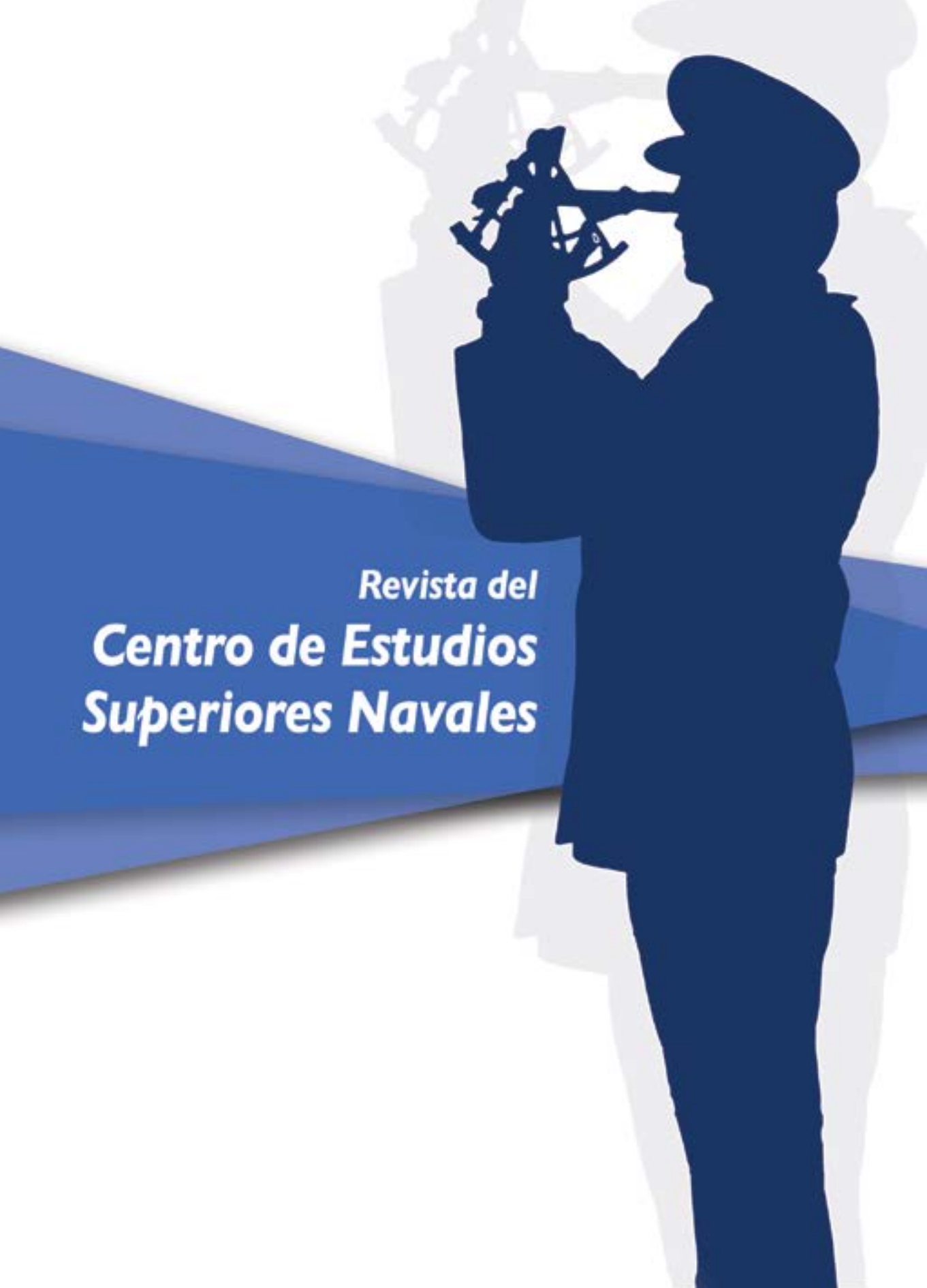
Revista del

Centro de Estudios Superiores Navales

octubre-diciembre, 2019. Volumen 40. Número 4. ISSN: 1870-5480



Revista del

Centro de Estudios Superiores Navales

Directorio

REVISTA DEL CENTRO DE ESTUDIOS SUPERIORES NAVALES. Volumen 40, No. 4, 2019, es una publicación trimestral editada por el Centro de Estudios Superiores Navales (CESNAV). Calzada de la Virgen #1800, Colonia Ex-Ejido de San Pablo Tepetlapa, Código Postal 04840, Ciudad de México. Teléfono: 555608 0847. Página web: *https://cesnav.uninav.edu.mx/cesnav/index_inicio.html*. Correos electrónicos: *cesnav.publicaciones@semar.gob.mx* o *revista.cesnav@hotmail.com*. Editor responsable: Alberto Medina Angeles. Reservas de Derechos al Uso Exclusivo Número 04-2019-072512023200-102, ISSN: 1870-5480. Certificado de Licitud y Contenido Número 14766, otorgado por la Comisión Calificadora de Publicaciones y Revistas Ilustradas de la Secretaría de Gobernación. Impresa en los talleres gráficos de la Dirección General Adjunta de Oceanografía, Hidrografía y Meteorología, de la Secretaría de Marina-Armada de México, Heroica Escuela Naval Militar, Número 861, Colonia Los Cipreses, Delegación Coyoacán, Código Postal 04830, Ciudad de México. Este número se terminó de imprimir el 30 de diciembre de 2019, con un tiraje de 500 ejemplares.

La Revista del CESNAV tiene como objetivo ser un foro abierto en el cual los miembros de la Armada de México y el personal civil interesados en temas marítimos puedan expresar sus ideas acerca de la Seguridad Nacional y temas afines al medio naval.

En caso de hacer referencia a algún trabajo de los aquí publicados, deberá de citar la fuente y el autor.

La Revista del Centro de Estudios Superiores Navales, comenzó su publicación en 1979, en idioma español. El contenido de la presente publicación refleja los puntos de vista del autor, que no necesariamente coinciden con el del Alto Mando de la Armada de México o la Dirección de este plantel.

La Revista del Centro de Estudios Superiores Navales se encuentra indexada en el Sistema Regional de Información en Línea para Revistas Científicas de América Latina, el Caribe, España y Portugal (LATINDEX), así como en la Base de Datos de Revistas de Ciencias Sociales y Humanidades (CLASE).

Consejo Editorial

Índice

Editorial

La construcción de una perspectiva holística a través de los años no solo es una cuestión de tiempo, también es constancia, un acto de perseverancia por alcanzar la excelencia, el reconocerse asimismo como un personaje de evolución constante es una motivación para el camino a la autorrealización. Los cambios son perceptibles si existe métrica y estadística en las variables. Estudiosos del tema miden en bloques temporales dichos avances, cada cantidad de años las fuentes de innovación deben ser perceptibles para que el significado de cambio tenga significante en la experiencia del inconsciente social.

El Centro de Estudios Superiores Navales esta por celebrar su aniversario 50, y su evolución es perceptible tanto en sus instalaciones, pero sobre todo en su modelo educativo. Haber iniciado con un único posgrado y ofrecer al día de hoy más de 21, es más que un logro, es un hito en la Educación Mexicana, que consagra a la Secretaria de Marina- Armada de México como una institución con un modelo con perspectiva holística educativa, la suma de todos sus centros educativos navales, lo hacen entenderse como un todo, integrándose de una forma global e integrada y no solo como la simple naturaleza de la suma de estos mismos. La Universidad Naval es el resultado de la evolución creativa del Centro de Estudios Superiores Navales.

Visión, pensamiento y mensaje, elementos palpables en cada párrafo contenido dentro de los trabajos de tesis de cada generación graduada, hablar de su formación a través de estos 50 años, merece dedicarle un número de aniversario, que está próximo a publicarse.

En esos tiempos de cambio es de destacar planteamientos que trazan interesantes panoramas científico-filosóficos. Como el artículo titulado «La inteligencia ante la cultura popular y el imaginario colectivo; expectativa y realidad» que propone que el entendimiento equivocado de aspectos de la realidad suele estar relacionado con una narrativa con la que se pretende establecer sentido y significado a hechos y procesos; esto no implica que por necesidad la narrativa sea fiel representación de la realidad a la que se refiere. Un caso de esto es el de la inteligencia, palabra con diversas interpretaciones, pero de interés para nosotros en tanto que nos indica el trabajo de dirección y planeamiento, determinación y obtención, procesamiento, análisis y producción, así como difusión y explotación para la toma de decisiones. A pesar de su importancia real, es un concepto con frecuencia mal comprendido por corresponder a una representación distorsionada por la cultura popular especialmente en el período de la Guerra Fría, así como prácticas represivas en el ejercicio de la función estatal de inteligencia. Esto ha propiciado que quienes deben tomar decisiones toman la inteligencia con ligereza o desconfianza. En nuestro país el orden jurídico basado en la Constitución, considera varios conceptos fundamentales como lo son seguridad nacional, inteligencia y contrainteligencia, y otros más que perfilan su contenido.

En este número también se presenta el trabajo del maestro Adolfo Arreola García en «Desafíos a las Estrategias de Ciberseguridad en América» quien

propone que «En el mundo hiperconectado del presente, los Estados deben contar con una estrategia que garantice el uso seguro del ciberespacio. Particularmente porque el impacto y frecuencia de los eventos que atentan contra la ciberseguridad se han multiplicado atentando no sólo contra la privacidad de los individuos, sino incluso poniendo en jaque la Seguridad Nacional. Por lo tanto, es preciso identificar las fortalezas y debilidades de los documentos rectores de la ciberseguridad en el continente americano para identificar los desafíos que enfrentan y reestimar las maneras para darles respuesta. El diseño de una Estrategia Nacional de Ciberseguridad otorga algunas de las herramientas necesarias para no solamente buscar, mantener o incrementar el ciberpoder en el nuevo campo de batalla de la era tecnológica, sino también para establecer un sistema de defensa activa.

La Doctora Mónica Rocha habla en este número del tema «El principio de la responsabilidad del superior jerárquico ante la corte penal internacional» quien escribe que «De jure o de facto, la Corte Penal Internacional con la sentencia de Bemba Gombo en 2016 equiparo obligaciones de los comandantes militares de ejércitos regulares a aquellos comandantes de Fuerzas Armadas de facto. Los criterios de responsabilidad, a saber, el nivel de conocimiento del comandante de lo que sus hombres hacen, están por hacer, hicieron o dejaron de hacer; las medidas razonables que tomo o está por tomar a fin de prevenir y/o reprimir la comisión de crímenes por parte de sus subordinados; el control efectivo que ejerce o ejerció o puede ejercer en términos reales de sus hombres a fin de evitar la comisión del injusto; así como si notifico o no a las autoridades competentes de lo que sucedió o está por suceder, se constituyen en los estándares a partir de los cuales se miden las obligaciones de los Superiores Jerárquicos.

El Superior Jerárquico no tiene responsabilidad de los crímenes que sus hombres materialmente comenten, sino porque incumplió en sus responsabilidades de mando. La actuación del comandante no se asume apriori, se debe analizar como lo ha reiterado la Corte Penal Internacional en concreto. Lo contrario sería excesivo. Las formas aiding and abetting en la omisión en el artículo 25 del Estatuto completan la presunta responsabilidad del Superior.

Como última aportación y acoplándose a la perspectiva de cambió presentada al inicio de esta editorial, la Maestría en Administración Naval promoción LVIII propone su ensayo «La evolución del Proceso Planeación en la Administración Pública Federa» que tiene como propósito determinar cómo ha sido la evolución del proceso de planeación democrática para el desarrollo de nuestro país. Así como, analizar la estructura de las rutas de navegación definidas en el Plan Nacional de Desarrollo 2019-2024 emitido por el Gobierno de México para arribar a ese puerto ideal, el desarrollo de México. Además, describe como los Programas Sectoriales coadyuvan a la planeación democrática nacional. México como un todo, puede ser comparado a un gran navío. El Titular del Ejecutivo Federal en nuestro país, es el líder que traza colegiadamente el plan de navegación que le da el rumbo a México. El Plan Nacional de Desarrollo es la carta de navegación que armoniza y foca-

liza el funcionamiento de las instituciones de la Administración Pública Federal para alcanzar las metas y objetivos nacionales. Finalmente, el Presidente de la Republica emplea su maquinaria, personificada en las dependencias y entidades de la Administración Pública Federal, para lograr el arribo a ese puerto ideal, el desarrollo de la sociedad mexicana.

Siendo esta publicación la antesala al 50 Aniversario del Centro de Estudios Superiores Navales, esta editorial recomienda plenamente el contenido del siguiente número. El cual será un homenaje a todos aquellos que colaboraron para que este Plantel sea la Máxima Casa de Estudios de la Universidad Naval.

Los cambios son inevitables, pero si estos cuentan con una base de planeación analítica y prospectiva, son parte de una estrategia evolutiva hacia un desarrollo exitoso.

La inteligencia ante la cultura popular y el imaginario colectivo; expectativa y realidad

The intelligence in light of pop culture and collective worldview; expectations and reality

Resumen

El entendimiento equivocado de aspectos de la realidad suele estar relacionado con una narrativa con la que se pretende establecer sentido y significado a hechos y procesos; esto no implica que por necesidad la narrativa sea fiel representación de la realidad a la que se refiere. Un caso de esto es el de la inteligencia, palabra con diversas interpretaciones, pero de interés para nosotros en tanto que nos indica el trabajo de dirección y planeamiento, determinación y obtención, procesamiento, análisis y produccion, así como difusión y explotación para la toma de decisiones. A pesar de su importancia real, es un concepto con frecuencia mal comprendido por corresponder a una representación distorsionada por la cultura popular especialmente en el período de la Guerra Fría, así como prácticas represivas en el ejercicio de la función estatal de inteligencia. Esto ha propiciado que quienes deben tomar decisiones toman la inteligencia con ligereza o desconfianza. En nuestro país el orden jurídico basado en la Constitución, considera varios conceptos fundamentales como lo son *Seguridad Nacional, inteligencia y contrainteligencia*, y otros más que perfilan su contenido.

Palabras clave

Narrativa, representación fiel de la realidad, inteligencia, cultura popular, Guerra Fría, ligereza, orden jurídico, *Seguridad Nacional, inteligencia, contrainteligencia*.

Abstract

The wrong understanding of aspects of reality is usually related to a narrative that seeks to establish sense and meaning to facts and processes; this does not imply that by necessity the narrative is a faithful representation of the reality to which it refers. One case of this is that of *intelligence*, a multivocal word but of interest to us as it indicates the work of collecting, analyzing and processing information for decision making. Despite its real importance, it is a concept often misunderstood for corresponding to a representation distorted by popular culture especially in the Cold War period, as well as repressive practices in the exercise of the state intelligence function. This has led decision makers to take intelligence lightly or distrustfully. In our country the legal order based on the Constitution, considers several fundamental concepts such as national security, intelligence and counterintelligence, and others that outline its content.

Keywords

Narrative, faithful representation of reality, intelligence, popular culture, Cold War, lightness, legal order, national security, intelligence, counterintelligence.

Discentes de la Especialdad en Análisis de la Información

Artículo recibido el 13 de octubre de 2019. Aprobado el 5 de diciembre de 2019.

Los errores remanentes son responsabilidad de los autores.
El contenido de la presente publicación refleja el punto de vista del autor, que no necesariamete coinciden con el del Alto Mando de la Armada de México o la Dirección de este plantel.

Hay en todas las culturas y en todos los idiomas, conceptos y palabras con las que se construyen, que se prestan a confusión por su aplicación y uso. Para ejemplificar, y a la vez dar un primer paso al desarrollo, nos referimos a *inteligencia*.

Antes, en diccionarios y enciclopedias como ahora en consultas en buscadores de internet encontramos una multiplicidad de significados del vocablo como son: *Inteligencia Financiera, Inteligencia Emocional, Inteligencia Artificial* (así, con mayúsculas)… Es hasta que uno insiste y llega a la desambiguación o relaciona la *inteligencia* con la palabra *espionaje*, donde se empieza a pisar terreno que en el primer vistazo parece firme pero en donde, a medida que se da un paso y otro, va resultando arena movediza.

Damos por sentado que para un especialista este enfoque resulta ingenuo si no es que necio, pero el propósito del trabajo es reflexionar acerca de cómo y en qué medida la actividad muy delicada, compleja y altamente especializada de ***inteligencia*** es incomprendida incluso por gente culta o que por su actividad propia debería tener nociones claras del concepto, así como de la actividad, su objeto, sus procedimientos, la evaluación y uso de sus resultados.

¿A qué se debe el desconocimiento o distorsión de lo que es la inteligencia? Una primera respuesta que cae en la obviedad: la «gente», no tiene por qué saber de qué se trata; una segunda respuesta sería: «Todo el mundo» sabe lo que significa espiar; pensemos tan solo en el alcance y la popularidad de esta actividad en el reino de lo cotidiano, al grado de que la Suprema Corte de Justicia de la Nación ha tenido que pronunciarse sobre la validez como prueba de mensajes de texto, audio o imagen obtenidos mediante artimañas, o la infinidad de información filtrada que ilustra los efectos de dejar sin contraseña el teléfono celular.

Nuestra idea de la realidad y cómo la percibimos, sin adentrarnos en discusiones teóricas propias de científicos y filósofos, depende de lo que recibimos de nuestro exterior (otras personas y el medio ambiente) y de cómo estamos constituidos; en el primer aspecto, que es el que ahora nos interesa, hablamos de cultura, entendiendo esta de manera muy amplia como un sistema mediante el cual el ser humano percibe, le confiere sentido y significado, comunica y modifica su entorno y su relación con este que abarca por supuesto sus relaciones con sus semejantes. Así, en el ámbito de la cultura, la comunidad y los individuos formulamos y utilizamos *marcos conceptuales de referencia*, es decir, conceptos y prácticas que nos permiten movernos **razonablemente bien** en el mundo de lo cotidiano. ¿Por qué enfatizamos «**razonablemente bien**»? Porque suele suceder que nuestro marco conceptual de referencia no necesariamente está construido por verdades contundentes, universales ni incuestionables; para la especie humana desde sus orígenes, desde que hubo alguna chispa de conciencia, todo a su alrededor y su propio ser requería ser identificado, nombrado y explicado; ¿cómo se dio, se ha dado y sigue dándose el conjunto de respuestas a los enigmas que enfrentamos los seres humanos, de manera que resulten más o menos convincentes, razonables, con un mínimo de sentido? A través de ***relatos***, esto es, la relación de hechos que tienen o aparentan tener sentido en conjunto y satisfacen nuestra necesidad de comprender un fenómeno.

Ahora bien, un relato de esta naturaleza contiene generalmente una mezcla de ficción y «datos duros», incluso cuando hablamos de fenómenos de carácter científico y que el lenguaje es insuficiente, como cuando se habla por ejemplo de la teoría de cuerdas, que para la mayoría no científica sugiere un universo deshilachado.

Nos hemos permitido este paseo en el bosque de las conjeturas para delimitar el problema que nos planteamos: ¿en qué medida la narrativa relacionada con el trabajo de inteligencia, producida en el campo de la ficción literaria y cinematográfica, nos genera concepciones distorsionadas o definitivamente falsas que llegan incluso a afectar el trabajo real, su desconocimiento o incomprensión de operadores, pero sobre todo de los productores y usuarios del trabajo de inteligencia?

Esto que nos planteamos no nos parece un asunto menor por lo siguiente: el llamado periodo de la Guerra Fría fue propicio para una actividad propagandística que aprovechó el miedo razonable subsistente de la Segunda Guerra Mundial respecto al «enemigo», miedo que fue alimentado en especial por los canales de difusión de ficciones como el cine y la literatura, explotando primero monstruos e invasores extraterrestres y luego, lo que nos interesa, el espionaje, los agentes secretos, las conspiraciones y la inminencia de una destrucción global.

A lo largo de este trabajo iremos ilustrando con productos cinematográficos y literarios cómo se fue construyendo la distorsión de lo que sería el trabajo de inteligencia y sus actividades correlativas, al grado de incorporarse al imaginario colectivo.

Una vez realizada la exposición y análisis de esos ejemplos, estaremos en aptitud de referirnos a algunos temas que nos parecen derivados de esta «contaminación» de un saber debido a la cultura popular o de masas que es el ámbito al que todos estamos expuestos. Entre estos temas desde ahora podemos señalar que la ***inteligencia*** ha estado injusta y equivocadamente relacionada en el imaginario colectivo al conspiracionismo delirante, la convicción de que el «secreto» y la inteligencia son propios de regímenes dictatoriales que, han basado la inteligencia en el espionaje y la denuncia en el interior de su propio territorio con el propósito de controlar y reprimir, es decir, lo que ha generado una percepción de la inteligencia como una labor incompatible con una sociedad libre y democrática.

Así, sin adelantar conclusiones, al final de este trabajo podremos enunciar a grandes rasgos lo que ***sí*** es la inteligencia, lo que se espera de esta labor y sus operadores, así como de sus productos y usuarios, es decir, este trabajo pretende contrastar expectativas (que son divertidas sin duda, incluso catárticas) y la realidad que deseamos y podemos transformar para hacerla mejor.

Es de fundamental importancia subrayar que el método a seguir para hacer un contraste idóneo entre expectativa y realidad, es anclar esta en la normatividad vigente en nuestro país donde la Ley de Seguridad Nacional define ***seguridad nacional, inteligencia, contrainteligencia*** y algunos otros conceptos, incluso un breve repaso de algunas iniciativas legislativas que han intentado acotar o ampliar estos conceptos fundamentales.

Ahora que de nuevo hay un auge de superhéroes, como que se extrañan los personajes ordinarios que se ven metidos en cuerpo y alma en situaciones extraordinarias, cómo batallan contra una adversidad que puede llevarlos incluso a morir

o, acaso en un resultado más trágico, sin una improbable resurrección sugerida en los créditos posteriores a la leyenda «The End».

También se echa de menos esos hombres y mujeres ordinarios que, porque se lo propusieron o porque asumieron las circunstancias, desarrollan capacidades propias que acaso negaban o desconocían para enfrentarse a la adversidad de la naturaleza que uno pueda imaginar; en esta categoría encontramos según lo que se plantea en este trabajo al espía, al agente secreto, generalmente hombre y ocasionalmente mujer.

Es importante subrayar el perfil básico promedio de ese tipo de personajes puesto que corresponde al hombre o mujer comunes que de alguna manera participaron en las guerras mundiales y más tarde, en la Guerra Fría. Piense el lector, de entrada, que se trata de gente ordinaria, común, como usted y nosotros, pero que se ve sometida a la necesidad de recibir un entrenamiento especial para cumplir los objetivos a enfrentar y, en su caso, aprovechar las capacidades y talentos propios de cada persona; estaremos de acuerdo en que por muchas causas, no todo el mundo puede someterse a ese entrenamiento, a esa preparación que, respecto al resto de los mortales le da cierto rasgo de *extraordinario* a quien la recibe. Es así que las guerras las pelean personas fuera de lo común, al menos en cuanto a lo que se necesita para ir a combate en condiciones que minimicen en cierto grado la probabilidad de morir en acción.

¿Qué sucede cuando hace falta cierto tipo de gente para operar en «las sombras»? Es obvio que aun en la cotidianidad, para ser aptos y elegidos deben cubrir un perfil; aquí es donde la imaginación tuerce caminos y produce espejismos.

En la memoria colectiva los recuerdos no tienen fecha de caducidad, así como tampoco permanencia garantizada; una forma de que esos recuerdos no se pierdan del todo es a través de las artes, sin perjuicio de la labor de historiadores, sociólogos, antropólogos y arqueólogos, entre otros muchos profesionales especialistas, en rescatar, clasificar, conservar y hallarle significado y sentido a indicios de tiempos pasados.

Las artes son, consideramos, la manera mas eficaz por emocional, de recuperar la memoria, de transmitirla e incluso hacer malabarismos con los recuerdos para imaginar hechos futuros probables o improbables. Las artes narrativas como la literatura, el teatro, el cine y el audiovisual (televisión, multimedia, youtube y recursos similares), al igual que los cuentos que se narraban en torno de una fogata y formaban los mitos subyacentes en la experiencia humana que la explican y le dan coherencia y sentido, siguen, hasta cuando no se nota, ciertas reglas, siendo la primera que exista un personaje protagónico que, para el propósito que nos ocupa es el espía y el agente secreto.

Un paréntesis para enfatizar la importancia de la narrativa en la formación, transmisión y consolidación de conceptos, valores, reglas en incluso sentimientos y maneras de interpretar la realidad con lo que esto conlleva en la práctica. Un ejemplo claro de la influencia de los relatos, de la narración en nuestras vidas lo encontramos en la obra del psicoanalista alemán Bruno Bettelheim «*El Psicoanálisis de los cuentos de hadas*», donde sostiene como tesis central que más aprendemos de un cuento, de un relato que de otro medio de expresión discursiva. Creemos que el planteamiento de Bettelheim tiene bases que se pueden comprobar empíricamente: ¿cuántas veces hemos adquirido conciencia de un peligro más bien por algo que nos cuentan que

por una advertencia dura y directa? Asusta más enterarse del tío que acabó escupiendo los pulmones de tanto fumar, que leer un reporte sobre tabaquismo en una revista científica, ¿o no?

Disculpe lector nuestra desviación, pero es fundamental para dejar claro que si bien espiar y el espía son una actividad y un oficio antiguos, recordemos a Sun Tzu que nos dice en el capitulo XIII de su obra *El arte de la guerra*: «La información previa no puede obtenerse de los espíritus, ni de las divinidades, ni del recuento de los acontecimientos pasados, ni de los cálculos. Se obtiene de hombres que conocen la situación del enemigo.»

Pues bien, en una época de guerra o post-bélica las fuerzas en pugna necesitan héroes o algo parecido, reales o ficticios para autojustificarse o descalificar al enemigo; esto implica una actividad de información dosificada con desinformación.

En particular, durante el periodo de la Guerra Fría las principales potencias y sus aliados recurrieron a la propaganda a través de los medios masivos de comunicación disponibles en esa época: libros y revistas, el radio, el cine y la televisión, para mostrar que había una amenaza, que esta ponía en peligro a cada persona y lo que le era más valioso y querido, al igual que conspiraba para demoler la civilización y poner a la humanidad entera en vía de extinción. ¿Cómo se planteaba el asunto? Enfrentando el bien y el mal, encarnado cada uno en un personaje, el protagónico lleno de virtudes, y el antagónico lleno de vicios; el muchacho «bueno» y «malo».

Ahora bien, ya que las circunstancias no eran las propias de un campo de batalla en regla y según los cánones de la guerra a lo grande, resultaba muy conveniente pasar el conflicto al mundo de las sombras, al de la clandestinidad: aquí es donde los espías y agentes de un bando y otro entran en acción y, lo más importante, penetran en el inconsciente colectivo.

¿Quién no conoce a *Bond, James Bond*? Personaje creado por el británico Ian Fleming basándose en su propia persona y experiencia como oficial de la Marina Británica, operador encubierto en zona enemiga en la Segunda Guerra Mundial y luego miembro de los servicios de inteligencia de su país para luego pasar a retiro y dedicarse a escribir novelas de espías en el marco de la Guerra Fría, aunque su personaje ha perdurado durante generaciones, hasta el día de mañana en que ya está anunciada una nueva película del agente 007, con licencia para matar.

Otros autores no menos conocidos o importantes han sido Eric Ambler, Somerset Maugham, Graham Greene, John Le Carré, Frederick Forsyth, mereciendo mención especial Graham Green por su novela *Nuestro Hombre en La Habana*, ya que en esta obra lleva la anécdota al absurdo más que mostrar algún dilema moral como en otros de sus trabajos, esto es, nos cuenta las peripecias de un distribuidor de aspiradoras inglés residente en la capital de Cuba en los años 50, que por ser comerciante y extranjero mantiene buenas relaciones con gente de la élite local, lo que induce a un empleado de la embajada del Reino Unido a reclutarlo como espía a cambio de una buena remuneración y gastos prácticamente libres. Aquí tenemos un anti-Bond, por supuesto.

Es cierto que la batalla propagandística alimentaba al público de todos los bandos con una mezcla de verdad y fantasía. No debe extrañar que los autores mencionados adoptaran actitudes ambiguas sobre su pasado como servidores públicos en el área de inteligencia.

Así fue que en especial durante los años 60 e inicios de los 70, proliferaró la literatura, películas y programas de televisión de espías y espionaje.

Si bien es cierto que la producción de obras de todo tipo que tenían como tema el espionaje, es decir, el enfrentamiento invisible pero que para todos estaba ahí muy a tono con la imagen común del trabajo de los servicios de espionaje y contraespionaje de los dos bloques característicos del período al que nos hemos estado refiriendo, que iban del drama hasta las comedia delirante, del *Espía que volvió del frío* (Martin Ritt, 1965) película emblemática basada en la novela del mismo nombre de John Le Carré, hasta *Casino Royale* (Val Guest y otros, 1967) con guion a partir de la novela de Ian Fleming, incluyendo la mexicana *El complot mongol* (Antonio Eceiza, 1978) cuya trama deriva de la novela de Rafael Bernal, quien relata un complot para asesinar al presidente de los Estados Unidos en una visita a nuestro país. Nada de esto impidió que la propaganda además de cumplir con su objetivo, formar en el público un temor ante la amenaza de un enemigo agazapado en la clandestinidad y los esfuerzos para vencer sus conspiraciones, se mistificara la realidad de la inteligencia, las agencias y sus operadores, de tal modo que en el imaginario popular crecieron los personajes fantásticos superhumanos, fríos, habilidosos en todos los terrenos, que lo mismo podían pilotar una avioneta que un submarino, atractivos y sexys, amorales, pero eso sí, leales a prueba de todo.

El efecto entre el público en prácticamente todos los países alcanzados por este tipo de propaganda no solo afectó a la gente común, sino también a un sector caracterizado incluso por tener una cultura superior al promedio y hasta educación universitaria.

Un ejemplo de esta distorsión nos la proporciona el novelista irlandés John Banville:

> «Boy adoraba el ceremonial del servicio secreto, los nombres en clave y los puntos de contacto, y todo lo demás. Criado a la sombra de Buchan y Henty, imaginaba su vida en los términos escabrosos de un *thriller* anticuado y a sí mismo osado protagonista de su extravagante trama, que hacía caso omiso de todos los peligros. En esa fantasía era siempre el héroe, por supuesto, nunca el malo a sueldo de una potencia extranjera.» Banville, John, *El innombrable*, Editorial Anagrama, 1999, Barcelona, p.141.

Es así que era tan eficaz la propaganda que, en esa mezcla de realidad y ficción se filtraban datos verdaderos, al grado de parecer dudosos aunque al paso del tiempo quedaron en evidencia, como se vio en los casos de Philip Agee y Víctor Marchetti, ex agentes de la Central Intelligence Agency (CIA por sus siglas en inglés), quienes sacaron a la luz pública las prácticas muchas veces reprobables de la agencia en cumplimiento de la Doctrina de Seguridad Nacional de su país que, paradójicamente extendía sus fronteras para estos efectos por todo el mundo. Más tarde, tras la caída del Muro de Berlín, con el desmoronamiento de la hegemonía soviética los países sujetos a su poder también se vieron orillados a un rápido proceso de transformación hacia la democracia liberal hasta entonces característica (aunque solo fuera en muchos casos con carácter exclusivamente nominal) del capitalismo de

occidente, resultando así que comenzaron a salir a la luz pública algunas prácticas que evidenciaron algo no nuevo, la utilización de la inteligencia, del espionaje para controlar e incluso reprimir a los habitantes del propio país. Un ejemplo de esto lo encontramos en la película alemana *La vida de los otros* (Florian Henckel von Donnesmarck, 2006), que se refiere de manera dramática a los procedimientos de la Stasi, policía política de la otrora República Democrática Alemana.

Sin duda, el efecto de este tipo de obras, insertas en el flujo de la acción propagandística gubernamental y hasta de particulares por iniciativa propia, llega hasta lo más profundo del imaginario popular que incide en el imaginario individual, personal de cada uno de nosotros, y esto incluye a nuestros dirigentes. En este orden de ideas cabe señalar otro aspecto: el desconocimiento generalizado del desarrollo del trabajo de inteligencia a través de los siglos y en todos los países.

Pero no solo la cultura popular crea modelos de representación inexactos. El historiador estadounidense Christopher Andrew, especialista en temas relacionados con temas de inteligencia y su desarrollo a través de los tiempos en todo el mundo, en su obra *The secret world, a history of intelligence* (2019), sostiene que en buena medida el desconocimiento de lo que es la labor de inteligencia, sus características e implicaciones se debe, nada menos, que a la condición «natural» en la que ese trabajo se desarrolla.

Tal ignorancia o, cuando hay conocimiento del tema pero se le mira con desdén, puede tener amplias y profundas repercusiones en la toma de decisiones de gobiernos u organizaciones privadas. A lo largo de la obra mencionada, el autor va ligando ejemplos de este fenómeno proporcionando datos puntuales, como por ejemplo cuando refiere que desde un año antes del ataque a Pearl Harbor, dada la rivalidad entre los criptoanalistas del ejército y la marina nortamericanos, desde las más altas instancias del gobierno se resolvió que de manera alternada cada grupo descodificara los telegramas diplomáticos de los japoneses; es probable que no fuera esta la causa determinante del pasmo de los estadounidenses que permitió el ataque sorpresivo de los kamikazes, pero sí revela la ligereza con la que se obró en relación con la importancia del trabajo de los servicios de inteligencia.

Otro ejemplo que proporciona Andrew, en otro sentido, el de la absoluta reserva pero con efectos similares de desconocimiento, es el del desciframiento de como funcionaban la maquina *Enigma*, ocultamiento que por razones tácticas se mantuvo en secreto durante el desarrollo del conflicto bélico, incluso dando pie a decisiones dramáticas de sacrificio para evitar que los alemanes sospecharan que su código había sido descubierto. Esto acaso permita comprender que el matemático británico Alan Turing, artífice de la proeza de neutralización del código enigma, en 1952 haya sido procesado sin miramiento alguno ni tomando en cuenta sus méritos que sirvieron para abreviar la guerra, por practicar la homosexualidad; fue hasta 2013 que el matemático fue reivindicado por la reina Isabel II, treinta años después de que el gobierno británico autorizara la salida a la luz pública de información relacionada con los esfuerzos que llevaron a descifrar el código *Enigma*.

Es con estos antecedentes y consideraciones que llegamos al momento de darle un giro al desarrollo de este ensayo, pero no sin antes señalar algunos puntos que nos parece indispensable tomar en cuenta:

- La historia ha mostrado que los individuos, las comunidades, las organizaciones y las naciones están, como siempre han estado, expuestos a amenazas y riesgos provenientes de algún ente exterior.
- Prevenir o enfrentar de manera eficiente y eficaz que la amenaza sea realizada y el riesgo se transforme en afectación real y actual, requiere conocimiento de lo que sucede en casa y/o fuera de ella, por usar un símil que incluye a individuos y entes colectivos.
- Ese conocimiento implica observación atenta para no distinguir amenazas y riesgos potenciales objetos de los imaginarios.
- De dicha observación resultan datos, mismos que requieren ser verificados, procesados para encontrarles significado y sentido, y planteados como información relevante en la toma de decisiones.
- Por otra parte, la observación en los términos a que nos estamos refiriendo, generalmente se realiza sin el conocimiento del ente de quien se pudiera esperar una condición de amenaza; obtener la información en esta situación probablemente requiera actos subrepticios de consecución de datos, sin perjuicio de obtenerlos revisando canales públicos de difusión de información que tal vez requieran un trabajo más estricto de análisis.
- El punto previo nos plantea un problema: ¿cuáles son los limites morales, éticos y legales para obtener información? A lo largo de la historia, la práctica de la tortura y diversas formas de intimidación se nos revelan como métodos extremos que no pocas veces han querido ser justificados al amparo de la tutela de un bien mayor como pudiera ser la conservación individual, comunitaria, organizacional o nacional, es decir, mantener un estado de seguridad ante cualquier amenaza.
- La historia también nos ha enseñado que el temor de ver afectada en cualquier forma nuestra seguridad individual o colectiva puede llevarnos al absurdo de imaginar conspiraciones de toda envergadura y alcance. Esto, en el caso de un Estado puede ser, desafortunadamente con frecuencia, aprovechado políticamente frente a otras naciones o instituciones internacionales, o respecto de la propia comunidad, considerando a sus integrantes en sospechosos mientras no quede acreditada su lealtad y sometimiento incluso mediante la muerte.
- Podemos reconocer en el desarrollo de los puntos precedentes que hay por una parte la inteligencia razonable y necesaria para conocer y enfrentar amenazas reales, externas o internas, y aquella que adquiere tintes de perversidad al considerar como real lo imaginario. Este punto es algo que merece conocimiento claro y, de ser posible, profundo, por parte de quienes tienen el poder de tomar decisiones y marcar rumbos, incluyendo a informadores y líderes de opinión.

