del nivel de madurez alcanzado por la entidad. Por consiguiente, la entidad tendrá una de las tres calificaciones que se muestran en la tabla 4.15, en cada uno de los ejes temáticos.

Tabla 4.15. Calificación asignada al eje temático

Calificación	Valoración numérica	Descripción
Inicial	Desde 0 hasta 14	La entidad no tiene ningún plan para administrar su ciberseguridad. Los controles para las áreas críticas de ciberseguridad son inexistentes o muy débiles. La organización no ha implementado un programa integral de seguridad cibernética. La preparación de ciberseguridad es inexistente en esta área. **Reproducible, pero intuitivo.**
Equilibrado	Desde 15 hasta 24	La organización está comenzando a centrarse en la ciberseguridad. Si existen tecnologías, debe enfocarse en las áreas clave para proteger los activos cibernéticos, al igual que en el personal, los procesos, los controles y las regulaciones. La preparación de la ciberseguridad se está desarrollando en esta etapa. Se requieren mejoras en las áreas clave en las que se han identificado debilidades. **Proceso definido.**
Evolucionado	Desde 25 hasta 30	La organización se ha destacado en la implementación de las mejores prácticas de ciberseguridad. Siempre hay un margen de mejora. Se debe mantener la documentación actualizada y revisar continuamente los procesos de ciberseguridad a través de auditorías. La preparación en ciberseguridad está en un nivel avanzado, pero la organización debe actualizar continuamente su estrategia de ciberseguridad. **Gestionado y medible.**

Fuente: Elaboración propia.

Como resultado de la auditoría, se puede identificar una serie de hallazgos por cada uno de los ejes temáticos. La suma total de los valores obtenidos en dichos ejes más el cálculo de las diez preguntas extra, que tienen interrelación entre los ejes temáticos y que se valoran de acuerdo con la explicación anterior, darán un valor máximo de doscientos puntos. Con esto, el resultado final de la implementación del modelo de auditoría arrojará una las calificaciones que se muestran en la tabla 4.16.

Tabla 4.16. Nivel de madurez en seguridad cibernética

Calificación	Valoración numérica (en puntos)	Descripción
Desfavorable	Menor de 69	Con respecto de la entidad, existen incumplimientos de las regulaciones establecidas que le han generado afectaciones económicas. Se observan riesgos que propician la falta de control en los activos de información a su disposición y afectan el cumplimiento de sus objetivos estratégicos y operacionales. Existen controles, pero no son reiterativos o documentados y se realizan de forma reactiva. El plan de prevención no tiene identificados algunos puntos vulnerables con relación a las deficiencias detectadas. Esto genera resultados negativos en determinados procesos de la entidad y perjudica la efectividad de las medidas adoptadas para minimizar los riesgos. En este caso, se requerirá la realización de una auditoría extraordinaria que verifique la adopción de las medidas correctivas adecuadas. Ante esto, se puede requerir la verificación de la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en la entidad.
Con oportunidad de mejora	Desde 70 hasta 150	Se requieren mejoras en las áreas clave en las que se han identificado debilidades. Si bien los hallazgos no afectan de manera significativa la ciberseguridad de la entidad, se debe validar cómo realizar el cumplimiento de los indicadores. Pueden existir vulnerabilidades que afecten las operaciones, siempre que no distorsionen la información en términos de confidencialidad, integridad y disponibilidad de manera significativa en la entidad.

		Los procesos relacionados con los controles de los activos de información dan cuenta de que los incumplimientos de la legislación aplicable y las debilidades comprobadas no influyen en los requerimientos de información ni en el patrimonio de la entidad. El plan de controles dispuestos para el set de indicadores de la entidad cumple con su objetivo en cuanto a su estructura y contenido. Están identificados los puntos vulnerables y las medidas adoptadas son efectivas y minimizan los riesgos de ciberseguridad.
Favorable	Mayor de 150	Se debe mantener la documentación correspondiente actualizada y revisar continuamente los procesos de ciberseguridad, a través de auditorías y con base en el marco general de riesgos. Se puede determinar que la entidad cuenta con un nivel de ciberseguridad eficiente y eficaz que asegura el funcionamiento correcto en las operaciones, pues se puede establecer un nivel alto de confiabilidad en la información. Cumple con las leyes, reglamentos y políticas establecidas. Garantiza un control razonable de los activos de información a disposición de la entidad. Se cumplen los indicadores establecidos para medir la efectividad de los seis ejes temáticos del presente modelo de auditoría cibernética.

Fuente: Elaboración propia.

10.3. Resultados y análisis

Se está en el proceso de desarrollo y prueba de los indicadores, a fin de identificar los más concluyentes y que permitan tener una visión holística del panorama de seguridad cibernética en la entidad.

Se considera que el modelo es bastante robusto, pues cuenta con un set específico de indicadores por eje temático. Con base en el método Delphi, permite tener una menor dispersión en la respuesta respecto al cumplimiento y control del mismo.

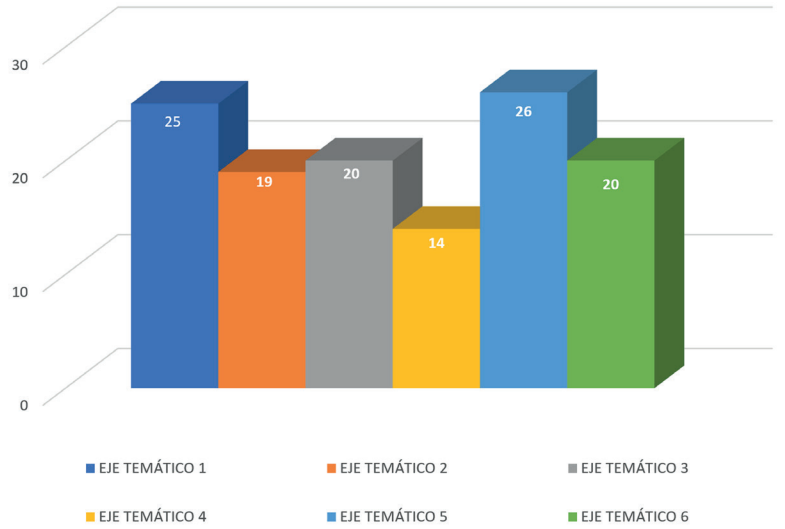
Con base en los resultados de la prueba del modelo *in situ*, los avances han demostrado que la propuesta de realizar las auditorías

cibernéticas por ejes temáticos puede ser muy efectiva para evaluar los controles. De ser requerido, no se realiza la auditoría completa, sino solo en el eje temático afectado. La tabla 4.17 expone la calificación de los ejes temáticos.

Tabla 4.17. Calificación de ejes temáticos en la entidad

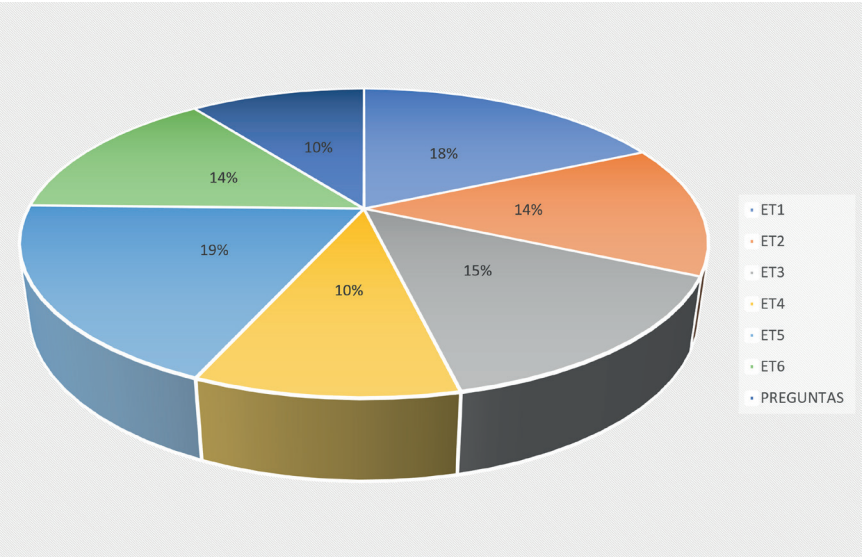
Eje temático	Temas valorados en el eje temático	Calificación
1	Seguridad, protección y resiliencia de los sistemas de información; y redes y telecomunicaciones que respaldan las infraestructuras tecnológicas.	25
2	Capacidades de prevención, detección, gestión, respuesta, investigación y coordinación frente a los incidentes cibernéticos; y fomento del intercambio de información sobre ciberamenazas.	19
3	Conocimientos, habilidades, experiencia y capacidades tecnológicas necesarias para alcanzar los objetivos de ciberseguridad establecidos en la estrategia de seguridad digital.	20
4	Activos de información, riesgos cibernéticos y planes de mitigación.	14
5	Gobernanza estratégica, arquitectura TI y marcos regulatorios y jurídicos.	26
6	Formación y concienciación en materia cíber, con el fin de contribuir a la creación de una cultura de ciberseguridad.	20

Figura 4.7. Calificación de los ejes temáticos



Fuente: Elaboración propia.

Figura 4.8. Porcentajes de los ejes temáticos



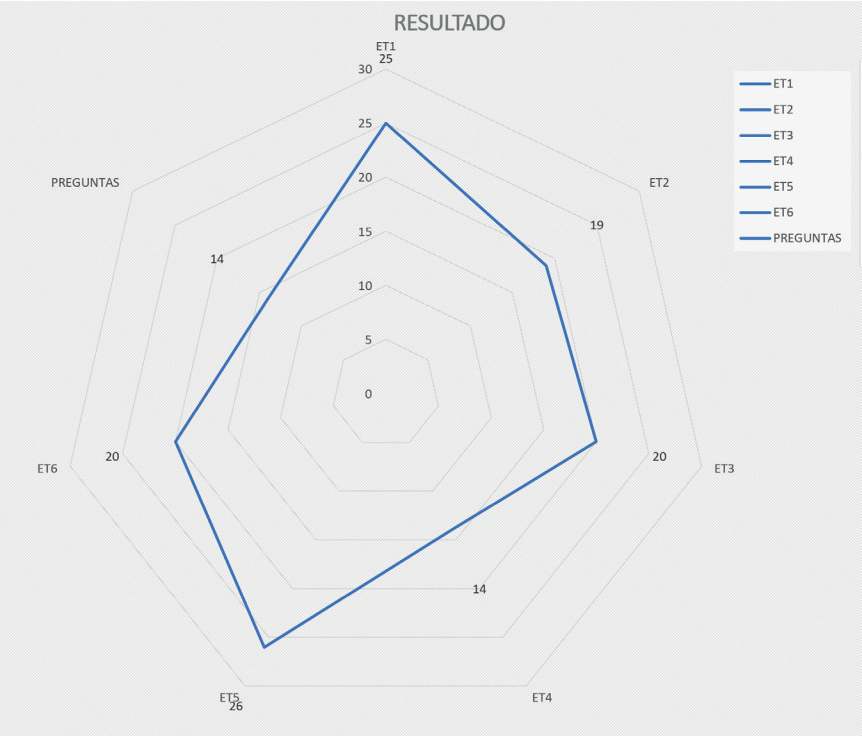
Fuente: Elaboración propia.

Según el análisis de las calificaciones obtenidas (figura 4.7) y su análisis (figura 4.8), se puede sostener que la entidad vinculada a la Alcaldía Mayor de Bogotá está en proceso de hacer cambios y obtener oportunidades de mejora en cuestiones de ciberseguridad. De igual manera, se observó que por parte de la alta gerencia se han establecido procedimientos documentados que están siendo objeto de actualización y que se requiere que se ajusten a la menor brevedad posible.

Por su parte, los controles tecnológicos se han implementado en la entidad, pero existen vacíos respecto al manejo de tablas de retención documental. Por lo tanto, es importante que las áreas involucradas se enfoquen en proteger los activos de información.

Frente a los procesos de capacitación, hay que trabajar con el área de Recursos Humanos e integrar el plan estratégico de tecnologías de la información con el plan de capacitación anual, a fin de trabajar en la ciberseguridad. La calificación final de madurez de ciberseguridad se posiciona en el nivel de "Oportunidad de mejora", con una calificación de 138 puntos, que se encuentra desagregado por ejes tal como lo muestra la figura 4.9.

Figura 4.9. Calificación general del modelo



Fuente: Elaboración propia.

11. Conclusiones

- Se cumplió con el objetivo general de esta investigación: diseñar y validar un modelo de auditoría cibernética que permita conocer el estado real del cumplimiento de los controles, mediante un proceso de auditorías integrales.
- Las organizaciones nacionales e internacionales e instituciones académicas están desarrollando metodologías para apoyar a la comunidad en general a diagnosticar y reducir el riesgo cibernético. De forma conexa, se puede entender cómo estos marcos son necesarios para aumentar la productividad y la eficiencia y reducir los costos.

- Si bien existe en Colombia una gran cantidad de referencias normativas, técnicas y jurídicas referentes a la ciberseguridad, no existe —a escalas nacional e internacional— un único marco unificado que permita hacer una auditoría y revisar el manejo de riesgos de manera conjunta.
- Se requiere el compromiso de la alta gerencia de atender y definir el alcance de la auditoría, pues de este depende el interés y los recursos asignados en el desarrollo del trabajo.
- Se observó la necesidad de identificar roles y responsabilidades para realizar el proceso de auditoría —interna o externa—, y se presentó una propuesta de los mismos.
- Ser partícipe de la toma de decisiones es un factor que contribuye a vencer las resistencias frente a los cambios; formar parte de los órganos decisorios al participar en estos procesos participativos convierte al Delphi en un instrumento generador de confianza.
- Con base en los resultados del modelo, los avances han demostrado que la propuesta de realizar las auditorías cibernéticas mediante la técnica de ejes temáticos puede ser muy efectiva para evaluar los controles. De requerirse, no se realiza la auditoría completa, sino solo en el eje temático afectado.
- Independientemente de haber sido probado en la entidad vinculada a la Alcaldía Mayor de Bogotá, el modelo propuesto no es exclusivo para esta entidad. Por el contrario, se puede utilizar para planificar, realizar y verificar auditorías cibernéticas en cualquier entidad del Gobierno o del sector privado.
- Valdría la pena validar la pertinencia de sistematizar el set de indicadores de cada eje temático, a fin de que la auditoría sea más dinámica.

CAPÍTULO V

ESTRATEGIA PARA LA ADOPCIÓN DE UNA CULTURA ORGANIZACIONAL DE CIBERSEGURIDAD EN LA ALCALDÍA DE NEIVA*

Yesica Tatiana Vanegas Silva

* Ponencia resultado del proyecto de investigación titulado *Gestión de riesgos en seguridad digital para la infraestructura crítica, de la Maestría en Ciberseguridad y Ciberdefensa*, de la línea de investigación *Seguridad Digital* del grupo de investigación *Masa crítica*, reconocido y categorizado en (B) por Minciencias, registrado con el código COL0123247, adscrito y financiado por la Escuela Superior de Guerra de la Republica de Colombia. Ponencia resultado de la investigación presentada como opción de grado para optar por el título de magíster en ciberseguridad y ciberdefensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto".

Resumen

Como consecuencia del aumento de los incidentes informáticos, la necesidad de proteger los activos de información y de cumplir con la legislación y la reglamentación nacional e internacional pertinentes, las organizaciones han tomado medidas técnicas y administrativas que permitan gestionar los riesgos cibernéticos. No obstante, diferentes estudios demuestran que no es suficiente establecer controles técnicos, pues quienes finalmente administran la información son personas. Por ello, el factor humano es fundamental en la ciberseguridad, pues es fuertemente influenciable por diferentes variables de su entorno, psicológicas, sociales y culturales, a escalas regional o nacional. Cualquier error humano, intencional o accidental, es una vulnerabilidad latente que puede ser explotada por diferentes amenazas. Por ello, este factor debe ser gestionado y cultivado dentro de la organización.