Ahora sí, podemos referirnos a nuestro caso, el mexicano, contrastando las reflexiones precedentes con nuestro marco normativo constitucional, con el propósito de que en la medida de lo razonablemente viable según los alcances de un trabajo como este, podamos contribuir a la comprensión de lo que es la inteligencia y su

importancia como actividad para consolidar la seguridad nacional como máximo valor que garantiza el desarrollo institucional de la República.

Dijimos «seguridad nacional» suponiendo que casi cualquier persona medianamente informada y atenta a los noticieros en medios tradicionales o en la red tiene cierta noción de qué se trata, de lo que involucra. Sin embargo, no nos queremos atener a una suposición cuando de lo que trata este ensayo es de desmistificar conceptos, como por ejemplo «inteligencia», que para muchos y fundamentales efectos estrechamente está ligado al de «seguridad nacional». ¿En qué nos basamos para apuntar esta relación?

Ya que hemos indicado con algo de detalle cómo la « ficción» llega a distorsionar nuestra experiencia de la «realidad», pasemos ahora a revisar el terreno sobre el que se ha construido y existe nuestra realidad como país, realidad para nosotros mismos como individuos y colectividad así como para otras colectividades, realidad que encuentra su expresión en el orden constitucional. No dejaremos de insistir en que nuestra intención es dejar claro que si vamos a apartarnos de lo fantasioso, tenemos que incursionar en el terreno firme de nuestra realidad como país. Así, nos estaremos remitiendo a la Constitución Política de los Estados Unidos Mexicanos y la legislación que de este dispositivo proviene, para ver qué tan importante es para la institucionalidad comprender los alcances de realizar un trabajo permanente y sistemático de inteligencia, lejos de concepciones erróneas, en el marco de la Ley.

Asumiendo que realizar labores de inteligencia es del tipo de acciones de gobierno que tienen como propósito la preservación e integralidad del Estado mexicano, nos resultará fácil comprender que en el artículo 89, fracción VI de la Constitución Política de los Estados Unidos Mexicanos, entre las obligaciones y facultades del titular del Ejecutivo se establece la de «Preservar la seguridad nacional, en los términos de la ley respectiva, y disponer de la totalidad de la Fuerza Armada permanente o sea del Ejército, de la Armada y de la Fuerza Aérea para la seguridad interior y defensa exterior de la Federación.» Se hace notar que es en la reforma de dicha fracción, publicada en el Diario Oficial de la Federación el 5 de abril de 2004, que se adiciona la parte de «Preservar la seguridad nacional, en los términos de la ley respectiva, (…)».

Este nuevo enfoque a una de las atribuciones del Presidente de la República une cuatro elementos:

- La preservación de la **seguridad nacional**.
- La existencia de una ley en materia de **seguridad nacional**.
- La facultad de disponer de las Fuerzas Armadas…
- …para la **seguridad interior** y defensa exterior de la Federación.

Enfatizamos los dos tipos de seguridad enunciados en el texto constitucional, **nacional** e **interior**, en atención a debates recientes que parecen haber partido de la confusión respecto del significado de ambas expresiones, que no es asunto menor, nos parece, ya que en alguna medida, por lo que a *inteligencia* se refiere y lo que esta parece significar para muchas personas en la actualidad, sigue siendo objeto de malas interpretaciones.

Sin embargo, si nos remitimos a la «ley en la materia», es obligado darle un vistazo a la Ley de Seguridad Nacional (LSN), publicada en el Diario Oficial de la Federación el 31 de enero de 2005. Es en este precepto donde podemos aclarar conceptos fundamentales y altamente aclaratorios que nos permitirán acotar el significado de *inteligencia* en el ámbito de la seguridad nacional, sin perjuicio de la labor que con propósitos similares se realice en materia de **seguridad pública**.

En el artículo 3 de la LSN se establece:

> «Para efectos de esta Ley, por seguridad nacional se entienden las acciones destinadas de manera inmediata y directa a mantener la integralidad, estabilidad y permanencia del Estado Mexicano, que conlleven a:

a) La protección de la nación mexicana frente a amenazas y riesgos que enfrente nuestro país;
b) La preservación de la soberanía e independencia nacionales y la defensa del territorio;
c) El mantenimiento del orden constitucional y del fortalecimiento de las instituciones democráticas de gobierno;
d) El mantenimiento de la unidad de las partes integrantes de la Federación señaladas en el artículo 43 de la Constitución Política de los Estados Unidos Mexicanos;
e) La defensa legítima del Estado Mexicano respecto de otros Estados o sujetos de derecho internacional, y
f) La preservación de la democracia, fundada en el desarrollo económico, social y político del país y sus habitantes.»

En complemento de lo que se dice en el artículo 3 de la LSN, el artículo 5 señala: «Para los efectos de la presente Ley, son amenazas a la seguridad nacional:

1. Actos tendentes a consumar espionaje, sabotaje, terrorismo, rebelión traición a la patria, genocidio en contra de los Estados Unidos Mexicanos dentro del territorio nacional;
2. Actos de interferencia extranjera en los asuntos nacionales que puedan implicar una afectación al Estado Mexicano;
3. Actos que impidan a las autoridades actuar contra la delincuencia organizada;
4. Actos tendentes a quebrantar la unidad de las partes integrantes de la Federación, señaladas en el artículo 43 de la Constitución Política de los Estados Unidos Mexicanos;
5. Actos tendentes a obstaculizar operaciones militares o navales contra la delincuencia organizada;
6. Actos en contra de la seguridad de la aviación;
7. Actos que atenten contra el personal diplomático;
8. Todo acto tendente a consumar el tráfico ilegal de materiales nucleares, de armas químicas, biológicas y convencionales de destrucción masiva;
9. Actos ilícitos en contra de la navegación marítima;
10. Todo acto de financiamiento de acciones y organizaciones terroristas;
11. Actos tendentes a obstaculizar o bloquear actividades de inteligencia o contrainteligencia, y

12. Actos tendentes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos.»

Como es notorio, el catálogo de amenazas a la seguridad es amplio y comprehensivo.

En cuanto a la **inteligencia para la seguridad nacional**, la LSN destina un Título Tercero, cuyo Capítulo I, De la información y la inteligencia, en el artículo 29 dice que «Se entiende por inteligencia el conocimiento obtenido a partir de la recolección, procesamiento, diseminación y explotación de información, **para la toma de decisiones en materia de seguridad nacional**.»

Es tomar en cuenta que en este precepto se hace referencia al crimen organizado como una amenaza potencial o real a la seguridad nacional, pero debemos ser cuidadosos de no saltar a conclusiones apresuradas: nuestro orden jurídico constitucional da mucha claridad respecto a las tareas que le corresponden al Estado en cuanto a seguridad pública, persecución de los delitos y administración de justicia en materia penal, así que la relación que se da entre el problema del crimen organizado y su inserción en el campo de la seguridad nacional es complementaria no en términos de sustitución de las instancias responsables de la prevención del delito, la procuración y la administración de justicia, esto es, la actividad de inteligencia desde la perspectiva de la seguridad nacional tiene como uno de sus objetivos propiciar la sana actividad institucional de la República sin perjuicio de no interferir con los entes responsables.

Más aún, la Carta Magna es precisa en cuanto a qué entes de la administración pública tienen la responsabilidad de actuar en temas de delincuencia común u organizada; asimismo, establece los procedimientos que deben seguir en su actuación como es en el Código Nacional de Procedimientos Penales.

Así, podemos establecer que la inteligencia en el ámbito de la seguridad pública está orientada a prevenir, por una parte, la actividad delictiva con el complemento de acciones de carácter disuasivo y, por otra parte, habiéndose cometido un delito, para establecer la realidad de éste y la probable responsabilidad de a quien se le atribuye su comisión. Esto implica que los protocolos derivados de la observancia de la legislación penal enfaticen de manera rigurosa que la actuación de la autoridad no debería presentar fallos que resulten en que no se pueda sancionar al responsable y hacer justicia para la víctima.

En cuanto a la orientación de la inteligencia en el campo de la seguridad nacional, no tiene como propósito prevenir ni sancionar el delito en ninguna modalidad, sino detectar todo aquello que de alguna manera ponga en peligro los ámbitos interno y externo la integralidad del Estado Mexicano, entendiendo que muchas de estas amenazas pueden implicar actos tipificados como de carácter penal, como por ejemplo el terrorismo y el sabotaje, o el impedir acciones de inteligencia y contrainteligencia en relación del crimen organizado, realizadas no tanto para constituir elementos de prueba sostenibles en un proceso penal, sino contener y en su caso desarticular hechos y circunstancias propicios para la actuación del crimen organizado; sin duda, esta perspectiva especial de la inteligencia en seguridad nacional complementa de manera muy importante, en ocasiones fundamental, lo que se realiza en el campo de la seguridad pública y la administración de justicia.

Por otra parte, cuando nos detenemos en la cuestión del crimen organizado no es desviándonos del propósito general de la inteligencia en el contexto de la seguridad nacional, sino porque desafortunadamente, el fenómeno ha adquirido magnitudes que probablemente ya se vislumbraban desde el cambio de milenio. Sin embargo, esto ilustra con claridad la importancia real que debe concedérsele a la inteligencia para sustentar decisiones de diferente calado pero de trascendencia para nuestro país.

Nos hemos permitido las extensas transcripciones de algunos preceptos porque consideramos que no siempre es conocido su contenido por quien debiera estar consciente del significado que para un Estado tiene el saber qué sucede de relevante que pueda afectarlo en lo interior y desde el exterior. Pensamos en servidores públicos pero también en comunicadores y líderes de opinión quienes, como propusimos al inicio de este trabajo, acaso compartan la mistificación de los que es la inteligencia, la seguridad nacional, la seguridad interior y la seguridad pública; veamos, por ejemplo la fallida Ley de Seguridad Interior que ahora está deshabilitada por vicios constitucionales fuertes.

Es cierto que en algunos regímenes y en lugares y épocas diversos la idea de seguridad interior ha sido ampliada para justificar paranoias y conspiracionismos, pero si como en el caso mexicano atendemos a nuestro orden jurídico que regula y acota la actuación de los órganos del Estado, que atendiendo a la observancia de tratados internacionales prescribe que dicha actuación debe observar y respetar los Derechos Humanos, podemos apostarle a que un buen trabajo de inteligencia de parte de las instancias autorizadas para realizarla puede, si es tomada en serio por quien deba aprovecharla, cimentar decisiones correctas para beneficio de México.

El Estado Mexicano enfrenta grandes desafíos, propios de los cambios que hemos podido observar en la historia del mundo en los últimos cien años; en este lapso, el estatus de potencias hegemónicas se ha transformado de manera vertiginosa dando lugar a esferas de influencia variables al paso del tiempo; las tecnologías de la información y la comunicación también han experimentado un desarrollo asombroso y aparentemente sin límites que modifica incluso nuestra percepción y consciencia de nosotros mismos y nuestro entorno. Adicionalmente, si lo económico ha sido la fuerza impulsora de Estados, corporaciones e individuos, esa fuerza se ha despojado de cualquier vestidura que disimule su rapacidad y se muestra en toda su crudeza, llevando esto a una competencia sin piedad por el dominio de los mercados de bienes y servicios, es decir, por alcanzar nuevas formas de hegemonía que pueden hacer tambalear la soberanía de un Estado nacional.

Frente a un entorno como este que se esboza, garantizar la seguridad nacional requiere que la labor de inteligencia y sus operadores además de incorporar nuevas tecnologías, vean con nuevos ojos que vivimos una realidad compleja, volátil y mutable, pero que, gracias a la inteligencia puede ser abordada y comprendida.

Referencias

- Andrew, Christopher, The secret world, A history of intelligence, Londres RU, Penguin Books, 2019.
- Banville, John, El intocable, Barcelona, Editorial Anagrama, 1999.
- Bettelheim, Bruno, Psicoanálisis de los cuentos de hadas, Barcelona, Crítica, 1994.
- Tzu, Sun, El arte de la guerra, Madrid, Editorial Fundamentos, 1981.

Bibliografía

- Bobbio, Norberto, Democracia y secreto, México, Fondo de Cultura Económica, 2013.

Desafíos a las Estrategias de Ciberseguridad en América
Challenges to Cybersecurity Strategies in America

Resumen

En el mundo hiperconectado del presente, los Estados deben contar con una estrategia que garantice el uso seguro del ciberespacio. Particularmente porque el impacto y frecuencia de los eventos que atentan contra la ciberseguridad se han multiplicado atentando no sólo contra la privacidad de los individuos, sino incluso poniendo en jaque la seguridad nacional. Por lo tanto, es preciso identificar las fortalezas y debilidades de los documentos rectores de la ciberseguridad en el continente americano para identificar los desafíos que enfrentan y reestimar las maneras para darles respuesta. El diseño de una Estrategia Nacional de Ciberseguridad otorga algunas de las herramientas necesarias para no solamente buscar, mantener o incrementar el ciberpoder en el nuevo campo de batalla de la era tecnológica, sino también para establecer un sistema de defensa activa.

Palabras clave

Seguridad Nacional, Ciberestrategia, Ciberseguridad Nacional, Ciberpoder, Ciberespacio

Abstract

In the current hyperconnected world, States must have a strategy that guarantees the use of cyberspace with security. Particularly because the impact and frequency of the events which attends against cybersecurity have been multiplied threatening not only the individual privacy, but also putting the national security in check. Therefore, it is necessary to identify the strengths and weaknesses of the cybersecurity guide documents in the American continent in order to identify the challenges that they face and re-estimate the manners for giving them an answer. The design of a National Cybersecurity Strategy provides some of the necessary tools to not only seek, maintain or increase the cyberpower in the new battlefield of the technological era, but also to establish an active defense system.

Key words

National Security, CyberStrategy, National Cybersecurity, Cyberpower, Cyberspace

Maestro
Adolfo Arreola García

Es profesor investigador en la Universidad Anáhuac México Norte y profesor en la Facultad de Estudios Superiores Acatlán, de la Universidad Nacional Autónoma de México (UNAM). De igual manera se desempeña como consultor independiente en ciberseguridad estratégica. Sus líneas de investigación se enfocan en temas de seguridad nacional, ciberseguridad en todos los ámbitos y tecnología aplicada a la seguridad nacional. Es doctorando del Doctorado en Seguridad Internacional de la Universidad Anáhuac México Norte.

correo: adolfoarreola@yahoo.com.mx

Artículo recibido el 20 de octubre de 2019. Aprobado el 5 de diciembre de 2019.

Los errores remanentes son responsabilidad de los autores.
El contenido de la presente publicación refleja el punto de vista del autor, que no necesariamete coinciden con el del Alto Mando de la Armada de México o la Dirección de este plantel.

Metodología

El presente trabajo se basa en el análisis literario, de discurso e histórico de diversos documentos oficiales, académicos, gubernamentales, tecnológicos y mediáticos que permiten abordar el tema desde perspectivas teóricas y mediático-realistas, es decir desde los acontecimientos que ocurren en el día a día. Lo anterior teniendo por objetivo la correlación de los acontecimientos cotidianos con la explicación teórica de los mismos; ya que la historia, al ser fuente esencial de información, presenta una serie de indicadores y eventos recurrentes que permiten anticiparse a los hechos aplicando los preceptos teóricos.

En la estrategia todo resulta muy simple, pero no por ello muy fácil.
Carl von Clausewitz

Introducción

En el mundo hiperconectado de la actualidad es imperativo contar con una estrategia para obtener las mayores ventajas y sufrir los menores daños en las operaciones diarias en el ciberespacio. Esta necesidad estratégica ha evolucionado debido a que en años recientes el número de incidentes que comprometen la ciberseguridad de los Estados ha ido en aumento poniendo en riesgo la integridad de la información, la confiabilidad de la red, la seguridad de los usuarios y la ciberseguridad nacional. El impacto de los ciberataques ha cruzado el Rubicón entre el mundo material y el virtual (Johnson y Tierney, 2011). A pesar de los numerosos métodos de ataque, las amenazas provienen de dos categorías de eventos adversos que podrían encajonarse en: 1) operaciones de ciberguerra y 2) actividades del cibercrimen.

Por un lado, de acuerdo con Manuel R. Torres (2010: 339) las acciones bélicas (ciberataques) icónicas de las últimas décadas son: la explosión en el sistema de distribución de gas en la Unión Soviética en 1982, el ciberataque contra empresas estadounidenses conocido como *Titan Rain* entre 2003 – 2005, el ciberataque contra Estonia del 2007, el ciberataque contra las defensas aéreas de Siria en 2007, las acciones de ciberguerra durante la guerra en Osetia del Sur en Georgia durante el 2008 y el ciberataque con Stuxnet contra el programa nuclear iraní descubierto en 2010. En general, los efectos y poder destructivo de la ciberguerra (entendido como conflicto entre fuerzas de dos Estados) se logra por medio de la manipulación de los sistemas de control y por el engaño de las ciberdefensas; es evidente, que la superioridad en el ciberespacio brinda la libertad de acción y la ventaja ofensiva por medio de la sorpresa.

Por el otro lado, en 2016, un informe conjunto de la Organización de los Estados Americanos (OEA) y del Banco Interamericano de Desarrollo (BID) señaló que el cibercrimen cuesta al mundo 575,000 millones de dólares lo que equivale a un 0.5% del PIB mundial. De esta cantidad el monto total correspondiente para América Latina es de 90,000 millones de dólares anuales (BID y OEA, 2016). El cibercrimen

engloba acciones como: la suplantación de identidad, el robo de información o de capitales, la venta de productos y servicios ilegales en internet, la pornografía infantil, el grooming, el ciberespionaje, entre muchas otras.

Sin importar si los eventos cibernéticos adversos son efectuados por Estados, organismos o individuos estos conllevan una serie de características particulares que han contribuido a su proliferación. Entre otras cosas, los ataques en el ciberespacio son de bajo costo, difíciles de rastrearse y no pueden ser atribuidos de manera precisa, lo que los convierte en una alternativa para generar daños importantes contra un enemigo sin ser castigado o ni siquiera ser identificado/detectado. Por lo tanto, para evitar ser culpados, algunos Estados inclusive han recurrido a la creación de grupos paramilitares o hacktivistas que sumados a los cibermercenarios han realizados acciones en favor de sus intereses sin establecer un vínculo identificable de manera fácil, precisa y oportuna.

Ante esta realidad compleja, en la cual la atribución de los ataques es la principal limitante para la respuesta de la víctima, los Estados en América cuentan con una capacidad de respuesta ya instalada. Sin embargo, solamente 10 han diseñado una estrategia de ciberseguridad nacional para proteger el ciberespacio y en su caso contar con elementos suficientes de ciberpoder.

El objetivo del presente trabajo es destacar los desafíos que enfrentan las diez primeras Estrategias de Ciberseguridad que se han aprobado en el Continente Americano poniendo énfasis en los aspectos técnicos, administrativos, de atribución, organizacionales y de recursos humanos necesarios para la lograr seguridad en el ciberespacio. Del mismo modo se hará referencia a las estructuras institucionales a cargo de la implementación y seguimiento de las distintas Estrategias. Todo lo anterior representa un ejercicio para identificar y mitigar los potenciales riesgos que pudieran surgir por un diseño inadecuado de los documentos rectores de la ciberseguridad nacional de los Estados.

El trabajo incluye primeramente una revisión de las características del ciberespacio y el ciberpoder, así mismo una propuesta de definición de ciberseguridad nacional a fin de establecer su importancia dentro de las Estrategias Nacionales de Ciberseguridad; posteriormente, se detallan las características de las Estrategias Nacionales vigentes en el continente americano; en el tercer apartado se definen algunos de los muchos desafíos que enfrentan las estrategias de ciberseguridad de los Estados de América y, finalmente; se presentan algunas conclusiones sobre el tema.

El ciberespacio, el ciberpoder y la ciberseguridad nacional

Ciberespacio

El ciberespacio ha sido considerado como el quinto ámbito de la guerra (Lynn, 2010) por lo tanto las operaciones militares se realizan utilizando el ciberespacio no solamente como el medio por excelencia, sino también como el campo de batalla (Arreola, 2016). De hecho, de acuerdo con Arreola (2016: 109) «el ciberespacio se ha convertido en un ámbito de la guerra en donde las vulnerabilidades del enemigo

son explotadas sin necesidad de la fuerza» ya que la tecnología, la información y el espectro electromagnético se convierten tanto en armas de ataque y destrucción de largo alcance y omnipresentes que ponen en práctica el ciberpoder, como en los medios esenciales para instalar una defensa en profundidad de la información e instalaciones críticas.

Es decir, sin importar si las operaciones en el ciberespacio son ofensivas o defensivas, según marque la estrategia de ciberseguridad nacional, el ciberespacio será la constante. En otras palabras, el ciberespacio facilita que los eventos bélicos escalen desde un ámbito regional a uno global, debido ya sea a daños colaterales en las actividades o ciberinfraestructuras internacionales, o por su capacidad para movilizar a los gobiernos y a la opinión pública mundial. De acuerdo con David Betz and Tim Stevens (2011: 39) la ocurrencia simultánea de la causa y el efecto en el ciberespacio tiene ramificaciones en el ejercicio del poder, ya que a pesar de la distancia física el efecto es casi inmediato permitiendo que el número de actores afectados por el ciberpoder se multiplique. Siendo el ciberespacio además una creación humana, es preciso reconocer las capas que lo componen para el reconocimiento de sus detalles. De acuerdo con Martin Libicki (2009: 12 y 13) el ciberespacio se compone de tres capas: física, sintáctica y semántica.

- En la capa física se integran todas los componentes y cableado, esta capa es esencial para la existencia del ciberespacio porque si se remueve desaparece el ámbito virtual.
- La capa sintáctica está compuesta por las instrucciones que tanto los diseñadores como los usuarios dan a las máquinas, así como por los protocolos que utilizan las computadoras para interactuar entre sí. Es nuestra visión que es en esta capa donde los hackeos tienen lugar y los ataques virtuales o ciberataques pueden realizarse con mayor impacto debido al uso del engaño, la invisibilidad y la sorpresa.
- La capa superior es la semántica que es donde se encuentra la información que se encuentra en la máquina en forma clara o en lenguaje de programación.

De hecho, la información que se encuentra en las computadoras se puede clasificar en aquella que sirve para manipular el sistema, aquella que controla a las máquinas y la información para el usuario. En otras palabras, una parte de la información que se encuentra en las computadoras sirve para manipular el sistema (aunque es sintáctica en su propósito es semántica en su forma), otra información incluye instrucciones o control de procesos que sirve para el control de las máquinas o procesos controlados por computadora y, finalmente; el resto de la información tiene significado únicamente para las personas ya que se encuentra en un lenguaje claro.

Además, el ciberespacio tiene una serie de características principales que permiten sentir sus efectos no sólo dentro del ciberespacio, sino en el resto de los ámbitos de la guerra y por ende en el ser humano. De acuerdo con John Sheldon (2011: 96-100) las principales características del ciberespacio son que: depende del espectro electromagnético, requiere de objetos fabricados por el hombre, puede ser constantemente replicado, es de bajo costo, la ofensiva es predominante, y consiste de cuatro capas (lo que complementa lo que fue afirmado por Libicki al agregar una capa para la infraestructura), todo lo anterior permite que el ciberpoder sea ubicuo/generalizado, complementario y furtivo.

Figura 1. Elementos del ciberespacio

Elaboración propia

Aunque el ciberespacio es el cúmulo de tecnologías desarrolladas por la sociedad de la información que ha revolucionado los asuntos militares y todas las actividades sociales, difiere de sus predecesores tecnológicos porque de acuerdo con Daniel T. Kuehl (2009: 28) se ha convertido en el medio predominante para crear, almacenar, modificar y explotar la información. Lo que remarca su diferencia con los anteriores dispositivos electrónicos que solamente transmitían y recibían información. Estas características han llevado a que las tecnologías de la información y comunicación permeen todas las actividades generando nuevas vulnerabilidades y creando el contexto estratégico para el empleo del ciberpoder. Sheldon (2011: 101) dice que «Esta expansión, profundización y dependencia cada vez más generalizada del ciberespacio es parte del mosaico del cambiante entorno geopolítico y económico mundial» que conforma el contexto estratégico internacional actual en donde el ciberpoder tiene y tendrá un papel preponderante.

Ciberpoder

A nivel global se están dando nuevos alineamientos geopolíticos que de acuerdo con Philip Stephens darán lugar a un mundo multipolar. En las palabras de Stephens (2010) esto es:

> Un mundo multipolar ha sido pronosticado durante mucho tiempo, pero siempre pareció estar posado con seguridad en el horizonte. Ahora se ha precipitado de repente al presente. . . La forma perezosa de describir el nuevo paisaje geopolítico es una disputa entre Occidente y el resto: entre las democracias liberales occidentales y las autocracias de economía de mercado oriental. A pesar de lo ordenadas que pueden parecer estas divisiones, extrañan las complejidades. Ninguno está más determinado, por ejemplo, que Rusia y China para evitar que India obtenga un asiento permanente en el Consejo de Seguridad de la ONU. Pocos están más preocupados que India por el crecimiento militar de China. . . Las naciones en ascenso premian el poder estatal sobre las

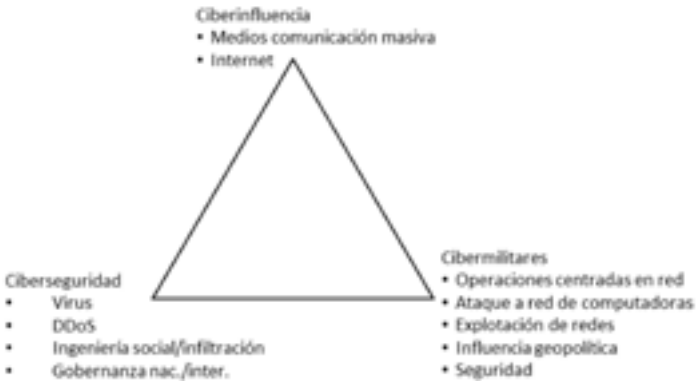
> reglas internacionales, la soberanía sobre el multilateralismo. Es probable que la transición a un nuevo orden vea más rivalidad y competencia que cooperación. Los hechos de la interdependencia no pueden ser desechados, pero ciertamente serán probados. Va a ser un viaje lleno de baches.

Es evidente que existe una lucha en el contexto internacional para modificar el juego geoestratégico. Sin duda, el «ciberpoder se puede utilizar en la paz y la guerra porque, entre sus muchos otros atributos, es sigiloso y encubierto, relativamente barato, y su uso favorece la ofensiva y es difícil de atribuir al autor» (Sheldon, 2011: 101) y se convertirá en una ventaja comparativa para los Estados técnicamente avanzados. Lo que se ve apoyado por el pensamiento de Bertrand Rusell (2004: 23) que dice que el poder debe ser visto como «la producción de los efectos pretendidos» que sería la percepción de los estrategas que piensan que la estrategia es desatar el poder inherente en las capacidades nacionales para que impacten en los resultados del interés nacional que compite con el resto de los actores de la sociedad internacional.

En el caso del ciberpoder, de acuerdo con Betz y Stevens (2011: 45-51) este se clasifica en obligatorio (uso directo de la coerción), institucional (control indirecto de actores por medio de las instituciones), estructural (mantiene las estructuras entre actores) y, productivo (produce y refuerza los discursos existentes – quizás el más importante de todos debido a la diplomacia pública y comunicación estratégica). La recomendación es utilizar las diversas formas combinadas en una fórmula flexible, dinámico y eficiente; es decir, «Sólo un trato redondeado de las diversas formas de ciberpoder proporcionará una base adecuada para otras consideraciones de lo que podría constituir el ciberpoder nacional como un componente integral de la estrategia nacional» (Betz y Stevens, 2011: 53).

En breve, el ciberpoder es la manifestación del poder en el ciberespacio, en donde el poder se entiende de acuerdo con Max Weber (Gerth y Mills, 1948: 180) como «la oportunidad de un hombre o de varios hombres de realizar su propia voluntad en una acción comunitaria, incluso contra la resistencia de otros participantes de la misma acción». Las actividades del ciberpoder incluyen: la ciberinfluencia, las operaciones cibermillitares y la ciberseguridad.

Figura 2. Actividades de ciberpoder



Ciberseguridad Nacional

Desde el punto de vista de la seguridad nacional, junto con la dependencia en las TIC en los diversos ámbitos del desarrollo de los Estados, existe una necesidad creciente de verificar la implementación segura de los sistemas cibernéticos en campos como la salud, la educación, los servicios gubernamentales o la industria; es decir, se deben construir capacidades para la ciberseguridad y la ciberdefensa con base en políticas públicas de largo alcance, así como en instituciones de carácter permanente que den vida a un sistema de ciberseguridad nacional. (Cano, 2011; Artiles, 2011; y Lynn, 2010).

Por lo tanto, ya que en el contexto internacional del siglo XXI las tecnologías de la información y comunicaciones tienen un papel preponderante, es preciso contar con un concepto y una estrategia[1] de ciberseguridad nacional que implementen acciones políticas y jurídicas para salvaguardar los recursos materiales en todos los ámbitos de combate[2] con un enfoque multidisciplinario, multidimensional y multinivel. Esta propuesta se hace como parte integral de la reconceptualización de la seguridad nacional e internacional que permite incorporar nuevos, ámbitos, actores, factores, temas y condiciones (Dalby, 1997).

Por ello, partiendo del concepto de ciberseguridad diseñado por la Unión Internacional de Telecomunicaciones (UIT, 2010) se propone que la ciberseguridad nacional se entienda como: las 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 informáticos de la nación, resguardar la infraestructura crítica o activos estratégicos, implementar la ciberseguridad pública, organizar la ciberdefensa, proteger la información y cuidar a los usuarios en el ciberentorno contra amenazas internas o externas. Que establece la división de la ciberseguridad nacional en dos ramas: la ciberseguridad pública (cibercrimen) a cargo de los organismos policiales y la ciberdefensa (ciberseguridad nacional) responsabilidad de las fuerzas armadas.

Las Estrategias Nacionales de Ciberseguridad en América

Ante la realidad que se vive en el mundo digital y los efectos crecientes de los ciberataques, hasta principios de 2018, en la región de América Latina y el Caribe un total de ocho países habían adoptado una Estrategia Nacional de Ciberseguridad. A los ocho anteriores hay que sumarles a EE.UU. y Canadá en la región de América del Norte (sin contar a México). Según Leiva (2015) el hecho de que para 2015 sólo seis Estados de América Latina hayan adoptado una Estrategia Nacional de Ciberseguridad fue resultado de dos factores que impidieron su adopción: primero, la falta de recursos dedicados a este tema; y segundo, la falta de experiencia práctica y conocimientos especializados para diseñar e implementar una estrategia nacional con eficacia. No obstante, la Organización de Estados Americanos (OEA) ha jugado un papel preponderante en lo que se refiere al apoyo técnico, y en casos como México también en apoyo administrativo.

1 La propuesta para el concepto de estrategia es: serie de acciones meticulosamente estudiadas y proyectadas encaminadas a lograr un fin determinado. Aunque se deriva del uso militar, todas las acciones del hombre están llenas de ella, porque es la aplicación de la inteligencia, el conocimiento y el raciocinio.

2 Existen cinco ámbitos del combate o de la guerra: aire, mar, tierra, espacio y ciberespacio.

Las Estrategias se enmarcan en la resolución de la OEA AG/RES. 2004 (XXXIV-O/04) denominada «Adopción de una estrategia interamericana integral de seguridad cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética» y la declaración sobre el «Fortalecimiento de la Ciberseguridad en las Américas» en marzo de 2012. De igual forma buscan cumplir con tratados internacionales como la Convención de Budapest que fue publicada en 2001.

Como se dijo anteriormente, hasta inicios de 2018, en América Latina y el Caribe eran ocho los Estados con una Estrategia Nacional de Ciberseguridad. El último en presentar su estrategia fue México (13 noviembre de 2017), uniéndose a Colombia (2011 y 2016), Panamá (2013), Paraguay (abril de 2017), Chile (abril de 2017) y Costa Rica (abril de 2017). Los dos países del Caribe que cuenta con una Estrategia Nacional de Ciberseguridad son Trinidad y Tobago (2013) y Jamaica (2015). Sin duda, tanto EE.UU. (2003) y Canadá (2018) son líderes en la región de América del Norte en el diseño e implementación de sus estrategias respectivas. En resumen, en 2017 solamente 10 Estados del total del Continente Americano contaban con una estrategia de ciberseguridad, lo que denota la poca consideración que se le da al tema en dicha esfera geográfica a pesar del incremento en el número e impacto de los ciberataques. En junio de 2018 Guatemala y República Dominicana publicaron su Estrategia Nacional de Ciberseguridad, pero no serán incluidas. Brasil no tiene estrategia, pero cuenta con una política robusta en temas de ciberseguridad.

América del Norte

Canadá

Una versión inicial fue creada el 2010. Ahora la Estrategia Nacional de Ciberseguridad cuenta con una versión que fue presentada en 2018 (Department of Public Safety and Emergency Preparadness, 2018). Busca atender los riesgos que han llegado con el uso intensivo de la tecnología en la vida diaria, creando confianza en el mundo digital con un sistema de ciberseguridad que acompañe a la innovación y sea el protector de la prosperidad. La Estrategia busca cumplir con los objetivos y prioridades de los canadienses en materia de ciberseguridad. La Estrategia de Canadá cuenta con tres pilares de acción: dar seguridad a los sistemas gubernamentales, hacer sociedad fuera del gobierno federal para asegurar los sistemas cibernéticos vitales y, ayudar a la sociedad canadiense a estar segura cuanto trabaja en línea. Menciona también los siguientes objetivos estratégicos: dar seguridad y resiliencia a los sistemas canadienses, innovación en cuestiones cibernéticas, así como liderazgo y colaboración.

La Estrategia canadiense menciona que existen tres tendencias que representan las áreas que deben ser fortalecidas para garantizar la ciberseguridad nacional. La primera tendencia engloba el apoyo al esfuerzo de las agencias de aplicación de la ley para combatir el cibercrimen al mismo tiempo que se respeta la privacidad; la segunda, menciona la necesidad imperiosa de contar con personal profesional con mejor conocimiento y habilidades en cuestiones de ciberseguridad; y la tercera, pide

el liderazgo absoluto del gobierno federal para impulsar la cooperación nacional, las inversiones, salvaguardar la información, cuidar los derechos humanos y las libertades de los ciudadanos.

De acuerdo con la Estrategia Nacional de Ciberseguridad de Canadá (2018) los principales desafíos que enfrenta son: el incremento del número de ciberataques y su impacto en los diferentes sectores del quehacer humano, el dilema que existe para brindar seguridad sin afectar la privacidad ya que la libertad requiere tanto de seguridad como de privacidad, y la reorganización de sus fuerzas para integrar un solo centro de mando y control. Por lo tanto, el gobierno canadiense propone generar un cultura de la ciberseguridad a nivel nacional, fortalecer los sistemas de ciberseguridad bajo control del gobierno, mejorar las capacidades de reacción de las fuerza pública para mitigar el impacto de los eventos cibernéticos adversos y responder al cibercrimen, procurar que los medios para lograr un sistema de ciberseguridad en todos los niveles y sectores productivos estén disponibles a precios accesibles, y aplicar las capacidades cibernéticas del gobierno para implementar una defensa activa de la infraestructura crítica. Para dar cumplimiento a los objetivos se tiene al Centro de Ciberseguridad de Canadá, la Unidad Nacional de Coordinación sobre Cibercrimen, que trabajan en conjunto con el Department of Public Safety and Emergency Preparadness.

EE.UU.

La Estrategia Nacional para asegurar el Ciberespacio (2003) es parte de esfuerzo nacional de EE.UU. para proteger su nación que fue presentado por el presidente George W. Bush. Define que el buen funcionamiento del ciberespacio es esencial para la economía y la seguridad nacional. Tiene como propósito involucrar y capacitar a los estadounidenses para asegurar las partes del ciberespacio que poseen, operan, controlan o con las que interactúan. Menciona tres objetivos estratégicos: prevenir ciberataques contra la infraestructura crítica estadounidense, reducir la vulnerabilidad nacional a ciberataques y, minimizar el daño y el tiempo de recuperación en caso de sufrir un ciberataque.

Esta estrategia posteriormente evoluciona con el presidente Barack Obama dando lugar a la Cyberspace Policy Review (2009), International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World (2011), Draft Strategy for Improving Critical Infrastructure Cybersecurity (2014), President's Executive Order on Drawing up a Strategy for Improving Critical Infrastructure Cybersecurity (2013) y, The Department of Defence Cyber Strategy (2015). El último de los documentos mencionados será considerado como la última versión de un esfuerzo nacional para garantizar la ciberseguridad (Carter, 2015). Actualmente, aunque cuenta con una amplia legislación sobre ciberseguridad no cuenta con una Estrategia Nacional de Ciberseguridad (Starks, 2018).

La ciberestrategia del Departamento de Defensa (DoD) tiene los siguientes objetivos estratégicos: Construir y mantener las fuerzas y capacidades listas para realizar operaciones en el ciberespacio; defender la red de información del DoD, asegurar los datos del Departamento de Defensa y mitigar los riesgos para las mi-

siones del Departamento de Defensa; estar preparado para defender a EE. UU. y sus intereses vitales contra ciberataques disruptivos o destructivos de consecuencias importantes; crear y mantener opciones cibernéticas viables y planificar el uso de esas opciones para controlar la escalada de conflictos y configurar el entorno de conflicto en todas las etapas; y crear y mantener asociaciones y alianzas internacionales sólidas para disuadir las amenazas compartidas y aumentar la seguridad y la estabilidad internacional.

La estrategia de seguridad de EE.UU. menciona que para ganar la superioridad estratégica se debe obtener el control del ciberespacio. Particularmente, la Estrategia Militar Nacional para las Operaciones Cibernéticas de 2005 menciona de manera explícita que «es una aproximación estratégica amplia para emplear las ciberoperaciones con el objetivo de asegurar la superioridad estratégica para EE.UU. en dicho dominio» (DoD, 2005: vii). La superioridad en el ciberespacio brindará la libertad de acción a las fuerzas amigas y la negará al enemigo. Es decir, el ciberespacio es un medio eficaz para lograr la superioridad estratégica tan necesaria para avanzar o lograr los objetivos políticos. A lo anterior hay que agregar los imperativos estratégicos que son definidos por el DoD (2005: 10) como «las consideraciones que se deben tomar en cuenta para operar exitosamente en el ciberespacio». Estos imperativos son: operaciones ofensivas/defensivas, integración, compartir información, habilidad para operar en situación degradada, relaciones de mando, mando y control, configuración de la gestión, aplicación de políticas y normas, comprender el ciberespacio y la defensa de EE.UU.

Lo anterior coincide con la visión de Sheldon (2011: 95) quien considera que el ciberpoder tiene como propósito estratégico alcanzar los objetivos políticos. Este propósito se desarrolla alrededor de la «habilidad tanto en la paz como en la guerra para manipular las percepciones del contexto estratégico para la ventaja propia al mismo tiempo que se degrada la habilidad del adversario para comprender dicho contexto». Lo que hace recordar que la transformación de los efectos del ciberpoder en objetivos de política es el arte y la ciencia de la estrategia, definida como «el manejo del contexto para lograr la ventaja continua según la política» (Dolman, 2005: 6). Lo anterior se sustenta con las palabras de Clausewitz (1976: 177) que considera la estrategia como «el uso de los combates para el objetivo de la guerra».

Para atender las necesidades de ciberseguridad EE.UU. cuenta con la dirección del Asesor Principal en cuestiones Ciber, que tendrá a su cargo el desarrollo de la política y estrategia de ciberseguridad del DoD. Dentro de las fuerzas armadas se ha organizado el Cibercomando de EE.UU. Además, cuenta con un total de 133 equipos de ciberdefensa y ciberdisuasión en el ciberespacio agrupados en Equipos Nacionales, Equipos de Ciberprotección, Equipos de Misiones de Combate y Equipos de Apoyo (DoD, 2018). Todos ellos se enfocan en el cumplimiento de las tres misiones principales: defender las redes, sistemas e información del DoD, defender la patria estadounidense y los intereses de EE.UU. contra ciberataques y, brindar apoyo a los planes de contingencia y operacionales de las fuerzas armadas.

México

La Estrategia Nacional de Ciberseguridad (ENC) de México identifica tres principios rectores, establece un objetivo general y cinco estratégicos, define ocho ejes trasversales e identifica a los actores involucrados. México presentó su ENC a finales de 2017 enlistando los siguientes tres principios rectores: 1) Perspectiva de derechos humanos, 2) Enfoque basado en gestión de riesgos y, 3) Colaboración multidisciplinaria y de múltiples actores. Por otro lado, la ENC de México tiene por objetivo general

> Fortalecer las acciones en materia de ciberseguridad aplicables a los ámbitos social, económico y político que permitan a la población y a las organizaciones públicas y privadas, el uso y aprovechamiento de las TIC de manera responsable para el desarrollo sostenible del Estado Mexicano. (Gobierno de México, 2017: 16).

Definición que se queda corta al mencionar solamente que el uso de las TIC será con responsabilidad sin aclarar que debe ser también con seguridad, no incluir la protección del ciberentorno, dejar fuera la ciberdefensa y ciberseguridad nacional, estar desvinculada de los objetivos estratégicos y no brindar una guía clara sobre las medidas que deben adoptarse. Los cinco objetivos estratégicos son: Sociedad y Derechos, Economía e Innovación, Instituciones Públicas, Seguridad Pública y Seguridad Nacional. Dicha ENC además comprende ocho ejes transversales (cultura de ciberseguridad; desarrollo de capacidades; coordinación y colaboración; investigación, desarrollo e innovación en TIC; estándares y criterios técnicos; infraestructuras críticas; marco jurídico y autorregulación; y, medición y seguimiento) que buscan cumplir con los siguientes cinco objetivos estratégicos.

En lo referente a la estructura institucional en 2017, se creó la Subcomisión de Ciberseguridad (Gobierno de México, 2018) compuesta por varias entidades y dependencias de la Administración Pública Federal, para velar por la ciberseguridad con el liderazgo de la Policía Federal Científica. Recientemente el Índice Global de Ciberseguridad 2017 que publicó la Unión Internacional de Telecomunicaciones (UIT), colocó a México como el tercer país mejor posicionado de América, sólo detrás de Estados Unidos y Canadá, ubicándolo por encima de todos los países de la región latinoamericana y en el lugar 28 de 165 países considerados por el estudio, lo cual es una cuestión que genera escepticismo entre los especialistas, y genera preguntas sobre sí ¿verdaderamente estamos preparados?

América Latina

Colombia y su Política Nacional de Seguridad Digital

Colombia fue el primer país latinoamericano en contar con una Estrategia Nacional de Ciberseguridad. Dicho documento fue aprobado en 2011; en el 2016 realizaron la primera revisión y modificación que dio lugar a la Política Nacional de Seguridad Nacional (CONPES, 2016). En esta nueva versión se pone énfasis en la reducción de la efectividad de las amenazas por medio del fortalecimiento de las

capacidades de los diversos actores.

La Estrategia establece un establece objetivo general, cinco objetivos específicos y 18 estrategias que se implementarán para lograrlos; además incluye un cronograma de implementación y un esquema detallado para su financiamiento. Los cuatro principios fundamentales de la Estrategia son: Salvaguardar los derechos humanos y los valores fundamentales, Adoptar un enfoque incluyente y colaborativo, Asegurar una responsabilidad compartida, y Adoptar un enfoque basado en la gestión de riesgos. Por otro lado, las cinco dimensiones estratégicas son: Gobernanza de la seguridad digital, Marco legal y regulatorio de la seguridad digital, Gestión sistemática y cíclica del riesgo de seguridad digital, Cultura ciudadana para la seguridad digital, y fortalecimiento de las capacidades para la gestión del riesgo de seguridad digital.

El gobierno en esta Política ha identificado que la ciberseguridad es una responsabilidad de todos y no solamente del gobierno. El objetivo general de la Estrategia es el de:

> Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país. (CONPES, 2016: 47).

Para cumplir con dicho objetivo fueron diseñados cinco objetivos específicos y dieciocho estrategias delimitadas por las cinco dimensiones estratégicas mencionadas anteriormente. Los cinco objetivos específicos son: Establecer un marco institucional para la seguridad digital, Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de la seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital, Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y transnacional, con un enfoque de gestión de riesgos, Fortalecer la defensa y la soberanía nacional en el entorno digital con un enfoque de gestión de riesgos, y Generar mecanismos permanentes y estratégicos para impulsar la cooperación, colaboración y asistencia en seguridad digital a nivel nacional e internacional.

Lo interesante de esta Política es que cuenta con un plan detallado de las estrategias, los tiempos requeridos y las instituciones responsables y los recursos necesarios para lograr tal objetivo. En resumen, la Política Nacional de Seguridad Digital incluye la gestión de riesgo como uno de los elementos más importantes para abordar la seguridad digital y, establece que las instituciones encargadas de ejecutar la Estrategia son el Ministerio de Defensa Nacional, el Ministerio de Tecnologías de la Información y las Comunicaciones, el Departamento Nacional de Planeación y la Dirección Nacional de Inteligencia.

Costa Rica

En el 2017 Costa Rica presentó su Estrategia Nacional de Ciberseguridad (MICITT, 2017), documento que marca la pauta a seguir en materia de ciberse-

guridad atendiendo los potenciales retos que se deben vencer. Dicho documento estratégico cuenta con un objetivo general, ocho objetivos específicos y 20 líneas estratégicas. El objetivo general busca:

> Desarrollar un marco de orientación para las acciones del país en materia de seguridad en el uso de las TIC, fomentando la coordinación y cooperación de las múltiples partes interesadas y promoviendo medidas de educación, prevención y mitigación frente a los riesgos en cuanto al uso de las TIC para lograr un entorno más seguro y confiable para todos los habitantes del país. (MICITT, 2017: 38).

Los cuatro principios rectores son: Las personas son prioridad, Respeto a los Derechos Humanos y la Privacidad, Coordinación y corresponsabilidad de múltiples partes interesadas y, Cooperación Internacional. El objetivo general se apoya en ocho objetivos específicos que son: Coordinación Nacional, Conciencia Pública, Desarrollo de la Capacidad Nacional de Seguridad Cibernética, Fortalecimiento del Marco Jurídico en Ciberseguridad y TIC, Protección de Infraestructuras Críticas, Gestión de Riesgo, Cooperación y Compromiso Internacional e, Implementación, Seguimiento y Evaluación.

Desde 2010 cuenta con la Comisión Nacional de Seguridad en Línea (CNSL). El Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) es el encargado de supervisar la implementación y hacer el seguimiento de las tareas que se le hayan asignado a cada uno de los actores implicados en la Estrategia. Además, dicho organismo cuenta con el Centro de Respuesta a Incidentes de Seguridad Informática (CSIRT – CR) para hacer frente a los incidentes de ciberseguridad. Del mismo modo, el MICITT es responsable de evaluar el cumplimiento de los objetivos. Por disposición de ley la estrategia debe ser revisada cada dos años.

Chile

Chile presentó su Política Nacional de Ciberseguridad (PNC) en 2017, documento en el cual expone de manera detallada las tareas que serán emprendidas en el corto y mediano plazo, así como las instituciones encargadas de la implementación de dicha política. Sus objetivos tienen como límite el 2022, pero la estrategia incluye un total de 41 medidas de política pública que deberán ser alcanzadas en el periodo 2017-2018. Los objetivos para el 2022 son seis que a su vez tienen diversos objetivos específicos (un total de 22) como se cita a continuación.

1. Desarrollar una infraestructura de las TIC que, bajo una óptica de gestión de riesgos, sea capaz de resistir y recuperarse de incidentes de ciberseguridad. Con los objetivos específicos siguientes. Identificación y gestión de riesgos, llevando a cabo medidas de monitoreo a fin de generar un ciberespacio resiliente; Protección de la infraestructura de la información; Identificación y jerarquización de las infraestructuras crítica de la información; Contar con equipos de respuesta a incidentes de ciberseguridad; Implementación de mecanismos estandarizados de reporte, gestión y recuperación de incidentes; y, Exigencia de estándares diferenciados en materia de ciberseguridad.

2. Garantizar los derechos de los ciudadanos en el ciberespacio. Que se complementa con los siguientes objetivos específicos: Prevención de ilícitos y generación de confianza en el ciberespacio; Establecimiento de prioridades en la implementación de medidas sancionatorias; Prevención multisectorial; y, Respeto y promoción de derechos fundamentales.
3. Desarrollar una cultura de ciberseguridad en torno a la responsabilidad en el uso de las TIC, a las buenas prácticas y a la educación. Indica los siguientes objetivos específicos: Una cultura de ciberseguridad; Sensibilización e información a la comunidad; y Formación para la ciberseguridad.
4. Establecer relaciones de cooperación con otros actores en materia de ciberseguridad y participar de forma activa en foros internacionales. Son cuatro sus objetivos específicos. Principios de política exterior chilena; Cooperación y asistencia; Reforzar la participación en instancias multilaterales y en instancias de múltiples partes interesadas; y Fomentar normas internacionales que promuevan la confianza y seguridad en el ciberespacio.
5. Desarrollar una industria de la ciberseguridad chilena, que sea útil a los objetivos estratégicos del país. Contiene cinco objetivos específicos: Importancia de la innovación y desarrollo en materia de ciberseguridad; Ciberseguridad como medio para contribuir al desarrollo digital de Chile; Desarrollo de la industria de ciberseguridad en Chile; Contribuir a la generación de oferta por parte de la industria local; y Generación de demanda de parte del sector público basado en los intereses estratégicos del Estado.

En lo que respecta a la organización del sistema de ciberseguridad la PNC prevé que una ley contemple la estructura y la gobernanza que debe ser preparada por las instituciones responsables. De manera temporal, el CSIRT Gob es la instancia encargada de gestionar los incidentes generados en la Red de Conectividad del Estado, mientras que a nivel político propone postergar y ampliar el mandato del Comité Interministerial cuyas funciones se circunscriben a los ámbitos de la comunicación, coordinación y seguimiento de las medidas contenidas en la PNC. En general, representa una estructura de la PNC muy similar a las adoptadas por el resto de los Estados de la región.

Panamá

Panamá elaboró en 2013 la Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas, título en donde sobresale la protección de las infraestructuras críticas del Estado. La Estrategia Nacional para la Innovación Gubernamental de Panamá busca el fortalecimiento de todas las instituciones del país. Aunque esta carente de profundidad en su propuesta, existe una legislación sustanciosa en ciberseguridad. El objetivo del Estado panameño, mediante el desarrollo de la Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas, es el de:

> aunar los esfuerzos de sus ciudadanos, empresas e instituciones públicas para redundar en un incremento de la seguridad cibernética que

> permita el uso confiable de las tecnologías de la información en todos los ámbitos nacionales, todo esto salvaguardando los derechos y libertades fundamentales de los ciudadanos y un entorno económico regulatorio favorable al crecimiento y desarrollo de las empresas y permitiendo el buen funcionamiento del Estado. (Consejo Nacional para la Innovación Gubernamental, 2013: 3).

Para lograr dicho objetivo las acciones se alinean en los ejes organizativo, legal, tecnológico y cultural. Al mismo tiempo, busca proteger los sistemas y redes informáticas y sensibilizar a las partes implicadas sobre los riesgos que enfrentan durante el uso de las TIC. No presenta de manera explícita los principios, pero se puede asumir que busca la protección de los derechos humanos y las libertades fundamentales, la no discriminación, la corresponsabilidad en el uso de las TIC y la colaboración entre las partes interesadas. Por otro lado, la Estrategia panameña indica seis pilares que son: Proteger la privacidad y los derechos fundamentales de los ciudadanos en el ciberespacio, Prevenir y detener las conductas delictivas en el ciberespacio o el uso de éste para cualquier tipo de delitos o actos ilícitos, Fortalecer la seguridad cibernética de las infraestructuras críticas nacionales, Fomentar el desarrollo de un tejido empresarial nacional fuerte en seguridad cibernética, como referencia para la región, Desarrollar una cultura de seguridad cibernética a través de la formación, innovación y la adopción de estándares y, Mejorar la seguridad cibernética y capacidad de respuesta ante incidentes de los organismos públicos.

Para lograr la implementación de la Estrategia y el objetivo general propuesto el gobierno panameño creará programas para mejorar la clasificación de información, adopción de las mejores prácticas y las capacidades de respuesta. Por ello, la Estrategia identifica y clasifica los riesgos que enfrenta la nación como un todo. Finalmente, indica que las instituciones encargadas de la ciberseguridad serán la Autoridad de Innovación Gubernamental, el Consejo Nacional para la Innovación Gubernamental y el Computer Security Incident Response Team (CSIRT) Panamá.

Paraguay

Paraguay presentó en 2017 el Plan Nacional de Ciberseguridad que es un documento estratégico fundamental para las políticas gubernamentales y nacionales que establece las líneas de acción a ser adoptadas para fortalecer la seguridad de sus activos críticos y proteger el ciberespacio. Dicho como plan en su diagnóstico afirma que Paraguay es el país con la población de usuarios que ha crecido con mayor velocidad entre 2010-2014, y en consecuencia es prioritario el fortalecimiento de la ciberseguridad en su territorio. Lo anterior se hará sin dejar de fomentar un entorno económico innovador y respetar los derechos fundamentales.

A diferencia de las otras estrategias de la región, el Plan Nacional de Ciberseguridad presenta una serie de objetivos generales bajo el nombre de ejes, 20 objetivos específicos para su lograrlos y 60 líneas de acción. El Plan Nacional de Ciberseguridad se concentra en los siguientes seis ejes de acción: (i) Sensibilización y Cultura; (ii) Investigación, Desarrollo e Innovación; (iii) Protección de Infraestructuras Críticas;

(iv) Capacidad de Respuesta ante Incidentes Cibernéticos; (v) Capacidad de Investigación y Persecución de la Ciberdelincuencia; y (vi) Administración Pública y (vii) Sistema Nacional de Ciberseguridad.

Sobresale que en este documento se mencionen los siguientes principios orientadores para la formulación e implementación de cualquier política pública de ciberseguridad: proporcionalidad, coordinación de esfuerzos y uso eficiente de recursos escasos, responsabilidad compartida, desarrollo e innovación, cooperación internacional y, monitoreo y evaluación. En cuestión de atribuciones, el Sistema Nacional de Ciberseguridad constituye la estructura institucional que aplica el Plan, cuyos componentes son el Coordinador Nacional de Ciberseguridad y la Comisión Nacional de Ciberseguridad. Este Plan y la Política Nacional de Ciberseguridad deben ser revisado cada tres años.

Región del Caribe

Jamaica

En el caso de Jamaica la ciberseguridad contó con un documento rector desde 2015 bajo el nombre de Estrategia Nacional de Seguridad Cibernética. Dicho documento reconoce que las TICs son una herramienta necesaria para el desarrollo nacional que conlleva riesgos que deben ser mitigados. La Estrategia identifica las siguientes áreas clave para lograr su objetivo: Medidas Técnicas; recursos humanos y desarrollo de capacidades; legal y regulatorio; y Educación y conciencia pública; que se desarrollan a través de 13 objetivos particulares. Además, la Estrategia agrega que busca generar confianza en el ciberespacio para que los jamaiquinos alcancen su máximo potencial. Busca ofrecer garantía de que se puede confiar en las tecnologías en las que depende diariamente, combatiendo los actos del cibercrimen contra las instituciones financieras, gubernamentales e infraestructura crítica.

De hecho, la Estrategia menciona que los costos por los delitos cibernéticos sobrepasan la suma del costo del tráfico de marihuana, cocaína y heroína. Lo anterior pone a la ciberseguridad como un tema prioritario dentro de la agenda de seguridad no sólo publica, sino nacional. Por ello, reconoce que el gobierno no puede solo con el desafío y acepta que la comunidad académica y el sector privado son actores fundamentales en la protección del ciberespacio. La Estrategia tiene los siguientes principios rectores: Liderazgo; Responsabilidades Compartidas; Protección de la Libertad y Derechos Fundamentales; la Gestión de Riesgos; Innovación y Desarrollo Empresarial; y Recursos Sostenibles.

Para cumplir los objetivos, cuenta con la Ley de Delitos Cibernéticos de 2010 que será actualizada y mejorada. En aspectos funcionales, la Estrategia complementa otras políticas y programas del gobierno jamaiquino como: La Estrategia Nacional de Tecnologías de la Información y Comunicaciones 2007-2012; Plan Nacional de Desarrollo 2030; La Política de Tecnologías de la Información y las Comunicaciones de 2011; y la Política de Seguridad Nacional de 2014.

En cuestión de organización y desempeño de las funciones de ciberseguridad han iniciado, con la asistencia de la Unión Internacional de Telecomunicaciones, los trabajos para la creación de un CSIRT nacional, así como la construcción y el despliegue de las capacidades técnicas necesarias. Ha establecido un Grupo de Trabajo Nacional de Seguridad Cibernética (NCSTF) que comprende una amplia transversalidad de partes interesadas de los sectores público, privado y academia. Además, cuenta con La Unidad de Comunicación Forense y Cibernética (CFCU) dentro de la Fuerza Policial de Jamaica (JCF) desde diciembre de 2010 y la Unidad de Delitos Cibernéticos y Evidencia Digital desde 2009. Queda claro que Jamaica cuenta con una organización incipiente pero numerosa de agencias de ciberseguridad. Establece tiempos de implementación de las primeras acciones y una revisión obligatoria de la Estrategia cada 3 años o cuando sea necesario.

Trinidad y Tobago

En el caso de Trinidad y Tobago, la ciberseguridad ha tenido un documento rector desde 2013. La Estrategia Nacional de Seguridad Cibernética reconoce que las actividades cotidianas son dependientes de las TICs., menciona que la realidad de este entorno trae consigo oportunidades, pero también riesgos a la seguridad. La estrategia se basa en el Marco de Política de Mediano Plazo 2011-2014 del Gobierno, en el que se destaca el papel de las TIC en la promoción del desarrollo; y tiene los objetivos:

1. Crear un entorno digital seguro que permita a todos los usuarios gozar plenamente de los beneficios que ofrece la Internet.
2. Proporcionar un marco de gobernanza en relación con todos los asuntos de seguridad cibernética mediante la identificación de las estructuras institucionales y administrativas necesarias, incluidas las de recursos humanos, capacitación y desarrollo de capacidades, y las relativas a las necesidades presupuestarias.
3. Proteger los activos físicos, virtuales e intelectuales de los ciudadanos, las instituciones y el Estado a través de la creación de un mecanismo eficaz para responder a las amenazas cibernéticas, sea cual fuere su origen.
4. Facilitar la seguridad de todos los ciudadanos promoviendo la sensibilización frente a los riesgos cibernéticos y elaborando medidas de protección eficaces y apropiadas para mitigar riesgos y ataques.

Y para lograr dichos objetivos se identificaron las cinco áreas de interés que se enlistan a continuación: Gobernanza; Gestión de Incidentes; Colaboración; Cultura; y Legislación. Que se verán sustentadas por treinta actividades. Todo con el objeto de crear un ciberentorno seguro y sólido, basado en la colaboración incondicional de todos los involucrados. A través de esta estrategia se pretende orientar todas las operaciones e iniciativas relacionadas con la ciberseguridad en el país. En ella se reconoce la necesidad prioritaria de un marco global de gobernanza, una apropiada legislación sobre delitos cibernéticos y el establecimiento de un equipo CSIRT. A lo anterior habría que sumarle la importancia de sensibilizar a todos los interesados generando una cultura de la ciberseguridad.

La Estrategia busca proteger el sistema financiero, servicios gubernamentales, los sistemas de control industrial tipo SCADA, la infraestructura de petróleo, gas y petroquímica, así como los servicios de transporte aéreo y terrestre. En la aplicación de la Estrategia se utilizará la Agencia de Seguridad Cibernética de Trinidad y Tobago (TTCSA, por sus siglas en inglés) como la principal responsable de la coordinación, la aplicación, el seguimiento, la mejora continua y la adecuada gestión de las iniciativas de seguridad cibernética. Además, el gobierno establecerá un CIRST como medio de protección de la infraestructura crítica. De manera complementaria, se promulgarán y aplicarán leyes generales de alcance nacional sobre delitos cibernéticos que sean aplicables y puedan armonizarse en el ámbito nacional e internacional.

Tabla 1. Resumen comparativo Estrategias Nacionales de Ciberseguridad

	Objetivo General	Objetivos Particulares	Estructura Orgánica	Recursos tecnológicos	Marco legal	Observaciones
Canadá 2018	√	√	√	√	√	Remasterizada y actualizada; es la más reciente.
EE.UU. Pendiente	√ Pendiente tener nueva ENCS	√ Pendiente tener nueva ENCS	√	√	√	No cuenta con una Estrategia Nacional de Ciberseguridad única. En el trabajo se utiliza la Ciberestrategia del DoD 2005. Bush presentó en 2003 la Estrategia Nacional para asegurar el Ciberespacio.
México 2017	√	√	√	√	√	Falta profundizar en los detalles de implementación, organización y funciones.
Colombia 2016	√	√	√	√	√	Incluye cronograma y detalles de financiamiento.
Costa Rica 2017	√	√	√	√	√	Incorpora medidas de educación, prevención y mitigación de riesgos. Se revisa cada 2 años.

Chile 2017	√	√	√	√	√	Detalla tareas de corto y mediano plazo, así como responsabilidades.
Panamá 2013	√	√	√	√	+ / -	No presenta de forma implícita los principios.
Paraguay 2017	√ Tiene varios	√	√	√	√	Presenta los principios orientadores.
Jamaica 2015	√	√	√	√	√	Señala que los costos de los delitos cibernéticos sobrepasan los del tráfico de drogas. Se revisa cada 3 años.
Trinidad y Tobago 2013	√	√	Por realizar	Por realizar	Por realizar	Reconoce medidas de marco global de gobernanza, la necesidad de un marco legal y la instalación de un CSIRT.

Elaboración propia. Con base en información publicada por los propios Estados.

Desafíos de las estrategias de ciberseguridad nacional

Si se parte de la definición de estrategia propuesta por Dolman (2005: 18) que dice que la estrategia es «plan para obtener la ventaja continua» entonces las Estrategias, planes o políticas de ciberseguridad que fueron enunciadas deberían estar orientadas a lograr, mantener o aumentar el poder (en este caso ciberpoder). Objetivo político que de acuerdo con Moisés Naím (2013: 47-49) se busca por medio de una mezcla de las cuatro formas distintas para ejercer el poder, también conocidas como tipos ideales o canales, que son: la fuerza, el código, el mensaje y la recompensa. Por lo tanto, bajo el supuesto de incrementar el poder en el ciberespacio solamente la Estrategia estadounidense parece cumplir con el cometido ya que expone que el ciberpoder es el elemento esencial para lograr la ventaja estratégica (DoD, 2005: vii). En contraste, la gran mayoría de las Estrategias Nacionales de Ciberseguridad lo que busca es fortalecer los instrumentos y las instituciones, aunque sin detallar de donde obtener los recursos ni definir funciones.

De la lectura de los documentos guía de las actividades de ciberseguridad se puede inferir que los desafíos que enfrentan las estrategias son diversos. Entre los problemas identificados se tienen aquellos referentes a la falta de una definición universal, la coordinación entre la iniciativa privada y el gobierno, la falta de un sistema educativo que cubra las necesidades de profesionales de la ciberseguridad, la adaptación de las fuerzas armadas y sus operaciones a los nuevos requisitos del

campo de batalla tecnológico, el incremento del impacto y frecuencia de los ciberataques, el desarrollo de tecnología endógena, el diseño de un sistema jurídico eficiente y alineado con los objetivos nacionales, las capacidades para ejercer influencia por medio del ciberpoder, el número de dispositivos conectados a la red, y la falta de tratados internacionales que regulen el cibercrimen, la ciberguerra y sus asuntos relacionados. Entre los desafíos destaca la construcción de confianza entre Estados al mismo tiempo que se contrarrestan amenazas provenientes de actores antagónicos; es decir, como confiar en quien busca dominar a través del ciberpoder.

Simplificando, los desafíos a las diversas estrategias de ciberseguridad pueden ser catalogados como técnicos, administrativos, organizacionales y de recursos humanos. Por lo tanto, en este trabajo solamente se mencionarán algunos de los muchos desafíos que se deslindan de estas categorías. Dentro de los desafíos técnicos se mencionará la dependencia tecnológica, en el plano organizacional la necesidad de contar con un organigrama vertical que centralice las misiones de ciberseguridad para mejorar la cooperación y reacción interinstitucional e internacional, y en cuestión de recursos humanos la falta de profesionales tanto técnicos como estratégicos que asuman las riendas del sistema de ciberseguridad con flexibilidad, conocimiento, ética y una estrategia. Los riesgos o desafíos que enfrentan los Estados en materia de ciberseguridad surgen de las características del ciberespacio que permiten mayor rentabilidad, facilidad de acceso e impunidad.

Primero, el principal desafío tecnológico de la mayoría de las estrategias de ciberseguridad es que los Estados no generan la totalidad de los componentes de los sistemas de cómputo y comunicaciones con los que construyen sus sistemas cibernéticos. Por ejemplo, de acuerdo con Adee (2008) existe una centralización de la producción de componentes esenciales como son los procesadores, ya que Taiwán produce 80 por ciento de los arreglos de compuertas de campo programable (FPGA por sus siglas en inglés) que son circuitos integrados genéricos que pueden ser personalizados por medio de programas de computadora abaratando los costos de manera importante cuando se compara con los circuitos integrados de aplicación especifica (ASIC). El costo baja desde un máximo de entre $4 a $50 millones a tan sólo $500 dólares.

Lo anterior pone en riesgo la seguridad nacional de EE.UU., y de todos aquellos que compren dichos dispositivos, debido a que muchos de sus contratistas de defensa son dependientes de dichos circuitos. Sin embargo, aunque el precio no se relaciona generalmente con la seguridad, en este caso no existe garantía de que estos circuitos integrados de bajo precio no hayan sido modificados para contar con un circuito de apagado o una «puerta trasera» que permita la manipulación remota del sistema en el que se monten dichos circuitos. Para generar este tipo de vulnerabilidades basta con agregar 1000 transistores adicionales en una configuración especial que permitirá su acción cuando le sea instruido por un agente externo (Adee, 2008).

El desafío es contar con una cadena de suministro de dispositivos y componentes de las TIC confiable y eficiente. Al respecto el Deparment of Defense (DoD) estadounidense en 2004 «creó el Programa de Fundiciones de Confianza para tratar de garantizar un suministro ininterrumpido de circuitos integrados seguros para el gobierno. Los inspectores del DoD ahora han certificado ciertas plantas de circuitos

comerciales como fundiciones confiables, tal es el caso de las instalaciones de IBM Burlingtony Vt.» (Adee, 2008). De igual manera, Libicki (2009: 22) ha denunciado que «A muchos en la comunidad de defensa les preocupa la creciente presencia de China en la fabricación de componentes situación que le brinda muchas oportunidades para hacer travesuras, y puede que no sea tímida a la hora de tomar ventaja de dichas oportunidades». Esto sin olvidar que «Ni los agentes ni los componentes modificados/corruptos violan los principios básicos discutidos anteriormente. Ninguno representa un acceso forzado. Ambas son formas de engaño y del tipo que una vez engañado no permite que caiga tan fácilmente otra vez» (Libicki, 2009: 21) Esto lleva al problema de la atribución que evita identificar positivamente a los atacantes y organizar una respuesta proporcional al ataque.

Aunado a lo anterior habría que sumar la complejidad, cantidad y efectividad de los ciberataques, que han convertido las operaciones militares en acciones tipo guerrilla o guerra asimétrica. Cada año se tiene noticia de ciberataques de gran impacto a las áreas estratégicas de los Estados, quienes debido a la diversidad, atomización y automatización de los actores se ha visto imposibilitado para dar respuesta efectiva. En este caso la mejor defensa es la prevención y mitigación de riesgos, pero sin la tecnología adecuada y eficiente esto es una misión casi imposible.

En breve, el mayor desafío tecnológico consiste en generar tecnología endógena con dispositivos seguros y confiables. No depender de tecnologías extranjeras brinda un alto grado de libertad de acción. El pensamiento estratégico dicta que se deben tomar las medidas necesarias para evitar la coerción de cualquier índole y reducir los riesgos de un ataque por sorpresa.

Segundo, en lo relativo a los problemas y desafíos tanto administrativos como organizacionales se puede ver que la falta de recursos y estrategias detalladas entorpece la buena voluntad de algunos gobiernos y actores de la sociedad civil. Particularmente los desafíos surgen de la no consideración de la ciberseguridad como un tema prioritario dentro de la agenda nacional de riesgos u otro documento similar y a la falta de un organismo central que organice y controle las actividades en materia de ciberseguridad nacional. Bajo el contexto actual en primer término se debe convencer a los dirigentes políticos sobre la seriedad y el alcance de los eventos cibernéticos adversos que podrían poner en jaque las actividades económicas, políticas, sociales y militares.

Todo lo cual sería un atentado contra la estabilidad, integridad y permanencia del Estado. Es decir, la ciberseguridad nacional debe ser considerada como una parte complementaria de la seguridad nacional dentro de la legislación vigente para que se asignen los recursos necesarios para fortalecer tanto la infraestructura digital como la educación/cultura en ciberseguridad. Los fondos asignados a la ciberseguridad nacional deben ser vistos como una inversión que garantiza la continuidad de las actividades diarias en el ciberespacio.

Una vez que la administración en turno comprenda la importancia de contar con un ciberespacio seguro y resiliente, identifique los sectores estratégicos de su infraestructura digital o ciberentorno, reconozca las amenazas que enfrenta y cuente con un diagnóstico situacional, podrá estructurar un sistema de ciberseguridad centralizado y vertical. Tendrá la obligación de estructurar un sistema de ciberseguridad

nacional compuesto por: 1) un sistema de ciberseguridad pública y 2) las fuerzas de ciberdefensa con atribuciones, obligaciones y prerrogativas estipuladas de manera clara y detallada.

Diagrama 1. Propuesta de un Sistema de Ciberseguridad Nacional

Elaboración propia. Propuesta de la orgánica de ciberseguridad y ciberdefensa. Aclarando que esta estructura no exime la participación de los diversos componentes en apoyo del resto o en operaciones conjuntas.

Sistema en el cual se define a la policía como el elemento bisagra o de enlace entre la ciberseguridad y la ciberdefensa. No se puede permitir que exista confusión en el papel que cada uno de los órganos que integren dicho sistema de ciberseguridad nacional deben cumplir, la política que deben seguir, los objetivos que deben alcanzar, la estrategia que deben adoptar, los instrumentos legales que puede requerir, las acciones que deben iniciar ni en el perfil de profesionistas que requieren. Todo lo cual representa una revolución en asuntos de ciberseguridad y un desafío a los gobiernos de algunos Estados de América Latina y el Caribe.

Tercero, al mismo tiempo que diseña la estructura orgánica que adoptará el sistema de ciberseguridad nacional, debe iniciar con un plan emergente de formación de cuadros profesionales en ciberseguridad. Particularmente porque la falta de una fuerza de trabajo profesional con especialización en temas de ciberseguridad atenta contra la seguridad de los sistemas informáticos, de la infraestructura crítica y de la información el «oro digital» de la sociedad de la información. De acuerdo con Arreola (2015: 160-163) la experiencia en la selección y reclutamiento de personal para el sistema de inteligencia ha dado como resultado requisitos morales, psicológicos, físicos e intelectuales que deben ser satisfechos para tener acceso a información estratégica o conocimiento privilegiado. Este tipo de reclutamiento puede ser emulado por el sistema de ciberseguridad. Por desgracia, a pesar de todas las medidas de selección de personal, las instituciones de ciberseguridad no pueden garantizar que los profesionales de la ciberseguridad no se vean tentados a cometer actos que pongan en riesgo la ciberseguridad nacional, las actividades de los organismos o la privacidad de los individuos.

Por ello, es recomendable contar con un sistema educativo que brinde una formación integral, que incluya aspectos de desarrollo físico, mental y ético entremezclados con los temas de uso seguro de las TIC. De manera ideal, la formación de cuadros para la ciberseguridad debería ser en instituciones creadas exprofeso para el caso, en donde se haga hincapié en los beneficios de servir por convicción en aras del bienestar público. A lo anterior, habría que sumar un sistema de evaluación y seguimiento del desempeño de cada uno de los elementos para detectar anomalías en su conducta, vida personal y desarrollo profesional que pudieran convertirse en una amenaza para la seguridad del sistema de ciberseguridad.