Para establecer una cultura organizacional no es suficiente un plan de concienciación y sensibilización. Así, este artículo contextualiza al lector en el concepto de *cultura organizacional*, desarrolla ocho factores que influyen en la construcción de una cultura organizacional de seguridad y propone una estrategia de cultura organizacional de ciberseguridad aplicable a la Alcaldía de Neiva. Para ello, toma como referencia investigación documental, trabajo de campo en la entidad, el esquema de cultura de seguridad de la empresa CLTRe AS de Oslo (Noruega), la investigación de cultura organizacional de la Agencia Europea de Seguridad de las Redes y de la Información y el kit de concienciación del Instituto Nacional de Ciberseguridad de España.

Palabras clave: cultura organizacional; ciberseguridad; apropiación; concienciación; cumplimiento; comportamiento.

Abstract

As a consequence of the increase in computer incidents, the need to protect information assets and to comply with relevant national and international legislation and regulations, organizations have taken technical and administrative measures that allow managing cyber risks. However, different studies show that it is not enough to establish technical controls, since those who ultimately manage the information are people. For this reason, the human factor is fundamental in cybersecurity, as it is strongly influenced by different variables of its environment, psychological, social and cultural, at regional or national scales. Any human error, intentional or accidental, is a latent vulnerability that can be exploited by different threats. Therefore, this factor must be managed and cultivated within the organization. To establish an organizational culture, an awareness and sensitization plan is not enough. Thus, this article contextualizes the reader in the concept of organizational culture, develops eight factors that influence the construction of an organizational culture of security and proposes a strategy of organizational culture of cybersecurity applicable to the Mayor's Office of Neiva. For this, it takes as a reference documentary research, field work in the entity, the security culture scheme of the CLTRe AS company in Oslo (Norway), the organizational culture research of the European Network Security Agency and the Information and awareness kit from the National Cybersecurity Institute of Spain.

Keywords: Organizational culture; cybersecurity; appropriation; awareness; fulfillment; behavior.

1. Introducción

La transformación digital ha implicado la evolución de las tecnologías tradicionales para dar paso a las disruptivas, es decir, aquellas que provocan un cambio en la forma de realizar y desarrollar ciertos procesos. Las más reconocidas son la impresión 3D, el *blockchain*, el internet de las cosas, la computación en la nube, la inteligencia artificial y el *big data*, pues han cambiado la forma de comunicamos, comprar, procesar y analizar la información. Sin embargo, esto ha traído consigo amenazas que atentan contra un nuevo activo organizacional: la información. Cuando su disponibilidad, confidencialidad e integridad quedan limitadas, dichas amenazas irrumpen las labores diarias, causan mala reputación y generan problemas económicos.

De acuerdo con un estudio sobre controles de seguridad mediante hackeo en empleados de Croacia, la seguridad de la información se basa en tres elementos básicos: personas (factor humano), procesos y tecnología (Lovrić Švehla et al., 2016, p. 1). Los riesgos de seguridad en el área técnica se pueden mitigar mediante controles definidos en *hardware* y *software*, gestión de riesgos, gestión de incidentes, políticas de seguridad, gestión de resiliencia y demás elementos descritos en la estrategia propuesta en cada organización. La pregunta es ¿cómo gestionar el factor humano haciendo que este sea consciente y cumpla con estas estrategias de seguridad establecidas por la entidad? El comportamiento humano no es consistente y puede estar fuertemente influenciado por las relaciones. Otra explicación es la creencia, general e ingenua, de que las cosas malas solo les suceden a otras personas (Johnston y Warkentin, 2010).

Según el estudio realizado en 2017 por Kaspersky Lab a más de 5000 empresas en todo el mundo, llamado "El factor humano en la seguridad de TI: cómo los empleados hacen que las empresas sean vulnerables desde dentro", el 52 % de las empresas admiten que los empleados son su mayor debilidad en seguridad de las tecnologías de la información (TI). El personal descuidado o desinformado, por ejemplo, es la segunda causa más probable de una infracción de seguridad grave, solo superada por el *malware*. Además, en el 46 % de los incidentes de seguridad cibernética en el último año, el personal descuidado o desinformado ha contribuido al ataque.

La principal conclusión de este estudio fue la siguiente:

> Las tendencias de movilidad significan que el personal descuidado o desinformado puede ser más propenso a cometer errores, y las amenazas como el *phishing* y la ingeniería social también ponen a las empresas en mayor riesgo por parte del personal que no sabe cómo diferenciar entre actividad legítima y maliciosa. (Kaspersky Lab, B2B International, 2017)

Para lograr que las personas de la Alcaldía de Neiva interioricen los conceptos, buenas prácticas, políticas, herramientas y demás avances establecidos en materia de seguridad y privacidad de la información, es necesario concientizarlas por medio de una cultura de ciberseguridad encaminada a los objetivos organizacionales y respaldada por la alta gerencia. Jo Malcolmson (2009) argumenta que la cultura de seguridad de la información está indicada por los supuestos, valores, actitudes, creencias y comportamientos de los empleados, pues estos pueden impactar la seguridad de la organización en la que trabajan.

El presente trabajo de investigación tiene como caso de estudio la Alcaldía Municipal de Neiva, encargada del tratamiento de datos personales y sensibles de la totalidad de la población del municipio, es decir, 345.806 habitantes, según las cifras del DANE. De ahí su importancia, además de salvaguardar la información, dar cumplimiento a lo establecido en la Ley 1581 de 2012, artículo 4.º denominado "Principios para el tratamiento de datos personales" y su principio de seguridad.

Así, se observan las motivaciones para abordar el concepto de *cultura organizacional de ciberseguridad*. Seguidamente, se abordan los ocho

factores clave que influyen y constituyen el éxito de una cultura de seguridad, como 1) el apoyo de la administración superior, 2) el establecimiento de una política eficaz, 3) la conciencia, 4) la capacitación y la educación, 5) el análisis y la evaluación de riesgos, 6) el cumplimiento, 7) las políticas de conducta ética y 8) la cultura organizacional.

En cuanto al caso de estudio de esta investigación, se analiza un contexto de la entidad en materia de procesos y normatividad aplicable a la misma; luego, se identifica su estado actual en lo referente a la ciberseguridad, seguridad de la información e informática, desde un enfoque documental y perceptivo, a través de encuestas realizadas a una muestra de la entidad. Este reconocimiento del contexto permitirá identificar riesgos de seguridad digital de cara al factor humano, los cuales son el insumo base para proponer la estrategia de cultura organizacional en esta entidad pública.

Por último, y teniendo en cuenta los conceptos identificados, se desarrolla la propuesta de una estrategia de cultura organizacional de ciberseguridad compuesta por cuatro etapas: 1) planeación, 2) métricas, 3) organización y 4) formación, teniendo como referencia el esquema de cultura de seguridad de la empresa CLTRe AS de Oslo, Noruega, la investigación de cultura organizacional de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) y el kit de concienciación del Instituto Nacional de Ciberseguridad de España (INCIBE).

2. La cultura organizacional de ciberseguridad como un componente fundamental de una estrategia de ciberseguridad

Luego de analizar las encuestas realizadas durante 2015 en el Reino Unido, el artículo “El comportamiento humano como un aspecto de la garantía de ciberseguridad” revela que el error humano inadvertido causó la mitad de las peores violaciones de seguridad, debido a que es muy difícil controlar el talento humano en las organizaciones, por el

constante cambio en su comportamiento. Prueba de esto es el estudio que realizó Cisco en 2015, a través del cual identificó cuatro perfiles de comportamiento de los usuarios que usan y administran la información en una organización.

1) El consciente es aquella persona consciente de los riesgos de seguridad y de las políticas establecidas en la organización. Cree en la responsabilidad compartida en la protección de los datos. 2) El bienintencionado conoce la política de seguridad, la cumple de manera aleatoria, pero no comprende completamente el impacto de sus acciones. 3) El complaciente no cumple con la política ni con los controles establecidos. Esta persona tiende a pensar que la seguridad es un obstáculo para sus labores diarias. Por último, 4) el aburrido y cínico es aquel que cree que el costo de la información está sobrevalorado; ha oído hablar de las políticas de seguridad en la organización, pero intenta evadirlas (Cisco, 2015).

Lo anterior demuestra que el factor humano es una vulnerabilidad latente en una organización, y no gestionarla facilita la materialización de riesgos que exponen los activos de información. Es fácil pensar que la concienciación y la sensibilización son la solución para mitigar este riesgo, pero diferentes investigaciones académicas demuestran que el hecho de conocer estos riesgos y su rol en la protección de los activos no significa que se cumpla con las políticas dispuestas. Por ello, es necesario abarcar toda una cultura organizacional de ciberseguridad que incluya otros componentes mencionados en el presente documento, de manera que permita generar un cambio en el comportamiento de las personas.

Las definiciones de *cultura organizacional* son diversas y dependen del contexto y del sector donde se desarrolle dicha cultura. En la tesis titulada *Auditoría del clima y cultura de seguridad en la empresa*, se reúnen las características sobresalientes de estas definiciones: "la cultura es un conjunto de valores aprendidos que pueden tomar fuerza en una organización mediante prácticas interpretadas a través de reglas y normas de conducta" (Hernández, 2007). ENISA (2017) define la *cultura organizacional de ciberseguridad* como "los conocimientos, creencias, percepciones, actitudes, supuestos, normas y valores de las personas con respecto

a la ciberseguridad y cómo se manifiestan en el comportamiento con las tecnologías de la información" (p. 7).

Teniendo en cuenta las definiciones anteriores, se puede observar cómo el comportamiento desempeña un papel vital para establecer una cultura organizacional, siendo conscientes de esto o no. Furnell y Thomson (2009) establecen que la cultura es un conjunto de percepciones y actuaciones, en ocasiones inconscientes, que determinan el comportamiento de las personas —como individuos y como integrantes de una comunidad—.

Schein, en su libro *La guía de supervivencia de la cultura corporativa* (citado en Furnell y Thomson, 2009), establece que para comprender la cultura organizacional es necesario conocer los tres niveles de la cultura corporativa: 1) los artefactos, 2) los valores propuestos y 3) los supuestos tácitos compartidos. Los artefactos son los comportamientos concretos de una persona; lo que ha visto, escuchado y sentido en una organización. Los valores propuestos son aquellas directrices establecidas y defendidas por la alta gerencia. Los supuestos tácitos compartidos son los comportamientos y los valores compartidos por los miembros de la entidad, apostando por su veracidad (Furnell y Thomson, 2009).

Para Van Niekerk y Von Solms (2009), estos tres niveles aplican para establecer una cultura organizacional, pero consideran necesario agregar un cuarto nivel llamado "conocimiento de seguridad de la información", para establecer una cultura organizacional de seguridad de la información. La razón es que no se puede asumir que las personas cuentan con la formación y la preparación necesaria para interiorizar la cultura, y es aquí donde la concienciación y la sensibilización desempeñan un papel importante.

2.1. Factores que constituyen e influyen en una cultura de seguridad de la información

En 2012, mediante su tesis doctoral titulada *Comprensión y medición de la cultura de seguridad de la información en países en desarrollo: caso de Arabia Saudita*, Mohammed A. Alnatheer realizó una investigación a

partir de una muestra de veinte altos directivos de compañías que administraran infraestructura de seguridad de la información y usaran prácticas de gestión de seguridad de la información con frecuencia.

En este estudio, el autor identificó tres factores que constituyen una cultura de seguridad de la información: el primer factor es la *apropiación*, que permite a los integrantes de la organización entender sus roles y sus responsabilidades frente a la seguridad, así como los riesgos asociados a sus acciones. Así, busca aumentar los niveles de conciencia de seguridad de las personas y el cumplimiento de la política de seguridad de la organización. El segundo factor es la *concienciación*, que es el grado en que los miembros de la organización comprenden la importancia de la seguridad de la información, el nivel de seguridad requerido por la organización y sus responsabilidades de seguridad individuales para actuar en consecuencia. El tercer factor es el *cumplimiento*, que se refiere al seguimiento de las políticas, prácticas y procedimientos de seguridad establecidos en la organización.

Según la Academia Real de la Lengua Española, *constituir* es "Formar, componer, ser" e *influir* es "Dicho de una cosa: producir sobre otra ciertos efectos". Por ser conceptos diferentes, Alnatheer, en 2015, identificó ocho factores de éxito que influyen en la construcción de una cultura organizacional de seguridad:

1. *El apoyo de la administración superior:* teniendo en cuenta que el cambio en el comportamiento del factor humano en la organización se logra con el respaldo de la alta dirección —la cual debe incluir dentro de su objetivo de negocio la protección de los activos de información y tecnológicos, ratificar su importancia asignando presupuesto para tal fin, siguiendo a Fourie (2003, citado en Alnatheer et al., 2012)—, esta debe establecer roles y responsabilidades y contar con el recurso necesario para establecer el monitoreo continúo del cumplimiento de las directrices propuestas.
2. *La creación* —por parte de la alta gerencia— *de una política eficaz de Seguridad de la información y ciberseguridad*, que establezca las estrategias, los responsables y los derroteros

que deben cumplir los empleados para alcanzar el objetivo propuesto.

3. *La conciencia*, factor que constituye e influye en la construcción de una cultura de seguridad. Sin este grado de interiorización y cumplimiento de las políticas establecidas en la organización, no sería posible establecer una cultura. La norma ISO/IEC TR 13335-1 (citada en Alnatheer, 2015) establece que la conciencia de seguridad de todos los empleados es un elemento esencial de la seguridad efectiva y contribuye positivamente a una cultura de seguridad mejorada. Para abordarla, es necesario establecer un plan de concienciación, que se articula perfectamente con el siguiente factor.
4. *Capacitación y educación*, sin este factor, es muy difícil ser consciente de los riesgos en el ciberespacio. Por tal razón, una estrategia de ciberseguridad en la empresa debe incluir un plan de "sensibilización, capacitación y educación", reconociendo que el ser humano, debido a que este es fuertemente influenciable, es el eslabón más débil de la cadena de seguridad.

   Howell (1982, citado en Thomson et al., 2006), consciente de que el conocimiento impartido a las personas mediante la sensibilización, la capacitación y la educación no garantiza el cumplimiento de las políticas y de los controles establecidos, y de que es necesario que las personas interioricen estos conocimientos para poder aplicarlos en su día a día de una manera inconsciente, desarrolló el modelo de aprendizaje de competencia consciente, dividido en cuatro etapas.

   En la primera etapa, *incompetencia inconsciente*, el empleado no cuenta con el conocimiento necesario para realizar una actividad específica ni conoce la importancia de esta. En la segunda, *incompetencia consciente*, el empleado es consciente de la importancia de su rol en la organización y puede discernir si su comportamiento es correcto o incorrecto, de acuerdo con las directrices establecidas; sin embargo, aún no cuenta con el conocimiento necesario para cumplir las funciones en su rol.

En la tercera, *competencia consciente*, ha recibido capacitación y cuenta con el conocimiento necesario, pero debe pensar en la forma y los pasos para poder realizar la acción. En la cuarta, *competencia inconsciente*, el empleado alcanza la habilidad de realizar las actividades a su cargo sin pensar en la manera de ejecutarlo. Según este modelo, se debe avanzar por cada una de las etapas mediante capacitación, cumplimiento y práctica, para lograr así un nivel óptimo de concienciación e interiorización de las políticas, valores o directrices dispuestas por la dirección.