Sin embargo, se sabe que las necesidades de cuadros profesionales se cubren por medio de la subcontratación de servicios, lo que se vuelve una fuente de potencial riesgo para el sistema. Por lo tanto, se deben establecer lineamientos estrictos para la contratación de terceros dentro del sistema de ciberseguridad con el fin de garantizar la seguridad de las operaciones y la ciberseguridad nacional. Según Arreola (2015: 160-163) el dilema de este tipo de contratación es que el proceso de selección lo realizan las propias compañías subcontratadas y no se puede garantizar que hay sido tan riguroso como las actividades de ciberseguridad lo requieren, al menos en cuestiones de valores morales como son: discreción, honestidad y lealtad. En consecuencia, no solamente se deben firmar acuerdos de confidencialidad, sino que es prioritario fortalecer el sistema legal para regular eficientemente la actuación de los prestadores de servicio en materia de ciberseguridad. De no hacerlo así se corre el riesgo de que áreas estratégicas para la seguridad nacional queden expuestas desde dentro a los embates de potenciales enemigos.

En resumen, de manera general los desafíos de las Estrategias Nacionales de Ciberseguridad son aquellos que se refieren: al fortalecimiento de la infraestructura y medios técnicos de manera personalizada y autónoma; a la creación, mantenimiento y fortalecimiento de un aparato estatal que garantice la ciberseguridad nacional al mismo tiempo que respeta los derechos humanos, privacidad e intimidad de sus ciudadanos; a la implementación de una cultura de la ciberseguridad que permee todos los niveles y sectores enfocándose en el fortalecimiento del eslabón más débil (el ser humano); y finalmente, a la conformación de un sistema educativo que genere los recursos humanos profesionales necesarios para organizar una fuerza de reacción capaz de tomar la iniciativa cuando sea necesario. Todo lo anterior sin olvidar que el internet se ha convertido en un bien común que por el momento aparenta estar bajo el control de nadie y de todos, convirtiendo la gobernanza del internet en un tema de cooperación y seguridad internacional.

En lo que respecta a ciberespacio este por sí mismo conlleva una serie de desafíos que están implícitos en su esencia y estructura. Estos desafíos se refieren a cuestiones de alcance (global), la velocidad para realizar un ataque o contraataque (nanosegundos), la dificultad para identificar de manera precisa al atacante (atribución), hace patente el ciberpoder y la posibilidad de realizar tanto operaciones ofensivas como defensivas (se dice que la ofensiva es dominante). Garantizar el ciberespacio global requerirá la cooperación internacional para crear conciencia, compartir información, promover estándares de seguridad e investigar y enjuiciar los delitos cibernéticos. Por ello, quién domine el ciberespacio, dominará al mundo.

Siguiendo el pensamiento estratégico de Sun Tzu (2008: 21), una estrategia nacional de ciberseguridad o ciberestrategia no garantiza que todos los ataques puedan ser contrarrestados, pero sin un documento guía puede asegurarse que los ataques contra su integridad serán exitosos y lo dañarán seriamente. Se debe recordar que la invencibilidad radica en uno mismo, por lo que la fortaleza propia radica en una defensa efectiva; y las posibilidades de vencer se encuentran en el ataque que explota las debilidades del oponente.

Conclusiones

La mayoría de las estrategias revisadas requieren de mayor trabajo para detallar las acciones concretas que realizarán para alcanzar los objetivos, conocer las necesidades de presupuesto y designar las instituciones que serán las encargadas de implementarlas. Se debe reconocer que la Estrategia de EE.UU., Canadá, Colombia, Paraguay y Chile son las que presentan un mayor grado de detalle. Por ejemplo, la Estrategia estadounidense describe la ciberestrategia militar de su gran estrategia, la Estrategia colombiana fue revisada para adoptar una segunda versión que incluye un cronograma para la consecución de los objetivos y la Estrategia Chilena plasma objetivos a mediano plazo que debe obtenerse para el 2022.

En contraste, la Estrategia de Panamá queda por debajo del promedio y aparenta ser más un compromiso político que un documento rector de la ciberseguridad nacional. A pesar de ello, se debe reconocer que Panamá fue el segundo Estado en adoptar una Estrategia Nacional de Ciberseguridad (2013), solamente detrás de Colombia que fue el primer Estado latinoamericano en contar con un documento rector de la ciberseguridad.

Es previsible que el diseño de estrategias nacionales de ciberseguridad traerá consigo un sentimiento de inseguridad para quienes no cuenten con ella; en consecuencia, el dilema de la seguridad seguirá predominando en el continente americano y en el mundo. De manera clara, la seguridad de uno es la inseguridad del resto. Esto será cierto particularmente para aquellos Estados en donde la tecnología se ha convertido en elemento esencial de las actividades cotidianas de la sociedad, organizaciones y gobierno.

No se puede pasar por alto que las estrategias nacionales de ciberseguridad están orientadas a proteger el ciberespacio que según Arreola (2016) se ha convertido en el campo de batalla de la era tecnológica. Sin lugar a dudas, la superioridad en el ciberespacio brindará la libertad de acción a las fuerzas amigas y la negará al enemigo. Lo que se busca a través de las estrategias de ciberseguridad nacional es la obtención, manutención e incremento del ciberpoder.

Una de las preocupaciones principales de las estrategias de ciberseguridad nacional debe ser la creación de centros educativos de excelencia en cuestiones ciencia y tecnología con un enfoque en todas las aristas de la ciberseguridad. Es decir, la formación de los nuevos profesionales de todas las áreas debe incluir conocimientos de ciberseguridad, esto facilitaría que las empresas y gobierno desempeñen sus funciones utilizando tanto el ciberespacio como las tecnologías de la información y comunicación de manera segura, innovadora y eficaz.

La ciberseguridad del conjunto es igual a la seguridad de su eslabón más débil. Ya que todos los elementos de la sociedad están expuestos y pueden convertirse en la principal vulnerabilidad, los gobiernos deben corregir las asimetrías que existen en el trato prioritario que se da a la ciberseguridad. Lo anterior se puede lograr por medio del asesoramiento, liderazgo, y ampliación del acceso a herramientas de ciberseguridad/seguridad de la información, así como del desarrollo de habilidades especializadas. El gobierno se convierte en el líder de la empresa llamada ciberseguridad nacional que requiere de un enfoque conjunto, multidisciplinario, multifactorial y multinivel para lograrse. La ciberseguridad nacional es un asunto de todos.

Como dicen Clarke y Knake (2014: 21) «la ciberguerra es real, la ciberguerra se desarrolla a la velocidad de la luz, la ciberguerra es global, la ciberguerra evita el campo de batalla y, la ciberguerra ha iniciado». Por ello, un buen inicio es contar con una Estrategia Nacional de Ciberseguridad que atienda de manera integral los pormenores del ciberespacio. No hay debe perder de vista que los ciberataques dependen del engaño para persuadir a los sistemas para hacer lo que los diseñadores originales no quieren que hagan.

La esencia de la ciberseguridad nacional radica en la protección de los equipos e infraestructura. Es prioritario para la estrategia que se garantice un diseño seguro de los componentes internos y accesorios de los diversos sistemas digitales. Para ello, tendría que crearse un área especialmente dedicada a la prueba funcional de los diversos dispositivos y componentes electrónicos con que cuentan las áreas estratégicas para la seguridad y el desarrollo. Remarcando que cualquier daño o pequeña modificación maliciosa puede ser devastadora para el sistema en su totalidad. Garantizar el ciberespacio global requerirá la cooperación internacional para crear conciencia, compartir información, promover estándares de seguridad e investigar y enjuiciar el delito cibernético. No se puede olvidar lo que John Boyd, coronel de la Fuerza Aérea de Estados Unidos, argumentó que «las máquinas no combaten guerras ... los humanos pelean guerras». (Coram, 2002: 341), porque es algo que esta en proceso de cambio.

Para hacer frente a los desafíos de la era de la información el hombre tendrá que diseñar e implementar estrategias integrales que tengan como epicentro la seguridad humana.

Bibliografía

- Adee, S. (2008). The hunt for the kill switch. *iEEE SpECtrum*, *45*(5), 32.
- Arreola, G.A. (2015). *Ciberespionaje, la puerta al mundo virtual de Estados e individuos*. Siglo XXI.
- Arreola, G. A. (2016). Ciberespacio, el campo de batalla de la era tecnológica. *Estudios en Seguridad y Defensa*, *11*(22), 109-138.
- Artiles, N. G. (2011). Situación de la Ciberseguridad en el ámbito internacional y en la OTAN. *Cuadernos de estrategia*, (149), 165-214.
- Banco Interamericanos de Desarrollo (BID) y Organización de los Estados Americanos (OEA) (2016). Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Recuperado de: https://digital-iadb.leadpages.co/ciberseguridad-en-la-region/
- Betz, D. J. and Stevens, T. (2011). *Cyberspace and the State: Towards a Strategy for Cyber-power.* Routledge.
- Cano, J. J. (2011). Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global. *SI*STEMAS (ASOCIACION COLOMBIANA DE INGENIEROS DE SISTEMAS), 119, 4-7.
- Carter, A. (2015). The DOD cyber strategy. April, 17, 2015.
- Clarke, R. A., & Knake, R. K. (2014). Cyber war. Tantor Media, Incorporated.
- Clausewitz, C. (1976). On War, Edited and translated by Michael Howard and Peter Paret, Princeton: Princeton University Press.
- Consejo Nacional para la Innovación Gubernamental (12 de marzo de 2013). Gaceta Oficial Digital. Nº 21. Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas. Recuperado el 11 de agosto de 2018, de https://www.unodc.org/res/cld/lessons-learned/pan/estrategia_nacional_de_seguridad_cibernetica_y_proteccion_de_infraestructuras_criticas_html/Estrategia_Nacional_de_Seguridad_Cibernetica_y_Proteccion_de_Infraestructuras_Criticas.pdf
- Coram, R. (2002). Boyd: The fighter pilot who changed the art of war. Hachette UK. pp. 341.
- Department of Defense (DoD). (11 de diciembre de 2005). The National Military Strategy for Cyber Operations. www.hsdl.org [Edición digital]. Recuperado el 06 de Agosto de 2018 de, https://www.hsdl.org/?abstract&did=35693
- Department of Defense (DoD). (2015). The DoD Cyber Strategy. EUA: DoD. www.defense.gov [Edición digital]. Recuperado el 06 de Agosto de 2018 de, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf
- Department of Public Safety and Emergency Preparadness. (2018). National Cybersecurity Strategy. www.publicsafety.gc.ca [Edición digital]. Recuperado el 12 de agosto de 2018 de, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf
- Documento CONPES 3854 (Consejo Nacional de Política Social y Económica). (2016). Política Nacional de Seguridad Digital. Recuperado el 10 de agosto de 2018, de http://bibliotecadigital.ccb.org.co/bitstream/handle/11520/14856/DNP-Conpes-Pol%2b%C2%A1tica%20Nacional%20de%20Seguridad%20Digital.pdf?sequence=1&isAllowed=y
- Dolman, E. (2005). Pure Strategy: Power and Principle in the Space and Information Age. Routledge.
- Gobierno de Chile (2017). Política Nacional de Ciberseguridad. Recuperado de: http://ciberseguridad.interior.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf
- Gobierno de Jamaica. (2015). Estrategia Nacional de Seguridad Cibernética. www.sites.oas.org

[Edición digital]. Recuperado el 15 de agosto de 2018 de, https://www.sites.oas.org/cyber/Documents/Jamaica%20National%20Cyber%20Security%20Strategy%20(Spanish).pdf

- Gobierno de la República de Trinidad y Tobago. (2013). Estrategia Nacional de Seguridad Cibernética. www.sites.oas.org [Edición digital]. Recuperado el 15 de agosto de 2018 de, https://www.sites.oas.org/cyber/Documents/Trinidad%20and%20Tobago%20-%20National%20Cyber%20Security%20Stategy%20(Spanish).pdf
- Gobierno de México. (2018). Por un internet más seguro en México: impulsa Gobierno de la República Estrategia Nacional de Ciberseguridad. www.gob.mx [Edición digital]. Recuperado el 15 de agosto de 2018 de, https://www.gob.mx/mexicodigital/articulos/por-un-internet-mas-seguro-en-mexico-impulsa-gobierno-de-la-republica-estrategia-nacional-de-ciberseguridad
- Gobierno de México. (2018). Por un internet más seguro en México: impulsa Gobierno de la República Estrategia Nacional de Ciberseguridad. www.gob.mx [Edición digital]. Recuperado el 15 de agosto de 2018, de https://www.gob.mx/mexicodigital/articulos/por-un-internet-mas-seguro-en-mexico-impulsa-gobierno-de-la-republica-estrategia-nacional-de-ciberseguridad
- House, W. (2003). The national strategy to secure cyberspace. Washington, DC: White House.
- Johnson, D. D., & Tierney, D. (2011). The Rubicon theory of war: how the path to conflict reaches the point of no return. International Security, 36(1), 7-40.
- Kuehl, T. D. (2009). Cyberspace and Cyberpower, in Cyberpower and National Security, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Dulles, VA: Potomac Books, 2009).
- Leiva, E. A. (2015). Estrategias Nacionales de Ciberseguridad: Estudio comparativo basado en Enfoque Top-Down desde una visión global a una visión local. Revista Latinoamericana de Ingeniería de Software, 3(4), 161-176.
- Libicki, M. C. (2007). Conquest in cyberspace: national security and information warfare. Cambridge University Press.
- Libicki, M. C. (2009). Cyberdeterrence and cyberwar. Rand Corporation.
- Lynn, W. J. (2010). Defending a new domain: the Pentagon's cyberstrategy. Foreign Affairs, 89(5), 97-108.
- Max Weber, 'Class, Status, Party', in Hans Gerth and C. Wright Mills (eds). (1948). From Max Weber: Essays in Sociology. London: Routledge and Kegan Paul, p. 180.
- MICITT (2017). Estrategia Nacional de Ciberseguridad de Costa Rica. Recuperado el 15 de agosto de 2018, de https://micit.go.cr/images/imagenes_noticias/10-11-2017__Ciberseguridad/Estrategia-Nacional-de-Ciberseguridad-de-Costa-Rica-11-10-17.pdf
- Naím, M. (2013). El fin del poder: Empresas que se hunden, militares derrotados, papas que renuncian, y gobiernos impotentes: cómo el poder ya no es lo que era. Debate.
- Observatorio CISDE (2017). Pronóstico de ciberseguridad para América Latina en 2018. Recuperado de https://observatorio.cisde.es/sin-categoria/pronostico-ciberseguridad-america-latina-2018/
- Organización de Estados Americanos (OEA). (2017). México presentó Estrategia Nacional de Ciberseguridad desarrollada con apoyo de la OEA. www.oas.org [Edición digital]. Recuperado el 15 de agosto de 2018, de http://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-082/17
- Russell, B. (2004). Power: A new social analysis. Routledge. p. 23.
- Secretaría Nacional de Tecnologías de la Información y la Comunicación (2017). Plan Nacional

de Ciberseguridad. Retos, roles y compromisos. Recuperado el 12 de agosto de 2018, de http://gestordocumental.senatics.gov.py/share/s/zkKW1CkKScSvapqlB7UhNg

- Secretaría Nacional de Tecnologías de la Información y la Comunicación (2017). Plan Nacional de Ciberseguridad. Retos, roles y compromisos. Recuperado de: http://gestordocumental.senatics.gov.py/share/s/zkKW1CkKScSvapqlB7UhNg
- Sheldon, J. B. (2011). Deciphering cyberpower: Strategic purpose in peace and war. Strategic Studies Quarterly, 5(2), 95-112.
- Sheldon, J. B. (2014). Geopolitics and cyber power: Why geography still matters. American Foreign Policy Interests, 36(5), 286-293.
- Starks, T. (12 de abril de 2018). A national cyber strategy may finally be on the way. www.politico.com [Edición digital]. Recuperado el 14 de agosto de 2018 de, https://www.politico.com/newsletters/morning-cybersecurity/2018/04/12/a-national-cyber-strategy-may-finally-be-on-the-way-167541
- Stephens, P. (16 de diciembre de 2010). On the way to a new global balance. Financial Times (Londres).
- Torres, M. (2013). Ciberguerra. En Jordán, J. (coord.), Manual de Estudios Estratégicos y Seguridad Internacional. pp. 329-348. Madrid: Plaza & Valdés.
- U.S. Department of Defense (DoD). The Department of Defense Cyberstrategy. www.defense.gov [Edición digital]. Recuperado el 14 de agosto de 2018 de, https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy/
- Unión Internacional de Telecomunicaciones (UIT). (2010). Resolución 181. Recomendación UIT–T X.1205. UIT. [Edición digital]. Recuperado el 13 de abril de 2017, del sitio http://www.itu.int/net/itunews/issues/2010/09/20-es.aspx
- Unión Internacional de Telecomunicaciones (UIT). (2017). Índice Global de Ciberseguridad 2017. www.itu.int [Edición digital]. Recuperado el 15 de agosto de 2017 de https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

La evolución del Proceso Planeación En La Administración Publica Federal
The Evolution of the Planning Process in the Federal Public Administration

Resumen

El presente ensayo tiene como propósito determinar cómo ha sido la evolución del proceso de planeación democrática para el desarrollo de nuestro país, así como, analizar la estructura de las rutas de navegación definidas en el Plan Nacional de Desarrollo 2019-2024 emitido por el Gobierno de México para arribar a ese puerto ideal: el desarrollo del país. Además, describe como los Programas Sectoriales coadyuvan a la planeación democrática nacional. México como un todo, puede ser comparado a un gran navío. El Titular del Ejecutivo Federal en nuestro país, es el líder que traza colegiadamente el plan de navegación que le da el rumbo a México y el Plan Nacional de Desarrollo es la carta de navegación que armoniza y focaliza el funcionamiento de las instituciones de la Administración Publica Federal para alcanzar las metas y objetivos nacionales. Finalmente, el presidente de la República emplea su maquinaria, personificada en las dependencias y entidades de la Administración Pública Federal, para lograr el arribo a ese puerto ideal, el desarrollo de la sociedad mexicana.

Palabras clave

México; Plan Nacional de Desarrollo; desarrollo nacional; planeación democrática nacional; evolución de la planeación mexicana.

Abstract

The purpose of this essay is to determine the evolution of the democratic planning process for the development of our country. As well as, analyze the structure of the navigation routes defined in the National Development Plan 2019-2024 issued by the Government of Mexico to arrive at that ideal port, the development of Mexico. In addition, it describes how the Sector Programs contribute to national democratic planning. Mexico as a whole, can be compared to a great ship. The Head of the Federal Executive in our country, is the leader who collects collectively the navigation plan that gives the direction to Mexico. The National Development Plan is the navigation chart that harmonizes and focuses the operation of the institutions of the Federal Public Administration to achieve national goals and objectives. Finally, the President of the Republic uses his machinery, personified in the dependencies and entities of the Federal Public Administration, to achieve the arrival to that ideal port, the development of Mexican society.

Key words

Mexico; National Development Plan; national development; national democratic planning; evolution of Mexican planning.

Cap. Frag. CG. MSI. José Antonio Diaz Lendeche
Cap. Frag. CG. PH. Juan Carlos Yuit Márquez
Cap. Frag. CG. PH. Moisés Alfonso Magallanes Casas

Cap. Frag. CG. Jose Manuel Bautista Esparza Bautista
Cap. Frag. CG. Diego Emmanuel Valenzuela Balderas
Cap. Frag. CG. Msp. Roberto Barra Solís
Cap. Frag. CG. Cesar Patricio Villalvazo Bailón
Cap. Corb. Oscar Juan Pablo Alay MacDonald

Artículo recibido el 10 de octubre de 2019. Aprobado 5 de diciembre de 2019.

Los errores remanentes son responsabilidad de los autores.
El contenido de la presente publicación refleja el punto de vista del autor, que no necesariamete coinciden con el del Alto Mando de la Armada de México o la Dirección de este plantel.

Introducción

La planeación es el conjunto de rutas de navegación que el aparato gubernamental emplea para arribar a puerto ideal; o bien, rectificar y llevar a buen término otras rutas que ya están en curso. Peter Drucker, considerado el mayor filósofo de la administración, cita en una de sus frases más célebres, «la planificación a largo plazo no es pensar en decisiones futuras, sino en el futuro de las decisiones presentes». Esta frase por sí sola, refleja la importancia de la planeación y la delicada relación que existe entre las acciones presentes y lo que se obtendrá en el futuro como resultado de estas, situación que se vuelve aún más delicada cuando se trata del guiar el rumbo de todo un Estado-Nación.

A lo largo de la historia, han transcurrido en México situaciones que han hecho necesario, en primera instancia crear la normatividad para la existencia de un Plan Nacional de Desarrollo. A pesar que existían intentos previos de formalizar la planeación de México, como el Plan Sexenal de Lázaro Cárdenas, este proceso inició formalmente en 1983 bajo la gestión del entonces presidente de la República Mexicana, Miguel de la Madrid Hurtado. Desde entonces y hasta la fecha ha sido necesario adecuar los documentos de planeación estratégica a las circunstancias propias de cada sexenio tanto en el plano nacional como en el internacional, considerando el presente y una visión futura. Un documento cuyos objetivos nacionales, se han encontrado orientados en todo momento a la consolidación de un país más desarrollado, seguro, próspero y con mejores condiciones de vida para todas y todos los mexicanos.

Actualmente, el Ejecutivo Federal, en coordinación con las dependencias, entidades gubernamentales, órganos autónomos, gobiernos estatales y sociedad, ha elaborado y publicado el Plan Nacional de Desarrollo 2019-2024 (PND 2019-2024), el cual engloba en tres ejes generales: a) Política y Gobierno, b) Política Social y c) Economía. Objetivos que han de alcanzarse para establecer y guiar las rutas de navegación del país hacia un mejor puerto, el desarrollo humano de la sociedad mexicana. En este plan, se establecen además 12 principios rectores que instituyen las normas de conducta que orienten el desempeño de los servidores públicos. Este PND 2014-2019, rige los procedimientos y actuación de las Dependencias de la Administración Pública Federal, las cuales, a través de sus propios planes y programas sectoriales, han de orientar sus acciones hacia el logro de los objetivos nacionales.

Dado lo anterior, el presente ensayo tiene como propósito determinar cómo ha sido la evolución del proceso de planeación democrática para el desarrollo de nuestro país. Así como, analizar la estructura de las rutas de navegación definidas en el Plan Nacional de Desarrollo 2019-2024 emitido por el Gobierno de México para arribar a ese puerto ideal, el desarrollo de México. Además, describe como los Programas Sectoriales coadyuvan a la planeación democrática nacional.

A. Definición y marco legal de la planeación

Cualquier país, por el simple hecho de emplear recursos públicos, necesita realizar procesos de planeamiento, no importando su sistema de gobierno. Isaac

Sánchez (2010) menciona que en el caso de los países democráticos los controles son más estrictos para la evaluación y rendición de cuentas. Otro de los autores más revolucionarios de la Administración y Gerencia del siglo XX, Ernest Dale, definía la planeación como «la determinación del conjunto de objetivos por obtenerse en el futuro y el de los pasos necesarios para alcanzarlos a través de técnicas y procedimientos definidos» (Sanchez, 2010, pág. 12). El reto final, es integrar las voluntades de los actores políticos, sociales y académicos en un solo documento que defina el rumbo del Estado-nación.

La Administración Pública Federal considera la planeación como un sistema que le permite enlazar los medios y los fines, diseñar normas y distribuir funciones. Sin embargo, sería muy relevante eficientar los objetivos sociales para que le permita hacer crecer la función pública. Para el desarrollo de sus actividades, «el gobierno realiza estas funciones a través de la Administración Pública Federal sirviendo de base a las atribuciones del presidente de la Republica, mismo que se apoya en las secretarías y dependencias del Estado» (Jiménez, 2015). El planeamiento gubernamental se enfoca en elaborar planes, seleccionar objetivos y seleccionar alternativas, estableciendo prioridades a las demandas de los grupos sociales existentes.

El planeamiento gubernamental es la carta náutica que fija el rumbo que debe recorrer el país. En ese sentido, la planeación encuentra su fundamento superior en la Constitución Política de los Estados Unidos Mexicanos (2019) la cual describe en su primer párrafo del artículo 26: «El Estado organizara un sistema de planeación democrática del desarrollo nacional que imprima solidez, dinamismo, competitividad, permanencia y equidad al crecimiento de la economía para la independencia y la democratización política, social y cultural de la nación»; de igual forma citado artículo establece que habrá un Plan Nacional de Desarrollo al que se sujetaran los planes y programas de la Administración Pública Federal. Precisando con ello, el rumbo del aparato gubernamental al puerto ideal.

La estructura del proceso de planeación pública tiene su quilla en un documento. El Plan Nacional de Desarrollo (PND) tiene como fin último, dar sustento a los objetivos de la nación, las estrategias y las prioridades de la Administración en curso. Dicho plan regula las actividades del gobierno para darle dirección y rumbo claros. Es el compromiso que el Gobierno de México establece con la sociedad, que le permitirá establecer objetivos y estrategias nacionales que servirán de base para los programas sectoriales, especiales, institucionales y regionales.

Por supuesto, dicho proceso de elaboración contempla sus correspondientes rendiciones de cuentas. El presidente de la Republica diseña el PND y luego lo remite al H. Congreso de la Unión para que, en ejercicio de sus atribuciones constitucionales y legales, haga las observaciones que considere pertinentes. Ambas cámaras se involucran para integrar las voluntades de sus representados. Este proceso se realiza en un plazo no mayor a 6 meses desde la concepción, elaboración, revisión y su aprobación final.

La Ley de Planeación encuaderna el proceso. Esta norma es de orden público e interés social y tiene como objetivo establecer los principios para llevar a cabo la planeación nacional de desarrollo y canalizar las actividades de la Administración Pública Federal (Ley de Planeación, D.O.F. 2018). Dicha ley contiene las bases para

la integración y funcionalidad del Sistema Nacional de Planeación, de tal forma, que le permite al Ejecutivo Federal coordinar sus actividades de planeación con las entidades federativas para promover y garantizar la participación democrática de los grupos sociales en la elaboración de los planes y programas. Dicho de otra manera, la Ley de Planeación apuntala el cómo, quién, porqué y con qué se desarrollarán las actividades de la Administración Pública Federal. Como se explica a continuación, la Ley de Planeación (D.O.F. 2018) establece:

«Artículo 1ro. – Las disposiciones de esta Ley son de orden público e interés social y tienen por objeto establecer:

I) *Las normas y principios básicos conforme a los cuales se llevará a cabo la Planeación Nacional del Desarrollo y encauzar en función de esta las actividades de la Administración Pública Federal;*
II) *Las bases de integración y funcionamiento del Sistema Nacional de Planeación Democrática;*
III) *Las bases para que el Ejecutivo Federal coordine las actividades de planeación de la Administración Pública Federal, así como la participación, en su caso, mediante convenio, de los órganos constitucionales autónomos y los gobiernos de las entidades federativas, conforme a la legislación aplicable*
IV) *Los órganos responsables del proceso de planeación;*
V) *Las bases de participación y consulta a la sociedad, incluyendo los pueblos y comunidades indígenas, a través de sus representantes y autoridades, en la elaboración del Plan y los programas a que se refiere esta Ley, y*
VI) *Las bases para que el Ejecutivo Federal concierte con los particulares las acciones a realizar para la elaboración y ejecución del Plan y los programas a que se refiere esta Ley».*

El proceso ha cambiado para proyectar una visión a largo plazo a beneficio de México. Si bien es cierto que los planes de desarrollo tienen una temporalidad de duración similar a la de cada gobierno en curso, en el 2015 se reformo el artículo 21 de la Ley de Planeación para modificar la duración de los mismos. En dicho proceso de planeación se debe incluir una visión a largo plazo de fomento económico nacional para impulsar elementos permanentes al desarrollo, crecimiento económico, sostenido y sustentable nacional. Por lo anterior, cada Presidente de la República debe considerar elementos de largo plazo con alcance hasta por 20 años para incentivar una política nacional de fomento y prosperidad económica.

B. Antecedentes históricos del Plan Nacional de Desarrollo

Nuestro país ha navegado muchas millas para adecuar el proceso de planeación democrática. A pesar de que el zarpe se inició desde tiempo atrás, se puede estimar que la principal pierna se recorrió en 1983. Como se indica en la Tabla 1, los planes nacionales de desarrollo de 1983 hasta 2018, tienen cualidades que los hacen diferentes uno del otro. Cada administración define los intereses nacionales conforme la situación que se vive en el país. A continuación, se describe la evolución de los planes nacionales de desarrollo durante el periodo 1983-2018.

Tabla 1.Características principales de los Planes Nacionales de Desarrollo 1983-2018

PERIODO	PRESIDENTE	PARTIDO POLÍTICO	CARACTERÍSTICAS
1983-1988	Miguel de la Madrid Hurtado	PRI	Se dio un salto evolutivo de la planeación nacional a través del Plan Nacional de Desarrollo (PND). En primera instancia, se promovió la reforma a los principios normativos de desarrollo económico y social de la Constitución Política de los Estados Unidos Mexicanos (CPEUM).
1989-1994	Carlos Salinas de Gortari	PRI	En este plan continuaron las transformaciones. Estuvo basado en los principios del Proyecto Nacional y en su estrategia de modernización. El plan tenía como objetivo primordial, la defensa de la soberanía y la promoción de los intereses de México en el mundo.
1995-2000	Ernesto Zedillo Ponce de León	PRI	El planeamiento de esta administración se enfocó en rescatar la economía del país. Se trataron los temas de soberanía, Estado de derecho, desarrollo democrático, desarrollo social y crecimiento económico. Sin embargo, se incrementó la pobreza, lo que conllevó a un cambio de preferencias políticas.
2001-2006	Vicente Fox Quesada	PAN	Este plan fue producto de un amplio proceso de participación ciudadana, dando como resultado la consolidación de tres grandes procesos: la planeación estratégica, el seguimiento y control, y el mejoramiento organizacional. Esta administración orientó sus acciones a los procesos de transición demográfica, social, económica y política.
2007-2012	Felipe de Jesús Calderón Hinojosa	PAN	Esta administración dio continuidad a la evolución de la planeación democrática. El plan consistió principalmente en el desarrollo humano sustentable y su propósito era crear nuevas oportunidades para las generaciones actuales y futuras. Los ejes y objetivos que conformaron este plan procuraban una mejor calidad de vida en la población.
2013-2018	Enrique Peña Nieto	PRI	El regreso del antiguo poder político derivó a generar nuevos cambios al Plan Nacional de Desarrollo. Por primera vez se buscó la articulación a nivel estratégico y se incorporaron indicadores que permitieron dar seguimiento al cumplimiento de los objetivos. Se alcanzaron logros importantes en materia de seguridad social y seguridad alimentaria, pero se rezagaron otras áreas como urbanización, vivienda, producción agrícola, pesquera y forestal.

Fuente: Elaboración propia.

1. Plan Nacional de Desarrollo 1983-1988

La evolución histórica legislativa del Plan Nacional de Desarrollo (PND), inicia desde 1983 durante el período presidencial de Miguel de la Madrid Hurtado. Al asumir como Titular del Poder Ejecutivo Federal el primero de diciembre de 1982, promovió la reforma a los principios normativos del desarrollo económico y social de la Constitución Política de los Estados Unidos Mexicanos (CPEUM). Como parte de citada reforma, el artículo 26 constitucional estableció que el Estado debía integrar un Sistema Nacional de Planeación Democrática. Derivado de ello se presentó el Plan Nacional de Desarrollo 1983-1988, publicado en el Diario Oficial de la Federación (DOF) el 31 de mayo de 1983, en los términos y en el plazo fijados por la nueva Ley de Planeación.

El plan respondía a la voluntad política de enfrentar los retos del desarrollo del país que se vivía en aquel tiempo, considerando mayor participación social. En ese sentido, se establecieron procedimientos para guiar y atender las demandas de la población, apoyándose en un proceso de diálogo y comunicación que implicaba foros de consulta ciudadana. Su propósito principal consistió en lo siguiente:

> «Mantener y reforzar la independencia de la nación, para la construcción de una sociedad que, bajo los principios del Estado de derecho, garantice libertades individuales y colectivas en un sistema integral de democracia y en condiciones de justicia social. Para ello requerimos de una mayor fortaleza interna: de la economía nacional, a través de la recuperación del crecimiento sostenido, que permita generar los empleos requeridos por la población, en un medio de vida digno; y de la sociedad, a través de una mejor distribución del ingreso entre familias y regiones, y el continuo perfeccionamiento del régimen democrático». (PND, 1983-1988, pág. 576)

Derivado de lo anterior, se define que el propósito principal para el gobierno de Miguel de la Madrid, se constituyó en cuatro rutas: primero, conservar y fortalecer las instituciones democráticas, segundo, vencer la crisis; tercero, recuperar la capacidad de crecimiento; y cuarto, iniciar los cambios cualitativos que requería el país en sus estructuras económicas, políticas y sociales. Finalmente, el Plan se llevó a cabo por el Poder Ejecutivo con la activa participación de la sociedad, planteándose como objetivo esencial enfrentar la crisis con eficacia y justicia que en ese entonces demandaba el país. (PND, 1983-1988).

2. Plan Nacional de Desarrollo 1989-1994

Más transformaciones siguieron. El PND 1989 – 1994 fue aprobado por decreto del entonces presidente Carlos Salinas de Gortari, el 31 de mayo de 1989. Estuvo basado en los principios del proyecto nacional contenidos en la CPEUM y en la estrategia de modernización nacional que el propio plan exige. Este plan tenía como objetivo primordial, la defensa de la soberanía y la promoción de los intereses de México en el mundo; la ampliación de la vida democrática; la recuperación del creci-

miento con estabilidad de precios y el mejoramiento del nivel de vida de la sociedad. En ese sentido, se tiene que el PND cumplía satisfactoriamente con el mandato constitucional y legal de dar orientación y otorgar de instrumentos básicos a los esfuerzos del Estado y la comunidad, para alcanzar los objetivos nacionales. Estaba orientado al compromiso político del Gobierno de la República de enfrentar, con el apoyo de todos, los retos del cambio que exigía la nación. Por ello, el plan estaba previsto para atender las demandas principales de los grupos mayoritarios, en los siguientes campos: seguridad pública, educación, salud y asistencia social, alimentación, vivienda, servicios básicos, cultura y esparcimiento. La estrategia fundamental en la que se basaba la ejecución de citado plan y el logro de las metas en él contenidas, era la modernización: modernización de la administración pública, modernización de las instituciones y modernización de la economía (PND, 1989-1994).

3. Plan Nacional de Desarrollo 1995-2000

El planeamiento de esta administración se enfocó a rescatar la economía del país. En el sexenio del entonces presidente Ernesto Zedillo Ponce de León, el plan fue publicado en el Diario Oficial de la Federación el 31 de mayo de 1995. Esta administración elaboró cinco capítulos muy concretos, como a continuación se describen: 1. Soberanía; 2. Por un Estado de Derecho y un país de leyes; 3. Desarrollo democrático; 4. Desarrollo social, y 5. Crecimiento económico. Conjuntamente, en un anexo se enlistaron los programas sectoriales.

En ese sentido, en el Plan Nacional de Desarrollo 1995-2000 se presentaron los cinco objetivos siguientes (PND, 1995-2000):

1) Fortalecer el ejercicio pleno de la soberanía nacional, como valor supremo de nuestra nacionalidad y como responsabilidad primera del Estado mexicano.
2) Consolidar un régimen de convivencia social regido plenamente por el derecho, donde la ley sea aplicada a todos por igual y la justicia la vía para la solución de los conflictos.
3) Construir un pleno desarrollo democrático con el que se identifiquen todos los mexicanos y sea base de certidumbre y confianza para una vida política pacífica y una intensa participación ciudadana.
4) Avanzar a un desarrollo social que propicie y extienda en todo el país, oportunidades de superación individual y comunitaria, bajo los principios.
5) Promover un crecimiento económico vigoroso, sostenido y sustentable en beneficio de los mexicanos.

Ernesto Zedillo abordó el país con una situación económica, política y social muy difícil. La población en estado de pobreza se había incrementado a un nivel muy alarmante. Además, se presentó el aumento de inconformistas armados en desacuerdo con el tipo de gobierno que se vivía en ese entonces. Dichas situaciones alentaron a la sociedad mexicana a cambiar sus preferencias políticas.

4. Plan Nacional de Desarrollo 2001-2006

Es importante hacer mención que el PND de este sexenio tuvo variantes respecto a los anteriores. Este plan fue producto de un amplio proceso de participación ciudadana que comenzó en el periodo de transición presidencial del año 2000 y culminó con la publicación de este documento. El cambio era necesario, dado que por primera vez llegaba al gobierno un presidente de un partido diferente al que había estado gobernando durante más de 70 años seguidos. Así, el presidente Vicente Fox Quesada y su gobierno (entre ellos personalidades de la iniciativa privada) adecuaron el Sistema Nacional de Planeación a tres grandes procesos: la planeación estratégica, el seguimiento y control, y el mejoramiento organizacional. En adición, la administración concentró sus acciones gubernamentales a los procesos de transición demográfica, social, económica y política, aceptando el reto de mitigar los costos y potenciar las oportunidades para que el plan de desarrollo fuera viable.

5. Plan Nacional de Desarrollo 2007-2012

La evolución de la planeación democrática en México también se dio en esta administración. Con el PND 2007-2012, el entonces presidente Felipe de Jesús Calderón Hinojosa arrumbó su aparato gubernamental a procurar como eje principal «el Desarrollo Humano Sustentable». Calderón al presentar su Plan mencionó que «el propósito del desarrollo consiste en crear una atmósfera en que todos puedan aumentar su capacidad y las oportunidades puedan ampliarse para las generaciones presentes y futuras» (2007). La administración de Calderón modeló de manera muy estrecha con los programas sectoriales, especiales, institucionales y regionales (Méndez, 2012). Los ejes y objetivos que conformaron ese PND procuraban una mejor calidad de vida de la población.

6. Plan Nacional de Desarrollo 2013-2018

El PND de esa administración también tuvo cambios. El 17 de mayo de 2013, el entonces presidente Enrique Peña Nieto presentó el Plan Nacional de Desarrollo 2013 - 2018, siendo publicado tres días después en el Diario Oficial de la Federación. La conformación de este plan fue por medio de foros de consulta ciudadana por internet, propuestas ciudadanas en ventanillas físicas y electrónicas, foros de consulta y mesas sectoriales (PND, 2013).

La administración de Peña Nieto designó cinco metas nacionales. El objetivo general en este sexenio fue llevar a México a su máximo potencial. Como indica la tabla 2, el PND estableció cinco metas nacionales y tres estrategias transversales.

Tabla 2. Metas nacionales y estrategias transversales del PND 2013-2018

Metas Nacionales	Estrategias transversales
México en paz	Democratizar la productividad
México incluyente	
México con educación de calidad	Gobierno cercano y moderno
México próspero	
México con responsabilidad global	Perspectiva de género

Fuente: PND 2013-2018

El proceso de evaluación y control del PND fue diferente. A través del Consejo Nacional de Evaluación de la Política de Desarrollo Social se elaboró el Balance del Sexenio, en donde por primera vez se buscó la articulación entre el nivel estratégico de la planeación nacional y el nivel operativo, a través de la vinculación de los objetivos e indicadores sectoriales con los programas sociales. Así mismo, se logró la incorporación de indicadores en la planeación nacional, que permitieron dar un seguimiento oportuno al grado de cumplimiento de los objetivos; significó un gran avance en la administración 2013-2018. Como resultado de análisis de referido balance se obtuvo una radiografía en este campo, dando como resultado la evidencia de «logros importantes en materia de seguridad social y de seguridad alimentaria, pero se rezagaron otras áreas, como urbanización y vivienda, producción agrícola, pesquera y forestal» (CONEVAL, 2018).

D. Plan Nacional de Desarrollo 2019-2024

La forma de elaboración del PND 2019 – 2024 es diferente. Este documento está orientado a redefinir la conducta de los servidores públicos y establecer el apoyo social como medio para generar e impulsar el desarrollo humano de la sociedad mexicana. A lo largo de este escrito se aprecia que el proceso de planeación democrática en las administraciones anteriores reflejó un marco convencional de objetivos, estrategias y líneas de acción. Sin embargo, más que describir una serie de pasos, la forma en que fue estructurado el PND 2019-2024 pudiera ser encaminada a describir un marco ideológico que convenza a las y los servidores públicos a desarrollar sus funciones en pro de la sociedad.

Esto lo describe en la introducción. En la presentación del PND 2019 – 2024, el titular del Ejecutivo Federal, Lic. Andrés Manuel López Obrador, hace una reseña de las acciones de los gobiernos pasados y el cambio que podría generar la «Cuarta Transformación». Lo que refiere de la siguiente forma:

> «Tenemos ante el mundo la responsabilidad de construir una propuesta posneoliberal y de convertirla en un modelo viable de desarrollo económico, ordenamiento político y convivencia entre los sectores sociales. Debemos demostrar que sin autoritarismo es posible imprimir un rumbo nacional, que la modernidad puede ser forjada desde abajo y sin excluir a nadie y

que el desarrollo no tiene porqué ser contrario a la justicia social» (PND 2019-2024, D.O.F. 12-07-2019, Pág. 4).

A continuación, se describen las características encontradas del PND 2019-2024.

I. Bases conductuales

La navegación del país se materializa con capital humano nutrido por valores. El plan actual establece doce principios rectores para la conducta de los servidores públicos. A continuación, se detallan dichos principios:

- Honradez y honestidad: encaminado a eliminar la corrupción por hecho o cohecho.
- No al gobierno rico con pueblo pobre: destinado a evitar los gastos superfluos y reprimir el robo al erario público. Además, de incentivar los programas sociales y la *Austeridad Republicana*.
- Al margen de la ley nada; por encima de la ley, nadie: orientando a mantener el cumplimiento de la ley y el Estado de Derecho. Procura además el convencimiento y el diálogo.
- Economía para el bienestar: inclina la economía del país al bienestar de la sociedad. Lo anterior, mediante austeridad y eliminando la corrupción.
- El mercado no sustituye al Estado: consolidar la figura garante de la soberanía del Estado y regulador de conflictos.
- Por el bien de todos primero los pobres: realizar programas sociales buscando el desarrollo de los «más débiles y desvalidos».
- No dejar a nadie atrás, no dejar a nadie fuera: establecer políticas públicas plurales e integrales.
- No puede haber paz sin justicia: desarrollar políticas en materia de seguridad pública encaminadas a reducir la criminalidad por medio de estrategias integrales de desarrollo humano. Así como, integrar la Guardia Nacional como policía de proximidad y desarrollar mayor inteligencia criminal.
- El respeto al derecho ajeno es la paz: mantener los principios de política exterior de no intervención, autodeterminación y el desarrollo colectivo.
- No más migración por hambre o por violencia: buscar que nuestros conciudadanos prefieran permanecer en el país mediante políticas públicas integrales, que aterriza en el principio de «no dejar a nadie atrás, no dejar a nadie fuera».
- Democracia significa el poder del pueblo: crear mecanismos de consulta ciudadana para empoderar a la sociedad e incentivar su participación en los asuntos de gobierno.
- Ética, libertad y confianza: generosidad, empatía, libertades a fin de reforzar el pacto social entre los mexicanos con su gobierno.

Dentro de estos principios se pueden apreciar pensamientos utópicos. Estos ideales deberán tener cambios de cultura, no solo hacia el interior de las instituciones, sino también hacia la misma sociedad mexicana.

2. Estructura y diseño

Comparando el contenido del PND 2019-2024 con otros planes, se observa que no fue diseñado con la estructura definida por la Ley de Planeación. Dicha diferencia pudiera traer conflictos normativos que habrán de regularse eventualmente. Conforme dicha Ley, su artículo número 21 Ter. establece que el PND deberá contener por lo menos lo siguiente:

1) Diagnóstico general: referente a la situación actual, temas prioritarios y perspectivas a largo plazo.
2) Ejes generales: donde se agrupen los temas prioritarios que impulsen el desarrollo nacional.
3) Objetivos específicos: objetivos que se pretenden alcanzar para atender los temas prioritarios.
4) Estrategias: mismas que sirven para ejecutar las acciones que permitan alcanzar los objetivos específicos.
5) Indicadores de desempeño: indicadores que permitan dar seguimiento al logro de los objetivos.

Tales inconsistencias pudieran ser subsanadas en un documento adicional. El escrito como tal, tendría que contemplar la adecuación de los objetivos estrategias y líneas de acción que permita la alineación de programas y proyectos públicos. Lo anterior se deduce toda vez que el PND 2019 – 2024, sin especificar tácitamente, identifica como directrices o ejes generales, los siguientes:

- Política y gobierno
- Política social
- Economía

Cada uno de estos, contempla temas que se pueden considerar como Objetivos. Así mismo, en política social y economía, considera programas sociales y proyectos regionales. A continuación, se detallan los ejes generales reconocidos:

1. Política y gobierno

Sin dar una clara concepción de lo que será este eje, define los siguientes cursos de acción:

1.1 Erradicar la corrupción, el dispendio y la frivolidad

1.1.1 Combate a la corrupción y conflicto de intereses

1.1.2 Reorientar los presupuestos a programas significativos y de alto impacto social y económico.

1.2 Recuperar el Estado de Derecho

1.2.1 Erradicar el robo de combustible y evasión fiscal.

1.2.2 Combate al lavado de dinero, tráfico de armas y otros ilícitos.

1.2.3 Reducir al mínimo diferencias salariales de servidores públicos dependiendo de rango y niveles.

1.3 Separar el poder político del poder económico

1.3.1 Estricta vigilancia a conflicto de interés.

1.3.2 Sancionar como delito grave todo intento de distorsión electoral.

1.4 Cambio de paradigma en seguridad

1.4.1 Cambio de medidas de guerra por una política de paz y seguridad integral, basado en la Estrategia Nacional de Seguridad Pública

1.4.2 Establecimiento de la Guardia Nacional y coordinaciones nacionales, estatales y regionales.

Del punto 1.4.1 Estrategia Nacional de Seguridad Pública enunciada en el plan en comento, se encontraron los siguientes objetivos:

1) Erradicar la corrupción, reactivar la procuración de justicia
2) Garantizar empleo, educación, salud y bienestar
3) Pleno respeto de los Derechos Humanos
4) Regeneración ética de las instituciones y de la sociedad
5) Reformular el combate a las drogas
6) Emprender la construcción de la paz
7) Recuperación y dignificación de las cárceles
8) Articular la seguridad nacional, la seguridad pública y la paz.

Se fortalecerán las capacidades institucionales para:

- Ejecución del Programa para la Seguridad Nacional del gobierno.
- Establecer un Sistema Nacional de Inteligencia.
- Actualizar catálogo y clasificación de instalaciones estratégicas.
- Fortalecer y mantener la seguridad interior y garantizar la defensa exterior del país
- Promover el concepto de cultura de Seguridad Nacional
- Mejorar las capacidades tecnológicas, de investigación científica y generación de inteligencia estratégica.

9) Coordinaciones nacionales, estatales y regionales.
10) Repensar la Seguridad Nacional y reorientar a las Fuerzas Armadas
    - El gobierno procurará incrementar la confianza de la población civil a las Fuerzas Armadas
    - El Ejército y la Armada de México conservaran sus tareas constitucionales en la preservación de la Seguridad Nacional y la integridad del territorio nacional, así como asistencia a la población en casos y zonas de desastre.
11) Establecer la Seguridad Nacional.
    - Se dispondrá de las instituciones castrenses en acciones de seguridad pública por cinco años hasta 2023.

– Estará adscrita a la Secretaría de Seguridad y Protección Ciudadana, quien presidirá la Junta de Jefes de Estado Mayor, compuesta por dependencias de Seguridad, Defensa Nacional y Marina.
– Será una institución de carácter mixto, con mando civil y sus integrantes tendrán entrenamiento, jerarquía y estructura militar.
– En su fase inicial se conformará con elementos de las Policías Militar, Naval y Federal.
– Como objetivos, su crecimiento hasta 140 mil elementos con cobertura en 266 regiones distribuidas en las 32 entidades federativas.

1.5 Hacia una democracia participativa:

La sociedad debe participar e involucrarse en las decisiones relevantes del país.

1.6 Revocación de mandato:

Establecer el mecanismo de Revocación de mandato, como una forma efectiva de control de los mandantes sobre los mandatarios.

1.7 Consulta Popular:

El gobierno federal someterá a consulta las decisiones estratégicas de interés nacional, consultará a las poblaciones los asuntos de interés regional y local.

1.8 Mandar obedeciendo

Los funcionarios públicos de todos los niveles están obligados a servir, no a servirse; a desempeñarse como representantes de la voluntad popular, no como usurpadores; a acordar no a imponer; a recurrir siempre a la razón no a la fuerza.

1.9. Política exterior, recuperación de los principios

1.9.1 La no intervención

1.9.2 Solución pacífica de controversias

1.9.3 La cooperación internacional para el desarrollo, principalmente con los países de América del Norte, América Latina y el Caribe

1.10 Migración, soluciones de raíz

1.10.1 Red de consulados como defensorías de migrantes

1.10.2 Creación de empleos dignos, desarrollo regional y edificación del Estado de Bienestar.

1.10.3 Garantizar la seguridad del libre tránsito de extranjeros.

1.10.4 Sensibilizar a la población para erradicar racismo, xenofobia y paranoia.

1.11 Libertad e igualdad

1.11.1 Priorizar las libertades sobre las prohibiciones

1.11.2 Igualdad efectiva de derechos entre individuos.

1.11.3 Libertad de elección ente todos los ciudadanos en todos los aspectos

2. Política social

La política social del Gobierno de la Republica tiene como propósito principal que los mexicanos convivan en un ambiente social de bienestar, incluyente, plural y con justicia social. El propósito del Gobierno Federal descrito en este documento será el de impulsar

«una nueva vía hacia el desarrollo para el bienestar, una vía en la que la participación de la sociedad resulta indispensable y que puede definirse con este propósito: construiremos la modernidad desde abajo, entre todos y sin excluir a nadie» (PND. 2019-2024, D.O.F. 12-07-2019, Pág. 13).

Estas acciones las desarrollará mediante los siguientes cursos de acción.

2.1. Construir un país con bienestar

2.1.1. Construir la modernidad desde abajo, entre todos y sin excluir a nadie.

2.1.2.Combatir la pobreza y marginación de sectores con el lema «primero los pobres».

2.2.Desarrollo sostenible

El Ejecutivo considerará los impactos que tendrán las políticas y programas en el tejido social, la ecología, y en los horizontes políticos y económicos del país.

2.3. Derecho a la educación

2.3.1. Garantizar el acceso a todos los jóvenes a la educación y revertir la reforma educativa.

2.3.2. Las Universidades para el Bienestar «Benito Juárez García» ofrecen en 100 planteles, 32 mil plazas para estudiantes que recibirán beca de $2,400 pesos mensuales.

2.4. Salud para toda la población

El derecho a la salud le es denegado parcial o totalmente al sector más desprotegido de la población.

2.5. Instituto Nacional de Salud para el Bienestar

Dará servicio en todo el territorio nacional, a personas no afiliadas al IMSS o al ISSSTE.

2.6. Cultura para la paz, para el bienestar y para todos

Promover la difusión, enriquecimiento y consolidación de la diversidad cultural.

2.7. Programas Sociales

2.7.1. Bienestar de las personas adultos mayores

2.7.2. Pensión para el Bienestar de las personas con discapacidad

2.7.3 Programa Nacional de Becas para el Bienestar «Benito Juárez»

2.7.4. Jóvenes Construyendo el Futuro

2.7.5. Jóvenes Escribiendo el Futuro

2.7.6. Sembrando Vidas

2.7.7. Programa Nacional de Reconstrucción

2.7.8. Desarrollo Urbano y Vivienda

2.7.8 Tandas para el Bienestar

3. Economía

El propósito principal de este eje rector es detonar el crecimiento. Este plan propone que dicho objetivo sea alcanzado por medio de los siguientes cursos de acción:

3.1. Mantener finanzas sanas

3.1.1. No se recurrirá a endeudamiento para financiar gastos del Estado

3.1.2. No gastará más dinero del que ingrese a la hacienda pública

3.2.3. Se respetará autonomía del BANXICO

3.2. No más incrementos impositivos

3.2.1. No habrá incrementos de impuestos en términos reales

3.2.2. Ni aumento a combustibles por encima de la inflación

3.2.3. Tarifas eléctricas se reducirán a mediados del sexenio.

3.3. Respeto a los contratos existentes y aliento a la inversión privada

El gobierno respetará los contratos suscritos por administraciones anteriores y se alentará la inversión privada.

3.4. Rescate del sector energético

3.4.1. Rehabilitación de refinerías existentes y plantas de fertilizantes

3.4.2. Construcción de una nueva refinería

3.4.3. Modernización de instalaciones generadoras de electricidad

3.5. Creación del Banco del Bienestar

Ofrecer servicios bancarios a beneficiarios de programas sociales, con 7 mil sucursales.

3.6. Construcción de Caminos Rurales

Comunicar 350 cabeceras municipales de Oaxaca y Guerrero.

3.7. Cobertura de Internet para todo el país

Mediante la instalación de internet inalámbrico en todos el país, se ofrecerá a toda la población conexión en carreteras, hospitales, plazas públicas, escuelas y espacios comunitarios.

3.8. Ciencias y tecnología

Promoverá investigación científica y tecnología, apoyo a estudiantes y académicos con becas y estímulos.

3.9. El deporte es salud, cohesión social y orgullo nacional

3.9.1 Prioridad a la activación física, deporte para todos

3.9.2. Creación comisión de fomento al beisbol, caminata y boxeo.

3.9.3. Apoyo al deporte de alto rendimiento con transparencia

3.10. Proyectos regionales

3.10.1. Tren Maya

3.10.2. Desarrollo del Istmo de Tehuantepec

3.10.3. Zona lLibre de la frontera norte

3.10.4. Aeropuerto internacional «Felipe Ángeles» en Santa Lucía

3.11. Autosuficiencia alimentaria y rescate del campo

3.11.1. Producción para el campo

3.11.2. Apoyo a cafetaleros y cañeros del país

3.11.3. Precios de garantía para los cultivos de maíz, frijol, trigo panificable, arroz y leche

3.11.4. Crédito ganadero a la palabra

3.11.5. Creación del Organismo Seguridad Alimentaria Mexicana (SEGALMEX)

Como se mencionó inicialmente, la redacción del PND 2019 – 2024 esta alejada de los formalismos y normas convencionales. La estructura, más que un Plan con objetivos y líneas de acción, refiere la construcción de un marco ideológico con principios y buenos propósitos, que bien diseñados pudieran ser alcanzados. Sin embargo, para lograr lo anterior, deben orientarse acciones destinadas a cambiar la cultura de las y los mexicanos. No es imposible, pero si muy difícil.

E. Programa Sectorial de Marina

El Programa Sectorial de Marina se deriva de los objetivos y estrategias del Plan Nacional de Desarrollo (PND). Los programas sectoriales indican los proyectos que cada dependencia de la Administración Pública Federal, requiere desarrollar para cumplir con sus funciones y atribuciones. Estos documentos son elaborados para sustentar la asignación de recursos destinados al cumplimiento de las metas proyectadas y estar en condiciones de coadyuvar con los objetivos del PND (SHCP, D.O.F., 2013). Los programas sectoriales deben de estar alineados con el PND, es decir, así como este plan tiene objetivos, estrategias líneas de acción e indicadores, de igual forma los programas sectoriales de las dependencias «cabezas de sector» deben de considerar esos mismos rubros, hablando también de los programas derivados del PND como son; programas sectoriales, institucionales, especiales y regionales (SEGOB, 2016).

El Programa Sectorial de Marina (PSM) es un instrumento de planeación. La Secretaría de Marina (SEMAR) como cabeza de sector elabora dicho programa, analizando las estrategias del PND con la finalidad de alinearlas en legalidad y propósito, hacia los objetivos, estrategias y líneas de acción que satisfagan los esfuerzos (SEMAR, 2013).

> «Para la elaboración de los diferentes planes y programas se debe de tomar en cuenta que existen niveles en la planeación, en el primer nivel se encuentra como plan rector el PND el cual por ser un proyecto de nación y herramienta que utiliza el estado para llevar a cabo los objetivos nacionales que expresa las aspiraciones y políticas de desarrollo, en el segundo nivel se encuentran los programas sectoriales, especiales, regionales e

> institucionales, considerando que a estos programas también se diseñan en base a objetivos específicos que define la acción gubernamental, y por último se tiene el tercer nivel que básicamente es el programa presupuestal, Este programa se desarrolla paralelamente a los planes y programas con la finalidad de considerar los objetivos prioritarios a fin de organizar las asignaciones de recursos» (SEGOB, 2019).

Puesto que los programas sectoriales se derivan del PND, se considera a nuestra Carta Magna como principal fuente normativa. Este programa también se fundamenta en la Ley de Planeación artículos 22, 23, 27, 29 párrafo sexto, 30, 31, 32, previo dictamen de la Secretaría de Hacienda y Crédito Público (SHCP) (Ley de Planeacion, D.O.F., 2018); la Ley Orgánica de la Administración Pública Federal artículo 9, atribuciones previstas en el numeral 30 fracción de la I a la XXVI (LOAPF, D.O.F., 2019); la Ley Federal de Presupuesto y Responsabilidad Hacendaria, artículo 24 fracción I y II, artículo 25 fracción I y III, artículo 27 fracción I, II y III (LFPRH, D.O.F., 2015); la Ley Orgánica de la Armada de México, artículos 1 y 2, fracción XVI (LOAM, D.O.F., 2017); el Reglamento Interior de la Secretaría Marina (RISM), artículos 1 y 3 (RISM, D.O.F., 2015); además de otras leyes que el Ejecutivo Federal tenga a bien disponer, de acuerdo con las políticas vigentes.

El proceso de elaboración del PSM o programas sectoriales de otras dependencias se lleva acabo de la siguiente forma: una vez aplicados los fundamentos de la elaboración del PND por el Ejecutivo, habiéndose entregado a la Cámara de Diputados y siendo aprobado este, paralelo a él se elaboran los programas presupuestarios. ¿Qué son los programas presupuestarios? «Los programas presupuestarios son programas que permiten organizar las asignaciones de recursos» (Trasparencia Presupuestaria, 2016) conforme a la clasificación por grupos y modalidades como son:

> «programas federales, de los cuales se derivan los programas sujetos a reglas de operación, programa de subsidio y otros programas para los proyectos de inversión y por último se tienen las actividades específicas de las cuales se derivan la prestación de servicios públicos, producción de bienes públicos, planeación, formulación, implementación, seguimiento y evaluación de las políticas públicas, etcetera. Con respecto a la clasificación de los programas derivados del PND se tienen los siguientes: programas sectoriales los cuales son dependencias denominadas también cabeza de sector, programas regionales los cuales son aquellos considerando al país dividido en cinco regiones geográficas, programas institucionales (SHCP, 2019)».

Estos programas son para aquellas dependencias como los institutos de seguridad social, los cuales dependen de una dependencia cabeza de sector, mismos que también deben elaborar su propio programa institucional para la asignación de recursos, por ejemplo: existe un programa sectorial de salud (Secretaría de Salud como cabeza de sector), aparte las instituciones dependientes de esa dependencia deben hacer su propio programa institucional, alineado con el programa de la cabeza de sector de su ramo; también se tienen «programas especiales los cuales son aquellos

programas que se crean para mejorar algún aspecto en un sector determinado, por ejemplo: programas para el desarrollo empresarial, para el desarrollo rural sostenible, de inversiones y finanzas públicas» (SHCP, 2019), etcetera, y por último se tienen los programas que son comunes en todas las dependencias, por ejemplo: el programa de equidad de género, el cual le es designado a una dependencia en particular para su administración y ejecución; sin embargo, todas las demás dependencias participan en su aplicación para ejecutarla, difundirla e implantarla como parte de las estrategias nacionales (SHCP, 2015); considerando que las demás dependencias deben de participar y apegarse a las mismas políticas, debiendo ser considerados debido a que para su implementación requiere la asignación de recursos de la federación.

Con base en lo anterior, la SEMAR como cabeza de sector (Sector Marina) no cuenta con órganos desconcentrados, únicamente depende de ella la Armada de México, misma que es el brazo armado del poder Ejecutivo nacional (LOAM, D.O.F., 2017).

Una vez autorizado el PND por presidencia, se llevan a un acabo reuniones con los titulares de cada dependencia (en este caso de Marina) interviniendo ejecutivos de la Secretaría de la Función Pública, la Oficina de la Presidencia de la República (PR) y de la SHCP (SHCP, 2019), con la finalidad de coordinar y desarrollar los programas estableciendo los vínculos y alineaciones entre el PND del período presidencial, con los programas, derivados de ese plan (sectoriales, institucionales, especiales y regionales) con los programas presupuestarios, integrando un proceso de planeación, programación, presupuestación y evaluación orientado al logro de resultados, definiendo los roles y responsabilidades de las dependencias de la Administración Pública Federal.

Una vez finalizado el dictamen y obteniéndose la aprobación del proyecto del Orograma Sectorial de la dependencia correspondiente (Marina) y con la finalidad materializar los proyectos de programas sectoriales, se lleva a cabo el proceso de validación, adecuaciones, opiniones y aprobación de los Proyectos de Programa Sectorial PPS. Esta fase concluye con la publicación del Programa Sectorial en el Diario Oficial de la Federación (D.O.F), por lo que la Secretaría de Marina procede a ejecutar citado plan, convirtiendo en acciones los objetivos y las estrategias planeadas (SHCP, 2019).

El PSM se proyecta a seis años y debe ser evaluado anualmente para analizar los resultados. Las actualizaciones al programa pueden ser realizadas cada año con la finalidad de alcanzar las metas programadas o ajustarlas al presupuesto, ya que este puede cambiar o reajustarse por recortes o implementación de nuevos programas. Las evaluaciones pueden ser llevadas a cabo por organismos autónomos los cuales comparan las metas y objetivos planeados y los resultados obtenidos, considerando el ciclo de Planeación, Programación, Presupuestación, Ejercicio y Control, Seguimiento, Evaluación, Rendición de cuentas y así sucesivamente de forma cíclica (SHCP, 2019). Actualmente el PSM 2019-2024 no ha sido publicado.

III. Conclusiones

México como un todo, puede ser comparado a un gran navío. El Titular del Ejecutivo Federal en nuestro país, es el líder que traza colegiadamente el plan de

navegación que le da el rumbo a México. El Plan Nacional de Desarrollo es la carta de navegación que armoniza y focaliza un objetivo que oriente el funcionamiento de dichas instituciones. Finalmente, el Presidente de la Republica emplea su maquinaria, personificada por las dependencias y entidades de la Administración Pública Federal, para lograr el arribo a ese puerto ideal, el desarrollo de la sociedad mexicana.

La evolución del proceso de planeación de la Administración Pública Federal tiene implicaciones circunstanciales. Las diferencias existentes entre los planes nacionales de desarrollo de 1983 a 2018, tuvieron razón a que cada gobierno en turno se enfocó en implementar acciones a mediano y corto plazo, para trasformar las condiciones económicas, políticas y sociales imperantes en el país. Cada administración generó estrategias para resolver dichas eventualidades y con ello, estimular la estabilidad y crecimiento de nuestro país. Sin embargo, la historia mostró que las circunstancias traspasaron los limites temporales de cada administración. La pobreza, desigualdad económica, carencias de oportunidades laborales y falta de atención de salud se mantienen presentes en nuestro país, sin importar la ideología del aparato gubernamental. Como consecuencia de ello, la población eligió buscar en otro tipo de ideología política, un líder que nos encamine hacia el desarrollo nacional.

El Ejecutivo Federal tiene como uno de sus principales retos, demostrar que el PND 2019-2024 llevará la navegación del país hacia un mejor futuro y que las líneas de acción trazadas son las adecuadas. Afirmar en este momento, mediante una evaluación objetiva, la efectividad del PND-2019-2024 sería muy apresurado, ya que la presente administración apenas comienza. Al término de esta, los resultados hablarán por sí solos y solo entonces se podrá emitir un juicio con mayor validez. Corresponde en estos momentos, a las dependencias y entidades de la Administración Pública Federal sumar toda su capacidad y esfuerzo al del Ejecutivo Federal, con el fin de alcanzar las metas establecidas.

Bibliografía

- Calderón, F. d. (2007). *Plan Nacional de Desarrollo 2007-2012.* México: Presidente de la República.
- CONEVAL. (15 de enero de 2018). *Consejo Nacional de Evaluación de la Política de Desarrollo Social.* Obtenido de https://www.coneval.org.mx/Evaluacion/IEPSM/Documents/PND_2013_2018_Balance_del_Sexenio.pdf
- CPEUM, D.O.F. (12 de julio de 2019). *Diario Oficial de la Federacion.* Obtenido de Diario Oficial de la Federacion: https://dof.gob.mx/nota_detalle.php?codigo=5565599&fecha=12/07/2019
- Jiménez, N. P. (29 de Enero de 2015). *Planeación de la Administración Pública. Ensayo.* Recuperado el 16 de Agosto de 2019, de https://www.gestiopolis.com/planeacion-de-la-administracion-publica-ensayo/
- Ley de Planeacion, D.O.F. (16 de febrero de 2018). *Camara De Diputados Del H Conreso De La Union.* Obtenido De Camara De Diputados Del H Conreso De La Union: http://www.diputados.gob.mx/LeyesBiblio/pdf/59_160218.pdf#targetText=Artículo%203o.-%20Para%20los%20efectos,Constitución%20y%20la%20ley%20establecen.
- LFPRH, D.O.F. (30 de diciembre de 2015). Camara De Diputados Del H Conreso De La Union. Obtenido De Camara De Diputados Del H Conreso De La Union: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPRH_301215.pdf
- LOAM, D.O.F. (19 de mayo de 2017). Camara De Diputados Del H Conreso De La Union. Obtenido De Camara De Diputados Del H Conreso De La Union: http://www.diputados.gob.mx/LeyesBiblio/pdf/249_190517.pdf
- LOAPF, D.O.F. (14 de mayo de 2019). Camara De Diputados Del H Conreso De La Union. Obtenido De Camara De Diputados Del H Conreso De La Union: http://www.senado.gob.mx/comisiones/desarrollo_social/docs/marco/Ley_OAP.pdf
- Méndez, A. A. (2012). Análisis al Plan Nacional. México: ANFECA.
- Nieto, E. P. (2013). Plan Nacional de Desarrollo 2013-2018. México: Presidente de la República.
- PND. (diciembre de 1983-1988). Plan Nacional de Desarrollo 1983-1988. Recuperado el 19 de agosto de 2019, de www.juridicas.unam.mx
- PND. (05 de 31 de 1989-1994). Decreto por el que se aprueba el Plan Nacional de Desarrollo 1989-1994. Recuperado el 19 de agosto de 2019, de http://www.coespo.sonora.gob.mx/documentos/Normatividad/PND/PND%201989-1994.pdf
- PND. (1995-2000). Plan Nacional De Desarrollo 1995-2000. Recuperado el 18 de agosto de 2019, de http://ual.dyndns.org/biblioteca/Finanzas_Publicas_II/Pdf/Unidad_18.pdf
- PND. (20 de mayo de 2013). Plan Nacional de Desarrollo 2013-2018.
- RISM, D.O.F. (17 de noviembre de 2015). Camara De Diputados Del H. Conreso De La Union. Obtenido De Camara De Diputados Del H. Conreso De La Union: https://www.dof.gob.mx/nota_detalle.php?codigo=5415535&fecha=17/11/2015
- Sanchez, I. (6 de Mayo de 2010). Administración General 1. Recuperado el 15 de Agosto de 2019, de https://adminteso1.blogspot.com/2010/05/3-planeacion.html
- SEGOB. (15 de agosto de 2016). Diario Oficial de la Federacion. Obtenido de Diario Oficial de la Federacion: http://www.dof.gob.mx/nota_detalle.php?codigo=5447909&fecha=15/08/2016
- SEGOB. (12 de julio de 2019). Diario Oficial de la Federacion. Obtenido de Diario Oficial de la Federacion.

- SEMAR. (s/f de febrero de 2013). SEMAR, Plan Nacional de Desarrollo. Obtenido de SEMAR, Plan Nacional de Desarrollo.
- SHCP. (20 de noviembre de 2015). mx/shcp/acciones y programas. Obtenido de mx/shcp/acciones y programas: https://www.gob.mx/shcp/acciones-y-programas/seguimiento-de-los-programas-transversales-especiales-sectoriales-regionales-e-institucionales-derivados-del-pnd-2013-2018
- SHCP. (30 de enero de 2019). lopezdoriga.com. Obtenido de lopezdoriga.com: https://lopezdoriga.com/wp-content/uploads/2019/02/pnd-2019-2024-anteproyecto.pdf
- SHCP. (16 de marzo de 2019). Plan Nacional de Desarrollo Diagnostico del Eje No. 2. Obtenido de Plan Nacional de Desarrollo Diagnostico del Eje No. 2: https://www.gob.mx/shcp/documentos/plan-nacional-de-desarrollo-diagnostico-del-eje-no-2
- SHCP. (17 de junio de 2019). Trasparencia Presupuestaria, Observatorio Del Gasto. Obtenido De Trasparencia Presupuestaria, Observatorio del gasto: https://www.transparenciapresupuestaria.gob.mx/es/PTP/Programacion
- SHCP, D.O.F. (s/d de diciembre de 2013). bancomext. Obtenido de bancomext: https://www.bancomext.com/wp-content/uploads/2014/07/guia_tecnica_pnd_2013-2018.pdf
- TRASPARENCIA PRESUPUESTARIA. (15 de marzo de 2016). Trasparencia Presupuestaria, Observatorio Del Gasto. Obtenido De Trasparencia Presupuestaria: https://www.transparenciapresupuestaria.gob.mx/es/PTP/Glosario
- Unión, C. d. (16 de Febrero de 2018). H. Congreso de la Unión. Recuperado el 16 de Agosto de 2019, de http://www.diputados.gob.mx/LeyesBiblio/pdf/59_160218.pdf
- Unión, C. d. (09 de Agosto de 2019). H. Congreso de la Unión. Recuperado el 16 de Agosto de 2019, de http://www.diputados.gob.mx/LeyesBiblio/pdf/1_090819.pdf

El principio de la responsabilidad del superior jerárquico
The Principle of Liability of the Superior Authorit

Resumen

De jure o de facto, la Corte Penal Internacional con la sentencia de Bemba Gombo en 2016 equiparó las obligaciones de los comandantes militares de ejércitos regulares a aquellos comandantes de fuerzas armadas de *facto*. Los criterios de responsabilidad, a saber, el nivel de conocimiento del comandante de lo que sus hombres hacen, están por hacer, hicieron o dejaron de hacer; las medidas razonables que tomó o está por tomar a fin de prevenir y/o reprimir la comisión de crímenes por parte de sus subordinados; el control efectivo que ejerce o ejerció o puede ejercer en términos reales de sus hombres a fin de evitar la comisión del injusto; así como si notificó o no a las autoridades competentes de lo que sucedió o está por suceder, se constituyen en los estándares a partir de los cuales se miden las obligaciones de los Superiores Jerárquicos.

El Superior Jerárquico no tiene responsabilidad de los crímenes que sus hombres materialmente comenten, sino porque incumplió en sus responsabilidades de mando. La actuación del comandante no se asume a priori, se debe analizar como lo ha reiterado la Corte Penal Internacional in concreto. Lo contrario sería excesivo. Las formas aiding and abetting en la omisión en el artículo 25 del Estatuto completan la presunta responsabilidad del Superior.

Palabras clave

Responsabilidad del Superior Jerárquico, Comandantes Militares, Conocimiento, Prevención, Control Efectivo, Notificación, Comandantes de jure, Comandantes de *facto*, ICTY, ICTR, TPIY, TPIR, Corte Penal Internacional, Yamashita, Bemba Gombo, Omisión, Estatuto de Roma, Jurisprudencia, *mens rea, actus reus, must have known, should have known, actual knowledge*, crímenes de guerra, crímenes de lesa humanidad, autoría mediata dominio del hecho.

Abstrac

De *jure or de facto*, the International Criminal Court with the Bemba Gombo ruling in 2016 equated the obligations of military commanders of regular armies to those commanders of de *facto* armed forces. The criteria of responsibility, namely, the level of knowledge of the commander of what his men do, are to be done, done or failed to do; the reasonable measures that it took or is about to take in order to prevent and / or repress the commission of crimes by its subordinates; the effective control exercised or exercised or can exercise in real terms of his men in order to avoid the commission of the unjust; as well as whether or not it notified the competent authorities of what happened or is about to happen, they constitute the standards from which the obligations of the Hierarchical Superiors are measured. The Hierarchical Superior is not responsible for the crimes that his men materially comment, but because he failed to fulfil his responsibilities of command. The action of the commander is not assumed a priori, must be analysed as reiterated by the ICC in concreto. The opposite would be excessive. The aiding and abetting forms in the omission in article 25 of the Statutecomplete the presumed responsibility of the Superior.

Key words

Superior's criminal liability, Military Commanders, Knowledge, Prevention, Effective Control, Notification, *De jure* Commanders, *De facto* Commanders, ICTY, ICTR, TPIY, TPIR, International Criminal Court, Yamashita, Bemba Gombo, Omission, Rome Statute, Jurisprudence, *mens rea, actus reus*, must have known, should have known, current knowledge, war crimes, crimes against humanity, author, control crime approach.