5. *Análisis y evaluación de riesgos*: el riesgo es la posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o un daño en un activo de información (Organización Internacional de Normalización, 2005).
   La gestión de riesgos es un factor que influye en la construcción de ciberseguridad, debido a que la evaluación de este brinda conciencia sobre el valor de los activos, sus pérdidas y sus daños. Asimismo, identifica que la falta de una cultura consciente de seguridad se debe a la carencia de conocimiento sobre seguridad y el incumplimiento de las políticas y buenas prácticas establecidas por la alta dirección (Alnatheer, 2015).
   Según la *Cartilla de administración de riesgos* del Departamento Administrativo de la Función Pública de Colombia (DAFP), el proceso para la administración del riesgo inicia con su identificación, análisis (determinación de su probabilidad, consecuencias y nivel) y valoración (controles, efectividad de controles y tratamiento), todo dentro de un monitoreo y una revisión continúa (Ministerio de Tecnologías de la Información y Comunicaciones, 2016).
6. *El cumplimiento*: no es suficiente establecer políticas, directrices y concienciación en la organización si las personas no cumplen con lo dispuesto. Así, Furnell y Thomson (2009) establecieron los *Niveles de cumplimiento de seguridad basados en comportamientos individuales*, en los que describen el nivel

de cumplimiento e incumplimiento de la seguridad, basados en los comportamientos de los empleados. En la tabla 5.1 se identifica una línea delgada entre el nivel de cumplimiento consciente y el incumplimiento ignorante, debido a que establecer una conciencia a través de un plan de concienciación o cualquier otro mecanismo no es suficiente para alcanzar una cultura. Para esto son necesarios, según ese estudio, la obediencia y el compromiso.

Tabla 5.1. Niveles de cumplimiento de seguridad basados en comportamientos individuales

Cumplimiento	Cultura	El estado ideal en el que la seguridad es parte implícita del comportamiento natural del usuario.
	Compromiso	La seguridad no es una parte natural del comportamiento, pero sí se proporciona una guía adecuada. Los usuarios aceptan la necesidad y realizan un esfuerzo asociado.
	Obediencia	Los usuarios no pueden aceptar los principios, pero se les puede hacer cumplir a través de la autoridad apropiada.
	Conciencia	Los usuarios son conscientes de su papel en la seguridad de la información, pero todavía no están cumpliendo completamente con las prácticas o los comportamientos asociados.
Incumplimiento	Ignorancia	Los usuarios no son conscientes de los problemas de seguridad y, por lo tanto, pueden presentar efectos adversos involuntarios.
	Apatía	Los usuarios son conscientes de su papel en la protección de los activos de información, pero no están motivados para adherirse a las buenas prácticas de seguridad de la información.

Resistencia	Los usuarios trabajan pasivamente contra la seguridad, oponiéndose a aquellas prácticas con las que no están de acuerdo.
Desobediencia	Los usuarios trabajan activamente contra la seguridad, con abusadores internos que infringen intencionalmente las reglas y eluden controles.

Fuente: Furnell y Thomson (2009).

7. *Políticas de conducta ética y cultura organizacional*: Hellriegel et al. (citados en Veiga, 2008) definen la *ética* como los valores y las reglas que distinguen el bien del mal. El comportamiento ético difiere dependiendo del contexto en que se encuentren las personas, pues una acción que se considere ética dentro de un territorio u organización no lo es en un contexto diferente. Por esto, la alta gerencia debe establecer parámetros aceptables de comportamiento entre los empleados, alineados con los objetivos estratégicos, con el fin de minimizar el riesgo de acciones que reduzcan la seguridad en la organización.

La conducta ética y la cultura organizacional van de la mano, teniendo en cuenta que se articulan para lograr un cambio en el comportamiento de las personas. La ética, dictamina las reglas y los valores, en cuanto a la cultura, se centra en el cumplimiento y adopción de estas reglas en una comunidad en el ámbito organizacional. En el artículo "Una aproximación al concepto de cultura organizacional", Álvarez (2005) establece que la *cultura organizacional* son las conductas de las personas dentro de un contexto, y que para lograr el éxito en la organización es necesario crear estrategias gerenciales que permitan que las personas interioricen los valores y las políticas establecidas para contribuir así al compromiso e identidad en los empleados (Álvarez, 2005).

2.2. El factor humano como amenaza interna para la ciberseguridad en una organización

Según el Informe de investigaciones de violación de datos de Verizon del 2019, el *phishing*, el *misdelivery* y *pretexting* se encuentran en el *ranking* de las principales amenazas, fuertemente relacionadas con el factor humano (Verizon, 2019). Diferentes autores de todo el mundo han concluido en sus investigaciones que un porcentaje muy alto de incidentes de seguridad son causados por errores humanos. Un ejemplo es un estudio de 2019 que analizó 7202 incidentes publicados por la Oficina del Comisionado de Información del Reino Unido. Según esta investigación, el 64.44 % de los incidentes tienen la "probabilidad"; el 35.14 %, la "posibilidad", y el 0.41 %, la "improbabilidad" de ocurrir por errores humanos (Evans et al., 2019). Asimismo, el 50 % de las organizaciones encuestadas en el estudio sobre incumplimientos de seguridad de la información, realizado en 2015 en el Reino Unido, respondió que el peor incidente sufrido fue por un error humano inadvertido (HM Government, 2015).

Las empresas líderes en ciberseguridad día a día desarrollan productos y servicios para salvaguardar los activos de *hardware*, *software* y redes de las constantes amenazas cibernéticas. Sin embargo, las amenazas internas (maliciosas o accidentales) cada año logran posicionarse en el top de las principales amenazas del mundo, según el *Informe del panorama de amenazas 2018* de Agencia Europea de Seguridad de las Redes y de la Información (2019). En 2017 y en 2018, se encuentran en el número 9 dentro del *ranking* (tabla 5.2).

Uchenna et al. (2015) afirman que para obtener eficiencia en la ciberseguridad no basta con disponer de "antivirus, *firewalls* y sistemas de detección/prevención de intrusos (ID/PS)" o de "procedimientos de seguridad estrictos" ni de "expertos en seguridad de TI altamente calificados", si el factor humano no se apropia de la seguridad establecida en la organización (p. 170). Por esta razón, describen que para contar con éxito en la protección de los activos, la ciberseguridad debe estar compuesta por la tríada "personas, procesos y tecnología" (figura 5.1).

Así, los autores definen a la ciberseguridad como "la armonización de capacidades en personas, procesos y tecnologías para asegurar y controlar tanto el acceso autorizado o ilegal como la interrupción o destrucción de los sistemas informáticos electrónicos (*hardware*, *software* y redes), los datos y la información que poseen".

Tabla 5.2. Descripción general y comparación de los panoramas de amenazas (2017-2018)

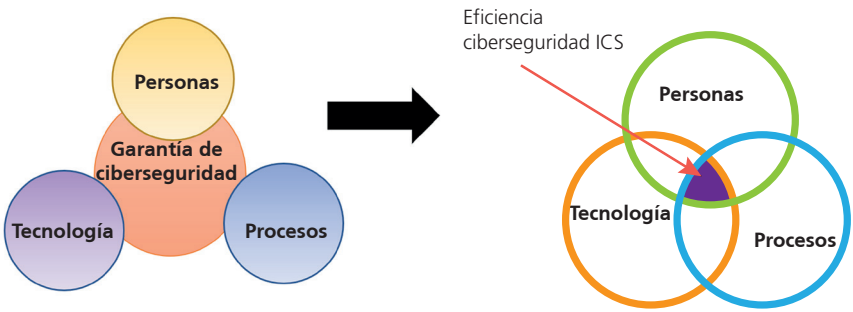
Top de amenazas en 2017	Top de amenazas en 2018	Cambio en el *ranking*
1. *Malware*	1. *Malware*	→
2. Ataques basados en la web	2. Ataques basados en la web	→
3. Ataques a aplicaciones web	3. Ataques a aplicaciones web	→
4. *Phishing*	4. *Phishing*	→
5. *Spam*	5. Denegación de servicios	↑
6. Denegación de servicios	6. *Spam*	↓
7. *Ransomware*	7. *Botnets*	↑
8. *Botnets*	8. Violaciones de datos	↑
9. Amenazas internas	9. Amenazas internas	→
10. Manipulación física, daño, robo o pérdida	10. Manipulación física, daño, robo o pérdida	→
11. Violaciones de datos	11. Fuga de información	↑

Top de amenazas en 2017	Top de amenazas en 2018	Cambio en el *ranking*
12. Robo de identidad	12. Robo de identidad	→
13. Fuga de información	13. *Cryptojacking*	NUEVA
14. Kits de explotación	14. *Ransomware*	↓
15. Espionaje cibernético	15. Espionaje cibernético	→

↑ Subiendo → Igual ↓ Bajando

Fuente: Elaboración propia con base en la información de la ENISA (2019).

Figura 5.1. Entidades colaborativas para una seguridad cibernética efectiva



Fuente: Adaptación propia con base en Uchenna et al. (2015, p. 170).

Las personas son trascendentales en la implementación de toda estrategia, pues son estas las que finalmente administran y desarrollan los procesos y los procedimientos de las organizaciones, y quienes permiten cumplir los objetivos estratégicos diseñados por la alta gerencia.

Es tan importante el factor humano, que el Gobierno de Colombia desarrolló el Modelo Integrado de Planeación y Gestión (MIPG), que en su dimensión n.º 1 desarrolla la Política de Gestión Estratégica de Talento Humano, en la que el factor humano aparece definido como "el

activo más importante con el que cuentan las entidades y […] el gran factor crítico de éxito que les facilita la gestión y el logro de los objetivos y los resultados" (Departamento Administrativo de la Función Pública, 2018, p. 4).

No obstante, si no se gestiona ni evalúa el comportamiento de las personas, estas pueden convertirse en una amenaza interna para la ciberseguridad en la organización. Para el Instituto de Ingeniería de Software de la Universidad Carnegie Mellon (2015), una *amenaza interna maliciosa* para una organización es

> … un empleado, contratista u otro socio comercial actual o anterior que tiene o ha tenido acceso autorizado a la red, al sistema o a los datos de una organización, e intencionalmente excedió o usó mal ese acceso de una manera que afectó negativamente la confidencialidad, integridad o disponibilidad de la información o los sistemas de información de la organización. Además, las amenazas internas también pueden ser involuntarias (no maliciosas). (p. 2)

Debido al cumplimiento de sus funciones y obligaciones laborales, las personas cuentan con perfiles de autoridad y confianza cuyo alcance se incrementa a medida que lo hacen la responsabilidad y el mando. Una persona que desee realizar alguna actividad maliciosa en la organización cuenta con mayores posibilidades de obtener su cometido, pues posee acceso sin restricción y privilegios al *hardware*, *software*, redes, información y demás activos de la organización. Además, debido a su experticia en el manejo de las herramientas y los procesos a su cargo, conoce el cómo, el cuándo y el dónde atacar. Por su parte, las amenazas externas deben realizar todo un procedimiento de reconocimiento de la víctima para lograr su meta.

Teniendo en cuenta las cifras anteriores e investigaciones realizadas, es necesario gestionar al factor humano en una organización, pues este es quien "diseña, implementa, opera, usa y abusa de los sistemas de información" abriendo paso a errores voluntarios e involuntarios, no obstante, este además es quien puede evitar que estos riesgos se materialicen (Lacey, 2009, pág. 1). Sin embargo, se debe tener en cuenta que no solo el mal comportamiento es un factor asociado al incremento de

incidentes informáticos, factores como el estrés, falta de conocimiento, falta de supervisión, fallos en las herramientas tecnológicas o procesos, es decir errores involuntarios causan estos incidentes, por esta razón se debe identificar el origen de estos errores para tomar las medidas pertinentes (Lacey, 2009).

3. Alcaldía de Neiva: contexto de la entidad

Como lo afirmó la Oficina de Tecnologías de la Alcaldía de Neiva en el PETI, Resolución 279 de 2017 (Alcaldía de Neiva, 2017), esta es una entidad pública cuyo principal objetivo es usar de manera adecuada los recursos económicos asignados al municipio desde las diferentes dependencias, en busca del bienestar físico, económico, social y cultural de todos sus habitantes para que gocen de una mejor calidad de vida. Así, la Alcaldía de Neiva realiza el tratamiento de la información personal, financiera, educativa y social de los 347.501 habitantes de la ciudad, según proyección censal del Departamento Administrativo Nacional de Estadística (DANE).

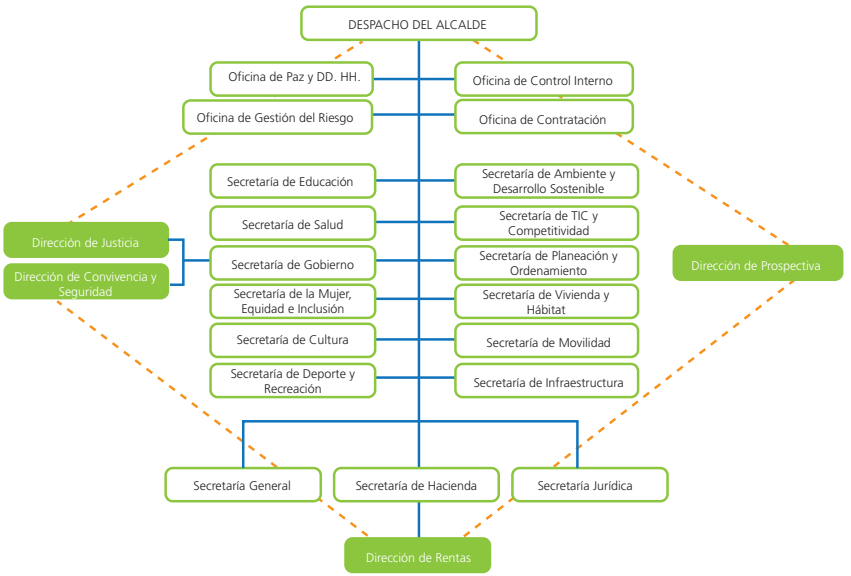
La figura 5.2 presenta la estructura administrativa de la Alcaldía de Neiva, según el Decreto Municipal 590 de 2016.

La entidad cuenta con veinte procesos, divididos en cuatro líneas principales: 1) estratégicos, 2) misionales, 3) apoyo y de evaluación y 4) control. Estos procesos son la columna vertebral de la administración, cumpliendo así con su misión, visión y objetivos estratégicos (figura 5.3).

Un aspecto importante por resaltar es que en este mismo Decreto Municipal 590 de 2016, por el cual se estableció la estructura de la alcaldía del municipio de Neiva y se creó la Secretaría TIC y Competitividad, se definió para esta Secretaría la función n.º 15, cuyo objetivo es

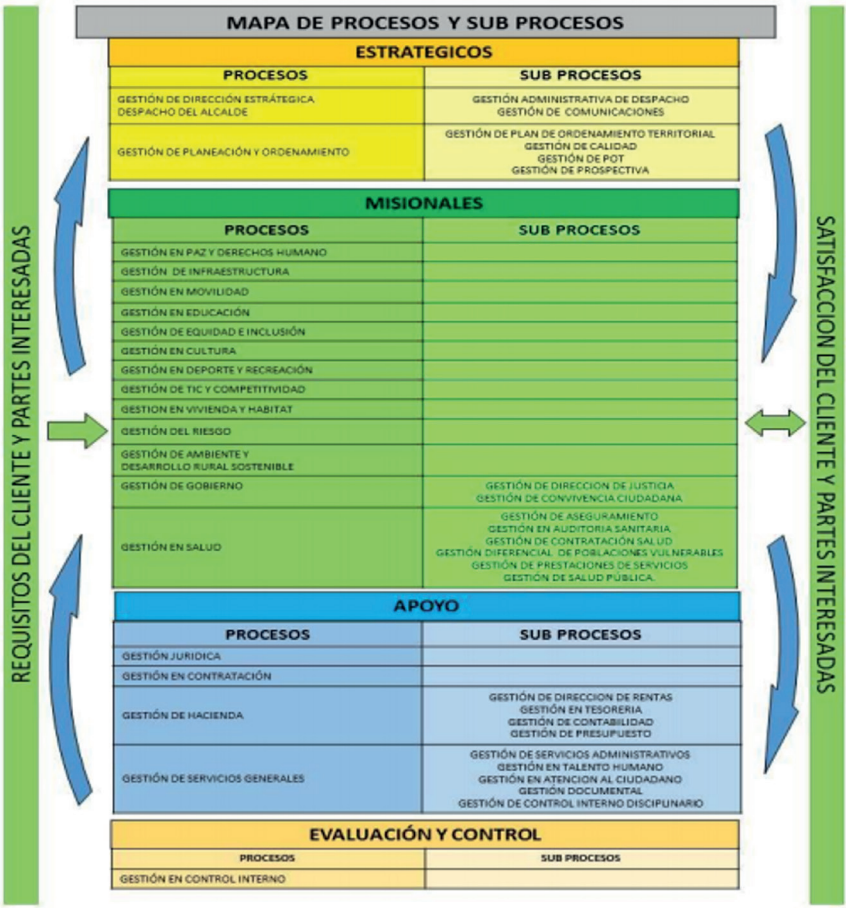
> Definir y desarrollar estrategias de gestión de información de la entidad territorial para garantizar la seguridad informática, ciberseguridad y ciberdefensa con el fin de lograr un flujo eficiente y disponible para el uso de ella en la gestión y toma de decisiones. (Alcaldía de Neiva, 2016)

Figura 5.2. Organigrama de la Alcaldía de Neiva



Fuente: Alcaldía de Neiva (2016).