Doctora
Mónica Rocha Herrera

PhD, Warwick UK; LLM Essex UK; Lic. Relaciones Internacionales UNAM México. Presidenta del Foro de Justicia Internacional A.C., Ciudad de México; Investigadora Externa del Instituto de Investigaciones Estratégicas de la Armada de México (SEMAR); Coordinadora del Grupo de Relaciones Internacionales y Ciencia Política del Instituto iberoamericano de la Haya para la Paz, los Derechos Humanos y la Justicia Internacional, La Haya, Países Bajos.

monica_rocha_h@hotmail.com

Artículo recibido el 3 de noviembre de 2019. Aprobado el 5 de jdiciembre de 2019.

Los errores remanentes son responsabilidad de los autores.

El contenido de la presente publicación refleja el punto de vista del autor, que no necesariamente coincide con el del Alto Mando de la Armada de México o la Dirección de este plantel.

Introducción

Éste es un ensayo sobre la doctrina y/o principio del Superior Jerárquico. De sus responsabilidades que adquiere en el ámbito penal conforme a la jurisprudencia internacional penal, así como el derecho positivo y vigente en los tratados internacionales aplicables como el Estatuto de Roma de la Corte Penal Internacional de 1998 y de la que México es Parte suscriptora y la Corte competente a partir del 1 de enero del 2006. Del Comandante militar pero también del Superior Jerárquico civil se abordan aquí sus responsabilidades que pueden ser penales cuando el Superior no observa sus obligaciones de mando conforme al derecho internacional penal en el Estatuto de Roma de la Corte Penal Internacional. Dicha responsabilidad se traduce en la aplicación de lo que se conoce en inglés como modes of liability o criterios de responsabilidad internacional penal cuando el Superior Jerárquico se percata de lo que sus hombres hacen, hicieron o están por hacer, así como de las medidas razonables a sus posibilidades reales para prevenir, reprimir y/o castigar, así como notificar a las autoridades competentes.

Se puede decir que dichos *modes of liability* a los que históricamente y jurídicamente están sujetos los Superiores Jerárquicos incorporan los siguientes estándares: A) el nivel de conocimiento ¿Cuánto en realidad sabe o se espera que sepa el Superior Jerárquico? ¿Supo, debería saber, omitió saber o tenía que saber de la comisión de los crímenes de sus subordinados? B) prevención, en términos reales ¿Qué posibilidades materiales el comandante tuvo o tiene para prevenirlos? ¿Qué medidas necesarias y razonables llevó o lleva a cabo en las circunstancias en las que se encuentra?

En materia de prevención, la obligación del comandante inicia cuando éste se percata o tiene una sospecha razonable de que un crimen se está cometiendo o está por cometerse por sus subordinados (*El Fiscal vs. Kristić (2004) TIPY*); C) control efectivo. Con relación a ello lo que realmente cuenta es el ejercicio efectivo de poder y control sobre los subordinados (El Fiscal vs. Delalić et al (2001) TIPY). Así también, hoy sabemos que un Superior puede quedar absuelto si demuestra que no estaba en posición de ejercer un control efectivo (SPI TPIY El Fiscal vs. Blaskić (2000); D) la notificación a las autoridades competentes, pues en la represión y castigo de los actos ilícitos de sus subordinados no se espera que el Superior Jerárquico imponga las penas correspondientes ella o él mismo.

Otras formas de intervención penal constituidas en el artículo 25 del Estatuto de Roma de la Corte Penal Internacional en la autoría, coautoría mediatas y en la colaboración por omisión de los Superiores Jerárquicos (*aiding & abetting*) conjuntamente con los estándares o *modes of liability*, conocimiento, prevención, control efectivo así como notificación en el artículo 28 del Estatuto de Roma forman parte del examen bajo el cual la actuación de los comandantes militares y Superiores Jerárquicos civiles se analizan hoy en los tribunales penales internacionales incluida la Corte Penal Internacional. Bemba Gombo, primer caso ante la Corte Penal Internacional donde se examinaron las responsabilidades del Superior Jerárquico conforme al artículo 28 del Estatuto, fue resuelto a la luz de estos estándares o criterios de responsabilidad (*modes of liability*) o actuación del Superior recogidos a lo largo de la evolución de la

doctrina del *command responsability* desde Yamashita pasando por los tribunales Ad Hoc de la ONU para la ex Yugoslavia (TPIY) y Ruanda (TPIR) respectivamente hasta el Estatuto de Roma de la Corte Penal Internacional en 1998.

1. Hacia una definición de la Responsabilidad del Superior Jerárquico

Con base en la evolución de la doctrina del *command responsibility*, o responsabilidad de los mandos militares, el principio de la responsabilidad del Superior Jerárquico se puede entender de la siguiente forma: los Superiores Jerárquicos tienen responsabilidades incluso penales ante la comisión de los crímenes de sus subordinados, no por los actos materiales de estos últimos, sino porque son los encargados de manera razonable de ejercer autoridad y control efectivos sobre sus hombres; imponen disciplina y transmiten valores de respeto de los principios humanitarios en la conducción de sus operaciones; el comandante militar y no el civil, se encuentra en campo y tiene el pulso de la situación. Su estado de conocimiento de lo que sucede es directo y lo que acontece le compete, porque él como militar es el responsable de manera razonable de la conducta y desempeño de sus subordinados. Ya Sun Tzu (2000) hace un par de milenios hablaba del oficio de los Generales de los que se puede leer no otra cosa sino la noción de ser comandante.

Se puede decir que del comandante militar en su oficio se espera que cree situaciones seguras en la ventaja militar y en la seguridad de sus hombres; de la disciplina que a través de ella recree la atmósfera de mando necesaria para el cuidado y debido control de las acciones de sus comandados. Del comandante operativo y su trabajo ético, depende no sólo la destreza militar sino la obediencia y el buen comportamiento de sus hombres que ven en él a su líder. Al ejercer su mando, las tareas del Superior Jerárquico incluyen prevenir lo que no ha sucedido, reprimir lo que va a suceder y notificar lo que ya sucedió. En principio no se espera de él que imponga las penas por los crímenes que cometan sus hombres, pero al comunicar y dar parte a sus superiores y autoridades competentes de lo que aconteció, entonces no solo está haciendo su trabajo, sino que está generando el ambiente adecuado de mando y espíritu de cuerpo adecuado en sus tropas, donde el mensaje que transmite es el de la intolerancia a la impunidad o permisividad en la comisión del injusto (Rocha, 2018).

Las responsabilidades del Superior Jerárquico no sólo son para su beneficio y el de sus tropas, sino mayor aún para la sociedad civil, que dependemos del buen actuar de los comandantes militares para que a través de su liderazgo y disciplina militar transmitan los valores de humanidad que nos son propios como civilización. Para el Superior Jerárquico no basta estar consciente de sus responsabilidades sino en recordar que los actos del injusto se suceden y por ello el comandante militar debe estar capacitado y vigilante en este conocimiento no sólo en su beneficio y el nuestro como sociedad, sino porque además de ser su obligación el saber, también es su derecho, conocer para poder prevenir y/o reprimir los actos de los elementos equivocados en sus filas.

Es verdad, el trabajo es continuo y su obligación es enorme, porque tienen que estar alerta todo el tiempo; como también es cierto, que sus pasos a tomar se exigen

en la medida de lo razonable en las circunstancias que les toca afrontar, lo contrario sería excesivo, como claramente está establecido en la jurisprudencia internacional. La Sala de Primera Instancia III de la Corte Penal Internacional apoyándose en la jurisprudencia del Tribunal Penal Internacional de la ONU para la ex Yugoslavia (TPIY) en Blaškić (2004); Brdanin (2004); Stakić (2003); Krnojelac (2002) Galić (2003), lo expresó así en Bemba Gombo (*La Fiscal vs. Jean Pierre Bemba Gombo* 2016, p. 92, para 200): El comandante, si ha ultimado su obligación de tomar todas las medidas necesarias y razonables en su poder, no puede ser responsable, incluso si los crímenes de hecho ocurren o si los perpetradores permanecen sin castigar.

Figura 1. De Jure Belli Ac Pacis [De los Asuntos de la Guerra y de la Paz] Hugo Groccio y de la Responsabilidad sobre Otros.

1.1 El principio de la Responsabilidad del Superior Jerárquico en la doctrina y el derecho internacional

Si nos referimos a los mandos militares entonces debemos retomar la doctrina del *Command Responsibility* la cual acontece desde tiempos inmemoriales. De hecho, hay coincidencias en decir que el *Command Responsibility* está bien sustentado en el derecho consuetudinario por la obligada relación con las leyes de la guerra (Henckaerts y Doswald Beck, 2005). Ya Hugo Groccio (1583-1645), padre del derecho internacional, había expresado con relación a la responsabilidad de otros, a aquellos con autoridad, «que, para hacer a un hombre responsable de las faltas de otro, debe haber una concurrencia entre conocimiento y permisividad» (Hugo Grotius, 2004, p. 454).

Para Nybondas (2010) debemos entender la palabra responsabilidad «como una cuestión de ser responsable, de ser juicioso por algo, por una persona o un cuerpo. La responsabilidad penal ya sea en la carga penal o moral está basada en la responsabilidad simple por algo que no necesariamente es penal» (p. 53). Es claro que la palabra responsabilidad no es penal en sí misma, pero en la doctrina de las obligaciones del

Superior Jerárquico ha podido adquirir esa carga además de su obligación moral. La carga moral es claramente cierta para los comandantes militares encargados de la disciplina militar y del bienestar de sus hombres. Pero dicha responsabilidad también puede ser moral en la culpa por los actos reprochables de sus hombres no cumpliendo con lo que se espera de él o de ella en el control de sus subordinados.

El derecho penal normalmente prohíbe ciertos actos. Es una disciplina que ordena se refrene en la comisión de ciertos actos que pueden ser lesivos. Es una disciplina de la prohibición de hacer por lo que es puesta en términos de lo que no se debe hacer. Sin embargo, en el terreno de la responsabilidad del Superior Jerárquico hay una excepción y es que su responsabilidad es de actuar, de una acción positiva que de no llevarlo a cabo viene interpretado como una omisión de su parte, que puede tener la forma de ser culposa o dolosa. Entonces con relación a la omisión al Superior Jerárquico se le impone una obligación de actuación positiva, de evitar que sucedan los crímenes y/o permitir que se sigan sucediendo. Esto es considerado así desde tiempos remotos donde la Responsabilidad del Superior Jerárquico «tiene sus orígenes en el Derecho Internacional Penal (DIP) y el Derecho Internacional Humanitario (DIH). Debido a su estrecha relación con la sanción de crímenes internacionales como los crímenes de guerra o de lesa humanidad» (Olásolo y Canosa, 2018, p. 449). Entonces, la Responsabilidad del Superior Jerárquico se construye en torno al principio de responsabilidad penal por omisión como lo dice Acevedo acertadamente (2017):

> Cuando existe una obligación jurídica de actuar. Su fundamento se encuentra en la obligación jurídica que, conforme al DIP [derecho internacional penal] y al DIH, tiene todo superior, civil o militar, en razón del control efectivo que despliega sobre sus subordinados, de adoptar las medidas necesarias y razonables a su disposición para prevenir, reprimir y someter a las autoridades competentes los crímenes internacionales cometidos por los mismos. Con ello se busca limitar la comisión de este tipo de crímenes (Acevedo en Olásolo y Canosa, p. 452).

La doctrina del Superior Jerárquico en el derecho internacional penal inicia con Yamashita, el General japonés comandante del 14º ejército imperial japonés en las Filipinas durante la invasión norteamericana en el pacífico de 1944 a 1945 durante la Segunda Guerra Mundial. Con Yamashita que enfrentó a Mac Arthur, se da inicio a la doctrina moderna de la responsabilidad del Superior Jerárquico (Rocha, 2018). En otras palabras, con el juicio del tribunal militar norteamericano en contra de Yamashita (1946), se comenzó a desarrollar la responsabilidad del Superior Jerárquico como forma de responsabilidad penal por los crímenes cometidos por los subordinados que no fueron prevenidos y/o reprimidos por el comandante. Yamashita, víctima de la «justicia de los vencedores» o villano, según como se le vea, los cargos en contra de él fueron por los crímenes que ordenó o escogió omitir.

De Yamashita siguieron casos emblemáticos durante la Segunda Posguerra Mundial con estándares muy rigurosos de conocimiento para los Superiores Jerárquicos de los crímenes perpetrados por sus subordinados, como el de la Alemania ocupada. Conforme a la Ley del Control Aliado No. 10 se cuentan entre ellos los

juicios militares de los Rehenes (EUA vs. Wilhem List et al, Tribunal Militar de los Estados Unidos, Núremberg, 1947-48) así como el del Alto Mando (EUA vs. Wilhem von Leeb et al, Tribunal Miliar de los Estados Unidos, Núremberg, 1948) en contra de militares alemanes (Rocha, 2018).

Los juicios de la Segunda Posguerra Mundial fueron en cortes militares. Sin embargo, se consolidan como precedentes de lo que años después se recogiera en derecho positivo internacional y nociones de la doctrina en el Protocolo I de 1977 Adicional a los Convenios de Ginebra de 1949. Sólo unos años más tarde la responsabilidad del Superior Jerárquico sería recogida en los Estatutos de los tribunales Ad Hoc de la ONU para la ex Yugoslavia (TPIY) y Ruanda (TPIR), en 1993 y 1994 espectivamente. Los TPIY y TPIR así como tribunales híbridos, mixtos e internacionalizados como la Corte Especial para Sierra Leona (CESL) y las Salas Extraordinarias para las Cortes de Camboya (SECC) desarrollaron con sus variates el contenido de las siguientes obligaciones del Superior Jerárquico como lo explican bien Olásolo y Canosa (2018):

> (i) prevenir la comisión de crímenes internacionales por sus subordinados (lo que incluye también el deber de poner fin a los que se estén cometiendo); y (ii) castigar a los subordinados que hayan estado involcrados en los mismos (lo que supone a su vez el deber de enviar la cuestión a las autoridades competentes cuando no se tenga la facultad jurídica para castigar (p. 453)

Sin embargo, será el artículo 28 del Estatuto de Roma de la Corte Penal Internacional de 1998 conjuntamente con la jurisprudencia que hereda de los tribunales Ad Hoc de la ONU (TPIY y TPIR) que la Corte Penal Internacional construye un contenido de las obligaciones jurídicas del Superior Jerárquico más acabado, a saber (Olásolo y Canosa, 2018):

> (i) prevenir la comisión de crímenes internacionales por sus subordinados,
>
> (ii) reprimir la comisión de dichos crímenes, en el sentido de poner fin a los que se estén cometiendo y castigar a los subordinados que hayan estado involucrados en los mismos; y
>
> (iii) enviar la cuestión a las autoridades competentes cuando no se tenga la facultad jurídica para castigar (p, 453).

El artículo 28 del Estatuto de Roma de la Corte Penal Internacional contiene la versión más completa de las responsabilidades del Superior Jerárquico en derecho internacional penal:

Artículo 28.- Responsabilidad de los jefes y otros superiores

Además de otras causales de responsabilidad penal de conformidad con el prsente Estatuto por crímenes de la competencia de la Corte:

a) El jefe militar o el que actúe efectivamente como jefe militar será penalmente responsable por los crímenes de la competencia de la Corte que hubieren sido com tidos por fuerzas bajo su mando y control efectivo, o su autoridad y control efectivo, según sea el caso, en razón de no haber ejercido un control apropiado sobre esas

fuerzas cuando:

i) Hubiere sabido o, en razón de las circunstancias del momento, hubiere debido saber que las fuerzas estaban cometiendo esos crímenes o se proponían cometerlos; y

ii) No hubiere adoptado todas las medidas necesarias y razonables a su alcance para prevenir o reprimir su comisión o para poner el asunto en conocimiento de las autoridades competentes a los efectos de su investigación y enjuiciamiento.

b) En lo que respecta a las relaciones entre superior y subordinado distintas de las señaladas en el apartado a), el superior será penalmente responsable por los crímenes de la competencia de la Corte que hubieren sido cometidos por subordinados bajo su autoridad y control efectivo, en razón de no haber ejercido un control apropiado sobre esos subordinados, cuando:

i) Hubiere tenido conocimiento o deliberadamente hubiere hecho caso omiso de información que indicase claramente que los subordinados estaban cometiendo esos crímenes o se proponían cometerlos;

ii) Los crímenes guardaren relación con actividades bajo su responsabilidad y control efectivo; y

iii) No hubiere adoptado todas las medidas necesarias y razonables a su alcance para prevenir o reprimir su comisión o para poner el asunto en conocimiento de las autoridades competentes a los efectos de su investigación y enjuiciamiento (Estatuto de Roma, 1998).

1.2 El El Superior Jerárquico Civil

El Superior Jerárquico puede ser un civil y no sólo un militar donde el command responsibility le es más aludido a este último (Nybondas, 2010). De hecho, pueden ser Superiores Jerárquicos formales o de jure, pero también puede haber Superiores de facto, civiles que en una especifica situación tengan una posición de autoridad por los crímenes cometidos por sus subordinados. Son civiles y no militares, pero ejercen autoridad y control efectivo sobre sus subordinados. Jean Paul Akayesu, Alcalde de la provincia de Taba en Ruanda fue el primer caso en el TPIR (1994) donde se utilizó el principio del Superior Jerárquico (SPI El Fiscal vs. Jean Paul Akayesu, 2001). Después le siguieron más casos de civiles cuyos escritos de acusación incluían cargos de responsabilidad de los Superiores Jerárquicos tanto en el TPIR (Nahimana, Barayagwiza y Ngeze (SA 2007); Musema (SPI 2001); Kayishema (SPI 2001); Rugambarara (SPI 2007) así como en el TPIY (Kordić y Cerkez (SA 2004); Stakić (SA 2006); Stanišić y Simatović (SA 2015), Karadzić (SPI 2016).

En la Corte Especial para Sierra Leona (CESL) tenemos el caso emblemático del ex Presidente de Liberia, Charles Taylor que fue condenado a 15 años de prisión por esta Corte mixta e internacionalizada por alentar y colaborar (aiding & abbeting) en la comisión de crímenes de guerra y crímenes de lesa humanidad perpetrados por las fuerzas rebeldes del Frente Unido Revolucionario (RUF por sus siglas en inglés) y el Consejo Revolucionario de las Fuerzas Armadas que tenían el objetivo de desestabilizar al vecino país de Sierra Leona y apoderarse de sus recursos minerales (SA El Fiscal vs. Charles Ghankay Taylor, 2012).

Con el Fiscal vs. Jean Pierre Akayesu en el TPIR (2001), además de haber sido la primera decisión en la cual uno de los dos Ad Hoc tribunales de la ONU libró una sentencia en materia del principio del Superior Jerárquico, de este caso y del Campo de Celebići (TPIY) se determinó la regla de que los civiles pueden ser responsables conforme al principio del Superior Jerárquico. La rica jurisprudencia de ambos tribunales Ad Hoc de la ONU, el TPIY y el TPIR así como el artículo 28 del Estatuto de Roma de la Corte Penal Internacional no hacen más que confirmar este hallazgo. Las sentencias del ex Presidente de Liberia, Charles Taylor por el CESL y la del autoproclamado Presidente de la República Serbia en Bosnia Herzegovina en la ex Yugoslavia por el TPIY, Radovan Karadzić (2016) lo confirman contundentemente. El Estatuto de Roma de la Corte Penal Internacional va más allá incluso, el caso de Jean Pierre Bemba Gombo ante la Corte Penal Internacional se refiere a un civil «actuando como un Jefe Militar» conforme al artículo 28 (a) del Estatuto (La Fiscal vs. Jean Pierre Bemba Gombo, SPI, 2016).

1.3 El Superior Jerárquico «actuando como Jefe Militar» (Estatuto de Roma, 1998)

Civiles «actuando como Jefes Militares» es una figura única en el Estatuto de Roma, sus contrapartes el TPIY y el TPIR carecen de esta especificación. Entonces el artículo 28 del Estatuto de Roma distingue claramente entre los comandantes militares y los Superiores Jerárquicos civiles dividiendo el artículo en dos párrafos cada uno señalando ambas categorías. Para ambos Superiores la responsabilidad penal de no haber ejercido control efectivo les es imputable. El inciso a se refiere «al jefe militar o al que actúe efectivamente como jefe militar» (Estatuto, 1998) lo que incorpora a civiles actuando como jefes militares. No sólo eso, los Superiores Jerárquicos pueden ser formales de jure o informales o de facto, como lo fue el caso de Bemba Gombo como líder del Movimiento de Liberación del Congo. Como se puede apreciar en el siguiente recuadro podemos ver como la Sala de Primera Instancia III de la Corte Penal Internacional describe a un comandante militar o a una persona actuando como Jefe Militar.

Figura 2. El Comandante de Facto o aquélla persona actuando como comandante militar en el Estatuto de Roma. El Fiscal vs. Jean Pierre Bemba Gombo (SPI III, 2016)

Es de mencionar que, a diferencia de la Corte Penal Internacional, el TPIY y el TIPR son los únicos tribunales internacionales penales hasta el momento que han pasado sentencias de civiles paramilitares en el derecho internacional penal. Vale la pena mencionar que durante el conflicto armado en la ex Yugoslavia de 1992 al 1995 entre los grupos paramilitares más importantes bajo el control de las distintas facciones gubernamentales en pugna, estaba el Batallón de Convictos de «Tuta» y «Štela», basados en Mostar al servicio de Croacia (Rocha, 2016). Estos líderes paramilitares fueron los únicos cabecillas de estos grupos delincuenciales en la guerra de Bosnia Herzegovina (1992-95) que enfrentaron un juicio en el TPIY y fueron condenados, en el caso de Mladen Naletilić alias «Tuta,» a veinte años de prisión y «Stela» subordinado de 'Tuta' a dieciocho años de prisión ambos por crímenes de guerra y de lesa humanidad (SPI El Fiscal vs Mladen Naletilić, a.k.a «Tuta» Vinko Martinović, a.k.a. «Stela», 2006).

2. Codificación del principio de Responsabilidad del Superior Jerárquico en el derecho internacional penal: orígenes

Los instrumentos legales del derecho internacional penal relativos al principio del Superior Jerárquico son documentos contemporáneos. Para los propósitos de este estudio uno de los instrumentos que antecede a la Segunda Guerra Mundial es el artículo 1 del Reglamento Relativo a las Leyes y Costumbres de la Guerra Terrestre de La Haya de 1907. El artículo 1 de dicho instrumento establece «las leyes, los derechos y los deberes de la guerra» aplicables no sólo a los ejércitos «sino también a las milicias y a los cuerpos de voluntarios» que reúnan las condiciones entre otras «de estar comandados por una persona responsable de sus subordinados» (Reglamento Relativo a las Leyes y Costumbres de la Guerra Terrestre, 1907, p. 22).

Esta provisión refleja ya la idea del mando responsable pero no explica de dónde se genera la presunta responsabilidad penal por los actos criminales cometidos por sus subordinados. Al momento de la adopción de los Protocolos Adicionales de 1977 a los Convenios de Ginebra de 1949, el artículo 1 del Reglamento Relativo a las Leyes y Costumbres de la Guerra Terrestre de 1907 sirvió como un antecedente en derecho positivo a lo que en la práctica de los Estados ya se asumía como una responsabilidad del Superior el prevenir la comisión de crímenes por sus subordinados. Sin embargo, dicho concepto aún carecía de una carga penal en la responsabilidad del Superior por no prevenir los crímenes de sus subordinados (Nybondas, 2010).

Llegamos a la Segunda Posguerra Mundial y aún se carecía de provisiones en materia de responsabilidad penal del Superior Jerárquico, plasmadas en tratados internacionales. Ni el Tribunal Militar Internacional de Núremberg (Tribunal de Núremberg) ni tampoco el Tribunal Militar Internacional del Lejano Oriente (Tribunal de Tokio) incluían provisiones sobre la responsabilidad de los Superiores Jerárquicos. Así tampoco los Cuatro Convenios de Ginebra de 1949 hacen mención específica de la responsabilidad penal impugnable a mandos y Superiores Jerárquicos por los actos ilícitos de sus subordinados.

La jurisprudencia existente hasta ese momento era producto de la jurisprudencia de tribunales nacionales, cortes militares internacionales y principios de derecho

general, así como Códigos Militares (Lieber) e incluso la moral militar, pero nada explícito y codificado en un tratado internacional. Aun así el artículo 13 del Convenio III de Ginebra de 1949 ya equiparaba de manera interesante actos ilegales con actos de omisión por la Potencia Detenedora al decir:

> Está prohibido y será considerado como infracción grave contra el presente Convenio, todo acto ilícito o toda omisión ilícita por parte de la Potencia detenedora, que comporte la muerte o ponga en grave peligro la salud de un prisionero de guerra en su poder (Convenio de Ginebra III, 1949).

El artículo anterior de manera interesante habla del acto de omisión y lo equipara con un acto criminal por parte de la Potencia Detenedora, pero no dice en realidad nada sobre la responsabilidad del Superior Jerárquico en lo específico. Sin embargo, es en el Convenio I de Ginebra de 1949 donde encontramos ya un vestigio de otro principio fundamental en el derecho internacional penal y ese es el principio de la Responsabilidad Individual Penal. Ello se encuentra en el artículo 49 del Convenio I, cuando se reconoce no sólo la responsabilidad individual sino las sanciones penales cuando dice:

> Las Altas Partes Contratantes se comprometen a tomar todas las oportunas medidas legislativas para determinar las adecuadas sanciones penales que se han de aplicar a las personas que hayan cometido, o dado orden de cometer, una cualquiera de las infracciones graves contra el presente Convenio definidas en el artículo siguiente (Convenio de Ginebra I, 1949).

Con toda certeza los Convenios de Ginebra de 1949, considerados por la Corte Internacional de Justicia de la ONU en su fallo del caso Nicaragua vs. EUA (Caso Concerniente a las Actividades Militares y Paramilitares en y en contra de Nicaragua, Nicaragua vs. EUA, 1986) como un «desarrollo del derecho internacional humanitario» (p. 103, para. 218), han servido de base firme como tratados y costumbre internacional para codificar la responsabilidad penal individual. Sin embargo, los Convenios de Ginebra de 1949 no proveen de una base legal plena para la responsabilidad de los mandos y de los Superiores Jerárquicos pues un componente de estos últimos es su responsabilidad cuando ellos no actúan u omiten actuar. Hay un avance más en el derecho internacional penal previo a los tribunales internacionales penales Ad Hoc de la ONU y ese se da al adoptarse la Convención sobre la Imprescriptibilidad de los Crímenes de Guerra y Crímenes de Lesa Humanidad de 1968 ratificado por México en el 2002, que en su artículo 2 impone obligaciones a los representantes de la autoridad del Estado cuando menciona:

> Si se cometiere alguno de los crímenes mencionados en el artículo I, las disposiciones de la presente Convención se aplicarán a los representantes de la autoridad del Estado y a los particulares que participen como autores o cómplices o que inciten directamente a la perpetración de alguno de esos crímenes, o que conspiren para cometerlos, cualquiera que sea su grado de desarrollo, así como a los representantes de la

> autoridad del Estado que toleren su perpetración (Convención sobre la Imprescriptibilidad de los Crímenes de Guerra y Crímenes de Lesa Humanidad, 1968).

El artículo anterior ya contiene el mensaje que, conforme al derecho internacional penal, no solamente aquellos que participan en los crímenes, pero aquellos que toleran su comisión pueden ser encontrados responsables penalmente refiriéndonos específicamente a los Superiores Jerárquicos, en este caso a los representantes de la autoridad del Estado que implica también civiles, pues la cláusula no es específica de mandos militares. En esta provisión de la Convención sobre la Imprescriptibilidad de los Crímenes de Guerra y Crímenes de Lesa Humanidad de 1968, los Superiores Jerárquicos pueden incurrir en responsabilidad penal donde el Superior no comete físicamente u ordena la comisión de un crimen, sino más bien omite reprimir la comisión de éste o de éstos no llevando a cabo las medidas necesarias para castigar a los infractores (Nybondas, 2010).

Va a ser hasta el Protocolo I de Ginebra de 1977 Adicional a los Convenios de Ginebra de 1949 cuando por primera vez en un tratado internacional se codifica de manera explícita el concepto de la Responsabilidad del Superior Jerárquico en la forma en la que en gran medida lo entendemos hoy en el derecho internacional penal. El Protocolo I introduce dos provisiones relevantes al principio de la Responsabilidad del Superior Jerárquico. El artículo 86 Fracción 2, establece la Responsabilidad del Superior Jerárquico por los crímenes de sus subalternos cuando supiera o tuviera información que le permitiera concluir que se cometieron o estaban por cometerse dichos crímenes:

> El hecho de que la infracción de los Convenios o del presente Protocolo haya sido cometida por un subordinado no exime de responsabilidad penal o disciplinaria, según el caso, a sus superiores, si éstos sabían o poseían información que les permitiera concluir, en las circunstancias del momento, que ese subordinado estaba cometiendo o iba a cometer tal infracción y si no tomaron todas las medidas factibles que estuvieran a su alcance para impedir o reprimir esa infracción (Protocolo I de 1977 Adicional a los Convenios de Ginebra de 1949).

La segunda provisión es el artículo 87 no menos importante pues configura en gran medida los elementos de mando necesarios para que un Superior al percatarse de una falta de sus subordinados, prevenga, suprima y notifique a la autoridad competente.

Artículo 87 - Deberes de los jefes

1. Las Altas Partes contratantes y las Partes en conflicto exigirán que los jefes militares, en cuanto se refiere a los miembros de las fuerzas armadas que están a sus órdenes y a las demás personas que se encuentren bajo su autoridad, impidan las infracciones de los Convenios y del presente Protocolo y, en caso contrario, las repriman y denuncien a las autoridades competentes.
2. Con el fin de impedir y reprimir las infracciones, las Altas Partes contratantes y las Partes en conflicto exigirán que los jefes, según su grado de respon-

sabilidad, tomen medidas para que los miembros de las fuerzas armadas bajo sus órdenes tengan conocimiento de las obligaciones que les incumben en virtud de lo dispuesto en los Convenios y en el presente Protocolo.

3. Las Altas Partes contratantes y las Partes en conflicto obligarán a todo jefe que tenga conocimiento de que sus subordinados u otras personas bajo su autoridad van a cometer o han cometido una infracción de los Convenios o del presente Protocolo a que se tome las medidas necesarias para impedir tales violaciones de los Convenios o del presente Protocolo y, en caso necesario, promueva una acción disciplinaria o penal contra los autores de las violaciones (Protocolo I de 1977 Adicional a los Convenios de Ginebra de 1949).

Los elementos anteriores conjuntamente con el establecimiento de una relación superior-subordinado se codificaron dando forma a la doctrina del mando responsable y principio del Superior Jerárquico en derecho internacional penal contemporáneo, que tendrá un desarrollo crucial con los dos tribunales Ad Hoc de la ONU para la ex Yugoslavia (1993) y el de Ruanda (1994), TPIY y TPIR respectivamente hasta llegar a la cúspide con el artículo 28 del Estatuto de Roma de 1998 de la Corte Penal Internacional.

3. Los Tribunales Ad Hoc de la ONU para la ex Yugoslavia (TPIY) y Ruanda (TPIR)

Los Estatutos del TPIY y del TPIR respectivamente incluyen provisiones del Principio de Responsabilidad del Superior Jerárquico que han sido aplicados a innumerables casos en estos tribunales, siendo el TPIY al día de hoy, el tribunal internacional penal con mayor número de casos militares y sentencias libradas con relación al principio del Superior Jerárquico. Los artículos relevantes en los Estatutos de cada uno de estos tribunales son idénticos en ambos, el 7(3) en el TPIY y el 6(3) en el TPIR:

> El hecho de que cualquiera de los actos contemplados en los artículos 2 a 5 del presente Estatuto haya sido cometido por un subordinado, no libera su superior de su responsabilidad penal si sabía o tenía razones para saber que el subordinado se aprestaba a cometer ese acto o ya lo hizo, y que el superior no tomó las medidas necesarias y razonables para impedir que dicho acto no fuera cometido, o para castigar a los autores (Estatuto del TPIY).

Como es claro de la definición, criterios del Principio de Responsabilidad del Superior Jerárquico como lo son el conocimiento, la prevención, el castigo de los autores del crimen, aparecen aquí además de la asunción de una relación de superior-subordinado. En el caso El Fiscal vs. Ratko Mladić de la Sala de Primera Instancia (SPI TPIY, 2017), el tribunal recordó los elementos esenciales del principio de responsabilidad del Superior Jerárquico. Dijo además que para que un Superior incurra en responsabilidad penal conforme al artículo 7 (3) del Estatuto con relación a un crimen de su jurisdicción el mismo debe ser perpetrado por su subordinado:

Para que el Superior incurra en responsabilidad penal conforme al artículo 7 (3) conforme a un crimen de la jurisdicción de este tribunal y que fue perpetrado por sus subordinados los siguientes elementos deben establecerse:

(a) La existencia de una relación de superior-subordinado.

(b) El Superior sabía o tenía razones para saber que sus subordinados estaban por cometer o habían cometido un crimen y;

(c) El Superior no tomó las medidas necesarias y razonables para prevenir la conducta criminal de sus subordinados o castigar a sus subordinados por tal conducta (Estatuto TPIY, 1993, pp. 1827-1828, para 3568).

Como se puede observar los elementos anteriores ya se habían identificado en el artículo 86 (2) del Protocolo I de 1977 Adicional de los Convenios de Ginebra que se vio antes. Asimismo, se ve una similitud en el nivel del criterio del conocimiento entre el artículo 86 (2) y los artículos 7 (3) del TPIY y 6 (3) del TPIR. En el Protocolo I de 1977 el estándar de conocimiento se refiere a si los Superiores «sabían o poseían información que les permitiera concluir, en las circunstancias del momento, que ese subordinado estaba cometiendo o iba a cometer tal infracción» (Protocolo I de 1977 Adicional a los Convenios de Ginebra de 1949), mientras que en los artículos 7 (3) del TPIY y 6 (3) del TPIR el Superior Jerárquico incurre en responsabilidad penal «si sabía o tenía razones para saber que el subordinado se aprestaba a cometer ese acto o ya lo hizo» (Estatutos TPIY y TPIR de 1993 y 1994).

Vale la pena destacar esta similitud pues como veremos más adelante el Estatuto de Roma de la Corte Penal Internacional en su artículo 28, sobre la Responsabilidad de los Jefes o Superiores Jerárquicos, contiene un estándar de conocimiento más estricto incluyendo el «hubiere debido saber» que se aplicó en el caso Yamashita, así como el «hubiere tenido que saber» (should have known), que aparece en la versión en inglés del Estatuto de Roma y no en la española y que se aplicó en los casos de los juicios militares en la Alemania ocupada conforme a la Ley del Control Aliado No. 10 (Caso de los Rehenes de 1947-48 y Caso del Alto Mando de 1948). Lo anterior es relevante pues el inglés es el idioma operativo de la Corte Penal Internacional y no el español, que al momento de escribir este ensayo el español sigue siendo sólo un idioma oficial de la Corte Penal Internacional (Rocha, 2018).

Para Nybondas (2010), los estándares de actuación del Superior Jerárquico antes aludidos contenidos en el artículo 7 (3) del Estatuto del TPIY, pueden ser divididos en objetivos y subjetivos respectivamente. Para los primeros es común denominarlos como actus reus y los subjetivos como mens rea. De los estándares referidos arriba en el Fiscal vs. Ratko Mladić (2017) los incisos a y c corresponden a los elementos objetivos, es decir a la relación superior-subordinado y a las medidas necesarias y razonables que el Superior debe tomar para prevenir la comisión de los actos criminales así como del castigo de los mismos. El elemento subjetivo o el mens rea se refiere al inciso b y ese es el criterio del conocimiento al que aludimos en el párrafo anterior, a si el Superior sabía o tenía razones para saber que un acto criminal estaba por suceder o había ya ocurrido.

3.1. Actus Reus

A fin de establecer cuándo y cómo existe una relación de superior-subordinado, en el caso del Campo de Celebići en la Sala de Primera Instancia del TPIY, el tribunal determinó varios factores relevantes en esta relación que puede ser de acusado y perpetrador. Ahí se reconoció que a fin de establecer una relación de superior-subordinado el acusado debía tener una posición de autoridad. Así mismo se determinó que dicha posición de autoridad podía tener la forma de una autoridad formal, es decir una posición oficial o de jure, pero también una no oficial o de facto. Incluso se mencionó que aunque la autoridad formal no exista y sí una de facto, el principio de responsabilidad del Superior Jerárquico no es inaplicable (El Fiscal vs. Zejnil Delalić et al [Celebići], SA, 2001, para 354).

Sin embargo, la autoridad de facto no es suficiente como tampoco la de jure o formal para adquirir responsabilidad penal por los crímenes de los subordinados -que no fueron prevenidos o castigados y/o notificados- sino que el mando o Superior Jerárquico muestre control efectivo sobre sus subordinados. Como en el caso del Campo Celebići la SPI del TPIY declaró lo siguiente con relación al control efectivo:

> La posesión de autoridad de jure en sí misma no es suficiente para encontrar responsable al Superior si éste no manifiesta control efectivo, aunque una Corte podría presumir la posesión del mismo prima facie a menos que se pruebe lo contrario (El Fiscal vs. Zejnil Delalić et al [Celebići], SA, 2001, para 418).

El otro elemento objetivo en la definición de la relación superior-subordinado esgrimida en El Fiscal vs. RatkoMladić (SPI 2017) pero que también ya se había mencionado en el caso del Campo Celebići (2001), es que la responsabilidad del Superior Jerárquico surge cuando el Superior no toma medidas para prevenir los crímenes o no castiga a sus subordinados que perpetraron los mismos. La Sala de Primera Instancia en El Fiscal vs. Ratko Mladić (2017) lo explicó de la siguiente forma:

> El Superior puede ser responsable sólo si él o ella tiene la habilidad material de prevenir y castigar los crímenes perpetrados por sus subordinados (control efectivo). La relación con el subordinado puede ser directa o indirecta dentro de una jerarquía ya sea formal o informal, de jure o de facto, civil o militar (p. 1828, para. 3569).

Con relación al elemento objetivo en el caso El Fiscal vs. Tihomir Blaškić (SA, 2004), la Sala de Apelaciones también esgrimió el principio de que la ausencia de control efectivo traducido en carencia de control material de los subordinados no originaba responsabilidad penal en el Superior que claramente fue a la conclusión que llegó la Sala con Blaškić.

3.2 Mens Rea

Parece haber en la jurisprudencia de los tribunales internacionales penales incluida la Corte Penal Internacional anuencia en que el elemento subjetivo del conoci-

miento de un Superior de los crímenes que se están por cometer o fueron cometidos por sus subalternos debe ser sustanciado por evidencia directa o circunstancial. Lo anterior es claro pues la posición del Superior Jerárquico en sí mismo no es suficiente para probar el conocimiento del mismo de los crímenes de sus subordinados, aunque si puede ser un indicio de control efectivo (SA TPIY Kordić y Cerkez 2004).

En el caso de los tribunales Ad Hoc de la ONU, el TPIY y el TPIR respectivamente se ha aclarado que el Superior Jerárquico puede ser responsable penalmente si sabía o tenía razones para saber de los crímenes de sus subordinados. El anterior es un estándar de conocimiento conjuntamente con el del Protocolo I de 1977 Adicional a los Convenios de Ginebra de 1949 menos estricto al que se asume en el artículo 28 del Estatuto de Roma de la Corte Penal Internacional de 1998. La clave para que una corte de derecho establezca el nivel del conocimiento del Superior, es en entender de manera directa y/o circunstancial, con cuanta información contaba el Superior que pudiera proporcionar al mismo un nivel de conocimiento que en el caso de los tribunales Ad Hoc le proporcionara «razones para saber» de la comisión de los crímenes que estaban por suceder o que se sucedieron. En el caso del Campo de Celebići (2001) la Sala de Apelación se refirió a este estándar:

> Un Superior puede ser penalmente responsable sólo si información específica estaba disponible a él la cual podía proveerle indicios de las ofensas cometidas por sus subordinados. Esta información no necesariamente debe ser suficiente en sí misma para llegar a la conclusión de la existencia de esos crímenes. Es sólo suficiente que el Superior se percate y busque mayor información o en otras palabras le indique la necesidad de investigar, a fin de concluir si las ofensas estaban por cometerse o se habían cometido por sus subordinados (El Fiscal vs. Zejnil Delalić et al [Celebići], SA, 2001, para. 393).

Asimismo en el caso El Fiscal vs. Ratko Mladić (SPI TPIY, 2017), la Sala de Primera Instancia se refirió de la siguiente manera respecto al estándar de conocimiento, haciendo alusión que el Superior Jerárquico tiene razones para saber cuándo tiene información disponible:

> Un Superior puede ser responsable sólo si cuenta con información ya sea general o específica disponible a él o ella lo suficientemente alarmante para ponerlo o ponerla en aviso de las ofensas cometidas o que estén por cometerse por sus subordinados que justifiquen investigación adicional de su Superior. Una inobservancia deliberada para conducir o concluir dicha investigación a pesar de que existan los medios para llevarlo a cabo, satisface este estándar (pp. 1828, para. 3570).

Por otro lado, el estándar de conocimiento should have known (hubiere tenido que saber) que los tribunales Ad Hoc de la ONU, el TPIY y el TPIR así como el Protocolo I de 1977 Adicional de los Convenios de Ginebra no incorporan, pero que el artículo 28 (a) (i) del Estatuto de Roma de la Corte Penal Internacional sí lo hace, representa un margen de apreciación más riguroso dónde con o sin información que pudiera alertar al mando o al Superior Jerárquico, deberá probarse más allá de la duda razonable, que él o ella sabían y/o tenían que haber sabido.

En otras palabras, el estándar should have known del artículo 28 (a) (i) del Estatuto de Roma de la Corte Penal Internacional que en inglés existe y que en su contraparte en español no existe (existiendo en su lugar el hubiere debido saber) significa negligencia – culposa o dolosa de parte del Superior (Hategekimana, 2009), mientras que el «tenía razones para saber» en los Estatutos de los Tribunales Ad Hoc de la ONU, el TPIY y el TPIR se equipara a «si tenía información disponible» como lo indica el Protocolo I de 1977 Adicional de los Convenios de Ginebra de 1977. El estándar should have known o hubiere tenido que saber está en el artículo 28 (a) (i) del Estatuto en su versión en inglés y se remonta a los casos de la Ley del Control Aliado No. 10 de la Segunda Posguerra Mundial en la Alemania ocupada de los cuales sobresale el caso del Alto Mando (1948) que estableció el estándar «should have known» (hubiere tenido que saber):

> El Caso del Alto Mando de 1948 (EUA vs. Wilhem von Lebb et al, Tribunal Militar de los Estados Unidos, Núremberg, 1948) fue un caso colectivo que lleva el nombre de su acusado más importante Wilhem von Lebb. El caso relata la comisión de atrocidades de unidades de la SS bajo el mando directo de Heinrich Himmler durante la Segunda Guerra Mundial sin el conocimiento, consentimiento o aprobación del acusado. La Corte Militar estadounidense que lo juzgó consideró que lo anterior «no podía ser utilizado como defensa por el comandante general de los territorios ocupados. Que la responsabilidad por el mantenimiento del orden, así como la prevención del crimen recaía en el comando general, por lo que el acusado no podía ignorar hechos obvios y argumentar ignorancia como defensa» (Bassiouni, 2003, p. 306).

Al día de hoy ante la Corte Penal Internacional sólo ha habido un caso de «un Jefe militar o el que actúe efectivamente como Jefe militar» (Estatuto de Roma, 1998), donde se ha aplicado el criterio de conocimiento del Superior Jerárquico en el artículo 28 (a) (i) y ese es el caso de La Fiscal vs. Jean Pierre Bemba Gombo, cuyo juicio de apelación tuvo lugar en el 2018. En este caso la sala de Primera Instancia III de la Corte Penal Internacional (2016) utilizó el estándar «hubiere sabido» o supo en el artículo 28 (a) (i) y no el hubiere debido saber y/o en su versión en inglés el should have known en la misma provisión. Sin embargo, la Sala de Apelación de la Corte Penal Internacional en Bemba Gombo (2018) hizo una referencia al estándar de conocimiento más estricto should have known (hubiere tenido que saber) sugiriendo que la Sala de Primera Instancia III (2016) erró pues tenía que haberlo utilizado:

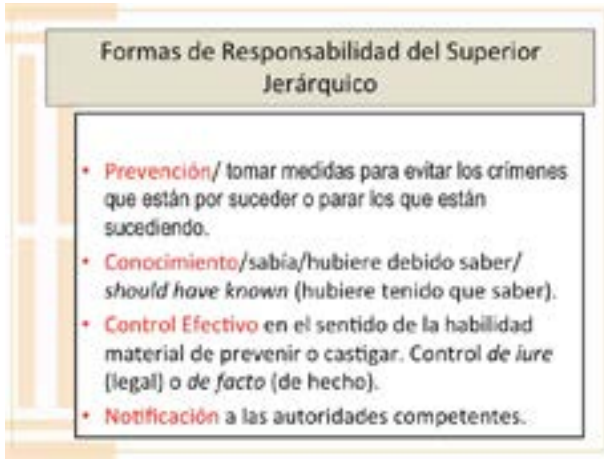
> La evaluación de si el comandante llevó a cabo todas las «medidas necesarias y razonables» debe ser basado en la consideración de los crímenes que el comandante sabía o hubiere tenido que saber en ese particular momento (La Fiscal vs. Jean Pierre Bemba Gombo, SA, 2018, p. 5, para 6).

Sin duda está todo por verse como la Corte Penal Internacional definirá a detalle en el futuro qué implica y qué extensión tiene el estándar «should have know» para los propósitos de los casos ante la Corte.

Figura 3. Formas o estándares de conocimiento en la doctrina de la responsabilidad del superior jerárquico (Rocha, 2018).

4. Formas de responsabilidad del Superior Jerárquico: análisis en La Fiscal vs. Jean Pierre Bemba Gombo (SPI 2016, SA 2018)

Figura 4. F derecho internacional penal y la Corte Penal Internacional.



4.1 Conocimiento

La Sala de Primera Instancia III de la Corte Penal Internacional al dictar su veredicto en Bemba Gombo (2016) concluyó qué estándar de conocimiento o accused's knowledge aplicar con base en el artículo 28 del Estatuto de Roma de la Corte Penal Internacional. Decidió utilizar el inciso (a) (i) que reproducimos aquí en su versión en inglés, por las razones antes explicadas a saber, al día de hoy el Estatuto

en inglés es la versión operativa conjuntamente con el francés y no el español, así como el estándar de conocimiento en el inciso referido, no corresponde fielmente en su versión en español a la operativa en inglés (Estatuto de Roma, 1998).

> a) […] A military commander or person effectively acting as a military commander shall be criminally responsible for crimes within the jurisdiction of the Court committed by forces under his or her effective command and control, or effective authority and control as the case may be, as a result of his or her failure to exercise control properly over such forces, where:
>
> (i) That military commander or person either knew or, owing to the circumstances at the time, should have known that the forces were committing or about to commit such crimes […] [Énfasis añadido].

La Sala de Primera Instancia III de la Corte Penal Internacional determinó que aunque consideró utilizar en el caso Bemba Gombo (2016) la forma alternativa de conocimiento en el artículo 28 inciso (a) (i) «the military commander […] should have known», después del análisis de las evidencias circunstanciales utilizaría la forma «actual knowledge» [hubiere sabido/ knew], a decir que conforme a las responsabilidades de Bemba Gombo como Comandante en jefe del MLC2, Bemba Gombo sabía de las acciones cometidas por sus soldados en la ratione temporis bajo análisis (pp. La Fiscal vs. Jean Pierre Bemba Gombo, 2016, 89-90, párrafos 192-196).

En otras palabras, dicha determinación de la Sala de Primera Instancia III (2016) estuvo basada en diversos factores «que incluían órdenes para cometer crímenes o el hecho de que el acusado estuvo informado personalmente de que sus fuerzas armadas estaban envueltas en actividad criminal» (La Fiscal vs. Jean Pierre Bemba Gombo, 2016, p. 89, para. 193). El estándar de conocimiento en el Estatuto should have known, fue desechado por la forma más simple [he] knew, o sabía.

Lo anterior a partir de la conclusión de la Sala de Primera Instancia III de la Corte Penal Internacional (2016) de que el acusado contó en todo momento «con información de inteligencia y de telecomunicaciones como radios, teléfonos satelitales, thurayas [proveedor de comunicaciones por satélite], telefonía celular entre otras comunicaciones llegadas a él a través de su Estado Mayor y/u otros canales de información» (La Fiscal vs. Jean Pierre Bemba Gombo, 2016, p. 346, para. 707), estando enterado todo el tiempo de las situaciones de combate, posiciones de las tropas, y alegatos de los crímenes cometidos por sus hombres.

Significativamente recibió reportes que se referían a varios actos cometidos por los Banyamulengués (grupos armados de origen ruandés leales a Bemba Gombo, Mr Bemba's men) y las tropas del MLC «que incluían robo, saqueos, violaciones sexuales, asesinato de civiles, acoso de personas y de transportes de suministros redirigidos a la República Democrática del Congo a través de Zongo y Libengue» (La Fiscal vs. Jean Pierre Bemba Gombo, 2016, p. 286). Asimismo, fue importante la determinación de que el acusado estaba consciente y seguía los reportes de la prensa internacional que al mismo tiempo discutía con altos oficiales del Estado Mayor sobre los crímenes cometidos por las tropas del MLC (La Fiscal vs. Jean Pierre Bemba Gombo, 2016, p. 347, párrafos 708-709).

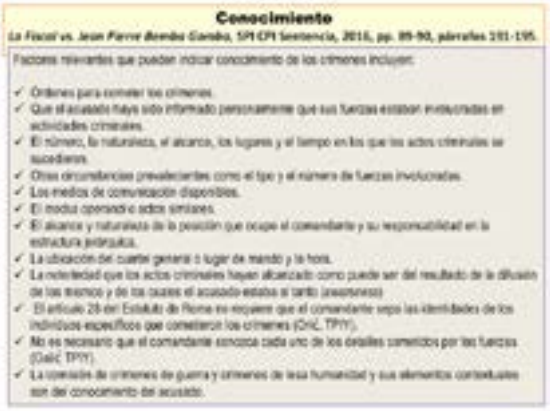
Sin embargo y de manera interesante, la Sala de Apelación en el caso Bemba Gombo (2018) argumentó error, en su fallo de parte de la Sala de Primera Instancia III (2016) en el veredicto de esta última sobre la evaluación del nivel de conocimiento del acusado Bemba Gombo, sobre lo que sus hombres hicieron. La Sala de Apelación (2018) dijo claramente que no bastaba «con decir qué medidas tenía que tomar como comandante, sino analizar in concreto lo que tenía que haber hecho» (La Fiscal vs. Jean Pierre Bemba Gombo, SA, 2018, p. 6, para. 7).

Claramente la Sala de Apelación (2018) urgió, en el primer caso de un Superior Jerárquico ante la Corte Penal Internacional, de la necesidad de la utilización de un estándar de conocimiento más riguroso como es el should have known (hubiere tenido que saber) e ir al análisis in concreto sobre lo que hubiere tenido que hacer. La referencia por parte de la Sala de Apelación (2018) al «hubiere tenido que hacer», ha levantado más de una ceja pues es controvertido decir hasta qué punto la Sala de Primera Instancia III (2016), hubiere tenido que decir qué medidas in concreto en la situación particular de Bemba Gombo tenía que haber tomado este Superior Jerárquico y sobre todo si le correspondía a la Corte decirlo.

El estándar should have known establece claramente el «hubiere tenido que saber», más no el «hubiere tenido que hacer». En otras palabras, no hay sustento ni en la doctrina ni en la jurisprudencia internacional para decir que el estándar de conocimiento alcance para que una corte de derecho le diga a un Superior Jerárquico lo que «hubiere tenido que hacer» en los hechos y circunstancias particulares del caso. El estándar de conocimiento en el artículo 28 (a) (i) establece el «should have known» no el «should have done».

En el siguiente recuadro se pueden apreciar algunos factores indicativos del criterio de conocimiento del Superior Jerárquico en el artículo 28 del Estatuto de Roma de la Corte Penal Internacional que la Sala de Primera Instancia III (2016) señaló en el caso Bemba Gombo (2016) basado en la rica jurisprudencia existente notablemente en el TPIY.

Figura 5. Factores indicativos del estándar de conocimie to en la jurisprudencia internacional penal. La Fiscal vs. Jean Pierre Bemba Gombo (SPI 2016).



La Sala de Primera Instancia III de la Corte Penal Internacional (2016) fue enfática al recordar que «conocimiento de parte del acusado en la comisión de los crímenes en la jurisdicción de la Corte implica el conocimiento como requisito contextual de crímenes de guerra y de crímenes de lesa humanidad» (2016, p. 90, para. 195).

En otro lugar en el veredicto la Sala de Primera Instancia III de la Corte Penal Internacional (2016) reconoció que, en el caso de crímenes de lesa humanidad, aunque no está explícito el elemento mental del asesinato en el artículo 7 del Estatuto y tampoco en los Elementos de los Crímenes, considera aplicable el artículo 30 en el Estatuto que incorpora «la intención y conocimiento en la comisión del crimen» (SPI, 2016, p. 50, párrafos 89-90).

En otras palabras, el mens rea del que hablamos antes que puede tomar la forma de negligencia culposa o dolosa y que se puede entender como el conocimiento criminal de que algo sucede, sucedió o está por suceder. Como correctamente señala Hategekimana (2009) «awareness of the risk involved» (p 44). Sin embargo, hay que señalar que dicho conocimiento negligente no es lineal, sino que puede ser deliberado e intencional (dolus specialis), pero también culposo donde el actor, en este caso el Superior Jerárquico, ignora el hecho de manera omisa o también por indiferencia (SA TPIY, 2010, El Fiscal vs. Mile Mrkšic et al.). Cabe señalar que existe la inacción del Superior Jerárquico con mens rea por otras razones ajenas a su voluntad, para lo cual será necesario estudiar el criterio del conocimiento conjuntamente con otro criterio fundamental en la ecuación y ese es el control efectivo que ejerce el Superior.

4.2 Control Efectivo

El artículo 28 del Estatuto de Roma en palabras de la Corte Penal Internacional está diseñado para reflejar la responsabilidad del Superior Jerárquico en virtud del control que ejerce sobre sus subordinados. Este criterio del control efectivo está orientado a asegurar que a través del comandante militar se lleven a la práctica de manera eficaz los principios del derecho internacional humanitario, que incluyen la protección de las personas y objetos durante el conflicto armado.

4.2.1 ¿Control efectivo absoluto de parte del Comandante?

La Corte Penal Internacional y prácticamente la jurisprudencia de los tribunales penales internacionales como el TPIY y el TPIR, dicen que el comandante debe tomar las medidas necesarias y razonables para la prevención de la comisión de los crímenes por parte de sus subordinados. En el caso El Fiscal vs. Ratko Mladić (2017), la Sala de Primera Instancia del TPIY recordó qué se entiende por control efectivo y cuál es la diferencia entre ejercer el anterior y la capacidad de castigar a los subordinados. Lo hace de la siguiente forma:

> Las medidas necesarias son aquellas medidas apropiadas llevadas a cabo por el Superior para cumplir su obligación de manera genuina a fin de prevenir o castigar, así como medidas razonables son aquellas que razonablemente caen en el poder material del Superior. La obligación

> de prevenir y el deber de castigar son obligaciones legales distintas y el Superior puede ser encontrado responsable por violar cualquiera de ellas. La obligación de prevenir se adhiere al Superior desde el momento en que él o ella sabe o tiene razón para saber que el crimen está por cometerse, mientras que el deber de castigar sólo surge después de la comisión del mismo. El deber de castigar incluye como mínimo la obligación de investigar posibles crímenes o de hacer que se investiguen si el Superior no tiene el poder de sancionar entonces deberá referirlos a las autoridades competentes (pp. 1829, para. 3571).

Del razonamiento anterior podemos concluir basado en la amplia jurisprudencia del TPIY y que la Corte Penal Internacional ha absorbido, que la obligación de prevenir o de castigar no siempre es una obligación en términos absolutos. Pues para que haya control efectivo se requiere de indicios que alerten al Superior de los acontecimientos, pero aún más importante, de control material y efectivo del Superior Jerárquico para poder ejercer su mando y control. No basta la autoridad ya sea de jure o de facto, sino que también se necesita un verdadero control efectivo, pero este último debe ser real y ello significa como se explicó antes, que el Superior ejerza un control material y realista de la situación y de sus subordinados.

En el caso La Fiscal vs. Jean Pierre Bemba Gombo, la Sala de Apelaciones (2018) tuvo a bien estimar el nivel mesurado y razonable del ejercicio del control efectivo, al decir que:

> No es el caso de que el comandante le sea requerido de emplear cada medida concebible dentro de su arsenal, independientemente de las consideraciones de proporcionalidad y viabilidad. El artículo 28 del Estatuto sólo requiere de los comandantes hacer lo que es necesario y razonable en las circunstancias (p. 6, para. 8).

También en este caso, el argumento de la Sala de Primera Instancia III (2016) de la Corte Penal Internacional en su veredicto sobre la falta de voluntad por parte del acusado de llevar a cabo las medidas de prevención y control efectivo de sus hombres, fue desechado por la Sala de Apelaciones (2018) la cual opinó:

> El hallazgo de que las medidas empleadas por el comandante fueron insuficientes para prevenir o reprimir una ola de crímenes no significa que esas medidas fueran insuficientes para prevenir o reprimir un limitado número de crímenes específicos por los que el comandante fue finalmente sentenciado (2018, p. 6, para 10).

Un caso elocuente en este espectro para entender si un comandante militar tuvo un control efectivo y material de las tropas a su mando es el caso del General Delić, del ejército bosnio durante el conflicto armado de la ex Yugoslavia de los años noventa del siglo XX. En El Fiscal vs. Rasim Delić (2008) del TPIY, el Comandante del Estado Mayor del Ejército de Bosnia Herzegovina (ABiH), el General Delić, que tenía a su mando el grupo paramilitar de los Mujahedines, conocidos por su notoriedad en la comisión de crímenes y alta proclividad para actuar por cuenta propia

(Rocha 2016), la Sala en su sentencia refiriéndose a la relación entre el superior y el subordinado y los perpetradores de los crímenes en Bikoši en 1993, mencionó lo siguiente:

> [L]a Sala recuerda que en sus hallazgos previos no fue probado más allá de la duda razonable, que los perpetradores, como alegado por la Fiscalía, hubieran sido Mujahedines del grupo de Poljanice. La Sala examinó sin embargo el argumento de la Fiscalía del 8 de junio de 1993, los Mujahedines de Poljanic habían sido de facto subordinados al 3er Cuerpo. En este aspecto, la Sala nota que no existe evidencia específica de órdenes recibidas por los Mujahedines de Poljanice de parte de unidades del ABiH. En particular, la evidencia solamente muestra que el 8 de junio de 1993 Mujahedines del Campo de Poljanice participaron en combate en contra de las fuerzas del HVO [Fuerzas Croatas de Defensa en Bosnia Herzegovina] en el Valle de Bila simultáneamente con unidades del ABiH. Es más, mientras la evidencia indica que Mujahedines del Campo de Poljanice y los soldados del ABiH estaban conscientes de la presencia de unos y de otros, la evidencia no es clara si los dos grupos actuaban conjuntamente. Por ello, la Sala no está satisfecha que los Mujahedines de Poljanice hubieran estado subordinados a Rasim Delić. El Fiscal vs. Rasim Delić (Resumen de la Sentencia para Rasim Delić).

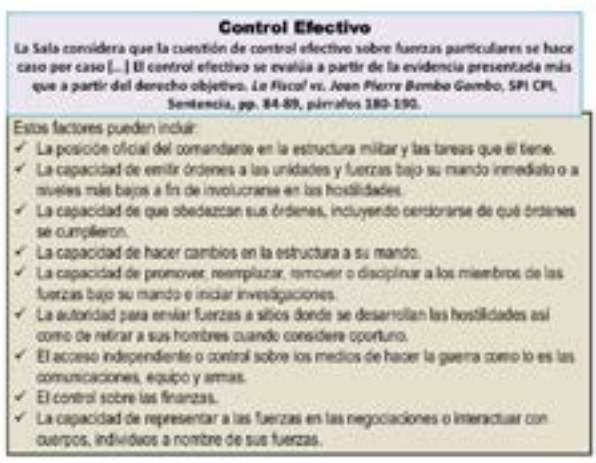
Conforme a la jurisprudencia internacional como la anterior, así como si retomamos las célebres palabras de Groccio -éste último al afirmar que «el conocimiento sin autoridad no se equipara a culpabilidad» (Hugo Grotius, 2004, p. 454), puede decirse con comodidad que no se pueden hacer generalizaciones a priori sin conocer las razones materiales en cada caso.

En este sentido los tribunales penales internacionales TPIY y TPIR respectivamente han dejado claro cómo la Corte Penal Internacional así como otros tribunales, mixtos, híbridos o internacionalizados como lo es la Corte Especial para Sierra Leona, y las Salas Extraordinarias para las Cortes de Camboya, que el análisis debe hacerse caso por caso conforme a la evidencia existente y el estándar de prueba que debe satisfacer a las Salas de una corte «más allá de la duda razonable» (artículo 7 (3) del Estatuto del TPIY y 6 (3) del Estatuto del TPIR). La Sala de Primera Instancia III de la Corte Penal Internacional en el caso Bemba Gombo (2016) esgrimió como lo hizo en Lubanga (2012), Katanga (2014), con relación al estándar de prueba a seguir que:

> Conforme al artículo 66 (1), el acusado se presumirá inocente mientras no se pruebe su culpabilidad ante la Corte deconformidad al derecho aplicable. Conforme al artículo 66 (2) incumbirá al Fiscal probar la culpabilidad del acusado. Para dictar sentencia condenatoria, la Corte deberá estar convencida de la culpabilidad del acusado más allá de toda duda razonable. En este sentido, la Sala de Apelación especifica que este estándar debe ser aplicado no en cada hecho de la sentencia de la Sala de Primera Instancia, pero «solo a los hechos que constituyan los elementos del crimen y la forma de responsabilidad en los cargos del acusado» (La Fiscal vs. Jean Pierre Bemba Gombo, 2016, p. 98, para. 215).

Como lo dijo entonces la Sala de Primera Instancia III de la Corte Penal Internacional en el caso Bemba Gombo (2016), el análisis debe hacerse in concreto. Lo anterior claramente se hizo en el caso específico del General Delić en el TPIY, sin embargo, recojamos la reflexión hecha en otra parte de este ensayo al decir que tener conocimiento no significa necesariamente un acto doloso, sin embargo, ello no significa tampoco que no pueda ser culposo y este es un principio básico en la teoría del delito (Rocha, 2018).

Figura 6. Factores indicativos del criterio de control efectivo del Superior Jerárquico esgrimidos por la Sala de Primera Instancia III de la Corte Penal Internacional en el caso Bemba Gombo (2016).

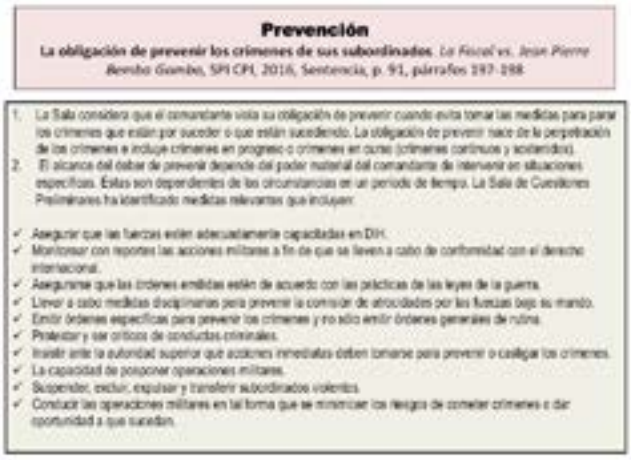


4.3 Prevención

La Corte Penal Internacional explicó que la determinación de si un comandante tiene control efectivo y autoridad se basa en el poder material de prevenir o reprimir la comisión de los crímenes perpetrados por sus subordinados, así como de someter la cuestión a la autoridad competente (SPI III, La Fiscal vs. Jean Pierre Bemba Gombo 2016, p. 343, para. 698). Hemos revisado a lo largo de este ensayo que la responsabilidad del superior jerárquico, debe analizarse a la luz de los elementos o los criterios de responsabilidad (modes of liability), a saber, el conocimiento y el control efectivo. Examinemos ahora la prevención.

En el siguiente recuadro podemos apreciar el análisis que hizo la Sala de Primera Instancia III de la Corte Penal Internacional en el caso Bemba Gombo (2016) de qué significa la labor de prevenir de un comandante militar conforme a la jurisprudencia internacional sobre todo del TPIY y del TPIR.

Figura. 7 La obligación de prevención del superior jerárquico en la jurisprudencia internacional. El caso Bemba Gombo en la Corte Penal Internacional (SPI III, 2016).



Prevención

La obligación de prevenir los crímenes de sus subordinados. *La Fiscal vs. Jean Pierre Bemba Gombo*, SPI CPI, 2016, Sentencia, p. 91, párrafos 197-198

1. La Sala considera que el comandante viola su obligación de prevenir cuando evita tomar las medidas para parar los crímenes que están por suceder o que están sucediendo. La obligación de prevenir nace de la perpetración de los crímenes e incluye crímenes en progreso o crímenes en curso (crímenes continuos y acabados).
2. El alcance del deber de prevenir depende del poder material del comandante de intervenir en situaciones específicas. Éstas son dependientes de las circunstancias en un periodo de tiempo. La Sala de Cuestiones Preliminares ha identificado medidas relevantes que incluyen:

- ✓ Asegurar que las fuerzas estén adecuadamente capacitadas en DIH.
- ✓ Monitorear con reportes las acciones militares a fin de que se lleven a cabo de conformidad con el derecho internacional.
- ✓ Asegurarse que las órdenes emitidas estén de acuerdo con las prácticas de las leyes de la guerra.
- ✓ Llevar a cabo medidas disciplinarias para prevenir la comisión de atrocidades por las fuerzas bajo su mando.
- ✓ Emitir órdenes específicas para prevenir los crímenes y no sólo emitir órdenes generales de rutina.
- ✓ Protestar y ser crítico de conductas criminales.
- ✓ Insistir ante la autoridad superior que acciones inmediatas deben tomarse para prevenir o castigar los crímenes.
- ✓ La capacidad de posponer operaciones militares.
- ✓ Suspender, excluir, expulsar y transferir subordinados violentos.
- ✓ Conducir las operaciones militares en tal forma que se minimicen los riesgos de cometer crímenes o dar oportunidad a que sucedan.

4.4 Notificación del asunto a las autoridades competentes para su investigación y enjuiciamiento

La obligación del Superior Jerárquico de comunicar el asunto a las autoridades competentes para su investigación y enjuiciamiento es un deber derivado de los elementos de la prevención y control efectivo, apenas se percata o adquiere conocimiento de la infracción. La Sala de Apelación de la Corte Penal Internacional en el caso Bemba Gombo (2018) lo definió en estos términos:

> El enfoque del deber de «llevar cabo todas las medidas necesarias y razonables» está intrínsecamente ligado a la habilidad material del comandante de prevenir o reprimir la comisión de los crímenes o de someter el problema a las autoridades competentes para su investigación y enjuiciamiento. De hecho, un comandante no puede ser culpado por no haber hecho algo donde él o ella no tenían el poder de hacerlo (p.5, para 5).

La obligación de notificar asegura que el comandante, que tiene la autoridad en materia disciplinaria en lo militar, no aplique la justicia por sí mismo, sino que coadyuve a evitar la impunidad y evitar futuros crímenes poniendo en manos de la autoridad competente el caso para su valoración y juicio si procede. En el caso de Bemba Gombo, la Sala de Primera Instancia III (2016) indicó que ya la Sala de Cuestiones Preliminares había tomado en cuenta que el acusado había llevado a cabo algunas medidas represivas en la comisión de crímenes por siete soldados del MLC por despojo (La Fiscal vs. Jean Pierre Bemba Gombo, pp. 301-303, paras 601-603). La misma no estuvo libre de controversias y aquí es donde la Corte Penal Internacional indica que debe haber un estándar mínimo que el comandante debe cumplir en su obligación de prevenir y ello consiste en asegurarse que se haga una investigación adecuada y capaz de enjuiciar a los perpetradores.

En el siguiente recuadro podemos apreciar los principios esgrimidos en la jurisprudencia internacional particularmente del TPIY que la Corte Penal Internacional incorporó para su análisis en Bemba Gombo (2016):

Fig. 8 La obligación de notificar a la autoridad competente y/o superior jerárquico

La Sala de Apelación del TPIY en Hadžihasanović reconoció que un superior jerárquico «no debe dispensar sanciones personalmente, sino que debe reportar al subordinado infractor a las autoridades competentes» (SA, El Fiscal vs. Enver Hadžihasanović y Amir Kubura, 2008, p. 64, para. 154). En ese caso, que incorpora el tratamiento de la autoridad y desempeño del Coronel Enver Hadžihasanović, Comandante del ABiH (Ejército de la República de Bosnia Herzegovina) en la guerra de la ex Yugoslavia de los años noventa del siglo XX es por otro lado un ejemplo claro de notificación satisfactoria a las autoridades competentes en el aspecto que nos ocupa. Conforme a la obligación de notificar a las autoridades competentes, la Sala de Apelación del TPIY consideró:

> [Q]ue el reporte entregado al procurador municipal en Bugoino en Bosnia Central de los crímenes en Slavonija, conjuntamente con las sanciones disciplinarias impuestas por el órgano militar competente, constituyeron medidas necesarias y razonables para castigar a los perpetradores (El Fiscal vs. Enver Hadžihasanović y Amir Kubura, 2008, p. 65, para 155).

Hadžihasanović, Comandante del 3er Cuerpo del ABiH, quien había sido promovido a Comandante Supremo del Estado Mayor de ese ejército, fue condenado conjuntamente con Amir Kubura, jefe de la 7ª Brigada de Montaña en el 2006, por su responsabilidad del Superior Jerárquico en el articulo 7 (3) del Estatuto del TPIY y violaciones de las leyes de la guerra en su responsabilidad de prevenir y castigar los crímenes bajo las tropas a su mando. Fueron sentenciados a cinco años y dos años y medio de prisión respectivamente. Sin embargo, la Sala de Apelaciones, en el caso de Hadžihasanović, desechó parte de los hallazgos y de la condena de la Sala de Primera Instancia la redujo a 3 años y seis meses. El reporte entregado al procurador

municipal en Bugoino en Bosnia Central de los crímenes en Slavonija hizo lo suyo y fue suficiente para demostrar que Hadžihasanović había llevado a cabo su labor de notificación a la autoridad competente (Rocha, 2018).

Las tareas del Superior Jerárquico incluyen prevenir lo que no ha sucedido, reprimir lo que va a suceder y notificar lo que ya sucedió. Para el mando militar como lo vimos en El Fiscal vs. Hadžihasanović y Amir

Kubura (2008), en principio no se espera del Superior Jerárquico que imponga las penas por los crímenes que cometan sus hombres, pero al comunicar y dar parte a sus superiores y autoridades competentes de lo que aconteció, entonces no solo está haciendo su trabajo sino que está generando el ambiente adecuado de mando y espíritu de cuerpo adecuado en sus tropas, donde el mensaje que transmite es el de la intolerancia a la impunidad o permisividad en la comisión del injusto (Rocha, 2018).

Su tarea es aún más ardua si se percata de que las autoridades competentes puedan actuar a su vez de manera corrupta e impune, dejando ver simulación y no un actuar genuino conforme a derecho. Pero ¿Sus obligaciones se extienden también aquí? Aquí hay un poco de controversia pues como lo hace notar la Sala de Primera Instancia III de la Corte Penal Internacional en Bemba Gombo (2016), los tribunales TPIY y TPIR han establecido el estándar mínimo de las medidas que el Superior Jerárquico debe cumplir en su obligación de castigar y ello consiste en asegurarse que se haga una investigación adecuada y capaz de enjuiciar a los perpetradores (TPIY SA Kvočka, 2005).

Si la remisión se hace a una autoridad no funcional o a una autoridad donde haya la posibilidad que se conduzca la investigación de manera inadecuada o el proceso de enjuiciamiento no sea el adecuado, las obligaciones del comandante no se consideran satisfechas (TPIY SA Boskosški &Tarčulovski, 2010).

Éste es un criterio estricto, sin embargo, es también en el TPIY que se ha considerado que la obligación de castigar o de poner en manos de las autoridades competentes el asunto, por parte del Superior Jerárquico a fin de que los perpetradores sean llevados a la justicia, termina con la obligación del comandante (TPIY SA Delalić, 2003). Aunque en apariencia más equilibrada esta segunda posición, como es costumbre en la práctica judicial internacional, el análisis se debe hacer caso por caso.