Figura 5.3. Procesos y subprocesos de la Alcaldía de Neiva



Fuente: Resolución 279 de 2017.

3.1. Ciberseguridad en la entidad

Con el objetivo de utilizar la tecnología como articulador transversal en la prestación de servicios a los ciudadanos del municipio, la Alcaldía de Neiva, desde 2015, ha avanzado, según los plazos establecidos, con la implementación del Decreto 1078 de 2015: "Estrategia de Gobierno en línea" en las entidades públicas a escala nacional. Esta estrategia desarrolló cuatro componentes: 1) TIC para servicios, 2) TIC para Gobierno

abierto, 3) Tic para la gestión y la seguridad, y 4) privacidad de la información.

En el mismo decreto, se establecen los plazos para el cumplimiento de estos cuatro componentes. Así, se define que para los municipios de categoría 3 —es decir, el municipio de Neiva—, para 2019, se debe cumplir con el 100 % del componente TIC para servicios; mantener el 100 % para Gobierno abierto; el 80 %, para la gestión, y el otro 80 % para seguridad y privacidad de la información. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2015)

La implementación de la Estrategia Gobierno en Línea permitió a la Alcaldía de Neiva posicionar la tecnología como un dinamizador y articulador de procesos y procedimientos, de cara a brindar un servicio óptimo a los ciudadanos. Por esto, para abordar el componente de Seguridad y Privacidad de la Información de esta estrategia nacional, así como para garantizar la confidencialidad, integridad y disponibilidad de la información en las entidades, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) diseñó el Modelo de Seguridad y Privacidad de la Información (MSPI).

Este modelo tomó como base la norma ISO/IEC de 2013, el esquema de ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST), los fundamentos de la arquitectura empresarial, algunas mejoras prácticas de ITIL y la Ley 1581 de 2012 de privacidad de la información y tratamiento de datos personales. Cuenta con un instrumento de diagnóstico basado en los dominios establecidos en la norma ISO 27002, con un avance en el ciclo PHVA y con un nivel de madurez y una calificación en mejores prácticas en ciberseguridad, de acuerdo con el esquema NIST. Adicionalmente, para su implementación, cuenta con 21 guías (cuadro 5.1).

Cuadro 5.1. Guías del Modelo de Seguridad y Privacidad de la Información

Guía 1	Metodología de pruebas de efectividad
Guía 2	Política General MSPI v1
Guía 3	Procedimiento de seguridad de la información
Guía 4	Roles y responsabilidades
Guía 5	Gestión de la clasificación de los activos
Guía 6	Gestión documental
Guía 7	Gestión de riesgos
Guía 8	Controles de seguridad de la información
Guía 9	Indicadores de gestión de seguridad de la información
Guía 10	Continuidad del negocio
Guía 11	Análisis de impacto del negocio
Guía 12	Seguridad en la nube
Guía 13	Evidencia digital
Guía 14	Plan de comunicación, sensibilización y capacitación
Guía 15	Auditoría
Guía 16	Evaluación de desempeño
Guía 17	Mejora continua
Guía 18	Lineamientos terminales de las áreas financieras de las entidades públicas
Guía 19	Aseguramiento del Protocolo IPv4_IPv6
Guía 20	Transición IPv4_IPv6
Guía 21	Gestión de incidentes

Fuente: Biblioteca de seguridad dispuesta por el MINTIC (2016).

Según el autodiagnóstico concertado en el MSPI, la Alcaldía de Neiva, en la evaluación de efectividad de controles, dispuestos en el Anexo A de la norma ISO 27001:2013, cuenta con un promedio de 18 sobre 100 puntos. Esta calificación la ubica en el nivel 1 o inicial, según la brecha entre el estado actual de la entidad y el nivel optimizado. La tabla 5.3 y la figura 5.4 presentan los dominios evaluados.

Tabla 5.3. Evaluación de efectividad de controles

Dominio	Calificación actual	Calificación objetivo	Evaluación de la efectividad del control
Políticas de seguridad de la información	60	100	Efectivo
Organización de la seguridad de la información	18	100	Inicial
Seguridad de los recursos humanos	31	100	Repetible
Gestión de activos	37	100	Repetible
Control de acceso	6	100	Inicial
Criptografía	0	100	Inexistente
Seguridad física y del entorno	13	100	Inicial
Seguridad de las operaciones	16	100	Inicial
Seguridad de las comunicaciones	16	100	Inicial
Adquisición, desarrollo y mantenimiento de sistemas	3	100	Inicial

Dominio	Calificación actual	Calificación objetivo	Evaluación de la efectividad del control
Relaciones con los proveedores	0	100	Inexistente
Gestión de incidentes de seguridad de la información	9	100	Inicial
Aspectos de seguridad de la información de la gestión de la continuidad del negocio	7	100	Inicial
Cumplimiento	33,5	100	Repetible
Promedio de la evaluación de controles	**18**	**100**	**Inicial**

Fuente: Alcaldía de Neiva, Comité Institucional de Gestión y Desempeño (2018).

Figura 5.4. Diagnóstico de seguridad y privacidad de la información de acuerdo con el Anexo A ISO 27001:2013

Fuente: Alcaldía de Neiva, Comité Institucional de Gestión y Desempeño (2018).

En cuanto al avance del ciclo de funcionamiento del modelo de operación (PHVA), en el componente de *planificación* se cuenta con un porcentaje de avance actual de la entidad del 12 % sobre un total deseado del 40 %; en el componente de *implementación*, del 1 % sobre el 20 %; en el componente de *evaluación de desempeño*, del 5 % sobre el 20 %, y en el componente de *mejora continua*, del 8 % sobre el 20 %. Estas cifras promedian el 26 % del avance actual de la entidad sobre el 100 % esperado (tabla 5.4).

Tabla 5.4. Avance en el ciclo de funcionamiento del modelo de operación

Componente	Avance actual (%)	Avance esperado (%)
Planificación	12	40
Implementación	1	20
Evaluación de desempeño	5	20
Mejora continua	8	20
Total	**26**	**100**

Fuente: Alcaldía de Neiva, Comité Institucional de Gestión y Desempeño (2018).

Luego de la puesta en vigencia del Decreto 1499 de 2017, el cual desarrolla la estructura del Modelo Integrado de Planeación y Gestión (MIPG), se establece una articulación y complementariedad con otros sistemas de gestión, como el Sistema Nacional de Servicio al Ciudadano, Gestión de la Seguridad y la Salud en el Trabajo, Gestión Ambiental y Seguridad de la Información. Asimismo, con 16 políticas de gestión y desempeño institucional (Departamento Administrativo de la Función Pública, 2017), entre las cuales figura la de Seguridad Digital y Gobierno Digital (antes, Gobierno en Línea).

Entre otras disposiciones, el Decreto 1499 de 2017 establece que la medición de la gestión y el desempeño institucional se debe realizar a

través del Formulario Único de Reporte y Avance de Gestión (FURAG). Este formulario se encuentra a disposición de las entidades obligadas a aplicar el MIPG. En la figura 5.5 se puede observar que, según lo reportado por la entidad, esta se encuentra en el rango *medio alto* en el avance de la implementación de la política de Gobierno Digital.

Figura 5.5. Avance en la implementación de la política de Gobierno Digital

Nivel de avance en la implementación de la Política de Gobierno Digital		Escala de 0 - 100
	Bajo	Menor a 20
	Medio bajo	Igual o mayor a 20 y menor a 40
	Medio	Igual o mayor a 40 y menor a 60
	Medio alto	Igual o mayor a 60 y menor a 80
	Alto	Igual o mayor a 80 y menor o igual a 100

Fuente: Alcaldía de Neiva (2019).

Teniendo en cuenta que la política de Gobierno Digital desarrolla tres habilitadores transversales (seguridad de la información, arquitectura empresarial y servicios ciudadanos digitales) (tabla 5.5), la herramienta evalúa el habilitador de seguridad de la información, que, según lo reportado por la entidad, se encuentra en un nivel *alto*. A continuación, se presenta el porcentaje de cumplimiento de los indicadores que pertenecen al habilitador de seguridad de la información establecido en el FURAG.

Tabla 5.5. Indicadores de cumplimiento para el habilitador en la seguridad de la información

Fase	Indicadores de cumplimiento	Porcentaje de cumplimiento (%)
Evaluación y planificación de la seguridad de la información	Diagnóstico de seguridad y privacidad de la información	100
	Política del MSPI	100
	Roles y responsabilidades del MSPI	100

Fase	Indicadores de cumplimiento	Porcentaje de cumplimiento (%)
	Procedimientos del MSPI	100
	Gestión de activos de seguridad de la información	100
	Gestión de riesgos de seguridad y privacidad de la información	100
	Plan de comunicación, sensibilización y capacitación en seguridad de la información	100
Implementación de seguridad de la Información	Implementación del plan de tratamiento de riesgos de seguridad de la información	100
	Plan de control operacional	100
	Indicadores de gestión de seguridad de la información	100
Seguimiento, evaluación y mejora de seguridad de la información	Seguimiento y evaluación del desempeño de la seguridad de la información	50
	Plan de mejoramiento continuo de seguridad de la información	0

Nota: Modelo de seguridad y privacidad de la información (MSPI).
Fuente: Elaboración propia con base en Alcaldía de Neiva (2019).

En cuanto a la sensibilización y concienciación en seguridad de la información y la ciberseguridad establecida en la entidad, la oficina de Tecnologías de la Información y las Comunicaciones estableció el documento titulado *Plan de sensibilización de seguridad y privacidad de la información, Alcaldía de Neiva*. El alcance de este es "maximizar la interiorización de los conceptos y su aplicación en la cotidianidad institucional y personal". Este documento cuenta con una serie de preguntas que, según el autor, permiten analizar la visión personal de cada encuestado

sobre el conocimiento y el compromiso en temas de seguridad y privacidad de la información, la definición del grupo profesional necesario para la implementación del plan y el despliegue de los elementos de sensibilización, como carteles, correos electrónicos y otros (Alcaldía de Neiva, 2018).

Según el enfoque metodológico de la presente investigación, para desarrollar la estrategia propuesta se realizó, en enero de 2020, una encuesta compuesta por trece preguntas, a través de la herramienta Formularios de Google. Fue aplicada a catorce dependencias de la entidad, con dos a tres funcionarios de cada dependencia seleccionada (una muestra de veintinueve personas que laboran de la Alcaldía de Neiva).

Los participantes de este estudio fueron auxiliares administrativos, abogados, ingenieros de sistemas, administradores y economistas. La encuesta se llevó a cabo con el fin de identificar la conciencia y la apropiación de la ciberseguridad y la seguridad de la información en la entidad, a través de preguntas centradas en el conocimiento de la política de seguridad y privacidad de la información y el plan de sensibilización y concientización propuesto por la oficina de tecnología de la entidad pública.

La Política de Seguridad y Privacidad de la Información es la directriz superior en cuanto a esa materia en la entidad, pues establece el compromiso para la protección de los activos de la organización. Sin embargo, el 58,6 % de las personas encuestadas manifiestan no conocer esta política, y el 34,5 % indica solo haberla leído. Así las cosas, es poco posible que dicha política se cumpla y se mitiguen los riesgos de seguridad en la entidad.

Por su parte, el 58,6 % de los encuestados indica no conocer la política de copias de seguridad; el 41,4 % indica que nunca realiza copias de seguridad, y el 31 % indica que las realiza una vez al mes. Esta mala práctica es un riesgo para los activos de información, pues al estar expuestos a su pérdida, imposibilitan la continuidad efectiva de la prestación de los servicios a los ciudadanos.

Por otro lado, el 41,4 % de las personas actualiza el sistema operativo de sus equipos de cómputo al menos una vez al mes, y el 39,9 % nunca lo hace. Asimismo, el 51,7 % de las personas señala contar

con *software* antivirus, pero no realiza actualizaciones periódicas. Esto demuestra niveles de conciencia reducidos en cuanto a la gestión de la actualización de los sistemas operativos y sus antivirus, por lo que los equipos de cómputo quedan vulnerables a posibles ataques cibernéticos.

Del total de los participantes, el 65,5 % indica que no conoce el plan de sensibilización y concienciación adoptado por la entidad, y el 34,5 % señala que solo lo ha leído. Estos datos demuestran que si bien la oficina de tecnologías ha generado y publicado en la página web institucional este documento, los funcionarios no lo han socializado. Este alto nivel de desconocimiento se debe al incumplimiento de las actividades propuestas en el plan, pues, según el documento, estas debieron llevarse a cabo durante cuatro meses, entre febrero y junio de 2019 (Alcaldía de Neiva, 2018).

A la pregunta ¿con qué frecuencia ha recibido capacitación, por parte de la entidad, en temáticas como seguridad de la información, informática o ciberseguridad?, el 89,7 % de las personas respondió que nunca ha recibido capacitación, y el 10,3 %, que al menos una vez al mes la ha recibido.

Es importante mencionar que en el plan de capacitación con vigencia de 2020 se identifica una formación llamada "Seguridad en el acceso de la información", aunque se encuentra pendiente por definir el tipo de capacitación, la fecha y la entidad que realizará la misma (Alcaldía de Neiva, 2020, p. 25).

Esta falta de concientización y capacitación por parte de la entidad se ve reflejada en el desconocimiento de los protocolos por seguir al ocurrir un incidente de seguridad de la información, pues el 72,4 % de las personas indica que no los conocen. Asimismo, el 75,9 % de los encuestados dice no conocer el significado de ataques informáticos tan comunes como *malware*, *phishing* y robo de información.

Es importante mencionar que en la evaluación de indicadores de cumplimiento del habilitador de seguridad de la información, según lo reportado por la entidad en el FURAG, la Política del MSPI y el Plan de comunicación, sensibilización y capacitación en seguridad de la información tienen el 100 % de cumplimiento (tabla 5.5). Sin embargo,

la mayoría de las personas encuestadas indica no tener conocimiento de estas temáticas, lo cual expone la necesidad de no solo aprobar y publicar en la página web institucional estos documentos, sino además de socializarlos con los funcionarios y velar por el cumplimiento de estos.

3.2. El factor humano como amenaza interna en la identificación de riesgos de ciberseguridad en la Alcaldía de Neiva

Dando cumplimiento al objetivo E1.2 del documento CONPES 3854 del 2016, que indica que se debe "Implementar en el Gobierno nacional un modelo de gestión de riesgos de seguridad digital" (Departamento Nacional de Planeación , 2016, p. 48), MINTIC elaboró el Modelo Nacional de Gestión de Riesgos de Seguridad Digital (MGRSD). Este modelo tomó como referencia las buenas prácticas nacionales e internacionales de gestión del riesgo, con el fin de realizar guías para identificar, analizar, evaluar y tratar los riesgos de seguridad digital en sectores estratégicos como el sector público y de Gobierno, el sector mixto y privado, el sector de la fuerza pública y la ciudadanía (MinTIC, 2018).

Con base en lo anterior, y teniendo en cuenta que la Alcaldía de Neiva es una entidad pública de orden territorial, para identificar los riesgos de ciberseguridad de cara al factor humano, la presente investigación ha consultado la *Guía de orientación de aplicación de la gestión de riesgos de seguridad digital en el sector público, territoriales y Gobierno nacional*.

Para identificar los riesgos, se toma como insumo la información recopilada en la etapa de conocimiento del estado actual de la entidad, a través de información documental y encuestas realizadas a los funcionarios en materia de seguridad de la información y ciberseguridad, para posteriormente convertirla en una matriz de riesgos que sirva como base para construir la Estrategia de Cultura Organizacional por proponer.

Se identifican once riesgos en los cuales el factor humano actúe como amenaza y vulnerabilidad para la materialización de aquellos. Luego, se identifican las consecuencias, el tipo de activo, el responsable y el tipo y clasificación del riesgo. Tres de estos riesgos se encuentran catalogados

en la zona de riesgo *alta* —denegación del servicio, fuga de información y descarga, instalación o uso de *software* no autorizado—, y ocho, en la zona de riesgo *moderada* —alteración de la información sin autorización, fraude y robo de información, daño o mal funcionamiento, acceso no autorizado a los activos de información, uso indebido o inadecuado de los sistemas de información e información, fuga de conocimiento a través de talento humano, alto nivel de dependencia de proveedores externos a la entidad, incumplimientos legales (anexo 5.1).

4. Estrategia de cultura de ciberseguridad propuesta

La estrategia de cultura organizacional de ciberseguridad propuesta nace para atender la necesidad latente en Colombia —específicamente en la Alcaldía de Neiva— de minimizar los riesgos de ciberseguridad provocados intencional o accidentalmente por el factor humano en las organizaciones. Toma como marco de referencia la investigación documental presentada en este artículo, enfocada en la identificación de los factores que constituyen —e influyen en— una cultura organizacional de seguridad, así como en la identificación y el conocimiento del estado actual en materia de seguridad cibernética —en términos de documentación y conciencia de los funcionarios— y en el esquema de cultura de seguridad desarrollado por la empresa CLTRe AS de Oslo, Noruega, bajo una licencia "Creative Commons Share Alike" —que indica que es libre de uso y modificación, con la condición de citar la fuente y compartir los aportes realizados a la comunidad creada por esta empresa.

Luego de una revisión de literatura, se identifica que este esquema reúne componentes importantes, como el establecimiento de metas, la medición de estas y elementos organizacionales y formativos para la construcción de una cultura organizacional de ciberseguridad

Este esquema tiene cuatro etapas: en la primera, *medición*, se identifica el estado actual por medio de un autodiagnóstico denominado As-is. También se deben definir las metas deseadas To-Be. En la segunda,

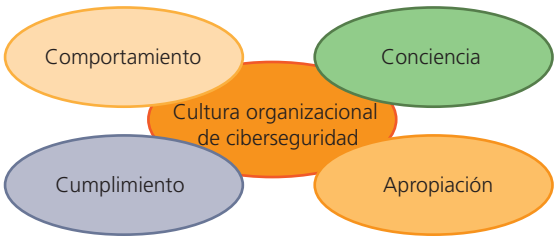
organización, se identifican los roles y las responsabilidades de los actores en la estrategia. En la tercera, *temas*, se describe el contenido de las temáticas que serán desarrolladas en las campañas de capacitación, a través de folletos y correos, entre otros. En la cuarta, *planear*, se identifican los objetivos, las metas y las actividades que deben incluirse en el desarrollo de este esquema de cultura de seguridad (CLTRe, 2019).

Esta propuesta de estrategia contribuye en el desarrollo de un plan de acción, actividades, métricas, roles en el contexto organizacional y contenido de formación, teniendo como referencia aportes propios, así como elementos importantes de la norma ISO 27001, la investigación sobre cultura organizacional de seguridad cibernética de ENISA y el kit de concienciación del INCIBE, enmarcado en cada una de las cuatro etapas del esquema descrito. El resultado es una estrategia que permea la cultura organizacional en su componente de ciberseguridad.

4.1. Objetivo de la estrategia

El objetivo de la estrategia de cultura organizacional de ciberseguridad para la Alcaldía de Neiva es gestionar el talento humano por medio de la articulación de factores como la conciencia, la apropiación, el cumplimiento y el comportamiento (figura 5.6), de manera que permita la mitigación de riesgos de ciberseguridad en la organización.

Figura 5.6. Objetivo de la cultura organizacional de ciberseguridad



Fuente: Elaboración propia.

La estrategia propuesta se compone de cuatro etapas que trabajan en pro del fortalecimiento de cuatro capacidades que garantizan la integralidad de la organización: tecnología, información, personas y procesos.

En la primera etapa, *planeación*, se define un plan de acción, con la descripción de las actividades necesarias para su cumplimiento. En la segunda, *métricas*, se define la medición que se realizará para evaluar el cumplimiento del plan de acción identificado en la primera etapa. En la tercera, *organización*, se definen los roles y las actividades que facilitan la implementación de la estrategia. En la cuarta, *formación*, se lista el contenido en materia de capacitación, formación y educación para lograr su concienciación y apropiación. Estas etapas se encuentran enmarcadas por un proceso de mejora continua. La figura 5.7 representa la estrategia propuesta.

Figura 5.7. Estrategia de la cultura organizacional de ciberseguridad

Fuente: Elaboración propia con base en el Security Culture Framework (2019).

4.2. Etapa de planeación y métricas

Teniendo como referencia que para establecer una cultura de ciberseguridad es necesario articular y abordar las capacidades tecnológicas, de información, personas y procesos en una organización, se establece la tabla 5.6, en donde se identifican las actividades y la medición para fortalecer cada una de estas capacidades, pues esta será la hoja de ruta para realizar la implementación de la estrategia que se propone en el presente estudio.

Tabla 5.6. Plan de acción y métricas para la estrategia de cultura organizacional de ciberseguridad propuesta

Capacidad	Plan de acción	Actividades	Métrica
Tecnología	Identificar la infraestructura tecnológica dispuesta en la organización para el cumplimiento de la misión.	Realizar un inventario de la infraestructura tecnológica de la organización, determinando su ubicación, responsables, valor estratégico y criticidad ante una interrupción no autorizada del servicio.	Inventario de infraestructura tecnológica realizado.
		Inventariar los sistemas de información, determinando su ubicación, roles a cargo de la administración, valor estratégico y criticidad ante una interrupción no autorizada del servicio.	Inventario de sistemas de información realizado.
Información	Gestionar los riesgos de seguridad de la información y la ciberseguridad.	Realizar el levantamiento de activos de información de la organización, en el cual se especifique el proceso al que pertenece cada uno, el tipo de activo, el custodio, la clasificación, la criticidad, las amenazas y las vulnerabilidades.	Inventario y clasificación de activos de información realizados.

Capacidad	Plan de acción	Actividades	Métrica
Información		Revisar periódicamente el plan de tratamiento de riesgos de seguridad de la información y la ciberseguridad, con el objetivo de controlar cambios planificados, no planificados y la consecuencia de estos.	Revisiones documentadas.
	Mantener una comunicación constante con entidades públicas y privadas para establecer una cooperación para la prevención y la atención de incidentes cibernéticos.	Recopilar información sobre ataques, vulnerabilidades y exposiciones, normatividad brindada por compañías de seguridad informática y centros de cooperación —como Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT), el Comando Conjunto Cibernético (CCOC), el Centro Cibernético Policial (CCP), el CSIRT de la Policía Nacional y el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)—.	Información recopilada y documentada.
Personas	Formar al factor humano en el conocimiento de los riesgos de seguridad por medio de programas de sensibilización, concienciación y educación en ciberseguridad.	Publicar consejos y buenas prácticas en ciberseguridad (a través de medios *online*, *offline* e híbridos), con miras a informar al personal operativo y técnico y la alta gerencia..	Resultado de las pruebas de conocimiento antes y después de implementar el programa de sensibilización.
		Realizar simulacros por medio de ataques dirigidos con el fin de identificar la conducta de la persona y probar su conocimiento en el procedimiento de resolución de incidentes y presentación de informes.	Número de empleados que siguen los protocolos de reporte de incidentes después de que los detectan.
		Entrenar al personal encargado de administrar la seguridad de la organización por medio de escenarios y juegos de guerra.	Número de empleados que pueden prevenir y detectar un ciberataque.
		Encuestar y entrevistar a los empleados con el fin de evaluar su percepción y conciencia en materia de ciberseguridad.	Encuestas y entrevistas realizadas.

Capacidad	Plan de acción	Actividades	Métrica
Procesos	Buscar el compromiso de las directivas con la estrategia de cultura organizacional.	Garantizar los recursos necesarios para implementar las actividades propuestas para fortalecer y mejorar continuamente la estrategia de cultura organizacional.	Recursos para la estrategia de cultura organizacional incluidos dentro del presupuesto anual.
		Crear un plan de incentivos laborales (económicos o morales) que sirva para motivar a los funcionarios a cumplir la estrategia propuesta y a adoptarla en su día a día.	Porcentaje de cumplimiento del plan anual de incentivos.
		Crear un equipo de cultura organizacional dispuesto a seguir la estrategia propuesta y a generar espacios propicios para la discusión con el personal.	Equipo de cultura organizacional de ciberseguridad creado.
		Crear una política de cultura organizacional que incluya el componente de ciberseguridad y no dependa del cambio de administración.	Política de cultura organizacional creada.
		Crear un código de conducta y de ética aceptables y de obligatorio cumplimiento.	Evaluación del cumplimiento del código por medio de procesos de control interno y control interno disciplinario.
		Crear el procedimiento de gestión del conocimiento y la cultura de la documentación.	Conocimiento documentado.

Capacidad	Plan de acción	Actividades	Métrica
Procesos	Generar los espacios para la participación.	Promover la participación del personal por medio de foros dispuestos en la intranet de la organización, los cuales sirvan para resolver inquietudes, brindar aportes, entre otros.	Inquietudes, sugerencias y aportes gestionados.
	Seguir y mejorar continuamente la implementación de la estrategia de cultura organizacional de ciberseguridad.	Diagnosticar el estado actual de la cultura organizacional de ciberseguridad de la audiencia objetivo.	Diagnóstico realizado.
		Realizar auditorías internas para verificar el cumplimiento de las métricas propuestas en la estrategia de cultura organizacional de ciberseguridad.	Número de auditorías realizadas.

Fuente: Elaboración propia con base en información de la ENISA y el INCIBE (2020).

4.3. Organización

Para implementar la estrategia de cultura organizacional de ciberseguridad, es necesario contar con un grupo interdisciplinario dispuesto a realizar seguimiento a la misma, desde su etapa inicial hasta de su mejora continua. Según la ENISA (2017), los roles que se deben identificar para la construcción de una cultura organizacional de ciberseguridad en la organización se describen en la tabla 5.7.

Tabla 5.7. Roles necesarios para una cultura de ciberseguridad

Rol	Papel
Alta gerencia	Aprobar las políticas, brindar respaldo económico, incluir la estrategia de ciberseguridad en la cultura organizacional y establecer la importancia de la gestión de riesgos de seguridad para el cumplimiento de la misión.
Grupo de TI	Aportar conocimiento y experiencia en la infraestructura tecnológica y los sistemas de información; intermediar el grupo de seguridad de la información y la alta gerencia.
Grupo de seguridad de la información	Articular los objetivos estratégicos del grupo de TI con los principios de seguridad de la información, con énfasis en la gestión del riesgo.
Recursos humanos	Acompañar al factor humano, por medio de un plan de incentivos o sanciones, para ejercer el cumplimiento de políticas y buenas prácticas dispuestas en la organización.
Comunicaciones	Promover la divulgación del programa de sensibilización en materia de ciberseguridad, por medio del uso de canales efectivos de comunicación.

Fuente: Elaboración propia con base en información de la ENISA (2017).

4.4. Formación

Teniendo en cuenta la identificación de riesgos de cara al factor humano detallados en el anexo 1 del presente documento y los resultados de la encuesta realizada en materia de conciencia y en ciberseguridad y seguridad de la información en la Alcaldía de Neiva (anexo 5.2), en esta etapa se tienen en cuenta temáticas dispuestas en el kit de concienciación de INCIBE, pues a través de estas se busca fortalecer el conocimiento y

la conciencia de los funcionarios de la entidad y, así, mitigar los riesgos de ciberseguridad identificados (INCIBE, 2020).

Tabla 5.8. Propuesta para una estrategia de cultura de ciberseguridad

Tema	Medio	Recurso	Receptor
Escritorio de equipo limpio y bloqueo de equipo en periodos de inactividad.	Correo electrónico o póster.	Personal que envíe el mensaje.	Todo el personal.
Creación de contraseñas seguras.	Correo electrónico o póster.	Personal que envíe el mensaje.	Todo el personal.
Control en el uso de dispositivos extraíbles (memorias USB, DVD).	Correo electrónico o póster.	Personal que envíe el mensaje.	Todo el personal.
Conexión remota con dispositivos de la entidad por medio de una red privada virtual (VPN).	Capacitación.	Capacitador, auditorio, herramientas (*video beam*, tablero, marcadores, fotocopias).	Todo el personal
Consejos como evitar las amenazas informáticas: ramsonware, phishing, robo de identidad, ingeniería social.	Correo electrónico o póster.	Personal que envíe el mensaje.	Todo el personal.
Divulgación de la política de seguridad de la información y la ciberseguridad.	Capacitación.	Capacitador, auditorio, herramientas (*video beam*, tablero, marcadores, fotocopias).	Todo el personal.

Tema	Medio	Recurso	Receptor
Cifrado de información sensible.	Capacitación.	Capacitador, auditorio, herramientas (*video beam*, tablero, marcadores, fotocopias).	Todo el personal.
Legislación en materia de protección de datos, seguridad y privacidad de la información.	Capacitación.	Capacitador, auditorio, herramientas (*video beam*, tablero, marcadores, fotocopias).	Todo el personal.
Control del acceso a sistemas de información y de la ubicación de infraestructura crítica.	Capacitación.	Capacitador, auditorio, herramientas (*video beam*, tablero, marcadores, fotocopias).	Administradores de sistemas de información.
Realización de copias de seguridad.	Correo electrónico o póster.	Personal que envíe el mensaje.	Todo el personal.
Seguridad en la red. Segmentación de red, *firewall*.	Capacitación.	Capacitador, auditorio, herramientas (*video beam*, tablero, marcadores, fotocopias).	Administradores de sistemas de información.
Actualizaciones de los sistemas operativos, sistemas de información y antivirus.	Correo electrónico o póster.	Personal que envíe el mensaje.	Todo el personal.
Conexión de dispositivos personales en la organización.	Correo electrónico o póster.	Personal que envíe el mensaje.	Todo el personal.

Tema	Medio	Recurso	Receptor
Amenazas y vulnerabilidades de ciberseguridad.	Capacitación.	Capacitador, auditorio, herramientas (*video beam*, tablero, marcadores, fotocopias).	Todo el personal.
Procedimiento para el reporte de incidentes de seguridad.	Capacitación.	Capacitador, auditorio, herramientas (*video beam*, tablero, marcadores, fotocopias).	Todo el personal.
Continuidad del negocio.	Capacitación.	Capacitador, auditorio, herramientas (*video beam*, tablero, marcadores, fotocopias).	Grupo de TI.