Entre otras dificultades, el comandante podría encontrarse con situaciones en las que notificar al superior inmediato no sea la mejor opción pues pueda ser peor por encontrarse ante un clima de permisividad asociado con la coautoría mediata a través de aparatos organizados de poder o lo que en el TPIY y TPIR asocian con el Joint Criminal Enterprise o empresa criminal conjunta. Héctor Olásolo (2013) se refiere acertadamente a la escuela de Claus Roxin cuando dice que este autor alemán desarrolló una teoría desde la cual los Superiores podían ser considerados como quienes, desde atrás, detentaban el dominio del hecho, en cuanto decidían si los delitos eran cometidos y de qué manera serían llevados a cabo por sus subordinados. De este modo se podía considerar a dichos Superiores como autores mediatos incluso en aquéllos casos en los que los subordinados autores directos fueran plenamente responsables por los delitos cometidos.

5. La Responsabilidad del Superior Jerárquico y las formas de intervención penal en el Artículo 25 del Estatuto de Roma de la Corte Penal Internacional, la autoría y coautorías mediatas en las Estructuras Organizadas de Poder

El concepto de autoría mediata a través de estructuras organizadas de poder fue aplicado por primera vez a nivel internacional por la Sala de Cuestiones Preliminares II del TPIY en su sentencia del 31 de julio de 2003 en el caso Milomir Stakić que fue condenado por coautoría mediata, aunque la Sala de Apelaciones del TPIY rechazó en el 2005 la aplicación conjunta de coautoría mediata y coautoría por dominio funcional del hecho tomando el enfoque de la Empresa Criminal Común (Olásolo, 2013).

La Corte Penal Internacional que incorpora el enfoque del dominio del hecho en las Estructuras Organizadas de Poder ha aplicado el concepto de autoría y coautoría mediata en la mayoría de los casos, significativamente con relación a los ex Jefes de Estado de Libia y Costa de Marfil (Muammar Gaddafi y Laurent Nbagbo), en el caso Keniata, en Katanga, Bemba Gombo y Ngudjolo y para el actual Presidente de Sudán Omar Al-Bashir. La coautoría mediata se utilizó por primera vez en el caso Bemba Gombo en el 2008 en la Orden de Arresto (Rocha, 2018).

El caso más reciente de una sentencia por coautoría mediata en los tribunales internacionales penales es el caso del General Ratko Mladić en el TPIY (2017) el cual es emblemático de este tipo de intervención penal. Al General Mladić además de su responsabilidad como Superior Jerárquico, se le acusó de ordenar el genocidio en Srebrenica en 1995 durante el conflicto armado en la ex Yugoslavia, en coautoría con el sentenciado a cuarenta años de prisión, Radovan Karadzić (SPI TPIY, El Fiscal vs. Radovan Karadzić, 2016). Mladić fue encontrado culpable y condenado a cadena perpetua (SPI TPIY, El Fiscal vs. Ratko Mladić, 2017).

Lo interesante aquí a señalar en materia de responsabilidad del Superior Jerárquico, son las otras formas de intervención penal en las que pueda incurrir un Superior y que ya están incorporadas en el artículo 25 del Estatuto de Roma de la Corte Penal Internacional. Nos referimos a aquellas formas de colaboración por omisión ya sea culposa o dolosa.

El caso del General Radislav Krstić subordinado del General Mladić es elocuente ¿Qué podía hacer el General Radislav Krstić, subordinado del General Ratko Mladić, en términos materiales ante la Empresa Criminal Conjunta (Joint Criminal Enterprise), donde sus Superiores eran los coautores o autores mediatos del crimen de genocidio que estaba por suceder? ¿Hasta qué punto fue responsable el General Radislav Krstić de que las Drina Corps a su cargo participaran en la matanza de alrededor de 8,000 bosnios musulmanes por órdenes expresas de sus Superiores?

La Sala de Apelación en el caso El Fiscal vs. Radislav Krstić (2004) en el TPIY redujo su sentencia por complicidad por genocidio de 46 a 35 años de prisión al encontrar factores mitigantes en su obligación de mando, como las órdenes por escrito que emitió de tratar humanamente a los musulmanes y por ser colaborador más no coautor de lo que la Sala de Apelación refirió al genocidio como el «crimen de crímenes» (El Fiscal vs. Radislav Krstić, 2004).

Sin embargo, la Sala de Apelación consideró que Radislav Krstić formó parte

de la Empresa Criminal Común (forma de participación penal) al haber evidencia de que por lo menos estaba al tanto del plan de conspiración para liquidar a los musulmanes. «You agreed to evil», la Sala de Primera Instancia (2001) le había dicho a Krstić cuando leyó la sentencia aludiendo a su omisión culposa por colaboración (aiding & abetting), pero reconociendo sin embargo, que el acusado no tenía ni la intención (dolus specialis) ni el control del hecho al no ser el autor o coautor del genocidio:

> La Sala de Primera Instancia no niega que usted es un soldado profesional que ama su trabajo. La Sala de Primera Instancia puede aceptar que usted no habría tomado por su propia cuenta la decisión de ejecutar a miles de civiles y personas desarmadas. Alguien más probablemente decidió ordenar la ejecución de todos los hombres en edad de combatir. Sin embargo, todavía es culpable, General Krstić, usted es culpable de haber participado deliberadamente en el traslado forzado organizado de mujeres, niños y ancianos en Srebrenica en el momento del ataque del 6 de julio de 1995 contra el área segura de las Naciones Unidas. Usted es culpable del asesinato de miles de musulmanes bosnios entre el 10 y el 19 de julio de 1995, ya se trate de asesinatos cometidos esporádicamente en Potoĉari o de asesinatos planeados en forma de ejecuciones en masa. Es culpable del increíble sufrimiento de los musulmanes bosnios, ya sean los de Potoĉari o los supervivientes de las ejecuciones. Es culpable de la persecución sufrida por los musulmanes bosnios de Srebrenica sabiendo que las mujeres, los niños y los ancianos de Srebrenica habían sido transferidos. Usted es culpable de haber aceptado el plan de realizar ejecuciones en masa de todos los hombres en edad de combatir. Por lo tanto, es culpable de genocidio General Krstić […] (Resumen de la Sentencia, 2001, pp. 9- 10).

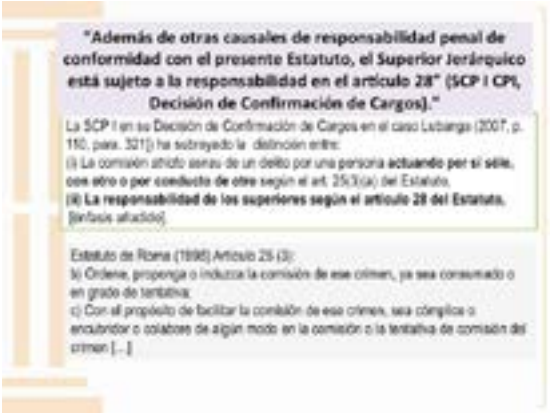
De complicidad en genocidio corregiría la Sala de Apelación por su omisión culposa (SA TPIY, 2004). Sin duda se seguirá hablando por más tiempo sobre cuánto control efectivo el General Radislav Kristić en realidad podía ejercer sobre sus hombres ¿Podía impedir Radislav Krstić los crímenes a sucederse ordenados directamente por sus Superiores Jerárquicos? ¿Era en realidad parte del plan de conspiración? ¿Estar al tanto significa actuar dolosamente? Dolosamente no pero culposamente si y esa parece haber sido la situación, el mens rea o estado de conocimiento del General Radislav Krstić. Probablemente no lo sepamos nunca certeza, pero ello reafirma lo que si sabemos con claridad, que para que el Superior Jerárquico pueda actuar y cumplir con sus responsabilidades debe contar con la capacidad material para ejercer control realista y efectivo sobre sus hombres.

En el último recuadro abajo se pueden apreciar las formas de responsabilidad penal en las que puede incurrir un Superior Jerárquico que han sido establecidas en la jurisprudencia y el derecho internacional penal en el Estatuto de Roma de la Corte Penal Internacional (1998), claramente con la Decisión de Confirmación de Cargos de Thomas Lubanga Dylo (SCP I CPI, 2007), donde se recogen las formas de responsabilidad penal individual en el artículo 25 y con ellas las formas de intervención

penal en lo que se conoce como el dominio del hecho en las Estructuras Organizadas de Poder así como la responsabilidad del Superior Jerárquico en el artículo 28 del Estatuto.

Se puede apreciar con toda certeza que la Corte Penal Internacional ha recogido no sólo el legado de los tribunales Ad Hoc de la ONU, el TPIY y el TPIR en materia de la responsabilidad del Superior Jerárquico, sino también las formas de colaboración por omisión (aiding & abetting) del Superior, encontradas en innumerables casos ventilados en estos dos tribunales internacionales penales que en el 2017 y 2015 cerraron sus puertas definitivamente al haber terminado su mandato por el que fueron creados en 1993 y 1994 respectivamente.

Figura 9. Causales de responsabilidad penal del Superior Jerárquico en el Estatuto de Roma de la Corte Penal Internacional (1998).



Conclusiones

Son frecuentes las preguntas de porqué el comandante militar tiene más obligaciones en campo que un superior jerárquico civil. Pareciera que los Superiores Jerárquicos civiles son tratados con más laxitud en los tribunales penales internacionales con relación a los Superiores Jerárquicos militares. En parte es verdad, pues la mayor parte de los casos de Superiores Jerárquicos llevados a juicio en la historia y en los tribunales penales internacionales han sido y continúan siendo en gran medida de comandantes militares. Ello ha provocado que haya más derecho en ello por la jurisprudencia que arroja y en esto el TPIY concentra la mayor parte de los casos militares, por lo que su estudio es valioso.

Al comandante militar se le asocia con una responsabilidad más estrecha de vigilancia y control por estar en campo, mientras que el Superior Jerárquico civil está generalmente a distancia. Estos factores explican por qué el enjuiciamiento de comandantes militares ha sido más común, más estrecho y más estricto, lo cual se ha traducido en una evolución de la doctrina del Superior Jerárquico militar mucho más rica y extensa que en los civiles.

El artículo 28 del Estatuto de Roma sin duda refleja esta tendencia al establecer en el inciso (a) (i) las obligaciones del «Jefe Militar o el que actúe efectivamente

como Jefe Militar» [que] «hubiere sabido» […] o «hubiere debido saber» [o hubiere tenido que saber si se lee la versión en inglés should have known]. El estándar es más estricto en este inciso que en el caso de los Superiores Jerárquicos civiles en el inciso (b) (iii) «no hubiera adoptado todas las medidas necesarias y razonables a su alcance (Estatuto de Roma, 1998).

El estándar para los Superiores Jerárquicos civiles deja sin duda un margen de argumentación mayor a la defensa de los acusados Superiores Jerárquicos Civiles. Sin embargo, no debemos dejar de apreciar, que la doctrina en relación a las obligaciones del superior jerárquico civil se está desarrollando con rapidez en los últimos años contando ya con sentencias condenatorias de altos jerarcas civiles en posiciones de mando como Charles Taylor, ex Presidente de Liberia, sentenciado por la Corte Especial de Sierra Leona por crímenes de guerra y crímenes de lesa humanidad cometidos en el conflicto armado de Sierra Leona de 1991 al 2002. O bien el autoproclamado presidente de la República Serbia en Bosnia Herzegovina Radovan Karadzić, sentenciado por el TIPY cuarenta años de prisión (2016), por su responsabilidad y coautoría en el plan de conspiración para cometer genocidio en Srebrenica en 1995.

Lo que es claro tanto para civiles como militares o aquellos «actuando como Jefes Militares» es que sus actuaciones deben ser analizadas a la luz de los criterios de responsabilidad aquí señalados que son el conocimiento, la prevención, el control efectivo y la notificación. Cada caso debe analizarse in concreto por lo que no puede haber generalizaciones. Otro principio fundamental en la doctrina del Superior Jerárquico es la existencia de una jerarquía entre Superior y subordinado, de lo contrario no es posible fincar responsabilidades al Superior. Dicha jerarquía puede ser de jure o de facto como hemos explicado, constituyendo la primera sólo un indicio de algo más importante, el control efectivo o la habilidad material realista de que ese Superior efectivamente ejerce un mando y esos son sus hombres o subordinados. Un grado menor de control es inefectivo y por lo tanto como se ha visto extensamente en este ensayo no puede ser atribuible al Superior Jerárquico.

En el caso más específico del command responsibility atribuible a los mandos militares, las formas de responsabilidad del Superior Jerárquico son para su beneficio y de sus tropas, pero mayor aún para la sociedad civil, que dependemos del buen actuar de los comandantes militares que a través de su liderazgo y disciplina militar transmiten los valores de humanidad que nos son propios como civilización. Eso lo sabemos, pero hay que estar conscientes de que aún con genuina voluntad y control férreo, así como disciplina ejercida por parte del comandante comprometido, sus retos son arduos. Ello porque no basta con estar conscientes sino en recordar que los actos del injusto se suceden y por ello el Superior Jerárquico debe estar capacitado y vigilante en este conocimiento, no sólo en su beneficio y el nuestro como sociedad, sino porque además de ser su obligación el saber, también es su derecho, conocer para poder prevenir y/o reprimir los actos de los elementos equivocados en sus filas.

Es verdad, el trabajo es continuo y su obligación es enorme, porque tienen que estar alerta todo el tiempo; como también es cierto, que sus pasos a tomar se exigen en la medida de lo razonable en las circunstancias que les toca afrontar, lo contrario sería excesivo, como claramente está establecido en la jurisprudencia internacional.

Como lo ha expresado la Corte Penal Internacional en Bemba Gombo (SPI 2016) apoyándose en la jurisprudencia del TPIY (Blaškić (2004); Brdanin (2004); Stakić (2003); Krnojelac (2002) Galić (2003), si el comandante ha ultimado su obligación de tomar todas las medidas necesarias y razonables en su poder, él no puede ser responsable incluso si los crímenes de hecho ocurren o si los perpetradores permanecen sin castigar.

Hacemos votos para que los ejércitos del mundo regulares y de facto, incorporen estos conocimientos para sus comandantes militares, para los Superiores Jerárquicos civiles, para que a través de ellos y su liderazgo, se transmitan y ejerzan estándares para el comportamiento adecuados a fin de proteger el bien jurídico mayor que es la noción de humanidad (Rocha, 2018).

Bibliográfia

Libros y artículos en libros y revistas especializadas

- Bassiouni, Cherif (2003) International Criminal Law, Oxford University Press.
- Grotius Hugo (2004) The Rights of War and Peace, In Three Books, Wherein are explained, The Law of Nature and
- Nations, and the principal Points relating to Government (translated into English by J. Barbeyrac), New Jersey:
- The Lawbook Exchange, Ltd (1738).
- Henckaerts, Jean Marie y Doswald Beck, Louise (2005) Customary International Humanitarian Law, 2, UK: Cambridge
- University Press.
- Nybondas, L. Maria (2010) Command Responsability and its Applicability to Civilian Superiors, The Hague: T.M.C. Asser
- Press.
- Olásolo, Héctor y Canosa, Jannluck (2018)» La Responsabilidad del Superior en el Acuerdo de Paz en Colombia a la
- luz del Derecho Internacional,» Política Criminal, 13 (25) (Enero 2018) Art. 12, pp. 444-500. Recuperado de
- http://www.politicacriminal.cl/Vol_13/n_25/Vol13N25A12.pdf
- Olásolo, Héctor (2013) «La aplicación del concepto de autoría mediata a tráves de aparatos organizados de poder por
- los tribunales penales internacionales; especial referencia a los casos « Al Bashir», «Al Gaddafi» y «Al Senussi»
- ante la Corte Penal Internacional,» en Maculan, Elena & Gil Gil, Alicia èd] Internvención delictiva y Derecho Penal
- Internacional, Madrid: Dickinson.
- Oswald, Mark (2001) The Howling Wilderness Courts- Martial of 1902, US Army War College, Carlisle Barracks, PA
- 17013.
- Rocha Herrera, Mónica (2018) «¿Cuáles son las obligaciones de un comandante militar en campo? Evolución Jurídica
- de la Doctrina de la Responsabilidad del Superior Jerárquico. De Yamashita a Bemba Gombo en la Corte Penal
- Internacional», Anuario Iberoamericano de Derecho Internacional, vol. 6, Bogotá, Colombia (En prensa, fecha
- aproximada de publicación octubre del 2018).
- Rocha Herrera, Mónica 2016 «Actores no Estatales, Grupos Armados, Milicias, Señores de la Guerra, Grupos Criminales
- Organizados y Paramilitares ¿Pueden acaso estos grupos cometer crímenes internacionales conforma al derecho

- penal internacional?», Anuario Iberoamericano de Derecho Internacional Penal, vol. 4, pp. 14-38, Bogotá,
- Colombia [Recuperado de
- http://www.iberoamericaninstituteofthehague.org/attachments/article/195/ANIDIP%20Volumen%204.pdf]
- Stryszak, Michal (2000) «Command Responsibility. How much a commander be expected to know?» Journal of Legal
- Studies.
- Sun Tzu (2000) El Arte de la Guerra (traducción de Jaime Barrera Parra), Colombia: Panamericana Editorial.

Documentos

- Convención sobre la imprescriptibilidad de los crímenes de guerra y de los crímenes de lesa humanidad 1968.
- Recuperado de http://www.ordenjuridico.gob.mx/TratInt/Mexico/DIH/PI36ABIS.pdf
- I. Convenio de Ginebra para aliviar la suerte que corren los heridos y los enfermos de las fuerzas armadas en
- campaña, 1949. Recuperado de https://www.icrc.org/spa/resources/documents/treaty/treaty-gc-1-5tdkna.htm
- III. Convenio de Ginebra relativo al trato debido a los prisioneros de guerra, 1949. Recuperado de
- https://www.icrc.org/spa/resources/documents/treaty/treaty-gc-1-5tdkna.htm
- Conferencia Diplomática de Plenipotenciarios de las Naciones Unidas sobre el Establecimiento de una Corte Penal
- Internacional (1998). Estatuto de Roma. Roma: Naciones Unidas, A/Conf. 183/9, 17 de julio de 1998 [Recuperado el 18 de abril del 2017,
- http://www.acnur.org/fileadmin/scripts/doc.php?file=fileadmin/Documentos/BDL/2002/0033].
- Comité Internacional de la Cruz Roja, Convención Relativa a las Leyes y Costumbres de la Guerra Terrestre H.IV. de
- 1907 La Haya. [Recuperado el 20 de abril del 2017, https://www.icrc.org/spa/resources/documents/misc/treaty-
- 1907-hague-convention-4-5tdm34.htm].
- Comité Internacional de la Cruz Roja, Protocolo Adicional I a los Convenios de Ginebra de 1949, Ginebra [Recuperado
- en https://www.icrc.org/spa/resources/documents/misc/protocolo-i.htm#25].
- Instructions for the Government of Armies of the United States in the Field, prepared by Francis Lieber, LL.D., Originally
- Issued as General Orders No. 100, Adjutant General's Office, 1863, Washington 1898: Government Printing
- Office. General Orders No. 100: The Lieber Code, Instructions for the Government of Armies of the United States
- in the Field. The Avalon Project, Documents in Law, History and Diplomacy, Lillian Goldman Law Library, Yale

- Law School [Recuperado 16 de abril 2017, http://avalon.law.yale.edu/19th_century/lieber.asp#sec3].
- Law Reports of Trials of War Criminals Selected and Prepared by the United Nations War Crimes Commission (1948)
- London: published by His Majesty's Stationery, vol IV [Recuperado el 17 de abril del 2017 en
- https://www.loc.gov/rr/frd/Military_Law/pdf/Law-Reports_Vol-4.pdf].
- Rome Statute of the International Criminal Court (1998). A/CONF.183/9 of 17 July 1998 [Recuperado el 29 de abril del
- 2017, https://www.icc-cpi.int/nr/rdonlyres/ea9aeff7-5752-4f84-be94-0a655eb30e16/0/rome_statute_ english.pdf].

Casos ante tribunales penales internacionales

- Corte Internacional de Justicia de la ONU, Case Concerning Military and Paramilitary Activities in and Against Nicaragua
- (Nicaragua v. United States of America), Merits, Judgment (1986). Recuperado de http://www.icj-cij.org/files/caserelated/
- 70/070-19860627-JUD-01-00-EN.pdf
- Corte Especial de Sierra Leona, Sala de Apelaciones (2012) El Fiscal vs. Charles Ghankay Taylor, Sentencia, Caso No.
- SCSL-03-01-A [Recuperado de http://www.rscsl.org/Documents/Decisions/Taylor/Appeal/1389/SCSL-03-01-A-
- 1389.pdf].
- Corte Penal Internacional, Sala de Apelación (2018) La Fiscal vs. Jean Pierre Bemba Gombo, Sentencia , No. ICC-
- 01/05-01/08 [Recuperado de https://www.icc-cpi.int/Pages/record.aspx?docNo=ICC-01/05-01/13-2276-Red].
- Corte Penal Internacional, Sala de Primera Instancia III (2016) La Fiscal vs. Jean Pierre Bemba Gombo. Veredicto con
- Anexos Públicos I, II y A –F, No. ICC-01/05-01/08 [Recuperado de https://www.icccpi.
- int/CourtRecords/CR2016_02238.PDF].
- Corte Penal Internacional, Sala de Cuestiones Preliminares II (2009). La Fiscal vs. Jean Pierre Bemba Gombo. Decisión
- de Confirmación de Cargos Conforme al artículo 61 (7) (a) y (b) del Estatuto de Roma, No: ICC-01/05.01/08.
- Corte Penal Internacional, Sala de Primera Instancia I (2012) La Fiscal vs. Thomas Lubanga Dyilo, Sentencia de
- conformidad al artículo 74 del Estatuto, No: ICC-01/04-01/06 [Recuperado de https://www.icccpi.
- int/CourtRecords/CR2012_03942.PDF].
- Corte Penal Internacional, Sala de Primera Instancia II (2014), La Fiscal vs. Germain Katanga, Sentencia de conformidad
- al artículo 74 del Estatuto, No: ICC-01/04-01/07. [Recuperado de https://www.icccpi.
- int/CourtRecords/CR2014_02618.PDF].
- Tribunal Penal Internacional para la ex Yugoslavia, Sala de Apelaciones (2004) El Fiscal vs. Radislav

Krs̆tić, Sentencia,
- La Haya, Caso No. IT-98-33-A [Recuperado de http://www.icty.org/x/cases/krs̆tic/tjug/en/krs-tj010802e.pdf].
- Tribunal Penal Internacional para la ex Yugoslavia, Sala de Primera Ins̆tancia (2001) El Fiscal vs. Radislav Krs̆tić,
- Resumen de la Sentencia, La Haya [Recuperado de http://www.icty.org/x/cases/krs̆tic/tjug/en/010802_
- Krs̆tic_summary_en.pdf]
- Tribunal Penal Internacional de la ONU para la ex Yugoslavia (2008) El Fiscal vs. Rasim Delić. Resúmen de la Sentencia
- de Rasim Delić, La Haya [Recuperado de
- http://www.icty.org/x/cases/delic/tjug/en/080915_Delic_summary_en.pdf].
- Tribunal Internacional Penal de la ONU para la ex Yugoslavia, Sala de Apelaciones (2008), El Fiscal vs. Enver
- Hadžihasanovic y Amir Kubura, Sentencia, La Haya, Caso No. IT-01-47-A. [Recuperado de
- http://www.icty.org/x/cases/hadzihasanovic_kubura/acjug/en/had-judg080422.pdf.
- Tribunal Internacional Penal de la ONU para la ex Yugoslavia, Sala de Apelaciones (2006) El Fiscal vs. Mladen
- Naletilić, a.k.a «Tuta» Vinko Martinović, a.k.a. «Ŝtela», Sentencia, La Haya, Caso No. IT-98-34-A [Recuperado
- de http://www.icty.org/x/cases/naletilic_martinovic/acjug/en/nal-aj060503e.pdf].
- Tribunal Internacional Penal de la ONU para la ex Yugoslavia, Sala de Apelaciones (2004) El Fiscal vs. Tihomir Blaškić,
- Sentencia, La Haya, Caso No. IT-95-14-A [Recuperado de http://www.icty.org/x/cases/blaskic/acjug/en/blaaj040729e.
- pdf].
- Tribunal Internacional Penal de la ONU para la ex Yugoslavia, Sala de Apelaciones (2001) El Fiscal vs. Zdravko Mucić,
- Hazim Delić & Esad Landžo, Sentencia, La Haya, Caso No. IT-96-21-A [Recuperado de
- http://www.icty.org/x/cases/mucic/acjug/en/cel-aj010220.pdf].
- Tribunal Internacional Penal de la ONU para la ex Yugoslavia, Sala de Apelaciones (2004) El Fiscal vs Dario Kordi¢ &
- Mario Čerkez, Sentencia, La Haya, Caso No. IT-95.14/2-A [Recuperado de
- http://www.icty.org/x/cases/kordic_cerkez/acjug/en/cer-aj041217e.pdf].
- Tribunal Internacional Penal de la ONU para la ex Yugoslavia, Sala de Primera Ins̆tancia (2016), El Fiscal vs. Radovan
- Karadzi¢, Sentencia, La Haya, Caso No. IT-95-5/18-T [Recuperado de
- http://www.icty.org/x/cases/karadzic/tjug/en/160324_judgement.pdf].
- Tribunal Internacional Penal de la ONU para la ex Yugoslavia, Sala de Primera Ins̆tancia (2017), El Fiscal vs. Ratko
- Mladi¢, Sentencia, vol. 1-5, La Haya, Caso No. IT-09-92-T [Recuperado de
- http://www.icty.org/x/cases/mladic/tjug/en/171122-4of5_1.pdf].

- Tribunal Penal Internacional de la ONU para Ruanda, Sala de Primera Instancia (2001), El Fiscal vs. Jean Paul Akayesu,
- Sentencia, Arusha, [Recuperado de http://unictr.irmct.org/sites/unictr.org/files/case-documents/ictr-96-4/appealschamber-
- judgements/en/010601.pdf].

Láminas e Imágenes

- Rocha Herrera, Mónica (noviembre 2016) Notas de clase en power point presentadas en el Curso de Derecho
- Internacional Penal y Litigio Internacional para Mandos, Jefes, Oficiales y Tropa en la Secretaría de la Defensa
- Nacional de México, Ciudad de México, México.
- Rocha Herrera, Mónica (mayo 2018) Notas en power point presentadas en la Conferencia Magistral El Principio del
- Superior Jerárquico ante la Corte Penal Internacional en el Centro de Estudios Superiores Navales de la Marina
- Armada de México, Universidad Naval, Ciudad de México, México.
- Hugo Grotius (abril 2017). Symploke.trujman.org [Pintura]. Recuperado de http://symploke.trujaman.org/index.
- php?title=Hugo_Grocio.

Política Editorial

La Revista del Centro de Estudios Superiores Navales es una publicación de tipo académica que tiene como objetivo ser un foro abierto en el cual los miembros de la Armada de México y el personal civil interesados puedan expresar sus ideas sobre temas de Seguridad Nacional y afines al ámbito marítimo.

Está dirigida a la comunidad académica, científica y/o de investigación interesada en temas relacionados con la seguridad nacional, la política, la estrategia, el ámbito marítimo, la ciencia, la tecnología, y la historia y cultura navales.

INDEXADA EN LATINDEX Y CLASE

La Revista del Centro de Estudios Superiores Navales se encuentra indexada en el Sistema Regional de Información en Línea para Revistas Científicas de América Latina, el Caribe, España y Portugal (LATINDEX), así como en la Base de Datos de Revistas de Ciencias Sociales y Humanidades (CLASE).

PRESENTACIÓN DE ESCRITOS

Los trabajos que se remitan para su publicación deberán ser originales, inéditos y no estar postulados de forma simultánea para su publicación en otras revistas u órganos editoriales o en línea, además de que los autores asumen la responsabilidad si se detecta falsificación de datos o falta de autenticidad en la investigación.

Cada artículo tendrá una extensión mínima de 15 cuartillas y una máxima de 20, incluidas las referencias, notas, cuadros y figuras. Los documentos deberán enviarse en Microsoft Word, escrito a espacio y medio entre líneas, con letra Arial a 12 puntos.

El margen izquierdo será de 2.5 cm. y el derecho, de 3 cm.

Presentará numeración ininterrumpida.

En caso de contar con material fotográfico, enviarlo en una carpeta aparte (en formato JPEG), con su respectivo pie de foto, con un mínimo de resolución de 300 dpi y un mínimo de tamaño de 800 x 600 píxeles.

DATOS DEL AUTOR

La primera hoja del artículo habrá de incluir título (que no debe exceder de 10 palabras) y nombre del autor (o autores), así como sus datos personales, a saber:

a) Título académico y universidad donde lo obtuvieron;
b) Institución donde laboran;
c) Breve currículo;
d) Dirección completa a la que se les enviará correspondencia;
e) Temas de especialización;
f) Número telefónico;
g) Correo electrónico;
h) Una breve declaración que indique que el artículo es original (exigencia de originalidad) y que no ha sido publicado y no está siendo considerado en ningún otro lugar.

Estos datos son indispensables para la revisión de los artículos.
No se aceptarán epígrafes ni dedicatorias.

SOBRE EL SISTEMA DE CITA

Sistema de citas APA (American Psychological Association). Con la finalidad de impedir el plagio y la copia indiscriminada del contenido de otros textos, el autor citará correctamente las fuentes empleadas en su trabajo, proponiéndose el empleo del modelo diseñado por la Asociación Americana de Psicología (APA).

Los editores se reservan el derecho de hacer las modificaciones de estilo que juzguen pertinentes.

TIPO DE ARTÍCULOS

Podrán presentarse artículos cuyo texto sea en idioma español y dentro de las categorías y estructuras siguientes:

Artículo Académico o Científico	Artículo No Académico o Tipo Ensayo
Título	Título
Resumen	Resumen
Abstract	Abstract
Palabras clave	Palabras clave
Introducción	Introducción
Materiales y Métodos	Análisis o discusión
Resultados	Conclusión
Discusión	Fuentes consultadas
Conclusiones	

Para consultar los criterios editoriales en su versión completa podrá acceder a la página *http:// www.cesnav.edu.mx/revista.html*

PROCESO DE DICTAMINACIÓN

Todos los trabajos se someten a dos etapas de dictaminación:

- Una primera lectura por parte del Consejo Editorial, con el objetivo de verificar si cubre los requisitos del perfil de la revista.
- En caso de ser aceptado, este organismo es quien propone dos dictaminadores especialistas en el tema a quienes será enviado para su arbitraje académico (de revisión por pares).
- Durante todo el proceso se conservará el anonimato tanto de los dictaminadores como de los autores.

- En el caso de discrepancia entre aceptado y rechazado, el texto será enviado a un tercer dictaminador, cuya decisión definirá su estatus de publicación; en este caso. El dictamen final es inapelable.

PERFIL DEL ÁRBITRO

El proceso editorial de la Revista del CESNAV, establece la obligatoriedad de arbitrar los artículos que sean considerados para su publicación. De acuerdo a lo anterior, se considera como árbitro al especialista cuyo perfil profesional le permita revisar la calidad y originalidad del texto referido, para después emitir sus recomendaciones al autor.

Cabe destacar que los árbitros deben contar con una trayectoria de reconocida capacidad profesional y ética; deben ser académicos o investigadores y garantizar la confidencialidad del proceso de revisión.

CESIÓN DE DERECHOS

Él o los autores conceden el permiso para que su material se difunda en la Revista del CESNAV, medios magnéticos y electrónicos. Los derechos patrimoniales de los artículos publicados son cedidos al Centro de Estudios Superiores Navales, tras la aceptación académica y editorial del original para que este se publique y distribuya tanto en versión impresa como electrónica. Él o los autores conservan sus derechos morales conforme lo establece la ley.

CONTACTO

Vicealmirante José Tomás Jorge Tress Zilly, Director.
Teniente de Navío Alberto Medina Angeles, Editor.
Correo: revista.cesnav@hotmail.com
Tel: 56 08 08 47 ext. 7660.

VERSIÓN ELECTRÓNICA

https://cesnav.uninav.edu.mx/cesnav/revista_conte.html

EDITORIAL POLICY

The Magazine of the Centro de Estudios Superiores Navales is an academic publication whose objective is to be an open forum in which the Mexican Navy members and interested civilians can express their ideas on National Security Topics and topics related to the maritime environment.

It is addressed to the academic, scientific and research community interested in topics related to national security, politics, strategy, maritime domain, science, technology, and naval and cultural history.

INDEXED IN LATINDEX AND CLASE

The magazine of the Centro de Estudios Superiores Navales is indexed in the Regional System for Online Information for Scientific Magazines from Latin America, the Caribbean, Spain and Portugal (LATINDEX), as well as in the Database of Social Sciences and Humanities Magazines (CLASE).

PRESENTATION OF WRITINGS

Writings that are submitted for their publication must be original, unpublished and not being proposed simultaneously for its publication in other magazines or editorial bodies or online. Authors assume the responsibility if any sign of data counterfeit or lack of authenticity in the research is detected.

Each article will be at least 15 pages long and a maximum of 20, including references, notes, figures and charts. Documents must be sent in a Microsoft Word file, 1 ½ space between lines, Arial font, size 12.

Left margin of 2.5 cm and right of 3 cm.

Continuous numbering is needed.

For photographical material, it must be sent in a separate folder (JPEG format), with photo caption with a minimum resolution of 300 dpi and a minimum size of 800 x 600 pixels.

AUTHOR DETAILS

The first page of the article must include a title (it must not exceed more than 10 words) and name of the author (authors), as well as personal details, for instance:

a) Academic Title and university where it was obtained;
b) Institution where he/she works;
c) Brief curriculum;
d) Full address where mail will be sent;
e) Specialization topics;
f) Phone number;
g) E-mail address;
h) A brief statement that states that the article is original (requirement of originality) and it has not been published nor being considered in any other place.

This data is essential for the review of articles.

Synopsis and inscriptions will not be accepted.

ABOUT THE CITATION SYSTEM

APA citation system (American Psychological Association). The author will cite correctly the sources used in his/her work with the purpose to use the designed model by the American Psychological Association (APA), aimed at preventing plagiarism and indiscriminate copying of the content of other texts.

Editors reserve the right to do style corrections to be considered appropriate.

TYPE OF ARTICLES

Articles written in Spanish and in accordance with the following categories and structures can be submitted:

Academic or Scientific Article	Non-Academic Article or Essay Type
Title	Title
Abstract	Abstract
Key words	Key words
Introduction	Introduction
Material and Methods	Analysis or discussion
Results	Conclusions
Discussion	Sources consulted
Conclusions	

To verify the editorial concept in its full version, you can access http://www.cesnav.edu.mx/revista.html

EVALUATION PROCESS

All work is subject to two stages of evaluation:

- A first reading by the Editorial Board, to verify if it covers the magazine profile requisites.
- If accepted, this body proposes two topic-specialist arbitrators who will do the academic arbitration (peer review).
- During all the process, anonymity of the arbitrators and authors willbe kept.
- In the event of discrepancy if accepted or rejected, the text will be sent to a third arbitrator, whose decision will define its publication status; in this case, the final judgment is indisputable.

ARBITRATOR'S PROFILE

The editorial process of CESNAV's magazine establishes the obligation to arbitrate the articles considered for publication. Accordingly, a specialist arbitrator, whose profile allows him(her) to review the quality and Revista del Centro de Estudios Superiores Navales. Abril-Junio de 2017. Volumen 38. Número 2. ISSN: 1870-5480 97 authenticity of the text, is considered and afterwards he (she) will issue his (her) recommendations to the author.

It is worth to stand out that the arbitrators must have solid tradition of professional and ethical capability; they should be scholars or researchers and must guarantee the confidentiality of the review process.

TRANSFER OF RIGHTS

The author(s) grant permission for their material to be published in CESNAV's magazine, in magnetic and electronic means. The property rights of the published articles are conferred to the Centro de Estudios Superiores Navales, after the academic and original editorial acceptation for its publication and distribution both in printed and electronic version. The author(s) retain their moral rights in accordance with the law.

POINT OF CONTACT

Vicealmirante José Tomás Jorge Tress Zilly, Director.
Teniente de Navío Alberto Medina Angeles, Editor.
Mail: revista.cesnav@hotmail.com
Tel: 56 08 08 47 ext. 7660.

ELECTRONIC VERSIÓN

https://cesnav.uninav.edu.mx/cesnav/revista_conte.html