Fuente: Elaboración propia con base en información del INCIBE (2020).

Las actividades propuestas en la tabla 5.6, así como los contenidos de formación descritos en la tabla 5.8, forman parte del plan de tratamiento de riesgos propuesto en la matriz de riesgos del anexo 1. La entidad deberá implementarlos, realizar una segunda valoración e identificar el riesgo residual. Será importante un monitoreo y un seguimiento para verificar la efectividad de las acciones en la mitigación de los riesgos identificados.

En cada una de las cuatro etapas descritas se observan las actividades, contenidos, roles y responsabilidades necesarios para implementar la Estrategia de Cultura Organizacional en la Alcaldía de Neiva. Con el objetivo de alcanzar la madurez en materia de cultura, es necesario involucrar un proceso de mejora continua, teniendo como insumo las auditorías internas descritas en el plan de acción (tabla 5.6).

5. Conclusiones

Con base en los referentes teóricos revisados en el desarrollo del presente artículo, se puede observar que el éxito de la seguridad cibernética se basa en establecer una visión estratégica que articule la construcción de capacidades en tecnología, información, procesos y personas, teniendo en cuenta que las amenazas pueden ser de diversa naturaleza, y una de estas es el factor humano. No es suficiente establecer controles técnicos si no se cuenta con una cultura organizacional que permita a las personas adoptar e interiorizar estos controles, conceptos y buenas prácticas, para cumplir con lo establecido de una manera inconsciente.

Este documento desarrolló los ocho factores que, según el autor consultado, influyen en la construcción de una cultura organizacional de ciberseguridad. Su desarrollo permitió comprender que no es suficiente crear un plan de concienciación pretendiendo cambiar el comportamiento de las personas. Por esto, debe existir un apoyo de la alta gerencia para que cree políticas de seguridad, promueva conductas éticas aceptables e incentive el cumplimiento.

Luego de identificar los riesgos de cara al factor humano, revisar la documentación referente al cumplimiento de las directrices establecidas por el Gobierno nacional en materia de seguridad digital y evaluar la conciencia y la percepción en la Alcaldía de Neiva al respecto, la entidad reporta un cumplimiento del 100 % en el establecimiento de la política MSPI y del plan de concienciación y capacitación. Sin embargo, esta cifra no se refleja en el comportamiento, cumplimiento, conciencia y percepción de los funcionarios de la entidad. La encuesta realizada demuestra que la conciencia en ciberseguridad es baja.

Con base en la investigación documental teórica y práctica desarrollada en el presente documento, se identifica la necesidad de gestionar el factor humano, considerado una amenaza interna de la organización. Para ello, se propone una estrategia de cultura organizacional de ciberseguridad, basada en el trabajo anterior de CLTRe, pero enriquecida con el aporte de los autores referenciados en el presente documento y

enfocada en la construcción y fortalecimiento de cuatro capacidades: tecnología, información, personas y procesos.

En la primera etapa de la estrategia propuesta, hay un plan de acción encaminado a generar conciencia en las personas, a partir de sesiones de capacitación y educación; un plan de incentivos; participación de los funcionarios en foros y actividades grupales; códigos de conducta ética y de cultura organizacional, y otras actividades complementarias.

En la segunda etapa, se establece la forma de medir el cumplimiento de las actividades del plan de acción. En la tercera, se desarrollan roles necesarios para la implementación, auditoría y mejora continua de la estrategia.

Por último, teniendo en cuenta los resultados de la encuesta realizada en materia de conocimiento en ciberseguridad y la identificación de riesgos de ciberseguridad de cara al factor humano en la Alcaldía de Neiva, se proponen los temas de formación, los recursos necesarios y las personas que serán receptoras de esta formación. Con la implementación de esta estrategia, se pretende facilitar la mitigación de los riesgos de ciberseguridad de cara al factor humano, para así cumplir con los objetivos estratégicos de la Alcaldía de Neiva.

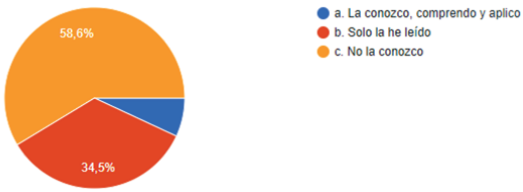
Se recomienda en un trabajo futuro implementar la estrategia aquí propuesta, con el fin de realizar un ejercicio de mejora continua que fortalezca los componentes aquí descritos.

Anexo 1: Matriz de niveles de riesgos de ciberseguridad de cara al factor humano de la alcaldía de Neiva

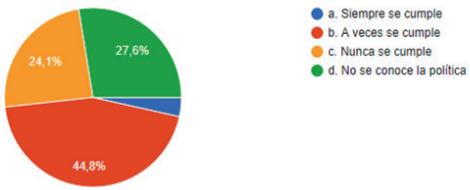
N.°	Riesgo	Definición y descripción del riesgo	Amenazas	Vulnerabilidad	Definición de los efectos de materialización del riesgo identificado	Activos de información asociados	Dueño o propietario del riesgo	Tipo de riesgo	Riesgo asociado			Clasificación del riesgo	Factores		Riesgo inherente						¿Se acepta?	Actividades, estrategia cultura organizacional a implementar
									Confidencialidad	Integridad	Disponibilidad				Posibilidad de ocurrencia		Impacto		Zona de riesgo			
1	Denegación del servicio	Indisponibilidad en los servicios como la página web, internet y software a causa de ataques contra el sistema, entrenamiento insuficiente en seguridad y ausencia de personal calificado	1. Ataques contra el sistema (por ejemplo, negación distribuida del servicio) 2. Intrusión en el sistema 3. Interceptación y espionaje 4. Código malicioso (por ejemplo, virus bomba lógica, troyano) 5. Incumplimiento en el mantenimiento del sistema de información	1. Entrenamiento insuficiente en seguridad 2. Mantenimiento insuficiente 3. Ausencia de personal calificado 4. Desconocimiento de política de copias de seguridad 5. Falta de conciencia acerca de la seguridad 6. Sistemas desactualizados	1. Pérdida de la imagen institucional 2. Incumplimiento de la misionalidad de la entidad 3. Costo financiero de las habilidades específicas para reparar el daño	Servicios/ software	Oficina de Tecnologías	Seguridad digital			X	Tecnológico	5	Recurso humano	3	Posible	3	Moderado	9	Alta	No	1. Crear programas de sensibilización por medios *online, offline* e híbridos en donde se dé a conocer consejos, buenas prácticas en materia de ciberseguridad 2. Realizar sesiones de entrenamiento con el personal encargado de administrar la seguridad de la organización por medio de escenarios y juegos de guerra 3. Crear un plan de incentivos laborales para el personal, económicos o Morales el cual motive a los funcionarios a cumplir la estrategia propuesta, así como adoptarla en su día a día 4. Recopilar información sobre ataques, vulnerabilidades y exposiciones, normatividad brindada por compañías de seguridad informática y centros de cooperación
2	Alteración sin autorización de la información	La falta de políticas de control de acceso, contraseñas de bases de datos no seguras, pueden facilitar una alteración no autorizada causando la pérdida de la integridad de la base de datos	1. Error en el uso 2. Manipulación no autorizada 3. Uso no autorizado del equipo	1. Uso incorrecto del *software* y *hardware* 2. Falta de conciencia acerca de la seguridad 3. Contraseñas de bases de datos no seguras 4. Falta de políticas de control de acceso	1. Divulgación ilegal de información 2. Destrucción de información 3. Investigaciones y sanciones	Datos/ bases de datos	Todos	Seguridad digital	X			Tecnológico	5	Recurso humano	2	Improbable	3	Moderado	6	Moderada	Sí	1. Implementar plan de formación descrito en la etapa 4 de la Estrategia de Cultura Oganizacional 2. Crear un código de conducta ética aceptable y de obligatorio cumplimiento
3	Fuga de información	La falta de conciencia en materia de seguridad, así como amenazas como la ingeniería social permiten que empleados con conocimiento deficiente, intencional o accidentalmente brinden información confidencial de la entidad	1. Ingeniería social 2. Intrusos (empleados con entrenamiento deficiente, descontentos, mal intencionados, negligentes, deshonestos o despedidos)	1. Línea de comunicación sin protección adecuada 2. Ausencia de terminación de la sesión cuando se abandona la estación de trabajo 3. Falta de conciencia acerca de la seguridad	1. Venta de información personal 2. Pérdida de datos de la información privada y con carácter de reservada	Información	Oficina de Tecnologías/ Planeación	Seguridad digital	X			Operativo	5	Recurso humano	3	Posible	3	Moderado	9	Alta	No	1. Realizar simulacros por medio de ataques dirigidos con el fin de identificar la conducta de la persona y probar su conocimiento en el procedimiento de resolución de incidentes y presentación de informes 2. Crear una política de Cultura organizacional en la cual se encuentra incluido el componente de ciberseguridad la cual no dependa del cambio de administración 3. Implementar plan de formación

Anexo 2

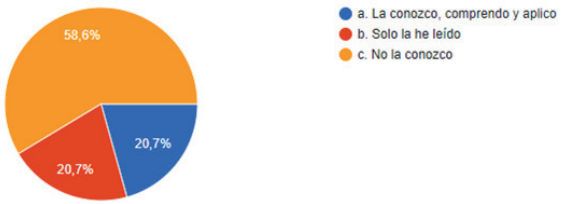
1. ¿Qué tanto conoce la política general de seguridad y privacidad de la información adoptada por la entidad?



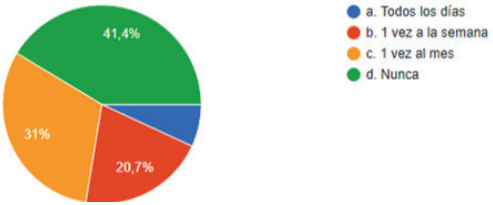
2. Según su percepción, ¿qué tanto se cumple con la política de seguridad y privacidad de la información dispuesta por la entidad?



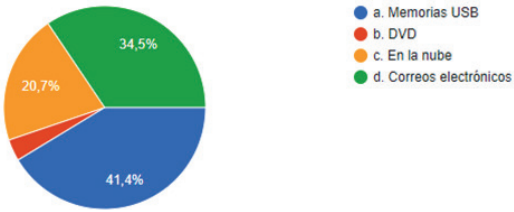
3. ¿Conoce la política de copia de seguridad o respaldo de la información?



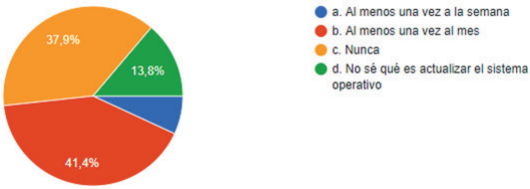
4. ¿Con qué periodicidad realiza copias de seguridad de su información?



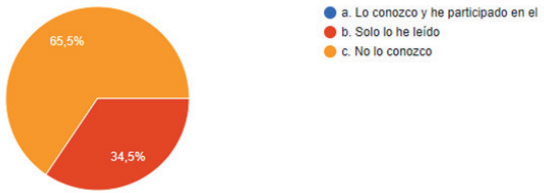
5. ¿Qué medio utiliza para almacenar información en la entidad?



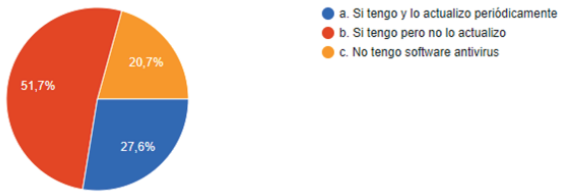
6. ¿Qué tanto conoce el plan de sensibilización y concienciación generado por la Oficina de Tecnologías de la Entidad?



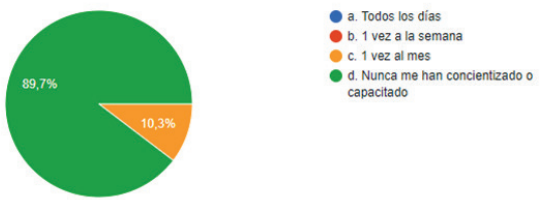
7. ¿Con qué frecuencia actualiza el sistema operativo de su equipo de cómputo?



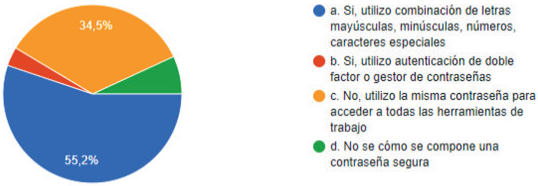
8. ¿Tiene instalado en su equipo de cómputo software antivirus?



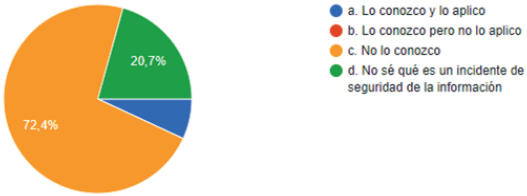
9. ¿Con qué frecuencia usted ha recibido capacitación, por parte de la entidad, en seguridad de la información, informática o ciberseguridad?



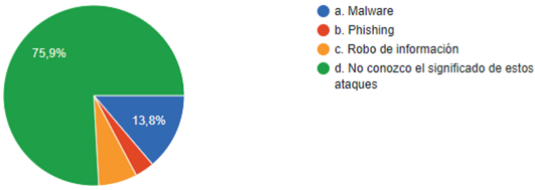
10. ¿Considera que su contraseña de acceso al equipo de cómputo, correo electrónico, páginas web y sistemas de información es segura?



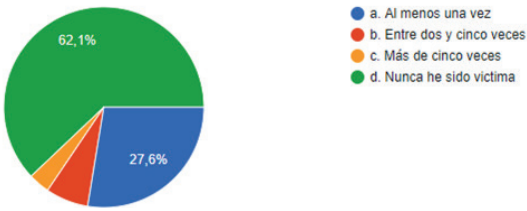
11. ¿Conoce el protocolo que se debe realizar en caso de un incidente de seguridad de la información en la entidad?



12. ¿Reconoce ser víctima de alguno de los siguientes ataques informáticos?



13. ¿Con qué frecuencia ha sido víctima de ataques informáticos?



REFERENCIAS

24 horas. (2017). Conoce los tipos de hackers y su forma de operar. https://www.24horas.cl/tendencias/ciencia-tecnologia/conoce-los-tipos-de-hackers-y-su-forma-de-operar--2299770

Acemoglu, D. y Robinson, J. A. (2012). *Why nations fail: The origins of power, prosperity, and poverty.* Crown Business.

Acosta, L. E. (2014). El conocimiento tradicional: clave en la construcción del desarrollo sostenible en la Amazonia colombiana. *Revista Colombia Amazónica, 114,* 101-118.

Acto Legislativo 01 (4 de abril de 2017), por medio del cual se crea un título de disposiciones transitorias de la Constitución para la terminación del conflicto armado y la construcción de una paz estable y duradera y se dictan otras disposiciones. *Diario Oficial* n.º 50.196.

Acto Legislativo 02 (27 de diciembre de 2001), por medio del cual se adiciona el artículo 93 de la Constitución. *Diario Oficial* n.º 44.663.

Agencia Europea de Seguridad de las Redes y de la Información. (2017). *Cultura de seguridad cibernética en organizaciones*. 10.2824/10543. https://bit.ly/2Qedfkz

Agencia Europea de Seguridad de las Redes y de la Información. (2019). *Informe del panorama de amenazas 2018*. https://bit.ly/2G5RHQ4

Aguilera, M. (2014). *Contrapoder y justicia guerrillera, fragmentación política y orden insurgente en Colombia (1952-2003).* Universidad Nacional de Colombia.

Alcaldía de Neiva, Comité Institucional de Gestión y Desempeño. (2018). *Evaluación MSPI de la Alcaldía de Neiva*. Alcaldía de Neiva.

Alcaldía de Neiva. (2016). *Decreto n.º 590 del 10 de octubre, por el cual se establece la estructura de la Alcaldía del Municipio de Neiva, se señalan las funciones de sus dependencias y se dictan otras disposiciones*. https://bit.ly/2lso1Es

Alcaldía de Neiva. (2017). *Resolución n.º 249, por la cual se adopta el Plan Estratégico de Tecnologías de la Información y las Comunicaciones 2016-2019 y la Política General del Modelo de Seguridad y Privacidad de la Información de la Alcaldía de Neiva.* https://bit.ly/2IcFDNS

Alcaldía de Neiva. (2018). *Plan de sensibilización de seguridad y privacidad de la información.* https://bit.ly/2SYZL9f

Alcaldía de Neiva. (2020). *Plan Institucional de Capacitación 2020*. Alcaldía de Neiva. https://cutt.ly/IrPWsZL

Alnatheer, M. A. (2012). *Understanding and measuring information security culture in developing countries: Case of Saudi Arabia* [Tesis doctoral sin publicar]. Queensland University of Technology. https://bit.ly/2JWBGfc

Alnatheer, M. A. (2015). Information Security Culture Critical Success Factors. *12th International Conference on Information Technology - New Generations*, 731-735. 10.1109/ITNG.2015.124

Alnatheer, M., Chan, T. y Nelson, K. (2012). Understanding and measuring information security culture. *PACIS 2012 Proceedings. Paper 144.* https://bit.ly/2UgYM8A

Álvarez, C. M. (2005). Una aproximación al concepto de cultura organizacional. *Universitas Psychologica*, *5*(1), 163-174. https://bit.ly/3bUbj9i

Amnistía Internacional. (2012, 10 de julio). Thomas Lubanga condenado por la Corte Penal Internacional a 14 años de prisión. *Amnistía Internacional*. https://www.es.amnesty.org/en-que-estamos/noticias/noticia/articulo/thomas-lubanga-condenado-por-la-corte-penal-internacional-a-14-anos-de-prision/

Armada Nacional. (2018, 31 de agosto). *Notas explicativas a los informes financieros y contables consolidados.* Armada Nacional.

Armada Nacional. (2019). *Plan de Navegación de Comando de la Armada de Colombia.* Armada Nacional.

Avocats Sans Frontières Canada. (2018, 15 de junio). ASFC acoge con satisfacción una decisión crucial de la Corte Constitucional de Colombia. *Avocats sans frontières*. https://www.asfcanada.ca/medias/nouvelles/asfc-acoge-con-satisfaccion-una-decision-crucial-de-la-corte-constitucional-de-colombia/

Baeza, J. y Escudero, M. C. (2017). *La reconfiguración del fenómeno del narcotráfico en Bolivia, Brasil, Chile, Colombia, Ecuador y Perú: Red de Política de Seguridad*. Instituto de Estudios Internacionales, Pontificia Universidad Católica del Perú.

Baños, P. (2017). *Así se domina el mundo: desvelando las claves del poder mundial.* Editorial Ariel.

Barceló, P. (2008). Poder terrestre, poder marítimo: la politización del mar en la Grecia clásica y helenística. *Potestas: Religión, Poder y Monarquía*, 131-147.

Bartholomees, J. B. (2006). *Guide to national security policy and strategy.* EE.UU.: U.S. Army War College.

Bartnes, M. y Brede Moe, N. (2017). Challenges in IT security preparedness exercises: A case study. *Computers and Security* (67), 280-290.

Becerra, C. M. (1986). *La Marina Mercante y el desarrollo nacional.* Universidad Nacional de Colombia.

Betancourt Vélez, R. O. S. (2012). OTCA: el Amazonas en el horizonte de la política exterior colombiana. En O. S. R. Betancourt Vélez, OTCA (Eds.), *El Amazonas en el horizonte de la política exterior colombiana* (pp. 343-365). Pontificia Universidad Javeriana.

Bilbao, A. P. (2015). Los aportes de Friedrich Ratzel y Halford Mackinder en la construcción de la geografía política en tiempos de continuidades y cambios. *Espacios. Revista de Geografía, 5*(9), 64-81.

Boots, F. (2009). *Regional crime: Latinamerica perspective.* Public Research.

Bueger, C. y Edmunds, T. (2017). Beyond seablindness: A new agenda for maritme security studies. *International Affairs, 93*(6), 1293-1311. https://doi.org/10.1093/ia/iix174

Buvinic, M., Morrison, A., y Orlando, M. B. (2005). Violencia, crimen y desarrollo social en América Latina y el Caribe. *Papeles de población, 11*(43), 167-214.

Cairo Carou, H. (2012). La geopolítica como "ciencia del Estado": el mundo del general Haushofer. Geopolítica(s). *Revista de estudios sobre espacio y poder, 3*(2), 337-345.

Cano, J. (2018). Repensando los fundamentos de la gestión de riesgos. Una propuesta conceptual desde la incertidumbre y la complejidad. *Revista Ibérica de Tecnología y Sistemas de la Información, E15*(4), 76-87.

Carnegie Mellon University, Sofware Ingineering Institute. (2015). *Vulnerability assessment: CERT Insider Threat Center*. https://bit.ly/2UPQwbp

Centro Cibernético Policial. (2017). *Amenazas del cibercrimen en Colombia 2016-2017*. Policía Nacional de Colombia. https://bit.ly/2ILo5H8

Centro Global de Capacidad de Ciberseguridad. (2019). *Portal Capacidad Ciberseguridad*. http://www.oas.org/es/sms/cicte/docs/ESP-Revision-de-capacidades-de-Ciberseguridad.pdf

CERT Division. (2017). CSIRT Frequently Asked Questions. *Carnegie Mellon University*. Software Engineering Institute. https://www.cert.org/incident-management/csirt-development/csirt-faq.cfm

CICR. (s. f.) *Estatuto del Tribunal Internacional para Rwanda.* Comité Internacional de la Cruz Roja. https://www.icrc.org/es/doc/resources/documents/misc/treaty-1994-statute-tribunal-rwanda-5tdmhw.htm

CISCO. (2015). *How to be agile and secure. The fundamental challenge facing organisations today*. https://bit.ly/2W89afd

CLTRe. (2019). *Security culture framework*. https://securityculturefframework.net/

Comisión Colombiana del Oceáno. (2016). *Hacia una potencia oceánica*. Secretaría Ejecutiva, Comisón Colombiana del Oceáno. http://www.cco.gov.co/cco/publicaciones/83-publicaciones/345-hacia-una-potencia-oceanica.html

Comisión Colombiana del Océano. (2017). *Politica Nacional del Océano y de los Espacios Costeros.* Secretaría Ejecutiva, Comisón Colombiana del Oceáno.

Comisión Colombiano del Océano. (2020). *Programa Antártico Colombiano.* Comisión Colombiano del Océano.

CONPES. (2020, 31 de marzo). CONPES 3990. *Colombia: potencia bioceánica sostenible 2030*. Consejo Nacional de Política Económica y Social.

Corte Constitucional. (2002). *Sentencia C-578 del 30 de julio.* Magistrado ponente: Manuel José Cepeda Espinosa.

Corte Penal Internacional. (2012). *Representación de víctimas ante la Corte Penal Internacional.* La Oficina Pública de Defensa de las Víctimas.

Corte Penal Internacional. (2012a). *Situación en Colombia: reporte intermedio.* Corte Penal Internacional.

Chaves, B. H. (2011). La *proyección regional y mundial de Brasil: un desafío para la política exterior del Estado colombiano. Más allá de la seguridad democrática.* Pontificia Universidad Javeriana. https://s3.amazonaws.com/academia.edu.documents/37325472/Mas_alla_de_la_seguridad_democratica1.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1527865360&Signature=A1QL7F5tBtjPYW4%2FZfG5tK2umII%3D&response-content-disposition=inline%3B%20filename%3DMarquez_Martha_Lucia_2010_Algunas_estrat.pdf#page=475

Deloitte. (2019) Ciber riesgos y seguridad de la información en América Latina & Caribe. Tendencias 2019. Reporte Colombia. *Deloitte.* https://www2.deloitte.com/co/es/pages/risk/articles/ciber-riesgos-y-seguridad-de-la-info-en-america-latina-y-caribe.html

Departamento Administrativo de la Función Pública. (2017). *Decreto 1499 del 11 de septiembre, por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.* https://bit.ly/30JnCfV

Departamento Administrativo de la Función Pública. (Abril de 2018). *Dimensión No.1 Talento Humano.* https://bit.ly/3lrRb1s

Departamento Nacional de Planeación. (11 de abril de 2016). *Política Nacional de Seguridad Digital. Documento CONPES 3854.* Departamento Nacional de Planeación. https://bit.ly/2QgOZ1j

Departamento Nacional de Planeación. (2011). *Documento CONPES 3701. Lineamientos de política para ciberseguridad y ciberdefensa*. Consejo Nacional de Política Económica y Social, República de Colombia, Departamento Nacional de Planeación. https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

Departamento Nacional de Planeación. (2016). *Documento CONPES 3854. Política nacional de seguridad digital*. Cámara de Comercio de Bogotá. http://hdl.handle.net/11520/14856

Departamento Nacional de Planeación. (2019). *Bases del Plan Nacional de Desarrollo 2018-2022: Pacto por Colombia, pacto por la equidad.* DNP.

Departamento Nacional de Planeación. (2019, mayo). Pacto Región Océanos: Colombia potencia bioceánica. *Bases del Plan Nacional de Desarrollo 2018-2022*.

Dirección General de Relaciones Institucionales, Instituto Español de Estudios Estratégicos. (2010). *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. Cuadernos de Estrategia, 149*. Ministerio de Defensa. https://bit.ly/2Fd9B2d

Esquivel Triana, R. (2015, junio). Intereses geopolíticos de Colombia. *Estudios en Seguridad y Defensa, 10*(19), 71-86.

Evans, C. (2012). *The right to reparation in international law for victims of armed conflict.* Cambridge: University Press.

Evans, M., Ying, H., Yevseyeva, I. y Janicke, H. (2019). Published incidents and their proportions of human error. *Information and Computer Security, 27*(3), 343-357. https://doi.org/10.1108/ICS-12-2018-0147

Facultad de Informática de la Universidad Complutense de Madrid. (2017a). *FDIwiki ELP.* https://informatica.ucm.es

Facultad de Informática de la Universidad Complutense de Madrid. (2017b). Ciberespacio. En *Wiki*. http://wikis.fdi.ucm.es/ELP/Ciberespacio

Federación Internacional por los Derechos Humanos. (19 de julio de 2007). *Los derechos de las víctimas ante la Corte Penal Internacional: manual para víctimas, sus representantes legales y ONG.* https://www.fidh.org/es/temas/justicia-internacional/corte-penal-internacional-cpi/Los-Derechos-de-las-victimas-ante

Foro Social Amazónico. (2017). *"Amazonía Viva, Humanidad segura" es el llamado del bosque.* http://www.forosocialpanamazonico.com/amazonia-viva-humanidad-segura-es-el-llamado-del-bosque-todosas-a-movilizarse-hoy-22-de-septiembre/

Furnell, S. y Thomson, K. L. (2009). De la cultura a la desobediencia: reconocer la aceptación variable de los usuarios de la seguridad de TI. *Computer Fraud & Security, 2009*(2), 5-10 https://doi.org/10.1016/S1361-3723(09)70019-3

Godet, M. y Durance, P. (2011). *Prospectiva estratégica para las empresas y los territorios.* UNESCO.

González, N. (2014). *La concesión minera en colombia: un análisis desde el marco normativo y regulatorio frente a los principios de seguridad y estabilidad jurídica.* Universidad Colegio Mayor de Nuestra Señora del Rosario.

Gutiérrez, V. (2017). *Mecanismos alternativos de reparación en el sistema de la Corte Penal Internacional.* Pontificia Universidad Javeriana.

Hernández, A. D. (2007). *Auditoría del clima y cultura de seguridad en la empresa*. Universidad de Valencia. https://www.tdx.cat/handle/10803/10188

HM Government. (2015). *Encuesta sobre incumplimientos de seguridad de la información.* Departamento de Negocios, Innovación y Habilidades. https://pwc.to/2AQVpHX

Holmes, J. (2019). *A brief guide to maritime strategy.* Naval Institute Press.

Instituto de Auditores Internos de España. (2016). *Ciberseguridad: una guía de supervisió*n. https://auditoresinternos.es/uploads/media_items/guia-supervision-ciberseguridad-fabrica-pensamiento-iai.original.pdf

Instituto de Criminoloxía, Universidad Santiago de Compostella. (2009). *Los delitos informáticos.* https://www.usc.es/export9/sites/webinstitucional/gl/institutos/criminoloxia/descargas/Los_Delitos_Informxticos.pdf

Instituto Nacional de Ciberseguridad (INCIBE). (s. f.). *Checklist de buenas prácticas en el área de informática.* https://www.incibe.es/extfrontinteco/img/File/empresas/dosieres/departamentos_de_informatica/contingencia_y_continuidad_de_negocio_plan_de_recuperacion.pdf

Instituto Nacional de Ciberseguridad de España. (s.f.). *Kit de concienciación*. Instituto Nacional de Ciberseguridad de España. https://bit.ly/2bmQdCv

ISACA. (2016). *IS Audit/Assurance Program – Cybersecurity: Based on the NIST cybersecurity framework*. ISACA.

JEP Visible. (15 de diciembre de 2017). Estructura de la JEP. https://jepvisible.com/la-jep/estructura-y-funciones

Johnston, A. y Warkentin, M. (2010). Las apelaciones de miedo y los comportamientos de seguridad de la información: un estudio empírico. *Management Information Systems Research Center, Universidad de Minnesota, 34*(3), 549-566. 10.2307 / 25750691

Kaldor, M. (2013). *New and old wars: Organised violence in a global era.* John Wiley & Sons.

Kaspersky Lab, B2B International. (2017). *El factor humano en la seguridad de TI: cómo los empleados hacen que las empresas sean vulnerables desde dentro*. https://bit.ly/2T2R3ql

Kaspesky Lab. (2019). *Ciberamenaza mapa en tiempo real.* https://cybermap.kaspersky.com/es/

Kuehl, D. (2009). From cyberspace to cyberpower: Defining the problem. En Kramer, F. D., Starr, S. y Wentz, L. (eds.), *Cyberpower and National Security* (pp. 24-49). National Defense UP.

Lacey, D. (2009). Entendiendo y transformando la cultura de seguridad organizacional. *Information Management & Computer Security, 18*(1), 4-13. 10.1108/09685221011035223

Laqueur, W. (2003). *La guerra sin fin.* Destino.

Laureano, R. C. (2012). Geopolítica. Origen del concepto y su evolución. *Revista de Relaciones Internacionales de la UNAM, 59,* 18-26.

Ley 1180 de 2007 (31 de diciembre), por medio de la cual se aprueba el "Acuerdo sobre los Privilegios e Inmunidades de la Corte Penal Internacional", hecho en Nueva York, el 9 de septiembre de 2002. *Diario Oficial* n.º 46.858.

Ley 1268 de 2008 (31 de diciembre), por medio de la cual se aprueban las "reglas de procedimiento y prueba" y los "elementos de los crímenes de la Corte Penal Internacional", aprobados por la Asamblea de los Estados Parte de la Corte Penal Internacional, en Nueva York, del 3 al 10 de septiembre. *Diario Oficial* n.º 47.219.

Ley 1273 de 2009 (5 de enero), por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado —denominado "de la protección de la información y de los datos"— y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. *Diario Oficial* n.º 47.223.

Ley 489 de 1998 (30 de diciembre), por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional, se expiden las disposiciones, principios y reglas generales para el ejercicio de las atribuciones previstas en los numerales 15 y 16 del artículo 189 de la Constitución Política y se dictan otras disposiciones. *Diario Oficial* n.º 43.464.

Ley 742 de 2002 (5 de junio), por medio de la cual se aprueba el Estatuto de Roma de la Corte Penal Internacional, hecho en Roma, el día diecisiete (17) de julio de mil novecientos noventa y ocho (1998). *Diario Oficial* n.º 44.826.

Ley estatutaria 1581 de 2012 (18 de octubre), por la cual se dictan disposiciones generales para la protección de datos personales. *Diario Oficial* n.º 48.587.

Ley Estatutaria 1957 (6 de junio de 2019). Estatutaria de la Administración de Justicia en la Jurisdicción Especial para la Paz. *Diario Oficial* n.º 50.976.

López Cabia, D. (2018). Economía azul. En *Economipedia*. Consultado el 10 de mayo de 2018. https://economipedia.com/definiciones/economia-azul.html

López, M. (2013). Primera sentencia de la Corte Penal Internacional sobre reparación a las víctimas: caso The prosecutor C. Thomas Lubanga Dyilo, 7 de agosto de 2012. *REDI, 65*(2), 209-226.

Lovrić Švehla, Z., Sedinić, I. y Pauk, L. (2016). Going white hat: control de seguridad mediante la piratería de empleados que utilizan técnicas de ingeniería social. *Convención internacional sobre tecnología de la información y la comunicación, electrónica y microelectrónica (MIPRO), 1419-1422,* 10.1109/MIPRO.2016.7522362

Mahan, A. T. (1890). *The influence of sea power upon history: 1660-1783.* Little, Brown and Co.

Malcolmson, J. (2009, 13 de noviembre). *What is security culture? Does it differ in content from general organisational culture?* [Conferencia]. 43ª Conferencia Anual Internacional de Carnahan 2009 sobre Tecnología de Seguridad. Zurich, Switzerland, pp. 361-366, doi: 10.1109/CCST.2009.5335511.

Martínez Pachón, M. G. (2014). *El poder de la estratégia para la seguridad del Estado.* Ave Viajera.

McKay, F. (2008). Victim participation in proceedings before the International Criminal Court. *Human Rights Brief, 15*(3), 1-5.

Medina, E. (2016, 23 de mayo). El cibercrimen se volvió una profesión. *El Tiempo*. https://www.eltiempo.com/archivo/documento/CMS-16601202

Ministerio de Defensa Nacional. (2014). *Política de Defensa y Seguridad Todos por un Nuevo País.* Ministerio de Defensa Nacional.

Ministerio de Hacienda y Crédito Público. (2017). *Informe de inversión pública por regiones*. Imprenta Nacional.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2015). *Decreto 1078 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías.* https://bit.ly/2XSbkBC

Montero, L., Barreto, J. y Salazar, P. (2017). Amenazas transnacionales, caso Colombia-Brasil. En: *Amazonía. Poder y Estrategia* (pp. 242-251). Editorial Escuela Superior de Guerra. https://esdeguelibros.edu.co/index.php/editorial/catalog/download /33/28/529-1?inline=1

Muñoz, J. (2017). *La Amazonía colombiana y su importancia estratégica a nivel internacional* [Trabajo de grado] Universidad Militar Nueva Granada.

Naciones Unidas, Consejo de Seguridad. (1993). *Resolución 827 del 25 de mayo.* http://blog.uclm.es/cienciaspenales/files/2016/10/1_42E49838CBAB-03C0E04015AC20201354.pdf

National Institute of Standards and Technology. (2011). *Managing information security risk. Organization, mission, and information system view.* https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

Niekerk, J. y Solms, R. (2009). Cultura de seguridad de la información: una perspectiva de gestión. *Institute for Information and Communication Technology Advancement, 29*(4). 10.1016/j.cose.2009.10.005

Nielsen, K. (2018). *Secretary Kirstjen M. Nielsen's National Cybersecurity Summit Keynote Speech*. https://www.dhs.gov/news/2018/07/31/secretary-kirstjen-m-nielsen-s-national-cybersecurity-summit-keynote-speech

Observatorio de la Complejidad Económica. (2016). https://atlas.media.mit.edu: https://atlas.media.mit.edu/en/profile/hs92/7108/

Organisation for Economic Co-operation and Development. (2018). *Revisión del gobierno digital en Colombia hacia un sector público impulsado por el ciudadano*. https://dx.doi.org/10.1787/9789264292147-es

Organización de las Naciones Unidas. (6 de mayo de 2003). *Proyecto de acuerdo entre la ONU y el Gobierno Real de Camboya relativo al procesamiento de los crímenes cometidos durante el periodo de la Kampuchea Democrática.* http://www.derechos.org/nizkor/impu/tpi/khmtrial.html

Organización Internacional de Normalización. (2005). *ISO/IEC 27001*. https://www.iso.org/isoiec-27001-information-security.html

Organización Internacional de Normalización. (2012). *ISO/IEC 27032. Information technology security techniques guidelines for cybersecurity*. https://www.iso.org/standard/44375.html

Pardo, R. (2019). "El país debe reconocer la importancia de la industria astillera y atender sus necesidades". *Semana*. https://www.semana.com/contenidos-editoriales/colombia-nada-como-el-mar/articulo/el-pais-debe-reconocer-la-importancia-de-la-industria-astillera-y-atender-sus-necesidades/607305?fbclid=iwar3g5cphvezummptmtf7smuy7jebbzhcsjian6qdm6tr27kpseudpuzkzga

Parlamento Europeo, Consejo de la Unión Europea. (2016). *Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo*. https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=uriserv:OJ.L_.2016.194.01.0001.01.SPA

Pierre, P. (2019). Pensar globalmente, actuar localmente. America Latina en Movimiento. https://www.alainet.org/es/articulo/198712

Prieto, C. A. (2013). Las Bacrim y el crimen organizado en Colombia. *Policy paper, 47*, 1-19.

Ramírez Benítez, E. (2018). Estrategias marítimas nacionales de Rusia, Estados Unidos, Chile y Colombia: semejanzas y diferencias. *Ensayos sobre Estrategia Marítima, 7*, 75-88.

Refsdal, A., Solhaug, B. y Stølen, K. (2015). *Cyber risk management*. Springer.

Reguant-Álvarez, M. y Torrado-Fonseca, M. (2016). El método Delphi. *REIRE, Revista d'Innovació i Recerca en Educació, 9*(1), 87-102. 10.1344/reire2016.9.1916

Republica Federativa do Brasil. (2012). *Estrategia Nacional de Defensa.* Republica Federativa do Brasil.

Republica Federativa Do Brasil. (2012). *Livro Branco de Defensa Nacional.* Republica Federativa do Brasil.

Rojas Sánchez, D. A. (2018). Geopolítica marítima del Caribe. En Y. O. Rojas Sánchez, *Intereses de Colombia en el mar: reflexiones y propuestas para la construcción de un país marítimo* (pp. 79-110). Escuela Superior de Guerra.

Rojas, F. (2008). Mayor presencia del crimen organizado: consecuencia de las crisis de gobernabilidad y el débil imperio de la ley. En L. G. Rojas, *Crimen organizado en América Latina y el Caribe* (pp. 95-108). Catalonia.

Roncallo Torres, T., Vélez Forero, M. R. y Sanabria Gaitán, G. (2019). ¿De qué manera podría la Armada Nacional tener un poder de influencia mayor en el teatro regional? En H. Rodríguez Ruiz (Ed.), *Ensayos sobre estrategia marítima, pp* 131-154.

Rosenberg, M. (2017). *Strategy and geopoltics: Understanding global complexity in a turbulent world*. Emerald Publishing Limited.

Rossman, V. (2017). *Capital cities: Varieties and patterns of development and relocation.* Taylor and Francis Group.

Sack, G. y Ierache, J. S. (2015, junio). *Controles de seguridad propuesta inicial de un framework en el contexto de la ciberdefensa*. [Conferencia]. XXI Congreso Argentino de Ciencias de la Computación, Buenos Aires, Argentina. Recuperado de http://sedici.unlp.edu.ar/handle/10915/50588

Sánchez Hurtado, J. R. (2012). *En la mente de los estrategas: ¿conoce usted su curva de rendimiento estratégico?* Escuela Superior de Guerra.

Sandino, D. F. T. y Fernando, D. (2012). Colombia y Brasil en la lucha contra el crimen transnacional: una revisión a sus posturas, acciones y estrategias de seguridad. En Pastrana, E., Jost, E. y Flemes, D. (Eds.), *Colombia y Brasil: ¿socios estratégicos en la construcción de Suramérica* (pp. 423-452). Pontifica Universidad Javeriana.

Sandino, D. F. T. y Fernando, D. (2012). *Los desafíos que la presencia de actores trasnacionales tiene para la proyección del poder estratégico en la Amazonia colombiana*. S. e.

Santamaría, L. (2016). Prólogo. En Uribe, S. Díaz, J. y Rodríguez, M., *Estrategia marítima: evolución y prospectiva.* Escuela Superior de Guerra.

Secretaría Jurídica Distrital. (1999). *Exposición de Motivos 527 de 1999 Nivel Nacional*. https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=10595

Semana. El cibercrimen en 2017: la amenaza crece sobre Colombia. (2017). https://www.semana.com/nacion/articulo/cibercrimen-en-colombia-balance-de-2017/551979

Sensibilización y Comunicación de Seguridad de la Información. Seguridad y privacidad de la información. Guía n.º 14. Ministerio de Tecnologías de la Información y las Comunicaciones. https://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf

Software Engineering Institute. (2007). *Governing for enterprise security. Implementation Guide.* https://resources.sei.cmu.edu/asset_files/TechnicalNote/2007_004_001_14837.pdf

Speller, I. (2014). *Understanding naval warfare.* Routledge.

Stavridis, J. G. (2017). *Sea power: The history and geopolitics of the world's oceans.* Penguin Randon House.

Stavridis, J. G. (2019). *Sailing true North: Ten admirals and the voyage of characte.* Penguin Publishing Group.

Swinnen, J. (2016). Las ventajas de los tribunales penales mixtos como modelo de justicia internacional para el futuro. ¿Una alternativa creíble a la jurisdicción penal internacional *ad hoc*? *Prudentia Iuris,* (82), 107-124.

Symantec. (2019). *Internet security threat report 2019, volume 24*. https://symantec.broadcom.com/symc-istr-v24-2019-6819

Talledos Sánchez, E. (2014). La geografía: un saber político. *Espiral* (Guadalajara), *21*(61), 15-49.

Terzago Cuadros, J. (2005). Alfred Thayer Mahan: su contribución como historiador, estratega y geopolítico. *Revismar, 1,* 47-64. https://revistamarina.cl/revistas/2006/1/terzago.pdf

Thomson, K. L., Solms, R. y Technikon, P. (2006). Towards an information security competence maturity model. *Computer Fraud & Security, 2006*(5), 11-15. https://doi.org/10.1016/S1361-3723(06)70356-6

Till, G. (2004). *Poder marítimo: una guía para el siglo XXI.* Crown House.

Tirado Mejía, A. (1984). *Introducción a la historia económica de Colombia.* El Áncora Editores.

Trigal, L. L. (2011). "Las leyes del crecimiento espacial de los Estados" en el contexto del determinismo geográfico ratzeliano. *Geopolítica(s)*, *2*(1), 157-163.

Uchenna P. D., Hongmei, M. y Ashutosh, T. (2015). Enfoque de evaluación de la capacidad humana para la ciberseguridad en infraestructura industrial crítica. *Avances en factores humanos en ciberseguridad, 501*, 169-182, 10.1007 / 978-3-319-41932-9_14

Unión Internacional de Telecomunicaciones (UIT). (2010). *Serie X: redes de datos, comunicaciones de sistemas abiertos y seguridad.* UIT.

Uribe Cáceres, S. (2015). *Estrategia marítima, evolución y prospectiva.* Escuela Superior de Guerra.

Uribe Cáceres, S. (2017). El poder marítimo en Colombia y su desarrollo en un escenario de posacuerdo. En *Políticas públicas de seguridad y defensa: herramientas en el marco del postconflicto en Colombia* (p. 19). Escuela Superior de Guerra.

Val, G. (julio de 2011). Redressing victims of international crimes: The International Criminal Court and the Trust Fund for Victims. *Revista Internacional de Trabajo Social y Ciencias Sociales* (2), 80-98.

Veiga, A. D. (2008). *Cultivating and assessing information security culture* [Tesis de doctorado, University of Pretoria]. Institutional Repository of the University of Pretoria. https://bit.ly/3qSRzqH

Verizon. (2019). *Informe de investigaciones de violación de datos*. https://vz.to/3077820

Went, A. (1992). Anarchy is what State make of it. En *The social construction of powers politics* (pp. 245-391). International Organization.

World Economic Forum. (2017). The Global Risks Report 2017. *World Economic Forum*. https://www.weforum.org/reports/the-global-risks-report-2017

Zabala, K. (2016). *Cooperacional bilateral: caso Colombia-Brasil.* Publicaciones UNICEN.

Zaidman, E. (2017). *Seguridad informática: ¿vulnerabilidades técnicas o errores humanos?* Universidad Nacional de La Plata.

AUTORES

Lisseth Paola Salazar Narváez

Contadora pública, especialista en alta gerencia. Correo electrónico: lisseth.salazar@esdegue.edu.co

María del Pilar Niño Campos

Ingeniera de sistemas con posgrado en Auditoría de Sistemas. Magíster en Derecho Informático y Nuevas Tecnologías. Correo electrónico: mapiripan@gmail.com

Nelson Eduardo Jiménez Valencia

Abogado especialista en derecho administrativo. Correo electrónico: vanel1978@hotmail.com

Nicolás Correa Ramos

Ingeniero electrónico, profesional en ciencias navales, teniente de navío de la Armada Nacional de Colombia. Correo electrónico: nicolas.correa@armada.mil.co

Yesica Tatiana Vanegas Silva

Ingeniera de sistemas. Correo electrónico: yesica.vanegas@esdegue.edu.co; yesiicavanegas@gmail.com

El libro *Hacia la construcción del concepto de seguridad y defensa, un aporte desde la investigación formativa* compila las ponencias magistrales de magísters en geopolítica y estrategia, derechos humanos y derecho internacional humanitario y ciberseguridad y ciberdefensa, en el marco del Seminario Virtual de Resultados de Investigación Formativa, realizado el 8 de mayo de 2020, a través de la plataforma virtual Blackboard AVAFP de la Escuela Superior de Guerra. Esta publicación reúne productos resultado de investigación de los siguientes proyectos de investigación: a) "Influencia del océano en la política nacional de Colombia", del grupo de investigación "Centro de Gravedad", reconocido y categorizado en (A1) por MinCiencias, vinculado a la Maestría en Estrategia y Geopolítica; b) "Esclarecimiento de la verdad histórica sobre la violencia estructural en Colombia, provocada al medio ambiente y a las víctimas del conflicto: aporte de las Fuerzas Militares en la reconstrucción del tejido social", del grupo de investigación "Memoria Histórica, Construcción de Paz, Derechos Humanos, DICA, Justicia", reconocido y categorizado en (C) por MinCiencias, vinculado a la Maestría en Derechos Humanos y Derecho Internacional de los Conflictos Armados, y c) "Gestión de riesgos en seguridad digital para la infraestructura crítica", del grupo de investigación "Masa Crítica", reconocido y categorizado en (B) por MinCiencias, vinculado a la Maestría en Ciberseguridad y Ciberdefensa; todos los grupos adscritos y financiados por la Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia.

esdeguecol
@esdegue
Escuela Superior de Guerra
Escuela Superior de Guerra
Escuela Superior de Guerra
esdeguecol

ESCUELA SUPERIOR DE GUERRA
"General Rafael Reyes Prieto"
#Esdegue
Carrera 11 No. 102-50
Conmutador 620 4066
Bogotá, D.C., Colombia

ISO 9001:2015
BUREAU VERITAS
Certification

esdeguelibros.edu.co